

eman ta zabal zazu



Universidad del País Vasco Euskal Herriko Unibertsitatea

DEPARTAMENTO DE DERECHO ADMINISTRATIVO,
CONSTITUCIONAL Y FILOSOFÍA DEL DERECHO

PROTECCIÓN DE DATOS PERSONALES Y *HABEAS DATA* EN LA
REPÚBLICA DOMINICANA, SU VINCULACIÓN CON EL ÓRGANO
DE CONTROL Y LAS TRANSFERENCIAS INTERNACIONALES
DE DATOS. UN ESTUDIO EN EL CONTEXTO EUROPEO Y
LATINOAMERICANO

Doctorando

Freddy Tomás Durán Reyes

Directora

Dra. Ana Rosa González Murua

Director

Dr. Iker Barbero González

Donostia/San Sebastián

2019

ÍNDICE	iii
ABREVIATURAS	iii
CAPÍTULO I	
INTRODUCCIÓN	1
1. Presentación y selección del tema	1
2. Antecedentes claves	8
3. Objetivos de la investigación	9
3.1. Objetivo general	9
3.2. Objetivos específicos	9
4. Hipótesis de la investigación	10
5. Métodos y fuentes	10
6. Hitos legislativos ocurridos durante el desarrollo del trabajo de investigación	12
7. ¿Desde dónde partimos ?	13
8. Estructura y orden de exposición	15
 CAPÍTULO II	
EI DERECHO A LA PROTECCIÓN DE DATOS Y <i>EL HABEAS DATA</i>. ESPECIALMENTE SU ORIGEN Y EVOLUCIÓN EN EUROPA Y LATINOAMÉRICA	19
I. EL ORIGEN DE LA PROTECCIÓN DE DATOS PERSONALES EN ESTADOS UNIDOS Y SU ORIGEN E INCORPORACIÓN EN EUROPA	19
1. Planteamiento de la cuestión	19
2. El nacimiento de la protección de datos en Estados Unidos. La <i>privacy</i>	24
3. Encaje distorsionado de la <i>privacy</i> norteamericana e incorporación de la autodeterminación informativa y el derecho a la protección de datos personales en Europa	26
4. La Sentencia sobre el Censo en Alemania. La autodeterminación informativa	28

5. La construcción del derecho a la protección de datos en el ámbito internacional	33
5.1. La protección de datos en la ONU	33
5.1.1. <i>Directrices de Protección de Datos de la ONU de 14 de diciembre de 1990</i>	36
5.1.2. <i>El derecho a la privacidad en la era digital: Resoluciones de la Asamblea General y del Consejo de Derechos Humanos. El papel del Relator especial</i>	38
5.2. La protección de datos en la OCDE	40
5.3. La protección de datos en el Consejo de Europa	46
5.3.1. <i>Convenio 108 sobre sobre Protección de Datos Personales</i>	49
5.3.2. <i>Protocolo Adicional del Convenio 108 de 2001</i>	52
5.3.3. <i>Protocolo de modificación del Convenio 108 de 1981 (2018)</i>	54
5.3.4. <i>Jurisprudencias del TEDH</i>	56
5.4 La protección de datos en la OEA	59
5.4.1. <i>Convención Americana</i>	59
5.4.2. <i>Jurisprudencias Corte Interamericana</i>	64
6. La construcción del derecho a la protección de datos en el ámbito de la Unión Europea	69
6.1. La protección de datos en la Carta de Derechos Fundamentales de la Unión Europea. Artículo 8	69
6.2. Directiva 95/46/CE relativa la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos	72
6.3. Reglamento (UE) 2016/679 relativa la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos	77
6.3.1. <i>Etapas previas en la implementación del Reglamento</i>	77
6.3.2. <i>Seguridad jurídica en el Reglamento</i>	79
6.3.3. <i>Disposiciones del Reglamento (UE) 2016/679</i>	80
7. La construcción del derecho a la protección de datos en España.	92
7.1. El artículo 18.4 de la Constitución española de 1978	92
7.2. Corrientes doctrinales más significativas	95
7.3. Los hitos en la jurisprudencia constitucional en torno al artículo 18.4 de la Constitución española	97
7.4. Ley Orgánica 5/1992, de regulación del tratamiento	100

automatizado de datos de carácter personal (LORTAD)	
7.5. Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD)	106
7.6. <i>Proyecto y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)</i>	110
8. Jurisprudencias europeas en materia de protección de datos	114
8.1. Preámbulo	114
8.2. Google Spain, SL y Google Inc., STJUE de 13 de mayo 2014 (C-131/12)	116
8.3. SCHREMS, STJUE de 6 de octubre de 2015 (C-362/14)	118
II. EL DERECHO A LA PROTECCIÓN DE DATOS EN LATINOAMÉRICA Y LA FIGURA DEL <i>HABEAS DATA</i>	122
1. Antecedentes	122
2. El origen del <i>habeas data</i>	124
3. Tipos y subtipos de <i>habeas data</i>	126
4. Razones de la asunción del <i>habeas data</i> en Latinoamérica frente al derecho a la protección de datos	130
5. <i>Habeas data</i> en las constituciones latinoamericanas	134
5.1. Puntualizaciones	134
5.2. Consideraciones del <i>habeas data</i> en el escenario latinoamericano	136
5.3. El proceso constitucional del <i>habeas data</i> en Latinoamérica	138
5.4. Incorporación del <i>habeas data</i> en normas generales de protección de datos	150
<i>Estados que no contemplan la figura del habeas data en sus normas constitucionales</i>	150
5.5. Perspectivas del derecho a la protección de datos en Latinoamérica	161
6. Ley Modelo Iberoamericana en materia de Protección de Datos	166
6.1. Consideraciones generales	166
6.2. Iniciativas de los Jefes de Estado y de Gobierno Iberoamericano en el proceso de normalización de la protección de datos en los Estados Iberoamericanos	168
6.3. Propuesta de viabilidad de creación de autoridades de control en los Estados Latinoamericanos	171
6.4. Planteamiento de Estándares internacionales para la protección de la privacidad, en relación con el tratamiento de	177

datos de carácter personal	
6.5. Iniciativas de los Estados en materia de protección de datos	181
6.6. Organizaciones internacionales y estandarización	181
6.7. Derecho a la intimidad/privacidad desde la óptica de los Comisionados de Protección de Datos y Privacidad	183
6.8. Convención internacional vinculante para los Estados	184
6.9. Estandarización de la protección de datos latinoamericana	186
6.10. Nuevos estándares de protección de datos latinoamericana	198
6.11. A considerar	204
6.12. Planteamiento de propuesta de modelos latinoamericanos	208

CAPÍTULO III

EI DERECHO A LA PROTECCIÓN DE DATOS Y <i>HABEAS DATA</i> EN LA CONSTITUCIÓN DE LA REPÚBLICA DOMINICANA, SU RELACIÓN CON OTROS DERECHOS	213
I. ANTECEDENTES CONSTITUCIONALES DEL DERECHO A LA PROTECCIÓN DE DATOS EN REPÚBLICA DOMINICANA	213
1. Introducción	213
2. Antecedentes constitucionales. Primeras reflexiones doctrinales sobre protección de datos y constitución de 2002	214
II. EL DERECHO A LA PROTECCIÓN DE DATOS EN LA CONSTITUCIÓN DEL 2010 y 2015. EL ARTÍCULO 44 NUMERAL 2	216
III. EL DERECHO A LA PROTECCIÓN DE DATOS EN LA CONSTITUCIÓN DE 2010 Y SU RELACIÓN, ESPECIALMENTE CON EL DERECHO A LA INTIMIDAD, LA VIDA PRIVADA Y EL LIBRE DESARROLLO DE LA PERSONALIDAD	225
IV. EL <i>HABEAS DATA</i> EN REPÚBLICA DOMINICANA	228
1. Consideraciones iniciales	228
2. <i>Habeas data</i>	229
V. EL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA Y SU RELACIÓN CON EL DERECHO A LA PROTECCIÓN DE DATOS	233
VI. ANÁLISIS DE LA JURISPRUDENCIA CONSTITUCIONAL	235
1. Antecedentes claves	235

2. Hallazgos constitucionales	239
3. STC/0011/12. El derecho de acceso a la información pública y su conexión con el derecho a la intimidad/privacidad y el derecho a la protección de datos personales	248
4. STC/0042/12. Un hito entre el derecho de acceso a la información pública, derecho a la intimidad y el derecho a la protección de los datos personales	250
5. STC/0010/13. El derecho de acceso a la información pública y el derecho a la protección de datos personales	254
6. STC/0024/13. <i>El habeas data</i>	255
7. STC/0062/13. Nuevas reflexiones de la STC/0042/12 y el derecho de acceso a la información pública, intimidad y la protección de datos personales	257
8. STC/0084/13. Su vinculación con la STC/0042/12 y el concepto de datos personales	261
9. STC/0404/16. <i>El habeas data</i>	266
10. STC/0475/18. Recalificación de la acción de amparo por <i>habeas data</i>	267
11. Conclusión	269
VII EL DESARROLLO LEGISLATIVO Y LA PERSPECTIVA DE LA PROTECCIÓN DE LOS DATOS PERSONALES EN REPÚBLICA DOMINICANA	270
1. Existencia de ley general de desarrollo y normativas sectoriales en materia de protección de datos. Sus antecedente	270
2. Propuestas legislativas de protección de datos personales	272
2.1. Proyecto de ley mediante el cual se crea las normas que regula y protege los datos personales o Ley de <i>habeas data</i>	273
2.2. Proyecto de Ley Orgánica sobre Protección de Datos de Carácter Personal	277
2.3. Estatus actual de los dos proyectos	282
2.4. Estudio comparado de las piezas legislativas	283
3. Actual ley de protección de datos personales de la República Dominicana	284
3.1. Análisis Ley de Protección de Datos Personales núm. 172-13	286
3.2. Comparación de la Ley núm. 172-13 con sus predecesoras.	297
3.3. Comparación de la Ley núm. 172-13 y la Directiva 95/46/CE	301
3.4. Comparación de la Ley núm. 172-13 con el Reglamento (UE) 2016/679	302
4. Jerarquización de derechos fundamentales	303
5. Acción directa de inconstitucionalidad contra artículos de la	305

Ley núm. 172-13

6. Tutela jurídica de los principios de protección de datos	310
6.1. Tutela de carácter administrativo	311
6.2. Tutela de carácter civil	312
6.3. Tutela de carácter penal	313
6.3.1. <i>Penas y sanciones</i>	314
6.3.2. <i>Código Penal</i>	318

CAPÍTULO IV

REFLEXIONES ENTORNO AL ÓRGANO DE CONTROL COMO VIGILANTE OMNIPRESENTE EN LAS TRANSFERENCIAS INTERNACIONALES EN EUROPA Y LATINOAMERICA, CON ESPECIAL ATENCIÓN EN LA REPÚBLICA DOMINICANA	319
--	------------

I. EI ÓRGANO DE CONTROL y LAS TRANSFERENCIAS INTERNACIONALES EN LAS NORMAS JURÍDICAS EUROPEAS Y LATINOAMERICANAS. REFLEXIONES OMNIPRESENTE.	319
--	------------

1. Consideraciones iniciales	319
2. Normas jurídicas previas, punto de partida	327
3. Aproximación europea	333
4. Concepto y característica del órgano de control en normas jurídicas europeas	336
4.1. Autoridad de control Vs. órgano de control	336
4.2. Incidencia del órgano de control en las normas legislativas	339
4.3. Tipos de autoridad de control	340
4.4. Funciones de la autoridad de control	340
4.5. Autoridad supranacional de control	342
4.6. Autoridad de control en las primeras normativas jurídicas europeas	345
4.6.1. <i>El Comisario de Protección de Datos de la Ley de Hesse</i>	346
4.6.2. <i>El Comisario Federal de Protección de Datos</i>	347
4.6.3. <i>La inspección de Datos de Data Lag Sueca</i>	349
4.6.4. <i>La Comisión de Protección de Datos / El Consejo de Protección de Datos en Austria</i>	349
4.6.5. <i>Comisión Nacional de Informática y Libertades</i>	350
4.6.6. <i>La Inspección de Datos Noruega</i>	350
4.7. Autoridades de control en el Convenio 108 del Consejo de Europa	352
4.8. Autoridades de control en la Directiva 95/46/CE	352

4.9. Autoridades de control en la Ley Orgánica 15/1999 (LOPD)	352
4.10. Autoridades de control en el Reglamento (UE) 2016/679	353
5. Transferencias internacionales de datos	356
5.1. Conceptos claves	356
5.2. Terminología y proceso	357
5.3. Transferencia de datos a terceros países u organismos internacionales	362
5.3.1. Niveles de protección de datos	362
5.3.2. Excepciones a las transferencias internacionales	367
5.3.3. Cláusulas contractuales tipo	370
5.3.4. Sistema de responsabilidades	372
5.4. Transferencia internacional en las primeras constituciones y legislaciones	374
5.4.1. Ley Austriaca de Protección de Datos Personales de 18 de octubre de 1978	375
5.4.2. Ley Noruega núm. 47 de Registros Personales de 9 de junio de 1978	373
5.5. Transferencia internacional en la ONU	375
5.6. Transferencia internacional en el Convenio 108 del Consejo de Europa	377
5.7. Transferencia internacional en la Directiva 95/46/CE	378
5.8. Transferencia internacional en la Ley Orgánica 15/1999 (LOPD)	379
5.9. Transferencia internacional en el Reglamento (UE) 2016/679	380
6. Órgano de control y transferencias internacionales en Latinoamérica	381
6.1. Autoridades de control latinoamericanas	381
6.2. Transferencias internacionales latinoamericanas	385
6.3. Niveles de protección latinoamericana	388
6.4. Niveles de autorización latinoamericana	389
6.5. Ámbito público, ámbito privado	391
6.6. Mecanismos de aseguramiento	392
II. EL ÓRGANO DE CONTROL y LAS TRANSFERENCIAS INTERNACIONALES EN LA REPÚBLICA DOMINICANA	394
1. Consideraciones iniciales	394
2. Órgano de control en los proyectos de ley	395
3. Órgano de control en la Ley de Protección de Datos Personales núm. 172-13	396
3.1. Origen del órgano de control	396
3.2. Funciones del órgano de control	398
3.3. Oficina de Servicio y Protección al Usuario (PROUSUARIO)	402
3.4. Instructivo de las Sociedades de Información Crediticia (SIC)	406
4. El principio de Transparencia	407

5. Órganos adscritos a la Presidencia gubernamental	426
6. La Oficina Presidencial de Tecnología de Información (OPTIC)	428
7. Administración electrónica, transparencia, buen gobierno, órgano de control, protección de datos	431
8. Transferencia internacional en los proyectos de Ley de Protección de Datos Personales	437
9. Transferencia internacional en la Ley de Protección de Datos Personales núm. 172-13	438
10. Opinión del Tribunal Constitucional dominicano respecto al órgano de control de la Ley núm. 172-13	439

CONCLUSIONES

BIBLIOGRAFÍA

ANEXOS

A las personas dispuestas a transitar por el sendero del conocimiento.

ABREVIATURAS

AGA	Alianza para el Gobierno Abierto
AGE/RES	Asamblea General / Resolución
ALC	América Latina y el Caribe
APEC	Conferencia Económica Asia - Pacífico
ARCO	Acceso, Rectificación, Cancelación, Oposición
BM	Banco Mundial
BOE	Boletín Oficial del Estado
CE	Comunidad Económica
CEE	Comunidad Económica Europea
CEP	Comisión de Ética Pública
CEPALSTAT	Estadística Comisión Económica para América Latina y el Caribe
CJI	Comité Jurídico Interamericano
CNECC	Comisión Nacional de Ética y Combate a la Corrupción
CNUCC	Convención de las Naciones Unidas Contra la Corrupción
CODEH	Consejo Dominicano de Derechos Humanos
DAS	Departamento Administrativo de Seguridad
DICOM	Dirección de Comunicaciones
DIDA	Dirección de Información y Defensa de los Afiliados
DIGEIG	Dirección General de Ética e Integridad Gubernamental
DOUE	Diario Oficial de la Unión Europea
DP	Defensor del Pueblo

DPCA	Departamento de Prevención de la Corrupción Administrativa
EEC	European Economic Community
ETS	European Treaty Series
FMI	Fondo Monetario Internacional
GDPR	Reglamento General de Protección de Datos
IADI	Instituto Audiovisual de Informática
ICDPPC	Conferencia Internacional de Comisionados de Protección de Datos
IFAI	Instituto Federal de Acceso a la Información de Protección de Datos
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
INAP	Instituto Nacional de Administración Pública
INDOTEL	Instituto Dominicano de las Telecomunicaciones
LGLAIP	Ley General sobre Libre Acceso a la Información Pública
LOPD	Ley Orgánica de Protección de Datos
LOPDCCP	Ley Orgánica de Protección de Datos de Carácter Personal
LOPDGDD	Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales
LORTAD	Ley Orgánica Sobre Regulación del Tratamiento Automatizado de Datos de Carácter Personal
MAP	Ministerio de Administración Pública
NORTIC	Normativas Tecnología y Telecomunicaciones
OAI	Oficina de Acceso a la Información

OCDE	Organización de Cooperación y Desarrollo Económico
OGP	Office Goberment Open
ONG	Oficinas No Gubernamentales
ONU	Organización de las Naciones Unidas
OPTIC	Oficina Presidencial de Tecnología de Información
PLD	Partido de la Liberación Dominicana
PROUSUARIO	Oficina de Servicios y Protección al Usuario
RAI	Responsable de Acceso a la Información
RGPD	Reglamento Europeo de Protección de Datos
RIPD	Red Iberoamericana de Protección de Datos
SAIP	Solicitud de Acceso a la Información Pública
SIB	Superintendencias de Bancos
SIC	Sociedad de Información Crediticia
SIDA	Síndrome de Inmunodeficiencia Adquirida
STC	Sentencia del Tribunal Constitucional
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
TC	Tribunal Constitucional
TCE	Tratado de la Comunidad Económica
TFUE	Tratado de Funcionamiento de la Unión Europea
TIC	Tecnología de la Información y Comunicaciones
TID	Transferencia Internacional de Datos
TJUE	Tribunal de Justicia de la Unión Europea
TSS	Tesorería de la Seguridad Social

TUE	Tratado de la Unión Europea
UE	Unión Europea
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
WPISP	Working Party on Information Security and Privacy

CAPÍTULO I

INTRODUCCIÓN

1. Presentación y selección del tema

Para nadie es un secreto que el mundo actual como lo conocemos hoy en día, no es el mismo de finales del siglo XIX¹ o principios de los años 70 del pasado siglo² y más, si el planteamiento se encuentra ligado a los ámbitos económicos, tecnológicos o jurídicos. Esto nos sitúa ante un nuevo escenario. Por una parte, la normativa sobre protección de datos refleja esa realidad cada vez más cambiante con nuevos instrumentos y garantías para la tutela de los derechos de las personas; y por otro lado, las posibles amenazas que rodean su entorno también mutan a merced del vertiginoso desarrollo tecnológico³.

¹ Aunque posteriormente trataremos este tema con detención, nos estamos refiriendo al hito precursor sobre la construcción de la privacy en Estados Unidos cual fue la publicación del artículo *The Right to Privacy* publicado en la Revista Harvard Law Review, vol. IV, núm. 5 del 15 de diciembre de 1890 dispuesto por los juristas Warren y Brandeis. Estos autores argumentaron el derecho a ser dejado solo de carácter subjetivo o *the right to be alone*, reconociendo el conflicto entre el derecho a la intimidad y el derecho a la información, dejando claro el poder que tenían las empresas, superior al poder existente, advirtiendo la capacidad que tenían las empresas por medio de sus publicaciones y fotografías instantáneas de invadir los espacios privados de las personas, eliminando, en consecuencia, la privacidad en los hogares. WARREN, S. & BRANDEIS, L., "The Right to Privacy", *Harvard Law Review*, vol. IV, núm.5, 15 diciembre 1890, pp. 193-219. Una traducción castellana del mismo se puede encontrar en PENDÁS, B. y BALSEGA, P., *El derecho a la intimidad*, Civitas, Madrid, 1995, p. 56.

² Es así como a partir de los años 70 se publican las primeras leyes de protección de datos, convirtiéndose en un momento clave de la historia jurídica contemplada entre el derecho a la privacidad? y la libertad informática, siendo esto reflejado en aquellas legislaciones creadas a partir del 1970 como es el caso de la iniciativa del 7 de octubre de 1970 (Land de Hesse) convirtiéndose en la primera ley sobre protección de datos orientada a la administración pública, la Data Lag Sueca de 1973, la Privacy Act de Estados Unidos en 1974 sirviendo de base para el proceso legislativo y constitucional que se avecinaba, tales son los casos de las Constitución de Portugal de 1977 y la Construcción española de 1978. Visto en FROSINI, V., "Bancos de datos y tutela de la persona", *Revista de estudios políticos (Nueva Época)*, núm. 30, Noviembre-Diciembre 1982, pp. 21-40. Disponible en: <file:///C:/Users/pc/Downloads/Dialnet-BancosDeDatosYTutelaDeLaPersona-26724.pdf>. (Última consulta en línea 12 de noviembre 2019).

³ GARRIGA DOMÍNGUEZ, A., "La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento general de protección de datos de la Unión Europea", *Revista Derechos y Libertades*, núm. 38, Época II,

Con los efectos de la globalización, la tecnología, los regímenes autoritarios y la existencia de débiles democracias a mediados de los 70, se propician riesgos, agresión o perjuicio a determinados derechos conectados con la protección de las personas físicas, situación observada en los Estados Latinoamericanos; por su parte, con las tecnologías de información y comunicaciones (TIC), se ventila una disminución de la distancia, acortando los tiempos de transferencias y obtención de información (imágenes, datos) desde grandes distancias, haciendo posible el conocimiento de informaciones impensables en otros tiempos; con la globalización, se produce un aumento en los flujos de mercancías, incrementando las transferencias de datos, colocando en peligro los datos de los nacionales de los Estados sometidos a ellas; con la caída de las dictaduras se instauran jóvenes democracias, dando paso a la creación, desarrollo e implementación de normas legislativas⁴ dirigidas a la protección de las personas físicas y su vinculación con la privacidad, intimidad, honor, protección de datos personales, autodeterminación informativa y la acción de *habeas*⁵ *data* tendente a la obtención de datos personales almacenados en el sector público, en especial los datos en manos de organismos de seguridad estatal.

Tales derechos, se mueven a largo y ancho del planeta, trasladando sus normas de privacidad, intimidad, autodeterminación informativa, *habeas data*, a las legislaciones de los Estados, siendo asumidas de manera parcial o integral, generando una homologación de las mismas.

enero 2018, Madrid, pp. 107-139. También puede verse en WHITAKER, R., *El fin de la privacidad*, 1ª ed. Paidós Ibérica. S. A., Barcelona, 1999, p. 173.

⁴ “Sin embargo, precisamente esa evolución tecnológica se desarrolla a una velocidad que no pueden asumir las leyes...”. DURÁN CARDO, B., *El Delegado de Protección de Datos en el RGPD y la nueva LOPDyGDD*, 1ª ed. Wolters Kluwer España, S. A., Madrid, 2019, p. 23.

⁵ “...la *Ortografía de la lengua española*, 2010, establece que los latinismos se escriben ahora en cursiva y sin tilde española....Por eso, *habeas corpus* figura en la edición del 2014 del DILE en cursiva y sin tilde, por lo que su derivado, *habeas data*, debe escribirse con esas mismas características”. Fundéu BBVA., ¿Finalmente cómo se debe escribir *hábeas data* o *habeas data*?, 2015. Disponible en: <https://www.fundeu.es/noticia/habeas-data/>. (Última consulta en línea 14 de noviembre 2019).

Ante esa realidad, Latinoamérica mantiene un estrecho vínculo y conexión con el desarrollo tecnológico⁶ imperante en el mundo⁷, no permaneciendo indiferente ante los posibles ataques e invasiones a las personas físicas respecto al tratamiento de sus datos personales y la libre circulación de estos datos en los Estados pertenecientes al espacio latinoamericano; una situación no ajena o a espaldas del desarrollo normativo llevado a cabo por los Estados, formando parte de los mismos, con normativas capaces de ejercer tal protección, caso de los Estados pertenecientes a la Unión Europea.

En igual contexto, el crecimiento global de la telefonía móvil equipara con la cantidad de personas existente en el mundo⁸, una situación no exenta de la República Dominicana, situación reflejada en el crecimiento de las comunicaciones móviles⁹, el desarrollo computacional¹⁰ y la capacidad de

⁶ “En América Latina y el Caribe el nivel de penetración de Internet pasó de 4 a 33 usuarios por cada 100 habitantes entre 2000 y 2009”. *Usuarios de Internet*, 2010. Fuente: CEPALSTAT según Base de datos de los indicadores de los Objetivos de Desarrollo del Milenio, División de Estadística de Naciones, CEPALSTAT Bases de Datos y Publicaciones Estadísticas, Comisión Económica para América Latina y el Caribe, Infográficos de América Latina y el Caribe, División de Estadísticas. Disponible en: <http://www.cepal.org/estadisticas/>. (Última consulta en línea 24 de noviembre 2018).

⁷ “...la región de ALC...el empleo se irá desplazando de la manufactura y la construcción hacia servicios como el comercio, la compraventa al por mayor, y la información y las comunicaciones (FEM,2016). El cambio tecnológico, principal motor de estas tendencias, ha creado una ola de transformaciones consideradas por mucho como “la cuarta revolución industrial” ...el cambio ..., la brecha digital puede dejar a muchos al margen de las oportunidades generadas por las TIC. Es preciso mejorar el acceso a plataformas de banda ancha que garanticen la participación en esta nueva ola tecnológica. Con casi la mitad de la población de ALC sin acceso a Internet, se considera que 301 millones de personas están desconectadas. En particular, Brasil, México y Colombia necesitan conectar todavía a unos 180 millones de personas – casi el triple de la población de Francia –. Cabe destacar que este cálculo no tiene todavía en cuenta el tipo o la calidad del acceso a Internet disponible (OCDE/BID, 2016)”. OCDE/CEPAL/CAF (2016), *Perspectivas económicas de América Latina 2017: Juventud, competencias y emprendimiento*, OECD Publishing, Paris. Disponible en: <http://dx.doi.org/10.1787/leo-2017-es>. (Última consulta en línea 4 de octubre 2018).

⁸ DUCOURTIEUX, C., ‘Comunicaciones en tiempo real’, *El atlas de las mundializaciones, le monde diplomatique en español*, UNED, Madrid 2012, p. 71.

⁹ BURRI, E., “Discurso Inaugural presidente de CODETEL”, *Revista Noticias CODETEL*, mayo 1992, p. 15.

¹⁰ TANENBAUM, A., *Estructuras de datos en C*, editora Prentice Hall Hispanoamericana, S. A., México 1993, p. 1.

almacenamiento, tal es el caso de los bancos de datos empleados¹¹ en el almacenamiento de información en el sector público y privado.

A raíz del origen, crecimiento y evolución tecnológica, los Estados se abocan en la construcción de barreras limítrofes a la informática¹², sustentado en el temor generado por las nuevas tecnologías en la sociedad, amparado en la capacidad de almacenamiento, procesamiento de información y velocidad de transferencia de datos, articulados por la informática y las tecnologías de información y comunicaciones (TIC).

Es así, cómo por medio de la creación de barreras limítrofes, fundamentadas en normativas en materia de privacidad, intimidad, honor, protección de datos en los Estados, se persigue la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos¹³. El proceso de globalización de las tecnologías¹⁴ de información y la capacidad de transferencia de datos entre los Estados, genera la necesidad de crear las pautas necesarias para el desarrollo y homologación de leyes nacionales y supranacionales, orquestadas en unos casos y apadrinadas en otros por organizaciones, cumbres internacionales e institutos, con el deseo

¹¹ HALSALL, F., *Data communications, computer networks and systems*, editora Addison Wesley, United States of America, 1988, p. 4.

¹² PÉREZ LUÑO, A. E., "Informática y Libertad. Comentario al artículo 18.4 de la Constitución Española", *Revista de Estudios Políticos (Nueva Época)*, núm. 24, Noviembre-Diciembre 1981.

¹³ *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* Disponible en:

<https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

(Última consulta en línea 2 de septiembre 2018).

¹⁴ "(...) la difusión de la tecnología. Aun cuando los países no sean inventores de tecnología, pueden beneficiarse de ella mediante la importación. Hoy en día, todos los países sin excepción utilizan ordenadores personales, y también los teléfonos móviles están llegando a la mayor parte de las regiones del planeta, incluso a zonas muy pobres. Las innovaciones pueden importarse mediante bienes de consumo, importaciones de capital por parte de empresas (en forma de maquinaria, por ejemplo), inversión extranjera directa (en la cual una compañía de alta tecnología establece una fábrica en un país pobre) ..." visto en SACHS, J., *El fin de la pobreza cómo conseguirlo en nuestro tiempo*, 2ª ed. Random House Mondadori, S. A., Barcelona, 2005, pp. 106-107.

expreso de los Jefes de Estado y de Gobierno mediante sus cumbres y reuniones.

Ante todo, existe una estrecha vinculación entre el derecho a la protección de datos personales y el derecho a la intimidad¹⁵. Cuando nos referimos a la protección de datos¹⁶ perseguimos la protección de las personas físicas por medio a una eventual protección de sus datos personales, es decir, hablamos del derecho a la protección de datos referenciado a una persona física identificada o identificable.

Su origen inicia en Estados Unidos con la *privacy*, moviéndose a largo y ancho del Atlántico, incursionando en Europa con la privacidad, intimidad y la protección de datos, insertándose en Latinoamérica por medio a la figura del *habeas data*, asumiendo la posición de garantía procesal de orden constitucional en el espacio latinoamericano y como no, de la República Dominicana, permitiendo el acceso a los datos personales almacenados en archivos, o bancos de datos públicos y privados.

En el espacio europeo, la protección de las personas físicas se construye mediante la creación de normas legislativas tendentes en garantizar la protección de datos desde el diseño y por defecto, con la finalidad de prevenir y anticipar la protección de datos personales desde el momento mismo de su concepción, al mismo tiempo, se crean órganos de controles independientes, se instauran mecanismos de coherencias, cooperación y se establece la figura del Comité, asegurando la correcta aplicación de las normas creadas para

¹⁵ ESTADELLA YUSTE, O., *La Protección de la Intimidad frente a la Transmisión Internacional de Datos Personales*, 1ª ed. TECNOS, Madrid, 1995, p. 24. También BING, I., *Personal Data System—A comparative perspective on a basic concept in privacy legislation*, in J. BING Y. K. SELMER (eds), *A Decade of Computers and Law*, Publ. Universitets forlaget, Oslo, 1980, p. 80 Citado por ESTADELLA YUSTE, O, *ibid.*, p, 25, nota 6.

¹⁶ “Mal llamadas porque su finalidad es proteger a las personas ante el mal uso de sus datos personales que se encuentren registrados en ficheros mecanizados y no proteger a los datos...” DAVARA RODRÍGUEZ, M. A., *Normativa para la protección de la intimidad: planteamiento general*, nota 3, p. 22, tomado de *IX encuentro 1991, implicaciones socio-jurídicas de las tecnologías de la información*, CITEMA, España, 1991.

estos fines, sin dejar de lado la instauración de figuras tales como el delegado de protección de datos, el responsable y el encargado de protección de datos.

Por su parte, Latinoamérica se enfoca en la creación de una Ley Modelo en materia de protección de datos, un esfuerzo impulsado por organismos internacionales como la Organización de Estados Americanos (OEA), Cumbres de Jefes de Estado y de Gobierno, redes iberoamericanas, etc.; propugnando la creación de mecanismos capaces de implementar, coordinar y homologar leyes en los Estados, ameritando la conformación de autoridades de control revestidas de independencia funcional y capacidad económica.

Se trata de una situación que nos permite presentar propuestas de recomendaciones para el desarrollo y homologación de las normas latinoamericanas en materia de protección de datos, una iniciativa que cuenta con el apoyo de las organizaciones internacionales, tal es el caso de la Organización de Estados Americanos (OEA), las Cumbres Iberoamericanas de Jefes de Estado y de Gobierno, consumada mediante las Conferencias de Jefes de Estado y redes de protección de datos entre otras, destacando la Red Iberoamericana de Protección de Datos (RIPD), dotando a los Estados Latinoamericanos de una Ley Modelo en materia de protección de datos personales para los Estados Latinoamericanos.

En tanto que, amparados en el uso de la tecnología de información y comunicaciones (TIC) en la población y la administración gubernamental, los gobiernos vuelcan su interés en transparentar la administración pública, permitiendo el acceso electrónico de la población a sus administraciones, sentando las bases del gobierno electrónico, y al mismo tiempo, tejiendo un acceso a la información pública reconocido como una variante o subtipo del *habeas data*, nos referimos al *habeas data* impropio o de acceso a la información pública. En ese sentido, la República Dominicana realizó ingentes esfuerzos en la construcción de su normativa legislativa en materia de protección de datos, una normativa materializada a partir de los dos proyectos de ley existentes en la cámara legislativa, materializado vía la Ley núm. 172-

13, que tiene por objeto la protección integral de los datos personales asentados en archivos, siendo sometida a una acción directa de inconstitucionalidad interpuesta por diversas organizaciones nacionales, entre ellas, el Consejo Dominicano de Derechos Humanos (CODEH) y la Alianza para los Derechos Fundamentales.

La tesis doctoral que nos ocupa, investiga mediante un análisis exhaustivo y pormenorizado la protección de datos personales y el *habeas data* en la República Dominicana desde la óptica del contexto europeo y latinoamericano, tomando como punto de partida el origen de la *privacy* en Estados Unidos, seguido por la Ley del Censo Alemana, hasta llegar a Latinoamérica con el nacimiento del *habeas data* en el Estado brasileño. Al mismo tiempo, se analizan los preceptos legislativos y jurisprudenciales de la Unión Europea y Latinoamérica, incluidas las últimas sentencias de la Unión Europea en materia de protección de datos, derecho de supresión (derecho al olvido), transferencias internacionales y las sentencias evacuadas por el Tribunal Constitucional de la República Dominicana en temas de intimidad, privacidad, acceso a la información pública etc.

En tal sentido, se examinan las normas de protección de datos orientadas a la protección de las personas físicas en el espacio europeo, tomando en cuenta las decisiones del Parlamento Europeo, la Comisión y el Consejo Europeo, incluida su pasada Directiva 95/46/CE y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, aplicable a partir del 25 de mayo de 2018, más el Convenio 108 del Consejo de Europa y su *Protocolo Adicional de la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a las transferencias de datos*.

Al mismo tiempo, se analizan las Cumbres Iberoamericanas de Jefes de Estado y de Gobierno de los Estados Iberoamericanos, la Organización de los Estados Americanos (OEA), las Conferencias Iberoamericanas de Protección de Datos, las Conferencias de Protección de Datos, la Organización de

Cooperación y Desarrollo Económico (OCDE) y sus propuestas de Estándares Iberoamericanos en materia de Protección de Datos.

La selección del tema ha sido fruto de varios factores, entre ellos: a) la República Dominicana no cuenta con una legislación adecuada a los últimos estándares y adelantos legislativos en materia de protección de datos. Muy al contrario de los proyectos presentados en la Cámara de Diputados y el Senado de la República Dominicana previo a la promulgación de la actual Ley núm. 172-13 de protección integral de datos personales y las normativas europeas y latinoamericanas en materia de protección de datos; b) el deseo manifiesto de organizaciones, Cumbres Iberoamericanas de Jefes de Estado y de Gobierno en homologar sus normas internas en materia de protección de datos personales en Latinoamérica; c) la imperiosa necesidad de crear una Ley Modelo de Protección de Datos Latinoamericana; y d) La urgente obligación gubernamental de transparentar la administración pública mediante el acceso a la información pública de sus nacionales.

2. Antecedentes claves

El trabajo toma en consideración el ensayo de la *privacy* americana de Warren y Brandéis¹⁷, seguido de diversos estudios legislativos en materia de protección de datos, tales como la Ley Federal de Protección de Datos de Alemania, la recomendación de la OCDE de 1980, el Convenio 108 del Consejo de Europa, la Ley Orgánica 5/1992 (LORTAD), Ley Orgánica 15/1999 (LOPD), la Directiva 95/46/CE y 97/66/CE; al mismo tiempo, se consideran los tratados, acuerdos y convenios internacionales, sin dejar de lado las Cumbres Iberoamericanas de Jefes de Estado y de Gobierno, así como las normas legislativas de los Estados Iberoamericanos en materia de protección de datos y *habeas data*.

¹⁷ WARREN, S. & BRANDEIS, L., "The Right to Privacy..." op. cit., pp. 193-219. Una traducción castellana del mismo se puede encontrar en PENDÁS, B. y BALSEGA, P., *El derecho a la intimidad...op. cit.*, p. 56.

3. Objetivos de la investigación

3.1. Objetivo general

Investigar y puntualizar mediante un análisis pormenorizado la protección de datos personales y el *habeas data* en la República Dominicana en un contexto europeo y latinoamericano, sin dejar de lado las transferencias internacionales, órgano de control, transparencia y acceso a la información pública en el espacio europeo y latinoamericano conectado con las tecnologías de información y comunicaciones (TIC).

3.2. Objetivos específicos

- Estudiar los principales avances y tendencias en materia de protección de datos, *habeas data*, transferencias internacionales, órganos de control, transparencia y acceso a la información pública en el espacio europeo y latinoamericano, con énfasis en la República Dominicana.
- Profundizar acerca del entorno global de la protección de datos, *habeas data*, transferencias internacionales, órganos de control, transparencia y acceso a la información pública en el espacio europeo y latinoamericano, con énfasis en la República Dominicana, vía video de expertos y Cumbres Iberoamericanas de Jefes de Estado y de Gobierno.
- Analizar el estatus actual de la protección de datos, *habeas data*, transferencias internacionales, órganos de control, transparencia y acceso a la información pública en el espacio europeo y latinoamericano con énfasis en la República Dominicana, mediante referencias bibliográficas, revistas académicas, Internet y conferencias.
- Ahondar en las últimas tendencias doctrinales en materia de protección de datos personales, *habeas datas*, transferencias internacionales, órganos de

control, transparencia y acceso a la información pública en el espacio europeo y latinoamericano con énfasis en la República Dominicana.

- Realizar un estudio de las principales sentencias emitidas por el Tribunal de Justicia de la Unión Europea (TJUE), el Tribunal Constitucional de la República Dominicana, la Corte Interamericana de Justicia en temas conectados con la protección de datos personales, derecho a la Información pública, *habeas data*, protección de la honra y la dignidad, derecho al olvido, puerto seguro.

4. Hipótesis de la investigación

La República Dominicana, no cuenta con una estructura legislativa en materia de protección de datos y *habeas data* que le permita estar al alcance de las principales normativas europeas y latinoamericanas en materia de protección de datos y *habeas data*.

La situación imposibilita su adhesión a importantes convenios internacionales como el Convenio n.º 108 del Consejo de Europa, y, por otro lado, obtener el reconocimiento de la Comisión Europea como Estado con normativa adecuada en materia de protección de las personas físicas en relación al tratamiento de datos personales y el libre trasiego de estos. Si lo anterior fuera logrado, se conseguiría un aumento en las transacciones comerciales con los Estados, incluido la Unión Europea y los Estados con legislaciones adecuadas como Argentina, Uruguay y México con normativa robusta y madura en la materia.

5. Métodos y fuentes

Para el conocimiento de las informaciones que rodean la protección de datos y el *habeas data* en la República Dominicana empleamos el método

descriptivo; de igual modo, utilizamos el método analítico, abordando de manera crítica estos derechos y su conexión con los antecedentes que dieron pauta al surgimiento de los mismos lo cual entronca con el método histórico. Por su parte, el método inductivo nos proporciona un marco general para estos derechos y sus diferentes ámbitos, llegando a la particularidad de los mismos.

La metodología empleada y cuenta con el soporte de diversas fuentes de derechos, permitiendo su estudio y materialización, tales son los casos de las fuentes primarias apoyadas en normas jurídicas, situación de los textos legislativos, pronunciamientos jurisprudenciales entre los que destacan los emanados por el Tribunal Constitucional de la República Dominicana, el Tribunal de Justicia de la Unión Europea, así como los precedentes de las legislaciones europeas, españolas, latinoamericanas etc. sin dejar de lado el repertorio doctrinal existente.

En ese sentido, y a manera de soporte, más allá del acervo doctrinal, jurisprudencial y legislativo incorporado en el trabajo, se realizó un acercamiento con diversos estamentos e instituciones del Estado como la Cámara de Diputados y el Senado de la República Dominicana, abordando los proyectos de ley en materia de protección de datos y *habeas data*, precursores de la actual Ley núm. 172-13. De igual forma fueron consultadas vía el Portal Único de Acceso a la Información Pública (SAIP) el Defensor del Pueblo, la Dirección General de Ética e Integridad Gubernamental, el Instituto Dominicano de las Telecomunicaciones, el Ministerio de Administración Pública, el Portal Único de Solicitud de Acceso a la Información Pública, la Superintendencia de Bancos y el Tribunal Constitucional, en temas relacionados con el órgano de control..

En igual contexto, se toman en cuenta las informaciones procedentes de congresos, comunicaciones, cursos de verano y exposiciones nacionales e internacionales. Por su actualidad y porque ha sido en la Comunidad Autónoma Vasca (concretamente en la UPV/ EHU) donde se ha concluido dicho trabajo, como botón de muestra cabe destacar entre otros: las informaciones vertidas

en el Congreso Internacional sobre *el Impacto del Reglamento Europeo de Protección de Datos: análisis nacional y comparado*, realizado los días 17 y 18 de mayo 2018, Universitat Jaume I, en Castellón, y el caso del discurso inaugural del curso de verano *Protección de Datos y Transparencia: Compañeros de Viaje*, presentado el 21 de junio 2018 por la directora de la Agencia Vasca de Protección de Datos D^a Margarita Uria Etxebarria, así como el curso de verano *Periodismo, privacidad y derechos digitales* realizado el 19 de junio 2019 (ambos en el Palacio de Miramar de San Sebastián).

6. Hitos legislativos ocurridos durante el desarrollo del trabajo de investigación

Somos partícipes de los cambios y transformaciones que ocurren a cada momento en los diversos estamentos de nuestra sociedad, una situación de la que no es ajeno el trabajo de investigación, razones por las que presentamos los cambios, transformaciones, derogaciones de leyes y proyectos acaecidos durante la elaboración del mismo, ameritando su exposición.

- Rescisión del proyecto de ley mediante el cual se crean las normas que regula y protege los datos personales o Ley de *habeas data* (autor diputado Demóstenes Martínez) (2013).
- Cancelación del proyecto de Ley Orgánica sobre Protección de Datos de Carácter Personal (autor senador Félix Ramón Bautista Rosario) (2013).
- Derogación de la Ley núm. 288-05, del 18 de agosto del año 2005, que regula las Sociedades de Información Crediticia y de Protección al Titular de la Información (2013).
- Materialización de la Ley núm. 172-13, que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados.

- Proclamación Constitución de la República Dominicana del 13 de junio de 2015.
- Implementación del Reglamento (UE) 2016/679 del Parlamento europeo y el Consejo.
- Entrada en vigor Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales 3/2018 de España.

7. ¿Desde dónde partimos ?

El trabajo se enmarca en una ola de estandarizaciones y deseos de encaminar la uniformidad u homogeneidad de las normas legislativas en materia de protección de datos en Latinoamérica y, como no, en la República Dominicana. De su parte, no han sido poco los autores que han versado sobre el asunto, unos abogan por la creación de autoridades supranacionales de control como es el caso de Olga Estadella Yuste¹⁸, otros, apelan por dotar a los Estados miembros del Mercosur¹⁹ de un nivel común de protección de datos²⁰, tal es el caso de la propuesta de Mario Viola de Azevedo Cunha, en cambio, para algunos como Nelson Remolina Angarita²¹, Oscar Puccinelli, no existen normativas globales en materia de protección de datos o convenios vinculantes para los Estados Latinoamericanos, en ese contexto, se han propuesto y elaborado diversas normativas de estandarizaciones y leyes modelos latinoamericanas de cara a la construcción de un modelo a seguir en los Estados Iberoamericanos, tales son los casos de las *Propuestas de Modelos*

¹⁸ ESTADELLA YUSTE, O., *La Protección de la Intimidación frente a la Transmisión Internacional* ...op. cit., pp. 147-148.

¹⁹ Estados miembros: Argentina, Uruguay, Paraguay, Brasil y Venezuela.

²⁰ DE AZEVEDO CUNHA, M. V., *Protección de Datos en el Mercosur: Hacia un Marco Común*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014, pp. 1126-1129.

²¹ REMOLINA ANGARITA, N., *Insuficiencia de la regulación latinoamericana frente a la recolección internacional de datos personales a través de Internet*, *Quaestiones Disputatae* 2, Pontificia Universidad Javeriana, Facultad de Ciencias Jurídicas, colección Doctorado en Ciencias Jurídicas, Bogotá, 2011, pp.182, 211, 220.

de Autoridad de Control de Protección de Datos²², la Resolución de Estándares Internacionales de Privacidad²³, la Ley Modelo Interamericana, el Proyecto de Principios y Recomendaciones Preliminares sobre la Protección de Datos (La Protección de Datos Personales)²⁴ y los Estándares de Protección de Datos Personales para los Estados Iberoamericanos²⁵.

Durante la exposición del trabajo, no realizaremos diferencia conceptual entre los términos Iberoamérica y Latinoamérica, así como sus correspondientes gentilicios iberoamericano y latinoamericano siendo tratados indistintamente a lo largo y ancho del trabajo, ya que a pesar de tener sus diferencias no forman parte de las consideraciones del mismo.

²² IV Encuentro Iberoamericano de Protección de Datos., *Informe de Viabilidad de creación de Autoridades de Control en el entorno Iberoamericano*, Huixquilucan (Estado de México), 4 de noviembre de 2005, pp. 1 y ss. Disponible en: <http://www.redipd.es/actividades/encuentros/IV/index-ides-idphp.php>. (Última consulta en línea 6 de mayo 2017).

²³ *En el V Encuentro Iberoamericano de Protección de Datos, Declaración de Lisboa 2007*, se aprueban las Directivas de Armonización de Protección de Datos en la Comunidad Iberoamericana, cuya finalidad busca la creación de iniciativas legislativas referentes para otros países en otras áreas geográficas. Al mismo tiempo, en la declaración del VI encuentro de la Red Iberoamericana de protección de datos en el documento “Un compromiso para alcanzar estándares internacionales de protección de datos y privacidad” se realiza un llamado a las conferencias internacionales en materia de protección de datos a que se avoquen en la adopción de un instrumento jurídico común en materia de protección de datos. *V Encuentro Iberoamericano de Protección de Datos, Declaración de Lisboa 2007*. Disponible en: <http://www.redipd.es/actividades/encuentros/V/index-ides-idphp.php>. (Última consulta en línea 08 de junio 2017).

²⁴ El Departamento de Derecho Internacional previamente presentó el proyecto de *Principios y Recomendaciones Preliminares sobre la Protección de Datos Personales CP/CAJP-2921 Rev.1*, mostrado en el cuadragésimo primer periodo ordinario de sesiones, el documento es presentado por el Departamento de Derecho Internacional de la Secretaría de Asuntos jurídicos, conforme al párrafo 11 de la parte dispositiva de la resolución AG/RES. 514 (XXXIX – O/09).

²⁴ AG/RES-2661 (XLI-O/11)., *Acceso a la información pública y protección de datos personales*. Disponible en: http://www.oas.org/es/sla/cji/docs/CJI-doc_402_12_rev2.pdf. (Última consulta en línea 16 de agosto 2017).

²⁵ Red Iberoamericana de Protección de Datos., *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*, Santiago de Chile, 20 de junio 2017. Disponible en: http://inicio.inai.org.mx/nuevo/Estandares%20PDP_iberopdf. (Última consulta en línea 29 de junio 2017).

8. Estructura y orden de exposición

El trabajo de investigación se encuentra estructurado por cuatro capítulos seguido por conclusiones, bibliografía y anexos; iniciamos con la introducción (capítulo I), continuando con la incursión de la protección de datos en América, Europa y Latinoamérica, sin dejar de lado la incorporación del *habeas data* en los plexos constitucionales latinoamericanos (Capítulo II), seguido por el análisis de la intimidad, protección de datos y el *habeas data* en el espacio dominicano vinculado a su doctrina, jurisprudencias constitucionales y normas legislativas internas existente en la materia (Capítulo III), continuando con el examen del órgano de control y las transferencias internacionales en Europa, y Latinoamérica, incluida la República Dominicana (Capítulo IV), finalizando con las conclusiones del trabajo.

Ante el escenario planteado, presentamos el desarrollo y orden de exposición de los capítulos, el primero se orienta a la Introducción, incluyendo los antecedentes, objetivos, hipótesis, así como al metodología y estructura de exposición; el segundo capítulo lo conforman dos subcapítulos dirigidos al origen de la *privacy* en Estados Unidos y su origen e incorporación en Europa, observando los primeros cimientos del nacimiento de la protección de datos y el *habeas data*, unos inicios que en materia de privacidad se mueven a largo y ancho del Atlántico, desde Estados Unidos a Europa, incursionando en la autodeterminación informativa con la Sentencia del Censo Alemana y las distintas corrientes doctrinales originadas a raíz de los textos constitucionales españoles y su desarrollo normativo, incluidos los provenientes de la Comunidad Europea y el Reglamento de la Unión Europea conectado con sus recientes jurisprudencias, una construcción de la protección de datos soportada, conectada e influenciada por normas internacionales, y orquestadas por organismos internacionales, entre ellos, la Organización de las Naciones Unidas (ONU), la Organización de Cooperación y Desarrollo Económico (OCDE), el Convenio del Consejo de Europa. Por su parte, el segundo subcapítulo desarrolla el derecho a la protección de datos en Latinoamérica y la figura del *habeas data* en las constituciones latinoamericanas, abordando propuestas y modelos legislativos como es el caso de la Ley Modelo

Latinoamericano en materia de Protección de Datos, un modelo sustentado en el planteamiento de mecanismos de controles independientes para los Estados Iberoamericanos.

En el tercer capítulo, analizamos el desarrollo del *habeas data* y la protección de datos personales incursionada en la Constitución de la República Dominicana del 2010, la actual Constitución dominicana del 2015, la *Ley núm. 172-1,3 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados*, las sentencias evacuadas por el Tribunal Constitucional en materia de *habeas data*, protección de datos personales, acceso a la información pública y al mismo tiempo, incursionamos en el análisis de la legislación actual y sus procesos normativos previos, finalizando con un estudio comparado de las propuestas legislativas.

El cuarto capítulo se orienta al órgano de control y las transferencias internacionales en el espacio europeo y latinoamericano, con especial énfasis en la República Dominicana, un capítulo compuesto por dos partes o subcapítulos, el primer subcapítulo se orienta al órgano de control y las transferencias internacionales en las constituciones europeas y americanas, iniciando con el desarrollo histórico de los eventos ocurridos, hasta llegar a la concesión actual del reconocido derecho a la protección de datos personales existente hoy en día, una situación que nos permite realizar un recorrido por el órgano de control y las transferencias internacionales desde el ámbito europeo y latinoamericano, soportado en sus constituciones, leyes y jurisprudencias; finalizando en el subcapítulo II con el análisis del órgano de control y la transferencia internacional de la República Dominicana, visto desde la óptica de los proyectos de ley y la actual Ley núm. 172-13, de su parte, se examina la transparencia gubernamental contemplada en la administración pública, siendo considerada en las normas de acceso a la información pública y los portales electrónicos vía la administración electrónica; finalizando con un análisis pormenorizado de la decisión del Tribunal Constitucional relativo a la acción

directa de inconstitucionalidad, incoada por sectores y organizaciones a diversos artículos de la Ley núm. 172-13, como es el caso del artículo 29 relativo al órgano de control dispuesto en la presente ley.

Finalizando con la exposición de las conclusiones y recomendaciones del trabajo de investigación. Una situación que nos permite avanzar diciendo que la Constitución de la República Dominicana del 2010 y la actual Constitución del 2015, reconocen vía los artículos 44 y 70 la figura del *habeas data* y la protección de datos personales. 3 años después de la reforma constitucional del 2010, se promulga la actual *Ley núm. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados, deberá ser sometida a un proceso de adecuación, permitiendo con la decisión, un acercamiento a las principales normativas europeas y latinoamericanas en materia de protección de datos personales, como es el caso del Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo de 27 de abril de 2016, el Estándar de Protección de Datos Personales para los Estados Iberoamericanos y otras normativas latinoamericanas conectadas con el tema, siendo reconocidas por la Unión Europea como Estados con normativas adecuadas en materia de protección de datos, tales son los casos de Uruguay, Argentina y México que a pesar de no ser reconocido como Estado adecuado por la Comisión de la Unión Europea, goza de poseer normas maduras y completas en materia de protección de datos. Ante esa situación, la actual Ley núm. 172-13 debe reformular, crear y disponer de un órgano de control con total independencia funcional y económica adscrito a la presidencia, dejando de ser un mero órgano de tercer y cuarto nivel, orientado a la inspección de los archivos destinados a proveer informes crediticios hasta convertirse en un órgano de primer rango conectado con la presidencia. La nueva normativa impulsará la instauración de la figura del Oficial de Protección de Datos (DPO) en las empresas o los responsables, así como implementar la privacidad por diseño y por defecto, instaurar la evaluación de impacto, reconocer el derecho a la portabilidad de datos, entre otros.*

El reconocimiento o certificación por parte de la Unión Europea, contribuirá con el acercamiento de la República Dominicana a los Estados europeos, permitiendo su posible adhesión al *Convenio 108 del Consejo de Europa del 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo Adicional al Convenio 108 relativo a las autoridades de control y las transferencias internacionales*, así como el reconocimiento por parte de la Unión Europea como un Estado con legislación adecuada en materia de transferencias internacionales de datos y normativas robustas en materia de protección de datos, obteniendo a posteriori la certificación de la Comisión Europea. La medida contribuye con el aumento de los flujos transfronterizos hacia y desde los Estados europeos y como no, de la Unión Europea en su conjunto, retribuyendo en una mejora del comercio de la República Dominicana con Europa y una eventual protección de los datos personales involucrados en las transferencias.

En ese contexto, Latinoamérica debe adoptar un Estándar en materia de protección de datos para la región, seguido por un proceso de instauración de órganos de controles en los Estados, revestidos de total independencia económica y funcional en los mismos, bajo la coordinación de un órgano de control central adscrito a la Organización de Estados Americanos (OEA), funcionando como un órgano de administración supranacional, responsable de homologar la normativa latinoamericana en la región, y con ello, hacer frente a las amenazas tecnológicas en la zona, a la vez, de impulsar el comercio en la región previo al reconocimiento de la Comisión Europea como Estados con legislaciones adecuadas en materia de protección de datos, impulsando el comercio en la zona, producto al aumento de las transacciones comerciales con los Estados europeos.

CAPÍTULO II

EL DERECHO A LA PROTECCIÓN DE DATOS Y EL *HABEAS DATA*. ESPECIALMENTE SU ORIGEN Y EVOLUCIÓN EN EUROPA Y LATINOAMÉRICA

I. EL ORIGEN DE LA PROTECCIÓN DE DATOS PERSONALES EN ESTADOS UNIDOS Y SU ORIGEN E INCORPORACIÓN EN EUROPA

1. Planteamiento de la cuestión

Previo al nacimiento y evolución de los avances tecnológicos de la época actual, no existía aún la necesidad de establecer legislaciones en materia de protección de las personas físicas relacionadas con la protección de datos. A juzgar por los hechos, previo a la existencia de cámaras fotográficas, comunicaciones cablegráficas, y telefónicas, era inimaginable pensar en la posibilidad de invadir o violar la intimidad de las personas en hogares, espacios privados o extraer informaciones personales almacenadas en archivos automáticos protegidos por las barreras del tiempo y el espacio.

En ese entonces, no era posible conservar por grandes períodos de tiempo las imágenes observadas, debido a la ausencia de medios capaces de retener la imagen o conservar las informaciones almacenadas en archivos físicos. De igual forma, el espacio era limitado, haciendo que las informaciones observadas no pudieran ser desplazadas a grandes distancias, convirtiéndose el espacio-tiempo²⁶ en barreras naturales de propagación de la vida privada e íntima²⁷ de las personas hacia lugares más allá de su entorno cotidiano.

²⁶ PÉREZ GÓMEZ, E. y CRESPO LÓPEZ, A., *La protección de datos en los centros de enseñanzas*, 1ª ed. Aranzadi S. A., Navarra, 2007, pp. 26-27.

²⁷ "...los problemas jurídicos suscitados por el tratamiento automático de la información, la protección de la intimidad y de las libertades individuales constituye quizás el aspecto más controvertido. Esta preocupación tan difundida se debe al uso generalizado de los ordenadores para el tratamiento de datos de carácter personal, a las grandes posibilidades que hoy ofrece el almacenamiento, la comparación, la interconexión, selección y acceso de los datos de carácter personal simultáneamente a disposición de millares de usuarios situados en lugares

Con la informática, surge el manejo de grandes volúmenes de datos almacenados en archivos electrónicos conectados con su gran velocidad de ejecución. De igual forma, con el advenimiento de: a) la telemática o transmisión a distancia de datos automatizados²⁸; b) el Internet²⁹ como red de redes; y c) las numerosas tecnologías de información y comunicaciones (TIC`s), se disminuyen los espacios, transmitiendo las informaciones a lugares inalcanzables nunca antes pensado, colocando la privacidad e intimidad de las personas al alcance de otros a pesar de la distancia, en ese contexto, con el nacimiento de la tecnología³⁰ (computador, informática, TIC, telecomunicaciones, Internet³¹), los términos espacio - tiempo dejaron de ser

geográficamente dispersos y permite reunir datos y crear redes complejas de datos a escala nacional e internacional...". Documentación Informática., *Flujo Internacional de Datos, recomendación de la OCDE de 23 de septiembre de 1980*, tratados Internacionales núm. 2, 1ª ed. Presidencia del Gobierno, serie amarilla, servicio central de publicaciones, Madrid, 1982, p. 26.

²⁸ ULL PONT, E., *Derecho público de la informática, protección de datos de carácter personal*, 2ª ed. UNED, Madrid, 2003, p. 17.

²⁹ El primer mensaje fue enviado el 29 de octubre de 1969, a las diez y media de la noche desde la universidad de California en los Ángeles a la universidad de Standford, con la siguiente información colocada en el diario de implementación (IMP LOG) "Talked to SRF Host to Host" hemos hablado con el centro de Standford de servidor a servidor; en la Universidad de California se encuentra una tarjeta con la siguiente información "IEEE Milestone in Electrical Engineering and Computing, Birthplace of the Internet, 1969, At 10:30 pm., 29 de October 1969, the first ARPANET message was sent from this UCLA site to the Stanford Researcg Institute. Based on packet switching and dynamic resource allocation. The sharing of information digitally from this first node of ARPANET launched the Internet revolution. October 2009." Presentamos la siguiente traducción en castellano "IEEE Hito en Ingeniería Electrónica e Informática, lugar de nacimiento de Internet, 1969, A las 10:30 p.m., 29 de octubre de 1969, se envió el primer mensaje de ARPANET desde este sitio de UCLA al Stanford Researcg Institute. Base de conmutación de paquetes y asignación dinámica de recursos. El intercambio de información digital desde este primer nodo de ARPANET lanzó la revolución de Internet. octubre de 2009" HERZOG, W., *Lo and Behold: Reveries of the Connected World*, NETFLIX, 2016.

³⁰Cfr. "the technology is becoming more transnational in character; the insecurity about these developments will promote a greater and more regular process of lesson drawing; international regimes will continue to promote harmonization; and countries that have not yet responded will be pressured to conform" correspondiendo su traducción en castellano a ".la tecnología se está volviendo más transnacional en su carácter; la inseguridad sobre estos desarrollos promoverá un proceso de extracción de lecciones mayor y más regular, los regímenes internacionales continuarán promoviendo la armonización; y los países que aún no han respondido serán presionados para conformarse". BENNETT, C., *Regulatin Privacy, Data Protection and Public Policy in Europe and the United State*, 1ª ed. Cornell University, New York, United States of America, 1992, p. 251.

³¹ "Internet es una realidad social que el Derecho no puede desconocer...configura un entorno económico que demanda una regulación jurídica que proporcione la seguridad necesaria para poder operar en la red con garantías". DAVARA RODRÍGUEZ, M. A. (Coordinador), *XVII*

barreras de la privacidad e Intimidad³², acercando los ciudadanos y los pueblos, cambiando la visión de un mundo global al de aldea global y como no, del hogar global, formando parte de una gran red con característica universal³³.

Es ahí cuando las normas legislativas se convierten en nuevas barreras limítrofes a la intimidad y la privacidad, imponiendo medidas de prevención, corrección y normas sancionadoras, con el objetivo de tutelar tales derechos fundamentales³⁴, otorgando *protección a las personas físicas en lo que respecta al tratamiento automatizado de datos personales y a la libre circulación de los mismos*, haciendo necesario la imperiosa necesidad de su regulación, una regulación amparada por organismos internacionales, normativas constitucionales en los Estados, conectadas con sus leyes generales y sectoriales en materia de protección de las personas físicas y sus derechos fundamentales, tales como, intimidad, privacidad, protección de datos personales.

Ante la imperiosa necesidad de establecer barreras limítrofes a los medios fotográficos, informáticos y asegurar una real protección de las personas físicas, los Estados inician una escalada de procesos regulatorios como la *privacy* americana³⁵, la Ley Alemana Federal de Protección de Datos de 1977,

encuentro sobre Informática y Derecho, Universidad Pontificia Comillas, Madrid 2002-2003, p. 6.

³² Cfr. "exposición de motivos *Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal*". Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189>. (Última consulta en línea 23 de junio 2018).

³³ PÉREZ LUÑO, A. E., *Internet y los Derechos Humanos, Derecho y conocimiento*, vol. 2, Facultad de Derecho. Universidad de Huelva, España, p. 103. Disponible en: <https://core.ac.uk/download/pdf/60638165.pdf>. (Última consulta en línea 26 de junio 2018).

³⁴ BARBA MARTÍNEZ, G. P., *Curso de Derechos Fundamentales, Teoría General*, Boletín Oficial del Estado, Universidad Carlos III de Madrid, Madrid, 1999. pp. 36-38.

³⁵ ".....los autores ingleses denominan <<Right to be alone>> o <<Right of privacy>>, los alemanes <<Recht auf der eigenen Geheimsphäre>>, los franceses <<droit au vie privée>>, los italianos <<diritto a la vida privada>> o <<derecho a la intimidad>>, y que viene a significar el derecho a ser dejado tranquilo, a no ser molestado en la intimidad de la vida privada.....", GARCÍA VITORIA, A., *El derecho a la intimidad, en el derecho penal y en la constitución de 1978*, 1ª ed. ARANZADI, S. A., Pamplona, 1983, p. 14.

el artículo 35 de la Constitución de Portugal, el Convenio 108 del Consejo de Europa y su Protocolo Adicional, la Constitución española de 1978 con su artículo 18,4 conectado en sus inicios a la legislación interna, tal es el caso de la *Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal* (conocida como LORTAD), subsecuentemente se desarrollaron nuevas normas legislativas como la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* (conocida como LOPD) y otras de carácter general aplicable a todos los Estados que forman parte de la Comunidad o Unión Europea, como son los casos de la *Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* y el *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* y por el que se deroga la Directiva 95/46/CE, un Reglamento de reciente creación, analizado y presentado en los próximos acápite³⁶.

Existe una estrecha vinculación entre el derecho a la protección de datos personales y el derecho a la intimidad³⁷, cuando nos referimos a la protección de datos³⁸, perseguimos la protección de las personas físicas por medio a una eventual protección de sus datos personales, es decir, nos referimos al derecho a la protección de datos referenciado a una persona física identificada o

³⁶ Durante la exposición del trabajo se manejará indistintamente los nombres de las normativas como sus abreviaturas.

³⁷ ESTADELLA YUSTE, O., *La Protección de la Intimidad frente a la Transmisión Internacional* ...op. cit., p. 24. También BING, I., *Personal Data System—A comparative perspective on a basic concept in privacy legislation*, in J. BING & K. SELMER (eds), *A Decade of Computers and Law*, Publ. Universitets forlaget, Oslo, 1980, p. 80 Citado por ESTADELLA YUSTE, O., *ibid.*, p, 25, nota 6.

³⁸ “Mal llamadas porque su finalidad es proteger a las personas ante el mal uso de sus datos personales que se encuentran registrados en ficheros mecanizados y no proteger a los datos...” DAVARA RODRÍGUEZ, M. A., *Normativa para la protección de la intimidad: planteamiento general*, nota 3, p. 22, tomado de *IX encuentro 1991, implicaciones socio-jurídicas de las tecnologías de la información*, CITEMA, Madrid, 1991.

identificable; algunos autores relacionan los términos protección de datos con la protección de la intimidad, expresando que su carácter diferenciador se encuentra más relacionado con el origen de su procedencia, nos referimos a los sistemas legales de *common law* o de *civil law*, los países con tradición de *civil law* emplean los términos de protección de datos, a diferencia de los países con bases jurídicas provenientes del *common law* que emplean los términos de protección a la intimidad³⁹; otros evitan tales diferencias por entender que la protección de datos está reemplazando al concepto de privacidad⁴⁰, conectando la protección de datos con la era informática.

Las pretensiones del trabajo están orientadas en realizar un estudio del nacimiento de la protección de datos personales en Estados Unidos y Europa. Por un lado, un buen número de autores ha venido sistematizando en sus trabajos las distintas “generaciones de protección de datos”⁴¹, reseñando el nacimiento y construcción de este derecho a ambos lados del Atlántico⁴². Por su parte, nuestro especial interés en señalar este origen obedece a que en estos momentos “suelen” o “empiezan a” convivir en Latinoamérica tanto la

³⁹ Así lo expresa ESTADELLA YUSTE, O., *La Protección de la Intimidad frente a la Transmisión ...op. cit.*, p. 25.

⁴⁰ (...) La privacidad y transferencia internacional de datos continúan siendo dos cuestiones importantes y vigentes..., REMOLINA ANGARITA, N., *Recolección internacional de datos personales: un reto del mundo post-internet*, 1ª ed. Agencia Española de Protección de Datos, Madrid, 2015, p. 37.

⁴¹ Cfr “the first generation of data protection law was enacted in many countries because the issue was defined separately and given its own political momentum.... the roots of data protection are individualistic... “La primera generación de la ley de protección de datos se promulgó en muchos países porque el problema se definió por separado y se le dio su propio impulso político.... las raíces de la protección de datos son individualistas.”. BENNETT, C., *Regulating Privacy, Data Protection...op. cit.*, p. 253.

⁴² Así cabe citar entre otras las obras en lengua castellana de PÉREZ LUÑO, A. E., *Libertad informática y leyes de protección de datos personales*, edición a cargo de LOSANO, M., PÉREZ LUÑO, A. y GUERRERO MATEUS, M., Centro de Estudios Constitucionales. Madrid, 1989, pp.145 y ss; LUCAS MURILLO DE LA CUEVA, P., *El derecho de la autodeterminación informativa*, Tecnos, Madrid, 1990, pp. 25 y ss; SERRANO PÉREZ, M. M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Civitas-Thomson, Madrid, 2003, p. 29 y ss; ARENAS RAMIRO, M., *El Derecho fundamental a la protección de datos personales en Europa*, Tirant Lo Blanch, Valencia, 2006, pp. 34 y ss.; GONZÁLEZ MURUA, A. R., *La Agencia Vasca de Protección de Datos y el Estado de las Autonomías. Estudio de su naturaleza jurídica y sus funciones en una perspectiva de Derecho comparado*, Servicio editorial UPV/EHU, Leioa, 2010, pp. 22 y ss.

protección de datos⁴³ (que hunde sus raíces en Estados Unidos y se construye en Europa), así como el *habeas data*, al que dedicaremos tiempo en epígrafes posteriores. Por tanto, es necesario, al menos, apuntar las claves históricas de este proceso para entender su incorporación en Latinoamérica.

2. El nacimiento de la protección de datos en Estados Unidos. La *privacy*

Cuando hablamos del origen y evolución de la protección de datos en Estados Unidos, debemos remontarnos a finales del siglo XIX, donde la burguesía jugaba un papel predominante. Su origen, por tanto, es anglosajón.

Ya en la obra de 1873 “The Elements of Torts” realizada por el Juez Norteamericano Cooley, define la privacidad como “el derecho a ser dejado en paz”, siendo formulado en años⁴⁴ posteriores por dos juristas norteamericanos⁴⁵.

En efecto, como hemos venido resaltando son los juristas Warren⁴⁶ y Brandeis⁴⁷ en su famoso artículo llamado *The right to privacy* que publicaron en

⁴³ “...no existe uniformidad en la doctrina para referirse al derecho a la protección de datos personales. Algunos autores también se refieren a este como el *derecho de habeas data*, *derecho a la libertad informática*, *derecho a la autodeterminación informativa...*” visto en REMOLINA ANGARITA, N., *Insuficiencia de la regulación latinoamericana frente a la recolección...*op. cit., p. 190.

⁴⁴ Es importante acotar lo externado por PIÑAR MAÑAS, J. L., *El derecho fundamental a la protección de datos personales. Contenido esencial y retos actuales. En torno al nuevo Reglamento de protección de datos. Legislación de protección de datos.* Iustel. Madrid 2008, p. 18, indicando que “Sin perjuicio de construcciones doctrinales anteriores, entre las que se destacan sin duda alguna Cooley, T. que en 1888, habló ya de “the right to be alone” y el tantas veces citado (que no siempre leído) artículo de Warren y Brandeis “The Right to Privacy”, lo cierto es que hasta la segunda mitad de los años sesenta del pasado siglo no se sientan las bases del derecho a la protección de datos tal como lo entendemos hoy”.

⁴⁵ CARRASCOSA LÓPEZ, V., *Informática y Derecho 1*, 1ª ed. Universidad Nacional de Educación a Distancia, Mérida, Sevilla, 1992, p. 11.

⁴⁶ Warren se había casado con la hija del senador Bayard y había principiado a llevar una vida de lujos y suntuosidades. Hecho que atrajo la curiosidad y cotilleo de la llamada prensa

la *Harvard Law Review*, el 15 de diciembre de 1890⁴⁸ quienes desarrollaron conceptualmente el derecho a la privacidad. En él argumentaron el derecho a ser dejado solo de carácter subjetivo o *the right to be alone*. De este modo, este derecho es entendido en el sentido de excluir a los demás del conocimiento de noticias, especialmente frente a la prensa. Pero el artículo no es solamente la exposición de un problema que se iniciaba en Occidente sino que los autores habían comprendido el naciente conflicto entre el derecho a la intimidad y el derecho a la información⁴⁹, tratando de establecer los límites precisos a la coexistencia equilibrada entre ambas necesidades⁵⁰.

El artículo quería dejar en claro el poder que tenía la prensa, superior al poder existente, previo a las publicaciones periodísticas, a tal punto que advertían la capacidad que tenían las empresas por medio de sus publicaciones y fotografías instantáneas de invadir los espacios privados de las personas, eliminando, en consecuencia, la privacidad en los hogares.

Lo más relevante, en definitiva, es que a partir de esta visión de *privacy* la ciudadanía va a empezar a ser protegida en esferas y en situaciones antes no

amarilla, hasta el punto de convertirse en un escándalo, especialmente en la puritana sociedad bostoniana de fin de siglo.

⁴⁷ Brandeis luego llegó a ser juez de la Corte Suprema de los EE.UU.

⁴⁸ WARREN, S. & BRANDEIS, L., "The Right to Privacy..." op. cit., pp. 193-219. Una traducción castellana del mismo se puede encontrar en PENDÁS, B. y BALSEGA, P., *El derecho a la intimidad...* op. cit., p. 56.

⁴⁹ PÉREZ LUÑO A. E., *El derecho a la intimidad*, Visto en BETEGÓN, J., LAPORTA, F. J., RAMÓN DE PÁRAMO, J. y PRIETO SANCHÍS, L. (Coordinadores), *Constitución y derechos fundamentales*, Ministerio de la Presidencia, Secretaría General Técnica, Centro de Estudios Políticos y Constitucionales, Madrid, 2004, pp. 639-665.

⁵⁰ Entre los grandes estudiosos de la *privacy* cabe citar a BALDASARRE, A., *Privacy e Costituzione, L'esperienza statunitense*, Bulzoni Editore, Roma, 1974; MILLER, A. R., *The Assault on Privacy*, The University of Michigan Press, Ann Arbor, 1971. Desde la doctrina española también se ha analizado minuciosamente esta sentencia. Véase por todos, LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, op.cit., pp. 56-69; MARTÍNEZ, R., *Una aproximación crítica a la autodeterminación informativa*, Thomson-Civitas, Madrid, 2004, pp. 65-82, pp. 101-132 y pp. 149-151; CONDE ORTIZ, C., *La protección de datos personales*, editorial Dykinson, Madrid, 2005, pp. 21 y ss.; URABAYEN, M., *Vida Privada e Información, un conflicto permanente*, editorial Eunsa, Pamplona, 1997, pp. 347-349.

previstas, pero que introduce la IV Enmienda, *The right to privacy* no sólo va a representar el derecho de proteger la esfera de la intimidad sino también la posibilidad de disponer con libertad sobre la información que procesan o almacenan otros, sean particulares o la propia administración⁵¹. Con esta IV Enmienda el concepto de *privacy* se extiende más allá de los derechos de la personalidad y este antecedente marca un hito histórico, el nacimiento del derecho a la protección de datos de carácter personal.

3. Encaje distorsionado de la *privacy* norteamericana e incorporación de la autodeterminación informativa y el derecho a la protección de datos personales en Europa

El antecedente arriba mencionado se trasladó a Europa -y también a Latinoamérica como después veremos- con resultados diferentes. El motivo principal es que al trasladar la *privacy* al continente europeo, en el mismo no hay un derecho de amplitud igual a la *privacy* lo cual generó dos situaciones:

- a) una nueva categoría para la protección de datos,
- b) la asimilación de intimidad y privacidad. En este segundo caso se trata de un craso error pues la *privacy* no corresponde en Estados Unidos a un concepto unitario y los conceptos de vida privada e intimidad limitan *a priori* las posibilidades de maniobra⁵².

En definitiva, la paulatina inclusión de la *privacy* en las legislaciones europeas y latinoamericanas -con traducciones además descontextualizadas y con un sistema bien distinto al de *common law*- ha hecho perder el verdadero sentido de los principios, circunstancias y realidades que llevaron al nacimiento

⁵¹ En este sentido, FROSINI, V., *Derechos humanos y constitucionalismo ante el tercer milenio (Los derechos humanos en la era tecnológica)*. Monografías jurídicas. Marcial Pons, Ediciones Jurídicas Sociales, Madrid, 1996, p. 96.

⁵² Así lo señala Mercedes Serrano. Para esta autora es un error ampliar la *privacy* a la intimidad del mismo modo que la *privacy* en Estados Unidos agrupa unos contenidos de una complejidad y variedad que no se pueden asimilar a una única figura existente en el idioma latino. SERRANO PÉREZ, M. M., *El derecho fundamental a la protección de datos...*, op. cit., pp. 34-36.

y construcción de este derecho. De este modo se encasilla *privacy* con el concepto de intimidad y se pierde de vista el verdadero derecho que emerge de su nacimiento, cuya dinámica por su entorno permite la actualización y nueva definición, realidad bien diferente a lo que suele ocurrir en los ordenamientos jurídicos europeos y latinoamericanos.

Con todo, se ha de señalar que si bien esta visión de *privacy* no permeó en el contexto europeo -concibiéndose ésta como uno más de los derechos de la personalidad- es evidente que en la recepción anglosajona marcó un punto de partida la construcción del derecho a la protección de datos⁵³ de carácter personal y en la incorporación de la misma en Europa y Latinoamérica⁵⁴.

Por su parte, mientras que, en Estados Unidos, ante el progreso informático, de quien más se recelaba era del Gobierno y se otorgaba importancia al valor del mercado, en Europa la justificación de la creación de bancos de datos centralizados se encontraba en el cumplimiento de la función de bienestar social. Ello no impedía ser consciente de los peligros que el almacenamiento ilimitado de información, en manos de empresas e instituciones, podía acarrear

⁵³ Cfr "...-over time, it became clear that the european concept of data protection was being used in much the same way as the term information privacy. some, however, see this term as overly technical and concentrating on the data rather than the person as the object of protection" traducido al castellano "...Con el tiempo, se hizo evidente que el concepto europeo de protección de datos se usaba de forma muy parecida al término privacidad de la información. algunos, sin embargo, ven este término como demasiado técnico y se concentran en los datos en lugar de la persona como el objeto de protección", BENNETT, C. & D. RAAB, C., *the governance of privacy, policy instruments in global perspective*, 2ª ed. London, England, 2006, p. 11.

⁵⁴ Así lo manifiesta Eligio Rodríguez en su tesis doctoral: RODRÍGUEZ MARCANO, E. R., *El derecho a la autodeterminación informativa en Venezuela*, Universidad nacional de educación a distancia, Madrid, 2013, pp. 17-18 y p. 385.

En este lugar, queremos agradecer al autor que nos diera con anterioridad autorización para citar el manuscrito de su tesis doctoral puesta en línea poco tiempo después -al que haremos referencia en un buen número de ocasiones pues sus aportaciones en el contexto latinoamericano nos han sugerido muchas relevantes cuestiones-. Asimismo, también lo hacemos extensivo a nuestra directora, la doctora Ana Rosa González Murua, como vocal del Tribunal de la defensa de dicha tesis, por habernos puesto en contacto con dicho autor. Se puede observar el texto en la siguiente dirección en línea <http://e-spacio.uned.es/fez/eserv/tesisuned:Derecho-Errodriguez/Documento.pdf> (Última consulta en línea 23 de Octubre 2018).

para los derechos y libertades de las personas⁵⁵. En este sentido, se han de citar que los primeros pasos legislativos se dieron en Europa con la Ley del *Land* de Hesse de 7 de octubre de 1970 en Alemania.

Todo ello, pronto originó un arduo debate, sobre todo inicialmente en dicho país, que concluyó con la bien conocida sentencia sobre la Ley del Censo de 1982. Con ella comienzan, las primeras construcciones a nivel jurisprudencial de nuevos derechos en el contexto europeo. Pasamos a exponer, este hito relevante y de impacto en los cimientos y posterior desarrollo de la protección de datos.

4. La Sentencia sobre el Censo en Alemania. La autodeterminación informativa

Excede el objetivo de este trabajo, realizar un examen pormenorizado de la Sentencia del Censo ya mencionada, pero sí creemos que, al menos, debemos señalarla como un punto de partida e impulso en la elaboración de este derecho⁵⁶. Como posteriormente analizaremos tanto la normativa, la doctrina y la jurisprudencia europea -y más tarde el ámbito latinoamericano- la han hecho suya formando parte de su proceso de configuración, transformación y adecuación.

Todo parte de la presentación de un recurso de amparo constitucional contra la Ley del Censo invocando que se lesionaban varios artículos de la Ley Fundamental de Bonn de 1949, referidos al derecho al libre desenvolvimiento

⁵⁵ GONZÁLEZ MURUA, A. R., *La Agencia Vasca de Protección de Datos y el Estado de las Autonomías...* op. cit., p. 25.

⁵⁶ Son muchos los autores que incluso en lengua castellana han analizado dicha sentencia. Véase por todos PIÑAR MAÑAS, J. L., "Protección de datos: origen, situación actual y retos de futuro" en *El derecho a la autodeterminación informativa*, dirigido por LUCAS MURILLO DE LA CUEVA, P., y PIÑAR MAÑAS, J. L., Fundación Coloquio Jurídico Europeo, Madrid, 2009, p. 90 y HEREDERO HIGUERAS, M., "La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del Censo de Población de 1983", Documentación Administrativa, núm. 198, p. 41.

de la personalidad y la dignidad, la libertad de expresión y las garantías procesales⁵⁷. La ciudadanía se sentía especialmente “amenazada” porque se le obligaba a responder a cuestionarios enormes bajo la imposición, si no se hacía, de fuertes sanciones pecuniarias.

Ante ello, el Tribunal Constitucional Alemán no sólo admite el mencionado recurso sino que dicta sentencia cautelar para suspender provisionalmente la ley. Finalmente, el 15 de diciembre de 1983 se dicta sentencia, siendo aprobada el 4 de marzo por el *Bundestag* (Parlamento Alemán) y publicada el 31 del mismo mes, acogiendo gran parte de las peticiones de los recurrentes y anulando parcialmente dicha norma. Desde el punto de vista constitucional, su principal interés radica en que por primera vez se habla del derecho a la autodeterminación informativa⁵⁸ (*informationelle Selbstbestimmungsrecht*) como

⁵⁷ Una traducción en castellano de esta sentencia se encuentra en DARANAS, M., “Jurisprudencia constitucional y extranjera. Tribunal Constitucional Alemán. Ley del Censo”, *Boletín de Jurisprudencia Constitucional*, núm.33, 1984.

⁵⁸ Extracto de los fundamentos más interesantes de la Sentencia:

(...) “Ahora bien, la autodeterminación del individuo presupone -también en las condiciones de las técnicas modernas de tratamiento de la información- que se conceda al individuo la libertad de decisión sobre las acciones que se vayan a realizar o, en su caso, a omitir, incluyendo la posibilidad de obrar de hecho en forma consecuente con la decisión aportada. El que no pueda percibir con seguridad suficiente qué informaciones relativas a él son conocidas en determinados sectores de su entorno social y quién de alguna manera no sea capaz de aquilatar lo que puedan saber de él sus posibles comunicantes puede verse sustancialmente cohibido en su libertad de planificar o decidir por autodeterminación. No serían compatibles con el derecho a la autodeterminación informativa un orden social y un orden jurídico que hiciese posible al primero, en el que el ciudadano ya no pudiera saber quién, qué, cuándo y con qué motivo sabe algo sobre él (...) El derecho fundamental garantiza, en efecto, la facultad del individuo de decidir básicamente por sí solo sobre la difusión y la utilización de sus datos personales”

“2.a) Toda coerción al suministro de datos de referencia personal exige que el legislador haya determinado la finalidad de la utilización con toda precisión en cuanto al ámbito y que los datos sean adecuados y necesarios para esa finalidad. La recolección de datos no anonimizados y su acopio para fines indeterminados o indeterminables serían incompatibles con este requisito. Además, todas las oficinas que recopilen datos de referencia personal para el cumplimiento de su respectiva misión deberán limitarse al mínimo indispensable para la consecución del objetivo indicado.

La utilización de los datos se reduce al objetivo fijado por la ley. Sólo a la luz de los peligros de la elaboración automática de datos resulta imprescindible una protección -fija y de oficio- contra toda desviación de finalidad mediante prohibiciones de transmisión y de aprovechamiento. También son esenciales como precauciones aseguradoras del orden jurídico-procesal las obligaciones de aclaración, información y cancelación.” Este derecho a la autodeterminación informativa no está sin embargo garantizado sin límites. El individuo no tiene ningún derecho sobre “sus” datos en el sentido de una soberanía absoluta e irrestringible, sino que es más bien una personalidad que se desenvuelve dentro de la comunidad social y está

consecuencia del derecho a la personalidad previsto en el texto constitucional. Es decir, al no existir en la *Grundgesetz* reconocido expresamente un derecho autónomo a la protección de datos de carácter personal ni a la intimidad ni a la vida privada, se considera, sin embargo, que todos ellos derivan del ya reconocido derecho fundamental a la personalidad.

Además, como se señala desde la doctrina, se observa cierto paralelismo entre los procesos norteamericano y alemán en la construcción de los derechos. Ambos parten de un tronco común. En el caso de Estados Unidos, la *privacy* sirve para extender el ámbito del derecho existente al nuevo mundo de las tecnologías de la información. Por su parte, en Alemania el derecho a la protección de datos hunde sus raíces en el derecho a la personalidad.

De esa forma, el nuevo derecho, aunque se relaciona con todos los derechos existentes y se identifica con valores como la libertad, personalidad o la intimidad, su contenido es diferente al de estos y precisa una nueva categoría⁵⁹ y -dadas sus especificidades- unos mecanismos diferenciados de protección.

Se ha de señalar que estos precedentes marcan el devenir del derecho a la protección de datos personales el cual se va a ir perfilando de manera distinta en los diversos contextos y países. Como hemos señalado previamente, a partir de los años 70 se publican las primeras leyes de protección de datos (la primera Ley del *Land* de Hesse de 7 de octubre de 1970 en Alemania a la que sigue la *Data Lag Sueca* en 1973, la *Privacy Act* de Estados Unidos en 1974, el reconocimiento más o menos expreso en las constituciones portuguesa de

llamada a comunicarse. La información, incluso en la medida en que se refiere a la persona como tal, ofrece un retrato de la realidad social que no cabe asignar exclusivamente al interesado (...) El individuo tiene pues que aceptar en principio determinadas limitaciones de su derecho a la autodeterminación informativa a aras del interés preponderante de la comunidad". Citado por ALMAZARA ALMAIDA, C. (Coordinador), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. LEX NOVA, S. L., Valladolid, 2007, p. 34, nota 4.

⁵⁹ SERRANO PÉREZ, M. M., *El derecho fundamental a la protección de datos...*, op. cit., p. 69.

1976 y española de 1978⁶⁰). Es, a partir de entonces, cuando comienza “el proceso de positivación de los derechos integrantes de la tercera generación, en particular de la libertad informática o derecho a la autodeterminación informativa”⁶¹.

El panorama, por tanto, presenta una importante heterogeneidad que se ha ido reduciendo con el paso de los años pero que obedece fundamentalmente a una doble distinción:

a) Países que expresamente en su texto constitucional se reconoce el derecho a la protección de datos de carácter personal;

b) Países en los que sus constituciones no reconocen expresamente el derecho a la protección de datos de carácter personal. Sin embargo, aquí se produce una subdivisión:

1) Los que a pesar de no prever reconocimiento expreso del derecho contienen disposiciones diversas sobre la materia,

2) Los que ni prevén reconocimiento expreso ni contienen disposiciones sobre la materia⁶².

Eso sí confluyen en que, por vía judicial, sus tribunales constitucionales han encontrado su sede o bien, en el primer caso, en las disposiciones sobre la materia o, en el segundo supuesto, los ha reconocido como parte integrante de

⁶⁰ BOE, *Código de legislación Informática*, Madrid, 1988, pp. 23-24. En donde se recogen dichos preceptos., el texto de la constitución española se encuentra en BOE núm. 311.1 de 29 de diciembre de 1978.

⁶¹ PÉREZ LUÑO, A. E., *Libertad informática y leyes de protección de datos personales*, op. cit., p. 145.

⁶² Una clasificación de los mismos hasta 2006 puede verse en ARENAS RAMIRO, M., *El Derecho fundamental a la protección de datos personales en Europa*, op. cit., pp. 378-379. Posteriormente, en el escenario europeo cada vez más países han reconocido expresamente el derecho a la protección de datos, Incluso en Alemania, Italia y España se han recogido en diversos textos subestatales el reconocimiento de estos derechos y sus correspondientes autoridades de protección. Véase en ese sentido, LÓPEZ BOFILL, H., “Reforma estatutaria y protección de datos personales” en *Revista digital Datospersonales.org*, núm.19, enero 2006; GONZÁLEZ MURUA, A. R., *La Agencia Vasca de Protección de Datos y el Estado de las Autonomías...* op. cit., p. 129.

otro derecho como el de la intimidad, libre desarrollo de la personalidad o la dignidad.

Esta configuración como derecho a la autodeterminación informativa o a la protección de datos -que se enmarcan en otros derechos por vía judicial- ha presentado dificultades interpretativas de calado tanto en el contexto europeo como en el latinoamericano como veremos posteriormente.

Aunque de momento, cerremos el tratamiento relativo a la autodeterminación informativa como anteriormente se señaló, esta construcción originó importantes corrientes doctrinales, entre las que destacamos las del sector español, ya que no sólo influyen de manera definitiva y definitiva en el ordenamiento español sino también en diversos ordenamientos latinoamericanos planteados en los próximos acápite. Pero, antes de abordar estas cuestiones, resulta imprescindible a continuación, al menos, señalar y dedicar un espacio a los más importantes hitos legislativos y jurisprudenciales en la construcción del derecho a la protección de datos desde el ámbito internacional (ONU, OCDE, Consejo de Europa, OEA), de la Unión Europea y español, pues este acervo es definitorio igualmente en Latinoamérica y, por tanto, también en República Dominicana. Tras ese necesario análisis, retomaremos con las corrientes doctrinales españolas para, posteriormente, saltar al otro lado del Atlántico y así conocer su realidad en esta materia, cómo ha ido recepcionando y recepciona todo este bagaje y, en definitiva, va construyendo su propio discurso sobre la protección de datos -eso sí- dentro de un mundo globalizado.

5. La construcción del derecho a la protección de datos en el ámbito internacional

5.1. La protección de datos en la ONU

Finalizada la segunda guerra mundial⁶³ y completado el proceso de ratificación del documento fundacional⁶⁴ por los Estados miembros⁶⁵, aparece⁶⁶ en el escenario internacional la Organización de las Naciones Unidas (ONU)⁶⁷.

Una organización⁶⁸ compuesta por importantes órganos como la Asamblea General, el Consejo de Seguridad, el Consejo Económico y Social, la Corte Internacional de Justicia y valiosos documentos en cuyos preámbulos y considerandos se contemplan la dignidad intrínseca y el valor de la persona humana. Así, cabe destacar la Carta Internacional⁶⁹ de Derechos Humanos de 1945⁷⁰, la Declaración Universal de los Derechos Humanos de 1948⁷¹, el Pacto

⁶³ 2 de septiembre de septiembre de 1945.

⁶⁴ La Carta de la ONU.

⁶⁵ 53 Estados miembros ratificaron el documento, en la actualidad la conforman 193 Estados miembros.

⁶⁶ 24 de octubre de 1945.

⁶⁷ Organización de las Naciones Unidas (ONU), *informe general.*, Disponible en: <https://www.un.org/es/sections/about-un/overview/index.html>. (Última consulta en línea 18 de octubre 2019).

⁶⁸ PINTO, M. (Compiladora), *Las fuentes del Derecho Internacional en la era de la Globalización*, 1ª ed. Universitaria de Buenos Aires, Buenos Aires, 2009, pp. 16-17.

⁶⁹ Texto oficial de la carta puede consultarse en la página Web perteneciente a la Organización: Disponible en: <https://www.un.org/es/sections/un-charter/chapter-i/index.html> (Última consulta en línea 30 de noviembre 2017).

⁷⁰ Preámbulo: a reafirmar la fe en los derechos fundamentales del hombre, en la dignidad y el valor de la persona humana, en la igualdad de derechos de hombres y mujeres y de las naciones grandes y pequeñas.

⁷¹ Considerando que la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad intrínseca y de los derechos iguales e inalienables de todos los miembros de la familia;

Internacional de Derechos Económicos, Sociales y Culturales de 1966⁷², los Protocolos Facultativos del Pacto Internacional de Derechos Económicos, Sociales, Culturales⁷³, y el Pacto Internacional de Derechos Civiles y Políticos de 1966⁷⁴.

La Carta⁷⁵ aboga por el fomento de relaciones de amistad entre las naciones, fundamentado en principios de la igualdad de derechos, por la cooperación y por la solución de problemas internacionales de corte económico, etc., sirviendo de eje armonizador de sus propósitos comunes⁷⁶ y reconociendo la independencia de los pueblos del mundo con un tratamiento igual para sus miembros y nacionales.

En ese sentido, y avanzando un poco más, con la Declaración Universal de los Derechos Humanos de 1948, se protege a las personas de cualquier ataque a su honra y reputación, evitando todo tipo de injerencias arbitrarias a la vida privada incluyendo la familia, el domicilio o la correspondencia (art. 12)⁷⁷.

⁷² Considerando que, conforme a los principios enunciados en la Carta de las Naciones Unidas, la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad inherente a todos los miembros de la familia humana y de sus derechos iguales e inalienables...reconociendo que estos derechos se desprenden de la dignidad inherente a la persona humana,

⁷³ Considerando que, conforme a los principios enunciados en la Carta de las Naciones Unidas, la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad inherente a todos los miembros de la familia humana y de sus derechos iguales e inalienables.

⁷⁴ Considerando que, conforme a los principios enunciados en la Carta de las Naciones Unidas, la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad inherente a todos los miembros de la familia humana y de sus derechos iguales e inalienables...reconociendo que estos derechos se desprenden de la dignidad inherente a la persona humana.

⁷⁵ VASAK, K. (Editor general), *Las dimensiones internacionales de los derechos humanos*, 1ª ed. Serbal, S. A., Barcelona, 1984, pp. 51-52.

⁷⁶ Numeral 2, 3 y 4 artículo 1; literal b artículo 55, *Carta de las Naciones Unidas*. Disponible en: <https://www.un.org/es/sections/un-charter/chapter-i/index.html> (Última consulta en línea 30 de noviembre 2017).

⁷⁷ Artículo 12.

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

De su parte, el Pacto Internacional de los Derechos Civiles y Políticos de 1966 tutela la vida privada, la familia, el domicilio, la violación a la correspondencia, así como los ataques ilegales a la honra y la reputación (art. 17)⁷⁸, acercándose más a la *privacy* americana.

A raíz del desarrollo, uso y empleo de las tecnologías de información y comunicaciones (TIC) por parte de los gobiernos, empresas, personas, se concibe la incursión de violaciones a la privacidad de las personas y, con ello, la afección de los derechos protegidos y reconocidos por el artículo 12 de la Declaración Universal de los Derechos Humanos y por el artículo 17 del Pacto Internacional de los Derechos Civiles y Políticos. Esta situación pronto dio origen al desarrollo de propuestas⁷⁹, directrices, decisiones y resoluciones de la Asamblea General del Consejo, en búsqueda de la protección de datos en el entorno de la ONU, el derecho a la privacidad en la era digital, planteados a continuación.

⁷⁸ Artículo 17.

1.- Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

2.- Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

⁷⁹ Recordando las resoluciones de la Asamblea General 68/167, de 18 de diciembre de 2013, 69/166, de 18 de diciembre de 2014, y 71/199, de 19 de diciembre de 2016, sobre el derecho a la privacidad en la era digital, y 45/95, de 14 de diciembre de 1990, sobre los principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales, la decisión 25/117 del Consejo de Derechos Humanos, de 27 de marzo de 2014, y la resolución 28/16 del Consejo, de 26 de marzo de 2015, sobre el derecho a la privacidad en la era digital, y todas las demás resoluciones pertinentes del Consejo, en particular las resoluciones 33/2, de 29 de septiembre de 2016, sobre la seguridad de los periodistas, la resolución 12/16, de 2 de octubre de 2009, y todas las demás resoluciones sobre el derecho a la libertad de opinión y de expresión, y las resoluciones 20/8, de 5 de julio de 2012,

5.1.1. Directrices de Protección de Datos de la ONU de 14 de diciembre de 1990

Las presentes directrices⁸⁰ han sido adoptadas vía la resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990, dejando en mano de los Estados la aplicación de los procedimientos para poner en práctica las normas concernientes a los archivos de datos automatizados en base a las indicaciones contempladas en las directrices⁸¹.

Estas directrices no son jurídicamente vinculantes, tratándose de un documento orientativo, dejando a la voluntad de los gobiernos sujetarse a unos principios que constituyen las garantías mínimas a ser previstas por las legislaciones de los Estados. Se establecen 10 principios⁸² orientados a la regulación de los archivos de datos personales automatizados y manuales, ya sean estos públicos o privados, así como los archivos de datos personales en manos de las organizaciones internacionales, formando parte de los objetivos de las directrices.

En base a los principios mencionados, la información debe ser recogida, procesada y utilizada de forma exacta, segura y lícita, cumpliendo con los fines establecidos, siendo pertinente, adecuada, limitada en el tiempo y disponible al interesado, permitiendo su acceso, verificación, corrección y supresión en caso de ameritarlo; bajo los límites establecidos en la Carta Internacional de Derechos Humanos.

⁸⁰ *Directrices de Protección de Datos de la ONU de 14 de diciembre de 1990*. Disponible en: <http://www.informatica-juridica.com/anexos/directrices-de-proteccion-de-datos-de-la-onu-de-14-de-diciembre-de-1990/>. (Última verificación en línea 18 de octubre 2019).

⁸¹ REMOLINA ANGARITA, N., *Recolección internacional de datos personales: un reto del mundo...* op. cit., 190.

⁸² 1. Principio de legalidad y lealtad, 2. Principio de exactitud, 3. Principio de especificación de la finalidad, 4. Principio de acceso de la persona interesada, 5. Principio de no discriminación, 6. Facultad para hacer excepciones, 7. Principio de seguridad, 8. Supervisión y sanciones, 9. Flujo transfronterizo de datos, 10. Campo de aplicación.

El documento considera la designación de una autoridad independiente, cónsona con el sistema jurídico de los Estados, disponiendo la aplicación de penas y sanciones en los Estados. Asimismo, permite el flujo transfronterizo de datos ante la similitud de los niveles de protección de la intimidad en los Estados; en caso contrario, incentiva a los Estados a no establecer trabas innecesarias que pudieran impedir el trasiego de información entre los mismos, siempre en la medida en que lo exija la protección de la intimidad.

De acuerdo a los preceptos de la ONU la transferencia internacional entre dos Estados es viable cuando el destinatario ofrezca unas garantías comparables al emisor o exportador. El principio 9 bajo el título de “Flujos de datos a través de las fronteras” permite el libre flujo de datos cuando las legislaciones de los Estados sean capaz de ofrecer garantías comparables de protección de la vida privada, estableciendo un libre flujo como si se tratara a lo interno de los Estados⁸³.

Las directrices también son aplicables a las organizaciones internacionales, quienes deberán designar una autoridad de supervisión para vigilar las orientaciones de las directrices.

Tras esta resolución de la década de los 90 en los siguientes años se nos abre un escenario que muta vertiginosamente. El desarrollo, crecimiento, aplicación, uso del Internet y las tecnologías de información y comunicaciones en el sector empresarial, gobierno e individuo permiten el movimiento de grandes flujos de información, aumentando la conectividad desde y hacia distintos puntos de conexión. La situación evidencia posibles riesgos de violación de información y más a raíz de las revelaciones de monitoreo y vigilancia difundidas por Edward Snowden. Este evento convulso permitió a países como Brasil y Alemania presentar un proyecto en el 2013 contando con el apoyo de más de 50 Estados. Dicha iniciativa arrojó como resultado una

⁸³ REMOLINA ANGARITA, N., *Recolección internacional de datos personales: un reto del mundo...* op. cit., p. 191.

serie de Resoluciones de la Asamblea General y el Consejo de Derechos Humanos y, tendentes a combatir las prácticas ilícitas llevada a cabo en ese sector, convirtiéndose en un esfuerzo constante de mejora en cada una de sus resoluciones. Pasamos a exponerlas, someramente, en el siguiente epígrafe.

5.1.2. El derecho a la privacidad en la era digital: Resoluciones de la Asamblea General y del Consejo de Derechos Humanos. El papel del Relator especial

El 18 de diciembre del 2013 la Asamblea General aprueba en el Sexagésimo octavo periodo de sesiones, la resolución 68/167 titulada *el derecho a la privacidad en la era digital*. En ella se ratifica el derecho a la privacidad del artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos vistos previamente.

La Asamblea reconoce el rápido crecimiento del Internet y el impacto de las tecnologías y comunicaciones con el desarrollo en todas sus vertientes, afirmando la necesidad de protección del derecho de las personas y la privacidad en las comunicaciones digitales. En este sentido, exhorta a los Estados, a proteger y adoptar medidas tendentes a finalizar posibles violaciones a esos derechos, así como a establecer mecanismos de Supervisión independientes en los Estados. por lo que solicitan preparar un informe⁸⁴ entorno a la privacidad en las comunicaciones digitales.

Avanzando en el tiempo, nace la resolución del Consejo de Derechos Humanos 28/16, de 26 de marzo de 2015. En ella se plasman observaciones tales como las relativas a los metadatos mas su aportación más genuina es

⁸⁴ “...informe sobre la protección y la promoción del derecho a la privacidad en el contexto de la vigilancia y la interceptación de las comunicaciones digitales y la recopilación de datos personales en los planos nacional y extraterritorial, incluso a gran escala, que incluya opiniones y recomendaciones, para que lo examinen los Estados Miembros”. El derecho a la privacidad en la era digital. Resolución 68/167. Disponible en: <https://undocs.org/es/A/RES/68/167>. (Última verificación en línea 18 de octubre 2019).

que deriva en el nombramiento de un Relator especial, con miras a trabajar en la preparación de los informes, a seguir debatiendo los temas y a abrir un espacio de diálogo en torno a los derechos humanos en Internet. El Relator en su primer informe⁸⁵ se ha detenido en los datos abiertos y el *Big Data* y su impacto para la privacidad o en los datos biométricos entre otras cuestiones; pero, especialmente, en el concepto de privacidad, pues si bien se da en todas las sociedades no se trata de un concepto universalmente homogéneo en su definición presentando en su desarrollo marcos normativos muy diversos. Además su protección está ligada a las múltiples circunstancias socioeconómicas y tecnológicas de cada país del mundo por lo que considera una prioridad establecer un mínimo común denominador en la privacidad universal que ha de ser, en consecuencia, un derecho necesario para la dignidad y libertad personales. Otro elemento del informe es el caso Schrems al que define como “el inicio del fin judicial de la vigilancia masiva” y en este sentido apuesta por la importancia de la defensa de estos derechos ante una institución supranacional. Este período finaliza con la propuesta de un taller de expertos⁸⁶.

Por su parte en la resolución del Consejo de Derechos Humanos 37/4, del 23 de marzo de 2017 se centra en cuestiones tales como la elaboración de perfiles que puedan suponer discriminación o el consentimiento libre y explícito, Además, se habla de mecanismos de supervisión de índole judicial, administrativa o parlamentaria, que cuenten con los recursos necesarios y sean independientes, efectivos e imparciales y de un acceso a un recurso efectivo. Otra novedad reseñable es que el Consejo de Derechos Humanos no exhorta

⁸⁵ El primer informe del relator especial se presenta en la 31 sesión del Consejo de Derechos Humanos de la ONU de 8 de marzo 2016 (numero A/HRC/31/64)

⁸⁶ *El derecho a la privacidad en la era digital*. Disponible en: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_34_L7_rev1.pdf. (Última verificación en línea 18 de octubre 2019).

sólo a los Estados, sino que se dirige ya directamente también a las empresas para que asuman su responsabilidad de respeto a los Derechos Humanos.⁸⁷

La ONU mantiene una secuela de actualización, más allá de las resoluciones 2017 ya vistas, tales son los caso de la resolución 42/15 del 26 de septiembre de 2019 relativa al derecho a la privacidad en la era digital⁸⁸, la 38/7, de 5 de julio de 2018, relativas a la promoción, protección y disfrute de los derechos humanos en Internet, el informe 40/63 del Relator Especial sobre el derecho a la privacidad del 27 de febrero del 27 de febrero de 2019, la resolución de la Asamblea General 73/179 del 17 de diciembre de 2018 relativa al derecho a la privacidad en la era digital⁸⁹, En ese mismo sentido manifiestan interés y preocupación en torno a la protección, garantías procesales, vigilancia del derecho a la privacidad en la era digital y otros derechos humanos. Así como la necesidad de instaurar mecanismos de protección en los Estados, velar por el acceso a la información, la libertad de expresión, la vigilancia en las comunicaciones digitales, los metadatos, la información biométrica sensible, la educación de calidad, entre otros.

5.2. La protección de datos en la OCDE

El Convenio de París de 1960⁹⁰ se convirtió en la base fundacional de la Organización de Cooperación y Desarrollo Económico OCDE⁹¹ u OECD (por

⁸⁷ Un acercamiento a estas Resoluciones y al primer informe del Relator se pueden encontrar en PÉREZ MIRAS, J., *El derecho a la protección de datos y a la privacidad. Una perspectiva comparada entre la Unión Europea y Estados Unidos*, Universidad de Sevilla, España, 2018, p. 26 y ss.

⁸⁸ El derecho a la privacidad en la era digital. Disponible en <https://undocs.org/es/A/HRC/RES/42/15> (Última verificación en línea 24 de noviembre de 2019).

⁸⁹ El derecho a la privacidad en la era digital. Disponible en: <https://undocs.org/es/A/RES/73/179> (Última verificación en línea 24 de noviembre de 2019).

⁹⁰ *Convención de la OCDE*. Disponible en: <http://www.oecd.org/centrodemexico/laocde/convenciondelaocde.htm>. (Última consulta en línea 20 de junio 2017).

sus siglas en inglés) creada en 1961. La OCDE contempló en sus objetivos la promoción de una mayor expansión de la economía, mejorando el nivel de vida de sus países miembros⁹² y al mismo tiempo, aumentar el comercio mundial cimentado en la no discriminación y el multilateralismo⁹³. Los Estados como México⁹⁴, Chile, Estados Unidos, España y Portugal son miembros de la OCDE⁹⁵ y otros candidatos en proceso de adhesión como Colombia y Costa Rica.

⁹¹ (...) Los países occidentales han creado un organismo de cooperación económica: la Organización de Cooperación y de Desarrollo Económico (Convención de París de 14 de diciembre de 1960), u OCDE...los Estados comunistas también han creado un organismo de cooperación económica: el COMECON, o Comité de Asistencia Económica Mutua, cuya sede está en Moscú. Reúne todos los Estados comunistas europeos (desde 1965)..visto en LUCHAIRE, F., *La ayuda a los países subdesarrollados*, 1ra. ed. en lengua castellana, ed. Oikos-Tau, Barcelona, 1971, pp. 78-79.

⁹² (...) la OCDE se dedica a promover mejores políticas para una mejor vida...buscar soluciones a problemas comunes...trabajar con los gobiernos para comprender como están cambiando la economía y ayudarlos a aprender unos de otros...estableciendo normas que funcionan en todo el mundo...cuando todos siguen las mismas reglas, nuestras economías son más sólidas y más justas; *The United States and OECD Partners for Better Lives*. Disponible en: <http://www.oecd.org/washington/oecdandus/>. (Última consulta en línea 7 de diciembre 2017).

⁹³ Artículo 1 Convenio del 14 de diciembre de 1960 en París
La Organización de Cooperación y de Desarrollo Económico (llamada en adelante la Organización) tiene como objetivos el promover políticas destinadas a:
a) Realizar la más fuerte expansión posible de la economía y del empleo y a un aumento del nivel de vida en los países miembros, manteniendo la estabilidad financiera y a contribuir así al desarrollo de la economía mundial;
b) contribuir a una sana expansión económica en los países miembros y en los no miembros en vías de desarrollo económico;
c) contribuir a la expansión del comercio mundial sobre una base multilateral y no discriminatoria, conforme a las obligaciones internacionales.

⁹⁴ (...) México forma parte de la OCDE desde el 18 de mayo de 1994, *Directrices de la OCDE que regulan la protección de la Privacidad y el flujo transfronterizo de datos personales (23 de septiembre de 1980)*, traducción en lengua española realizada de los textos en inglés y/o Francés, versiones oficiales de esta publicación, titulados, 2004, Organisation for Economic Cooperation and Development (OECD), París y Ministerio de administraciones Públicas, Secretaría General Técnica, España Publicada con la autorización de la OCDE, NIPO: 326-04.034-7 Catálogo general de publicaciones oficiales. Disponible en: <http://publicaciones.administracion.es>. (Última consulta en línea 7 de diciembre 2017)

⁹⁵ Documentación Informática., *Flujo Internacional de Datos, recomendación de la OCDE de 23 de septiembre de 1980*, tratados Internacionales núm. 2, 1ª ed. Presidencia del Gobierno, serie amarilla, servicio central de publicaciones, Madrid, 1982, p. 32. Disponible en: <http://www.oecd.org/centrodemexico/paisesmiembros.htm>. (Última consulta en línea 7 de diciembre 2017).

En vista de las disparidades y falta de homogenización entre las leyes nacionales de los Estados se observó la necesidad de formar a finales de los 60 (1969) un subgrupo de trabajo experto en la materia, con la finalidad de realizar actividades o estudios de la informática en el sector público, con el objetivo de disminuir los obstáculos en las transferencias internacionales de datos⁹⁶. En el 1978 se procede con la formación de un Grupo de Expertos para estudiar y desarrollar directrices encaminadas a la solución de obstáculos en las transmisiones internacionales de datos personales y no personales, dando paso a la declaración de flujos de datos transfronterizos del 1985, donde se abordan cuestiones políticas y se reafirma el compromiso de trabajar en post del fortalecimiento de los flujos de datos personales más allá de las fronteras de los Estados, sustentado en soluciones armonizadas; y con la declaración ministerial sobre protección de la privacidad de las redes globales de 1998 “un mundo sin fronteras”, se comprometen los Estados a evitar restricciones innecesarias en los flujos transfronterizos de datos personales en el marco de las directrices de privacidad de la OCDE⁹⁷.

Hemos visto como el Consejo de la OCDE, fundamentado en sus deseos de contribuir con la expansión del comercio mundial y basado en la capacidad de hacer recomendaciones a los Estados miembros, presentó una serie de reconocimientos y recomendaciones⁹⁸ tendentes a evitar obstáculos a los flujos transfronterizos de datos. En ellos se reconoce la necesidad de llegar a una sana avenencia entre la privacidad y el libre flujo transfronterizo ya que -a pesar de ser valores fundamentales- también son opuestos entre sí. Los flujos

⁹⁶ Reuniones en París 1974 y en Viena 1977 así lo expresa ESTADELLA YUSTE, O., *La Protección de la Intimidación frente a la Transmisión...* op. cit., p. 25.

⁹⁷ Resumen Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, declaración sobre flujos de datos transfronterizos (1985). Disponible en: <http://www.oecd.org/sti/ieconomy/15590267.pdf>. (Última consulta en línea 4 de diciembre 2017):

⁹⁸ (...) Los países de la OCDE se aglutinan en base a: democracia pluralista, respeto de los derechos humanos y economías de mercado abiertas; *Resumen Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*, Declaración sobre flujos de datos transfronterizos (1985). Disponible en: <http://www.oecd.org/sti/ieconomy/15590267.pdf>. (Última consulta en línea 4 de diciembre 2017).

transfronterizos de datos personales contribuyen con el desarrollo socioeconómico de los Estados⁹⁹; para contribuir con tal desarrollo fue necesario incrementar los flujos de información transfronterizos eliminando las barreras innecesarias¹⁰⁰, evitando obstáculos injustificados amparados en leyes nacionales, de ahí la recomendación del Consejo para que los Estados miembros se conviertan en entes de colaboración en la implantación de las directrices del Consejo.

Las directrices que regulan la protección de la privacidad y los flujos transfronterizos de datos personales del 23 de septiembre de 1980¹⁰¹, se componen de 5 partes distribuida en 22 puntos, dirigido al sector público y al sector privado en tema de datos personales, unas directrices reproducida en varios idiomas, formando parte el alemán, el portugués, el holandés, y otros idiomas de países miembros¹⁰².

La primera parte de las directrices se orienta a las definiciones de los términos empleados y alcance de las directrices; la segunda, contiene los principios básicos de aplicación nacional¹⁰³; la tercera se refiere a los principios

⁹⁹ *Recomendación del Consejo relativa a las directrices que regulan la protección de la privacidad y el flujo transfronterizo de datos personales (23 de septiembre de 1980)*, traducción en lengua española realizada de los textos en inglés y/o Francés, versiones oficiales de esta publicación, titulados, 2004, Organisation for Economic Co-operation and Development (OECD), París y Ministerio de Administraciones Públicas, Secretaría General Técnica, España Publicada con la autorización de la OCDE, NIPO: 326-04.034-7 Catálogo general de publicaciones oficiales. Disponible en: <http://publicaciones.administracion.es>. (Última consulta en línea 7 de diciembre 2017).

¹⁰⁰ “El motivo que guió a la OCDE a tratar este tema fue la preocupación que algunos países (en particular los Estados Unidos) sentían por las iniciativas nacionales sobre protección de datos, temiendo que esta normativa legal creara barreras proteccionistas en el comercio internacional” así lo expresa: ESTADELLA YUSTE, O., *La Protección de la Intimidad frente a la Transmisión Internacional...* op. cit., p. 30.

¹⁰¹ Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales “directrices de privacidad”.

¹⁰² Documentación Informática., *Flujo Internacional de Datos, recomendación de la OCDE de 23 de septiembre de 1980*, tratados internacionales núm. 2, 1ª ed. Presidencia del Gobierno, serie amarilla, servicio central de publicaciones, Madrid, 1982, p. 9.

¹⁰³ Las directrices contemplan 8 principios básicos de aplicación nacional.

1) Principio de limitación de recogida, 2) Principio de calidad de los datos, 3) Principio de especificación de los fines, 4) Principio de limitación de uso, 5) Principio de salvaguarda de la

básicos de aplicación internacional distribuidos en libre flujo y restricciones legítimas; la cuarta, se orienta a la implantación nacional de políticas, leyes, medios y sanciones que garanticen cualquier tipo de discriminación desleal; la quinta contiene la cooperación internacional, por medio a ella, se exhorta a los miembros difundir las directrices, establecer procedimientos para facilitar el intercambio de información relacionada con las directrices, y el establecer ayuda mutua en temas de investigación y procedimientos relacionados con las directrices; al mismo tiempo, trabajar en la elaboración de principios nacionales e internacionales que regulen las leyes orientadas o aplicable a los flujos transfronterizos de datos personales.

La OCDE integra los grupos de trabajo con dimensiones internacionales que trabajan examinando y perfeccionando los marcos de privacidad alrededor del mundo como la Unión Europea, el Consejo de Europa, y el Foro de Cooperación Económica Asia-Pacífico (APEC). A raíz de los trabajos ejecutados y en proceso de elaboración en materia de privacidad, la OCDE estimó que era el momento adecuado para realizar los preparativos y aprestos de revisión de los lineamientos de sus directrices presentadas el 23 de septiembre de 1980¹⁰⁴. Los preparativos se inician en el 2010 en el contexto del 30 aniversario de las directrices de 1980, tomando en cuenta los trabajos previos y presentados por la OCDE en el marco de sus objetivos¹⁰⁵

Seguridad, 6) Principio de transparencia, 7) Principio de participación individual, 8) Principio de responsabilidad.

¹⁰⁴ Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013), *The OECD privacy Framework*, OECD 2013, p. 21. Disponible en: http://www.oecd.org/sti/economy/oecd_privacy_framework.pdf. (Última consulta en línea 3 de diciembre 2017).

¹⁰⁵ Previo a los preparativos del 2010 y posterior a la recomendación del 23 de Septiembre de 1980, fueron presentadas: a) la declaración relativa a los flujos de datos transfronterizos del 11 de abril de 1985; b) la recomendación relativa a las directrices de política criptográfica adoptada por el Consejo de la OCDE el 2 de marzo de 1997; y c) declaración relativa a la protección de la intimidad en las redes Globales del 7-9 de octubre de 1998, Ottawa, Canadá; *Declaración relativa a la protección de la intimidad en las redes globales*, conferencia “un mundo sin fronteras: comprender el potencial del comercio electrónico global”, DSTI/ICCP/REC(98)10/FINAL. Disponible en: http://www.oas.org/es/sla/ddi/docs/Declaracion_OCDE_Proteccion_Intimidad_redes.pdf. (Última consulta en línea 3 de diciembre 2017).

fundamentados en los avances tecnológicos de alcance e impacto global presentes en el siglo XXI.

El proceso de creación de las nuevas recomendaciones¹⁰⁶ se ampara en el Grupo de Trabajo para la Información, Seguridad y Privacidad (WPISP, por sus siglas en inglés) con el apoyo voluntario de un Grupo de Expertos en materia de privacidad¹⁰⁷. Los trabajos finalizaron con “*la Recomendación del Consejo relativa a Pautas para la protección de la privacidad y flujos transfronterizos de datos personales (2013)*”, fruto de la revisión de la Recomendación del Consejo sobre las directrices que rigen la protección de la privacidad y las cuestiones transfronterizas de los flujos de datos personales del 23 de septiembre de 1980, proyectando alcanzar altos niveles de privacidad, acompañados de una globalización de la privacidad, condicionando el libre flujo de información de datos a iguales o similares niveles de protección de la directriz 2013¹⁰⁸.

De las mismas cabe destacar que la OCDE reconoce ya a las Autoridades de control públicas como elementos de referencia en las políticas de privacidad y responsables en su aplicación normativa e incluso integra principios reconocidos en el actual Reglamento de la Unión Europea como es el principio de responsabilidad proactiva o “accountability”, desarrollado por las Autoridades de control de los Estados. Asimismo, el documento aborda los

¹⁰⁶ Recomendación del Consejo relativa a Pautas para la protección de la privacidad y flujos transfronterizos de datos personales (2013). Disponible en: <https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>. (Última consulta en línea 3 de diciembre 2017).

¹⁰⁷ El Grupo de Voluntario Expertos lo formaban, gobiernos, autoridades implementadoras de la privacidad, académicos, empresas, sociedad civil, comunidades técnicas de Internet, representante del Consejo de Europa, la Unión Europea, expertos activos en APEC, dirigido por Jennifer Stoddart, comisionado de privacidad de Canadá “(..) experts from governments, privacy enforcement authorities, academics, business, civil society, and the Internet technical community. Participants also included representatives of the Council of Europe and the European Union, as well as experts active in APEC. This multi-stakeholder group was chaired by Jennifer Stoddart, Privacy Commissioner of Canada...”. Disponible en: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, p. 21. (Última consulta en línea 3 de diciembre 2017).

¹⁰⁸ REMOLINA ANGARITA, N., *Recolección internacional de datos personales: un reto del mundo...* op. cit., p. 191, nota 155.

temas de cooperación internacional e interoperabilidad contenido en la parte sexta de las directrices¹⁰⁹.

5.3. La protección de datos en el Consejo de Europa

El Consejo de Europa¹¹⁰ es una Organización de carácter internacional, orientada al espacio europeo¹¹¹, enfocada en la defensa, protección y fomento de los derechos humanos conectado con la privacidad y la protección de datos, abrazando la paz y la democracia en el entorno europeo.

La Convención para la salvaguarda de los Derechos Humanos y de las Libertades Fundamentales presentada para firma¹¹² en 1950¹¹³ conocido habitualmente como Convenio Europeo de Derechos Humanos¹¹⁴ se convirtió en una de las primeras Convenciones del Consejo de Europa¹¹⁵. Con respecto a nuestro objeto de estudio es su artículo 8 el que reconoce el derecho de la vida privada y familiar.

¹⁰⁹ PÉREZ MIRAS, J., *El derecho a la protección de datos y a la privacidad. Una perspectiva comparada entre la Unión Europea y Estados Unidos*, Universidad de Sevilla, España, 2018, p. 26.

¹¹⁰ Creado a partir del Tratado de Londres del 5 de mayo de 1949.

¹¹¹ Durante sus inicios 10 Estado participaron en su formación, entre ellos Bélgica, Dinamarca, Francia, Holanda, Irlanda, Italia, Luxemburgo, Noruega, Reino Unido y Suecia; actualmente 47 Estados miembros forman parte de la organización.

¹¹² España firmó el 24 de noviembre de 1977.

¹¹³ DÍEZ PICAZO, L. M., *Sistema de Derechos Fundamentales*, 3ª ed. Thomson Civitas, España, 2008, p. 36

¹¹⁴ Entró en vigor el 3 de septiembre de 1953. Es abundantísima la bibliografía sobre el Convenio Europeo de Derechos Humanos y excede el objeto de nuestro trabajo detenernos en ello. Nos parece realmente exhaustivo y muy clarificador la exposición que del mismo realiza ARENAS RAMIRO, M., *El Derecho fundamental a la protección de datos personales en Europa...*op, cit., pp.44-54, quién conecta el discurso con el Tribunal Europeo de Derechos Humanos y lo ejemplifica en relación a la protección de datos, Además en estas páginas se encuentra muy interesante bibliografía en varias lenguas

¹¹⁵ RECALDE DIEZ, J. R., (Presentación), *Informática Judicial y Protección de Datos Personales*, 1ª ed. Servicio Central de Publicaciones del Gobierno Vasco, Vitoria- Gasteiz, 1994, p. 17.

“Artículo 8.- Derecho al respeto a la vida privada y familiar.

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás”. (Art. 8)

El Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales suscrito en Roma, incorpora su Protocolo Adicional y los Protocolos Anexos n.º 4, n.º 6, n.º 7, n.º 11, n.º 12, n.º 13, n.º 14. Ahora bien, va a ser concretamente el *Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal* el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos.

En ese sentido, el Consejo de Europa, motivado por la intensificación de flujo entre las fronteras de los Estados consideró deseable ampliar la protección de los derechos y las libertades fundamentales, en especial el derecho a la vida privada, teniendo en cuenta que la finalidad del Convenio es contribuir con una unión más íntima entre sus Estados miembros, fundamentada en la preeminencia del derecho, los derechos humanos y las libertades

fundamentales¹¹⁶. Y es así, como se convirtió la protección de datos personales en un objetivo político y jurídico de la organización europea¹¹⁷.

Pero antes del Convenio 108, también la labor desarrollada por el Consejo de Europa puede ser considerada como pionera en el área de la protección de la intimidad individual respecto a la informática¹¹⁸. A raíz de un estudio realizado por el Comité de Ministros, originado por una solicitud de la Asamblea Nacional en 1968¹¹⁹, se determinó una no alineación de las legislaciones nacionales con los cambios tecnológicos o desarrollos informáticos para ese entonces. Dichas razones abocaron entre 1973 y 1974 a la conformación de un Comité Intergubernamental, dando como resultado un conjunto de principios básicos de protección de datos personales a ser incorporados por los Estados miembros en sus legislaciones nacionales. Estas son las Resoluciones (73)22 y (74)29¹²⁰ y son considerados los primeros textos internacionales que recogen “pautas de conductas” en materia de protección de datos para los Estados¹²¹.

¹¹⁶ Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

¹¹⁷ PAVÓN PÉREZ, J. A., “La Protección de Datos Personales y el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales”, *Anuario de la Facultad de Derecho*, 2001, p. 238. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=831270>. (Última consulta en línea 24 de octubre 2017).

¹¹⁸ Así lo señala ESTADELLA YUSTE, O., *La Protección de la Intimidad frente a la Transmisión Internacional...* op. cit., p. 64.

¹¹⁹ “Los esfuerzos en tutelar la privacidad e intensidad en el seno de la Unión Europea parten de las primeras iniciativas llevadas a cabo en el 1967, para ello, fue constituida una comisión con la finalidad de analizar la vulneración de los derechos de las personas por el impacto de la tecnología, dando como resultado la resolución 509 del consejo de Europa “los derechos humanos y los nuevos logros científicos y técnicos” así lo expresa ALMAZARA ALMAIDA, C. (Coordinador), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. editora LEX NOVA, S. L., Valladolid, 2007, p. 33. También se observa en ULL PONT, E., *Derecho público de la informática, protección de datos...* op. cit. p. 53.

¹²⁰ Resolución R (73) 22 relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado y la Recomendación R (74) 29, relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público

¹²¹ ESTADELLA YUSTE, O., *La Protección de la Intimidad frente a la Transmisión Internacional...* op. cit., pp. 64-65.

Tales decisiones mueven al Comité de Ministro a constituir en 1976 un Comité de Expertos para desarrollar el artículo 8¹²² del Convenio Europeo de Derechos Humanos.

La vida privada y familiar forma parte del Convenio (ex art. 8 CDH) pero desde su nacimiento se ha generado un incremento en la recolección de los datos un gradual uso de la informática y un aumento de las injerencias privadas cada vez más conectadas con los datos personales. Tras 4 años de negociación¹²³, y, soportado en las resoluciones (73)22 y (74)29¹²⁴ presentadas previamente, se procede con el desarrollo y ampliación de los principios ya vistos, desencadenando en la elaboración y publicación de un texto decisivo y unánime en el ámbito legal de la protección de datos personales reconocido como el Convenio 108 presentado en el 1981¹²⁵ y mostrado a continuación.

5.3.1. Convenio 108 sobre Protección de Datos Personales¹²⁶

El Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal es un

¹²² ARZOZ SANTISTEBAN, X., *Derecho al respeto a la vida privada y familiar*, visto en LASAGABASTER HERRARTE, I. (Director), *Convenio Europeo de Derechos Humanos*, 3ª ed. Aranzadi S.A., Pamplona, 2015, p. 339.

¹²³ El Convenio108, se presentó para la firma el 28 de enero de 1981, entró en vigor el 1 de octubre de 1985 tres meses después de su ratificación.

¹²⁴ ULL PONT, E., *Derecho público de la informática, protección de datos de carácter personal*, 1ª ed. UNED, Madrid, 2003, p. 53.

¹²⁵ ALMAZARA ALMAIDA, C. (Coordinador), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. LEX NOVA, S.L, Valladolid, 2007, p. 34.

¹²⁶ Son muchísimos los autores y las autoras que estudian este Convenio en el desarrollo de sus obras por ser una pieza clave en la protección de datos. Véase por todos, además de las obras a las que haremos referencia ARENAS RAMIRO, M., *El Derecho fundamental a la protección de datos personales en Europa...*op, cit., pp. 153-157

*Convenio firmado el 28 de enero de 1981 y entró en vigor el 1 de octubre de 1985 tres meses después de la quinta firma del mismo por los Estados*¹²⁷.

El Convenio tiene como objetivo y fin el respeto a la vida privada relacionado con el tratamiento automatizado de los datos de carácter personal, sin menoscabo de la nacionalidad o residencia de la persona¹²⁸ y persigue la conciliación de dos valores fundamentales, el de la vida y la libre circulación de la información entre los pueblos.

El Convenio está compuesto por VII capítulos distribuidos en 27 artículos. El primer capítulo contiene las disposiciones generales, seguido por el capítulo II con sus 8 principios básicos de la protección de datos¹²⁹ aplicable a los datos recogidos por autoridades públicas, o por personas o instituciones privadas, independientemente de los sectores (ya sean estos, médico, seguridad social, seguros, banca, empleo, marketing directo, estadísticas, telecomunicaciones, policía), siendo el capítulo más relevante y destacable dentro del Convenio¹³⁰, pues estos principios se acompañan de las garantías complementarias (derecho a conocer la existencia de ficheros, acceso, rectificación, cancelación y derecho a recurrir la resolución).

Los flujos transfronterizos de datos pertenecen al capítulo III y aplica a las transmisiones de datos realizadas vía las fronteras nacionales, utilizando cualquier medio y sin la posibilidad de prohibir o colocar obstáculos cuando se trate de proteger la vida privada, o cuando provenga de flujos transfronterizos

¹²⁷ “España firmó este Convenio el 28 de enero de 1982 y lo ratificó el 27 de enero de 1984 (BOE 274 de 15 de noviembre de 1985)”. SERRANO PÉREZ, M. M., *El derecho fundamental a la protección de datos...op. cit.*, p. 90.

¹²⁸ Artículo 1, Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

¹²⁹ Principios Básicos para la Protección de Datos, Convenio 108 °. Finalidad, Lealtad, Exactitud, Publicidad, Acceso, Seguridad

¹³⁰ ALMAZARA ALMAIDA, C., *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. LEX NOVA, S. L., Valladolid, 2007, p. 36.

con destino al territorio de otra parte, con la posibilidad de presentar excepciones. Con respecto a las transferencias internacionales a terceros países, posteriormente veremos como la Directiva 95/46/CE contempla un nivel de protección adecuado, mientras el protocolo sugiere niveles de protección equivalentes¹³¹, reflejando la preocupación del Consejo con los temas de transferencias internacionales, debido al constante aumento de los flujos de datos.

Para el cumplimiento del presente Convenio, las autoridades de control deben mantener una estrecha colaboración y asistencia, brindando protección a las personas que se encuentren en el extranjero o en el territorio de otra parte, como lo expresa el capítulo IV titulado ayuda mutua (arts. 13-17) siendo la primera vez que se exige la creación de Autoridades de control en el derecho interno en el ámbito del Consejo de Europa¹³²

El Convenio contempla en el capítulo V la creación de un Comité Consultivo con el objetivo de establecer mejoras, enmiendas y opiniones al procedimiento. Asimismo, el Convenio permite la adhesión de Estados no-miembros del Consejo de Europa para ello debe contar con una invitación del Comité de Ministro¹³³.

El capítulo VI corresponde al proceso de enmiendas al Convenio, finalizando el Convenio con el capítulo VII referido a las cláusulas finales incluida la fecha

¹³¹ RECALDE DIEZ, J. R., (Presentación), *Informática Judicial y Protección de Datos Personales*, 1ª ed. Servicio Central de Publicaciones del Gobierno Vasco, Vitoria- Gasteiz, 1994, p. 26.

¹³² GONZÁLEZ MURUA, A. R., "Protección de datos de carácter personal" en *La Carta de los Derechos Fundamentales de la Unión Europea Ugartemendia* Eceizabarrena, J.I. Thomson Reuters Aranzadi, Cizur Menor, 2012, p. 42.

¹³³ Así lo establece en el artículo 23.1 del Convenio "Después de la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa podrá invitar a cualquier Estado no miembro del Consejo de Europa a que se adhiera al presente Convenio mediante un acuerdo adoptado por la mayoría prevista en el artículo 20, d), del Estatuto del Consejo de Europa y por unanimidad de los representantes de los Estados contratantes que tengan el derecho a formar parte del comité.

de entrada del Convenio, su adhesión, cláusula territorial, reservas, denuncias y notificaciones.

En conclusión, se trata del primer instrumento jurídicamente vinculante internacionalmente en la materia de protección de datos y como señala la doctrina dicho Convenio representa “..sin duda alguna, la máxima expresión del deseo de que las citadas divergencias normativas quedasen superadas”¹³⁴

Es así como los Estados miembros firmantes del Convenio reconocen en sus considerandos la necesidad de ampliar en sus legislaciones nacionales el tema de la protección de los derechos y de las libertades fundamentales materializado en la vida privada ante el incremento de los flujos transfronterizos o circulación de los datos de carácter personal objeto de los tratamientos automatizados, asignándole importancia capital a las transferencias internacionales de datos; desarrollando en el 2001 su *Protocolo Adicional al Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a las transferencias de datos* presentado a continuación.

5.3.2. *Protocolo Adicional del Convenio 108*¹³⁵ de 2001

Más allá del Convenio 108, se presenta en la palestra el Protocolo Adicional del Convenio 108 del 8 de noviembre de 2001, relativo a las transferencias de datos. Ya en el preámbulo del Protocolo se puede observar la relevancia

¹³⁴ TÉLLEZ AGUILERA, A., *La protección de datos en la Unión Europea: Divergencias normativas AS y anhelos unificadores*, EDISOFER S. L, Madrid, 2002, p. 329.

¹³⁵ *Protocolo adicional del Convenio n.º 108 para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencia de datos*. Disponible en: <http://www.informatica-juridica.com/anexos/protocolo-adicional-del-convenio-no-108-para-la-proteccion-de-las-personas-con-respecto-al-tratamiento-automatizado-de-datos-de/> (Última verificación en línea 23 de noviembre 2019), también en PAVÓN PÉREZ, J. A., “La Protección de Datos Personales y el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos Personales”, *Anuario de la Facultad de Derecho*, 2001, p. 38. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=831270>. (Última consulta en línea 24 de octubre 2017).

asignada a las autoridades de control y su independencia con la aplicación de sus funciones, garantizando una protección efectiva de las personas respecto al tratamiento de datos personales.

El incremento de las transferencias de datos personales entre las fronteras, es un hecho reconocido en el Protocolo, razones valederas para proteger los derechos humanos y las libertades fundamentales, dando hincapié a la privacidad y a la inadecuada protección de los datos personales que se mueven entre las fronteras de los Estados.

El Protocolo, compuesto por un preámbulo previamente analizado, está dispuesto por 3 artículos. El primer artículo se refiere a la autoridad de control responsable de asegurar el cumplimiento de los principios contenidos en los capítulos II y III del Convenio, conectado con las transferencias internacionales. Además, el Protocolo contempla la necesidad de implementar una o varias autoridades de control que implementarán las medidas necesarias para asegurar los principios planteados, con poder de investigación, intervención, iniciar procedimientos legales y gestionar cualquier proceso interno con las autoridades judiciales nacionales, en aras de dar cumplimiento a los principios mencionados, siempre manteniendo una total independencia en el ejercicio de sus funciones y una estrecha colaboración entre las mismas.

Al mismo tiempo, el Protocolo contempla las provisiones necesarias para las transferencias hacia aquellos Estados que no formen partes del Convenio. En estos casos, los Estados y las organizaciones deberán asegurar un nivel adecuado de protección y las partes acuerdan la ejecución de las transferencias en base a su derecho interno o cuando existan las garantías suficientes para su ejecución.

La aprobación del Protocolo se conecta con el Convenio manteniendo una estrecha vinculación con el mismo, ya que no se puede aprobar el Protocolo sin

desvincularlo del Convenio¹³⁶, situación muy diferente a la observada en el Protocolo de modificación del Convenio 108 de 1981 expuesto a continuación.

5.3.3. Protocolo de modificación del Convenio 108 de 1981 (2018)

El interés y esfuerzo constante del Convenio en actualizar y modernizar su normativa lo acercan cada vez más a los cambios y transformaciones generados en su entorno de escala y relevancia global, cumpliendo con el rol preeminente de la protección del individuo con relación al procesamiento de los datos personales, y más aún, en la protección de los derechos humanos y libertades fundamentales. Todo ello se materializa en el Protocolo de modificación del Convenio del 10 de octubre del 2018, el cual se sustenta en una serie de iniciativas sobre protección de datos y privacidad tendentes a la materialización del Protocolo. Para ello, se tomaron en cuenta diferentes iniciativas como: la Resolución n.º 3 adoptada en la 30 Conferencia de Ministros de Justicia realizada en Estambul, Turquía del 24-26 de noviembre de 2010; la Resolución 1843 del 2011 relativa a la protección de la privacidad y datos personales en Internet; la Resolución 1986 del 2014 sobre las mejoras de protección al usuario y su seguridad en el ciberespacio y el Dictamen 296 (2017) por el que se modifica el Proyecto del Protocolo y su Memorando Explicativo del 24 de noviembre de 2017¹³⁷.

El Protocolo de modificación del Convenio contiene 40 artículos, a diferencia de su predecesor con 27 artículos, motivos suficientes para entender que estamos delante de una propuesta normativa intencionada en dejar una estela

¹³⁶ Artículo 3, párrafo 2

El presente protocolo...un signatario del presente protocolo no podrá ratificar o aprobar el mismo salvo que haya ratificado o aprobado con carácter previo o simultáneo al Convenio o se haya adherido al mismo...

¹³⁷ Preámbulo Protocolo del Convenio para la protección de las personas con respecto al procesamiento automático de datos personales, *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Council of Europe Treaty Series – N.º 223, Strasbourg, 2018. Disponible en:

<https://www.coe.int/t/web/conventions/search-on-treaties/-/conventions/rms/09000016808ac918>. (Última consulta en línea 14 de octubre 2018).

de cambios respecto a su predecesora consumada hace ya 27 años adaptándose a los nuevos tiempos. En ese sentido apela al fortalecimiento de la cooperación internacional entre los signatarios del Convenio, tejiendo ingentes esfuerzos en fortalecer la cooperación, esclareciendo los flujos transfronterizos de datos, aumentando la cooperación de las autoridades de protección de datos. Se refuerza el tema de las autoridades de supervisión en el Convenio mediante la inserción de un capítulo de autoridades de supervisión, importando desde el Protocolo Adicional al Convenio n.º 108 del 2001 (ETS N.º 181) la figura de las autoridades de supervisión que goza de poderes de investigación, intervención, independencia, imparcialidad, competencia y la capacidad de imponer sanciones administrativas etc.

En el Protocolo de Modificación se sustituye el término Comité Consultivo por el de Comité de la Convención, con capacidad de presentar recomendaciones en los Estados miembros a diferencia del Comité Consultivo. Así, a nuestro juicio, se eleva su nivel de empoderamiento y toma de decisiones para los Estados y se vislumbra un acercamiento con las normas europeas en materia de protección de las personas físicas en relación al tratamiento de datos personales y la libre circulación establecidos en el Reglamento (UE) 2016/679 de la Unión Europea y del Consejo de 27 de abril de 2016.

En materia de protección de las personas físicas respecto al tratamientos de datos personales y su circulación en el espacio europeo, específicamente en los Estados que conforman el Consejo de Europa, la tutela efectiva de tales derechos se encuentra resguardada no solo por las legislaciones que se ciernen sobre ellos sino, por sentencias capaces de cambiar las reglas del juego e influir en las normas ya establecidas y en fase de elaboración.

Para finalizar el epígrafe del Consejo de Europa con respecto a la contribución del derecho a la protección de los datos personales, en este último apartado nos centraremos en al acervo jurisprudencial más relevante para nuestro estudio del Tribunal Europeo de Derechos Humanos (en adelante

TEDH). Si bien es cierto que, en el Capítulo IV con respecto a los órganos de control específicos hagamos también referencia expresa al Comité Consultivo y al Comité de Expertos en Protección de Datos, no obstante en páginas anteriores ya hemos apuntado sobre su creación y misión. Pasamos, por tanto, a analizar la jurisprudencia del TEDH, pues nos alineamos con la doctrina en el sentido de que estos órganos a los que acabamos de mencionar también cubren una importante labor y su efectividad es incluso mayor en otros ámbitos (realizar propuestas, coordinar u homogenizar sobre derechos y libertades fundamentales) pero al no revestir una conformación judicial es el Tribunal Europeo de Derechos Humanos quien constituye la herramienta más efectiva de garantía de los derechos y libertades fundamentales a nivel europeo¹³⁸. Como veremos a continuación, también ha sido una herramienta valiosísima en la construcción del derecho a la protección de datos/vida privada ex artículo 8 CEDH.

5.3.4. Jurisprudencias del TEDH

El Tribunal Europeo de Derechos Humanos nace en el CEDH¹³⁹. Con sede en Estrasburgo, como hemos adelantado, es acreedor de copiosas e importantes jurisprudencias sustentada en el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH).

Muestra de ello puede observarse en la publicación del Consejo de Europa del TEDH relativa a la difusión de sentencias del 2018, vinculadas a los casos

¹³⁸ REBOLLO DELGADO, L., y SERRANO PÉREZ, M. M., Manual de protección de datos, 2ª ed. Dykinson, Madrid, 2017, p. 230.

¹³⁹ Se firmó el 4 de noviembre 1950 y entró en vigor en septiembre de 1953. Una vez más excede las pretensiones del trabajo estudiar este Tribunal ya que en este epígrafe nos centraremos muy concretamente en relación a su jurisprudencia ex art.8 CEDH, sin embargo, creemos necesario poner de relieve a la doctrina que ha tratado su configuración, legitimación, procedimiento encuadrado como una garantía genérica determinante en materia de protección de datos. Así, cabe resaltar a ARENAS RAMIRO, M., *El Derecho fundamental a la protección de datos personales en Europa...*op, cit., pp. 174-184.

*de derechos de la Corte Europea de Derechos Humanos relativa a la protección de datos personales*¹⁴⁰ agrupadas en: a) acceso a datos personales; b) equilibrio entre la protección de datos con la libertad de expresión y el derecho a la información; c) consentimiento del interesado; d) correspondencia; e) base de datos de ADN; f) datos GPS; g) datos de salud; h) identidad; i) información sobre actividades personales; j) interceptación de Comunicaciones; k) fotos; l) vida privada en el trabajo; m) tratamiento de datos personales por parte de la policía; n) métodos de vigilancia; o) videovigilancia.

Debido a la gran variedad y cantidad, resulta una labor ímproba revisar todas ellas. Por tal motivo, en este lugar, se sintetizará la jurisprudencia más relevante en torno al artículo 8, sin perder de vista nuestro objetivo de su contribución en materia conceptual a la protección de datos.

Iniciaremos con una de las principales sentencias conectadas con el artículo 8 del CEDH en tema de intimidad y vida privada, nos referimos al caso Leander contra Suecia (n.º 9248/81 de 26 de marzo 1987), considerada pionera en relación al derecho de acceso a los datos.

El caso tiene su origen en una demanda interpuesta por el sr Leander contra Suecia a raíz de que éste no fue contratado por no haber llenado una encuesta previa de control del Ministerio de defensa cuyas instalaciones estaban cerca del lugar de trabajo, el sr Leander se ve invalidado a ser seleccionado para la posición. El gobierno Sueco alega que por los niveles de seguridad (acceso restringido e informaciones secretas en manos del Ministerio de Defensa) y el hecho de estar la base próxima al lugar de trabajo, así como información secreta depositada en el Consejo de Policía cuyo acceso no pudo ser posible por el sr. Leander. El Tribunal reconoce la amplitud de apreciación de los Estados y su prevalencia, comparado con los intereses del demandante, más al

¹⁴⁰ Council of Europe., Case law of the European Court of Human Rights Concerning the protection of personal dataStrasbourg, june 2018. Disponible en: <https://rm.coe.int/t-pd-2018-15-case-law-on-data-protection-may2018-en/16808b2d36>. ((Última consulta en línea 19 de octubre 2018).

analizar entiende que la injerencia del Sr. Lander no es desproporcional al fin perseguido, razones por la que desestima posibles violaciones al artículo 8¹⁴¹.

El próximo caso mantiene el mismo lineamiento de la anterior, nos referimos al caso *Gaskin contra Reino Unido* (n.º 10454/83, de 7 de julio de 1989) otra sentencia pionera en materia de acceso a ficheros, establecida entre el Sr. Gaskin ante el ayuntamiento de Liverpool por denegación de acceso a documentos personales en poder de esa institución, conectado con posibles abusos realizados al Sr. Gaskin durante su vida de orfandad en ese lugar.

En esta sentencia los casos se orientan a posibles violaciones del artículo 8 ya comentado y el artículo 10 sobre acceso a la información, en tal sentido el TEDH después de analizar el caso entiende que “derecho del señor Gaskin a recibir informaciones, protegido por el artículo 10, no sufrió ninguna injerencia” estando ajustada a derecho, no obstante considera violaciones realizadas al artículo 8 planteado¹⁴².

Continuaremos con el pronunciamiento del caso *Malone contra el Reino Unido* identificado con el no. 8691/79¹⁴³. El Sr. Malone fue acusado en el 1977 de manejo deshonesto de bienes robados, siendo absuelto a posteriori. Durante el Juicio se evidenció la interceptación de la conversación telefónica bajo una orden del Ministerio del interior, también se piensa que fueron intervenidos el correo y las líneas telefónicas, registrando incluso los dígitos marcados vía la colocación de un aparato, por su parte, el gobierno no admite, ni niega las acusaciones, a pesar de considerar como medida preventiva y regla general la interceptación en individuos sospechosos amparados en una orden.

¹⁴¹ PÉREZ MIRAS, J., *El derecho a la protección de datos y a la privacidad...op, cit.*, p. 271.

¹⁴² PÉREZ MIRAS, J., *El derecho a la protección de datos y a la privacidad., op, cit.*, p. 274.

¹⁴³ Caso no. 8691/79, *MALONE v. THE UNITED KINGDOM*, Council of Europe., Case law of the European Court of Human Rights Concerning the protection of personal dataStrasbourg, june 2018. Disponible en: <https://rm.coe.int/t-pd-2018-15-case-law-on-data-protection-may2018-en/16808b2d36>. ((Última consulta en línea 19 de octubre 2018).

El Sr. Malone inicia un proceso Civil vía el Tribunal Superior contra el Comisionado de la Policía Metropolitana, aspirando a que se declare ilegal cualquier tipo de conversación sin su consentimiento, situación por la que el Tribunal concluye que las interferencias detectadas no estaban de acuerdo con la ley, ya que en un sistema democrático deben proveerse las garantías adecuadas contra el abuso, por tal sentido no se encuentran en consonancia a lo estipulado en el párrafo 2 del Artículo 8.

El próximo pronunciamiento que nos ocupa se refiere a TEDH, Khelili contra Suiza, sustentado en el n.º 16188/07, la policía de Ginebra registra como prostituta a una ciudadana Francesa debido a documentación insinuante portada por esta y detectada durante un registro policial, prohibiéndole residencia en Suiza como medida temporal. El TEDH considera muy ligera la apreciación policial en detrimento de la Francesa, con la medida tomada por la policía le fueron vulnerado los derechos contemplados en el artículo 8 del CEDH. Como justa compensación el TEDH dispone de una indemnización de 15, 000 euros a favor de la Sra. Khelili ¹⁴⁴

5.4. La protección de datos en la OEA

5.4.1. Convención Americana

El continente Americano, como hemos puntualizado y venimos comentando, guarda y mantiene una estrecha vinculación con la región o el escenario europeo, a pesar de las diferencias existentes desde el punto de vista de sus realidades, ya sean estas históricas, políticas o sociales que abordan las regiones o los continentes; una semejanza reflejada en los orígenes de sus tratados internacionales, caso de la Convención Americana de Derechos Humanos, el Convenio Europeo y -como no- del Sistema Interamericano de Derechos Humanos y el Sistema Europeo. En definitiva, nos encontramos con

¹⁴⁴ PÉREZ MIRAS, J., *El derecho a la protección de datos y a la privacidad...op, cit.*, P. 277.

una situación que nos conecta con la semejanza de ambos, convirtiéndose el Sistema Europeo en un modelo representativo a seguir en la construcción del Sistema Interamericano¹⁴⁵.

En esta sección, observamos la protección de datos personales desde la óptica de la Organización de los Estados Americanos (OEA) como organismo regional¹⁴⁶ y vista desde sus principales normas jurídicas que rodean tan importantes temas, como es el caso de la Convención Americana de Derechos Humanos¹⁴⁷. Dicha Convención se establece, declara y ratifica por medio al pacto de San José (Costa Rica) del 7 al 22 de noviembre de 1969, y en ella se reconocen aquellos derechos ligados con la persona, aceptado desde la óptica internacional y consagrados como principios en las constituciones de los Estados, la Carta de la Organización de los Estados Americanos, la Declaración Americana de los Derechos y Deberes del Hombre y en la Declaración Universal de los Derechos Humanos¹⁴⁸.

Por medio a la Carta de la Organización de los Estados Americanos suscrita en Bogotá (Colombia) el 30 de abril de 1948 en la novena Conferencia Internacional Americana y por reformas vía sus protocolos¹⁴⁹, los Estados

¹⁴⁵ FAÚNDEZ LEDESMA, H., *El Sistema Interamericano de Protección de los Derechos Humanos, Aspectos institucionales y procesales*, 3ª ed. Instituto Interamericano de Derechos Humanos, San José, 2004, p. 999.

¹⁴⁶ Cfr. Preámbulo *Carta de la Organización de los Estados Americanos*. (1948). Disponible en: http://www.oas.org/dil/esp/afrodescendientes_manual_formacion_lideres_anexos.pdf. (Última consulta en línea 24 de enero 2019).

¹⁴⁷ La República Dominicana es signataria de la OEA formando parte de la Convención Americana de Derechos Humanos a partir del 19 de abril 1979.

¹⁴⁸ Cfr. Preámbulo *Convención Americana sobre Derechos Humanos (Pacto de San José)*, 1969.

Disponible en:

https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm. (Última consulta en línea 24 de enero 2019).

¹⁴⁹ Reformada por el Protocolo de Reformas a la Carta de la Organización de los Estados Americanos "Protocolo de Buenos Aires", suscrito el 27 de febrero de 1967, en la tercera Conferencia Interamericana Extraordinaria, por el Protocolo de Reformas a la Carta de la Organización de los Estados Americanos "Protocolo de Cartagena de Indias", aprobado el 5 de diciembre de 1985, en el décimo cuarto período extraordinario de sesiones de la Asamblea General, por el Protocolo de Reformas a la Carta de la Organización de los Estados

Americanos reafirman el principio de solidaridad y cooperación económica entre los Estados y la declaración de los derechos fundamentales de la persona humana sin la posibilidad de ser susceptibles de merma, entre otros. En ese sentido, la Carta Democrática Interamericana presentada en el 28 Período Extraordinario de sesiones del 11 de septiembre de 2001 en Lima (Perú) considera como elementos esenciales para la democracia representativa *el respeto a los derechos humanos y las libertades fundamentales*¹⁵⁰.

Es importante acotar que la Convención Americana data del 1969, una condición que no permite identificar el mencionado derecho de protección de datos pero sí coincidir con aquellos derechos conectados con la persona humana, como son el derecho al honor, a la intimidad y a la privacidad, un escenario a cambiar en la medida que la Convención se aproxime a las normativas actuales en materia de protección de datos

La Convención garantiza el derecho de toda persona a su integridad moral, el derecho a la protección de la honra y el reconocimiento de la dignidad, así como el de evitar posibles injerencias arbitrarias o abusivas que puedan darse en su entorno privado y familiar, incluyendo su domicilio o violaciones a la correspondencia o posibles ataques generados a la honra y reputación de las personas¹⁵¹.

Americanos "Protocolo de Washington", aprobado el 14 de diciembre de 1992, en el decimosexto período extraordinario de sesiones de la Asamblea General, y por el Protocolo de Reformas a la Carta de la Organización de los Estados Americanos "Protocolo de Managua", adoptado el 10 de junio de 1993, en el decimonoveno período extraordinario de sesiones de la Asamblea General. *Carta de la Organización de los Estados Americanos*. Disponible en: http://www.oas.org/dil/esp/afrodescendientes_manual_formacion_lideres_anexos.pdf. (Última consulta en línea 24 de enero 2019).

¹⁵⁰ Artículo 3, *Carta Democrática Interamericana, 2001* Disponible en: http://www.oas.org/dil/esp/afrodescendientes_manual_formacion_lideres_anexos.pdf. (Última consulta en línea 24 de enero 2019).

¹⁵¹ Cfr. Artículo 5 disposición 1, así como el artículo 11 "Protección de la Honra y la Dignidad". Disponible en: https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm. (Última consulta en línea 24 de enero 2019).

La Convención Americana emplea indistintamente los términos *right to privacy* y protección de la honra y de la dignidad para referirse al mismo derecho, una disposición manifiesta en el artículo 11 de la versión inglesa y castellana de la Convención Americana, ejemplo de ello se presenta a continuación.

“Article 11. Right to Privacy 1. Everyone has the right to have his honor respected and his dignity recognized. 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation. 3. Everyone has the right to the protection of the law against such interference or attacks”¹⁵².

“Artículo 11. Protección de la Honra y de la Dignidad 1. Toda persona tiene derecho al re de injerencias arbitrarias o abusivas en su vida privada, en la de su fan domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques”¹⁵³.

Como ya expusimos, el concepto de *privacy* es originario de la *privacy* americana de Warren y Brandeis y, a nuestro entender, el concepto crea confusión al momento de ser expuesto, adoptado, asumido e integrado en el escenario jurídico de los Estados miembros vía sus constituciones, leyes, jurisprudencias y doctrinas.

¹⁵² American Convention on Human Rights “Pact of San José, Costa Rica”, Disponible en : https://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.pdf (última verificación en línea 25 de noviembre de 2019)

¹⁵³ Convención Americana sobre Derechos Humanos (Pacto de San José) https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.pdf. (última verificación en línea 25 de noviembre de 2019).

La privacidad, tal como se estipula en el Convenio, aplica para todos los integrantes de la familia situados en su domicilio. El artículo 17 de la Convención Americana hace referencia a la protección de la familia. El artículo 11¹⁵⁴ contempla la protección de las informaciones contenidas en la correspondencia del individuo. De acuerdo a lo planteado, tenemos una privacidad enfocada en el individuo y su domicilio, a la cual llamaremos privacidad física por estar conectada con su espacio físico como su domicilio, un espacio despejado y libre de toda injerencia arbitraria de acceso, penetración, entrada, o visita sin consentimiento. Pero, el Convenio no solo se refiere o denota a la parte física, como hemos llamado, sino, que involucra las informaciones contenidas en la correspondencia del individuo, la cual no está ligada a posible aprehensión física o más bien, de aquellas informaciones que provienen directamente del individuo. Nos referimos a una relación vinculada con el individuo y su domicilio como la imagen y los actos realizados por éste en su espacio declarado como tal, muy distante de las informaciones provenientes del individuo. Y que, a pesar de estar contenida en medios físicos como la correspondencia, reflejan informaciones provenientes de sus actividades y comportamientos conectados con la honra y la dignidad del individuo, siendo afectados al ser expuesta a terceros sin su consentimiento. Las informaciones existentes en medios físicos como las correspondencias, guardan informaciones vinculadas con el comportamiento, hábitos, creencias etc. que puedan afectar la honra y la dignidad del individuo por medio al conocimiento de terceros no autorizados o sin consentimiento.

Por medio a esas injerencias se persigue la protección, custodia, defensa, amparo, cuidado, tutela del honor, de la honra, de la reputación y -como no- de la dignidad de las personas, es así como a favor de la protección de la honra y

¹⁵⁴ Artículo 11. Protección de la Honra y de la Dignidad

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

la dignidad de las personas se propugna velar por la protección de su privacidad.

El artículo 11 ha sido materializado, reconocido y ampliado vía la evacuación de diferentes sentencias de la Corte Interamericana de Derechos Humanos¹⁵⁵, una situación que, debido a su magnitud, trataremos de puntualizar fruto a los puntos externados en las mismas.

5.4.2. Jurisprudencias Corte Interamericana

Partiremos de la sentencia de la Corte Interamericana de Derechos Humanos del 8 de Julio de 2004¹⁵⁶ referida al caso de los hermanos Emilio Moisés y Rafael Samuel Gómez Paquiyauri, conocida comúnmente como el *caso de los hermanos Gómez Paquiyauri vs Perú*. Es la primera sentencia que hace referencia al artículo 11 relativa a la protección de la honra y de la dignidad. El caso mencionado fue presentado por medio de una demanda de la Comisión Interamericana de Derechos Humanos contra el Estado del Perú vía la Corte Interamericana de Justicia por franca violación a diversos artículos de la Convención Americana. Todo ello parte de la solicitud interpuesta por los familiares de los hermanos Gómez Paquiyauri debido a que ambos hermanos

¹⁵⁵ Cfr. "...Fue recién en 2006, con el *Caso de las Masacres de Ituango*, que la Corte Interamericana comenzó a desarrollar de una manera más sistematizada el contenido y alcance del artículo 11 de la Convención Americana en su doble dimensión. Como veremos en este comentario, desde entonces se han añadido 8 nuevas decisiones en casos contenciosos que han involucrado la vulneración de dicho artículo: uno durante 2007 (*Escué Zapata*), dos en 2009 (*Tristán Donoso y Escher y otros*), tres para 2010 (*Manuel Cepeda Vargas, Fernández Ortega y otros y Rosendo Cantú y otra*), uno en (*Fontevicchia y D'Amico Atala Riffo e Hijos*). Salvo las decisiones en *Gómez Paquiyauri* y *Manuel Cepeda Vargas*, un rasgo en común que comparten estos casos es que, al referirse al artículo 11 de la Convención Americana, sus sentencias colocan un particular acento en la segunda de las dimensiones que hemos descrito, es decir, el derecho a la vida privada...". STEINER, C. & URIBE, P. (Coordinadores), *Convención Americana sobre Derechos Humanos*, comentada, 1ª ed. D. R. Konrad Adenauer Stiftung, República Federal de Alemania, 2014, p. 274. Disponible en: <http://www.corteidh.or.cr/tablas/30237.pdf>. (Última consulta en línea 5 de febrero 2019).

¹⁵⁶ Cfr. Corte IDH. *Caso de los Hermanos Gómez Paquiyauri Vs. Perú*, Fondo, Reparaciones y Costas, Sentencia de 8 de julio de 2004. pp. 1 y ss. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_110_esp.pdf. (Última consulta en línea 5 de febrero 2019).

fueron detenidos por la policía nacional supuestamente ejecutados por estos y presentados como terroristas a la población, ocasionando daños materiales e inmateriales a sus familiares y prole. Ante esta situación la Comisión solicita a la Corte Interamericana de Justicia la imposición de medidas pecuniarias y no pecuniarias tendentes a resarcir los daños causados por el Estado peruano.

Los representantes de las víctimas y sus familiares alegaron la violación del artículo 11.2 por parte del Estado peruano a los hermanos Gómez Paquiyauri al considerarlos terroristas, delincuentes y criminales ante la opinión pública, afectando a su honra y reputación, cuestión que no sólo afecta a los hermanos fallecidos sino, también, a la familia de los hermanos incluida su prole¹⁵⁷. A pesar de constituirse en la primera sentencia que aborda el artículo 11 de la Convención Americana como ya hemos comentado, no recibe el reconocimiento de la Comisión y a su vez, no cuenta con el reconocimiento del Estado al momento de plantear la supuesta violación del artículo 11.

Las alegaciones al artículo 11.2 externadas por los representantes de las víctimas y sus familiares se sustenta en el daño ocasionado a la honra y reputación de los jóvenes, al ser estos considerados terroristas y delincuentes ante la opinión pública, siendo sometidos a la incursión de su hogar y, con ello, a una invasión a la vida privada de la familia.

El Tribunal de la Corte Interamericana de Justicia acepta el alegato presentado por los representantes y familiares relacionados con la violación del artículo 11 de la Convención Americana. En este sentido, genera una sentencia de reparación de daños para los acreedores de las reparaciones, estableciendo indemnizaciones a sus sucesores ante el deceso de las víctimas. Esta reparación de daño no sólo la aplica e incursiona a la reparación material sino a reparaciones materiales ocasionada por daños inmateriales, resarciendo aquellos daños no físicos que afectan la honra y la dignidad de las personas y que, a su vez, pueden ser resarcidos económicamente mediante las sanciones dispuestas por la sentencia del Tribunal de Justicia a sugerencia de la

¹⁵⁷ Nora Emely Gómez Peralta, hija de Rafael Samuel Gómez Paquiyauri.

Convención y de las propuestas de los representantes y familiares de sus víctimas.

Es importante subrayar la dificultad de evaluar el daño inmaterial y lograr una adecuada retribución material. Así, se tejen diferentes formas de resarcir el daño, una de ellas se encuentra conectada con el aspecto pecuniario y la otra, orientada en resarcir de forma no pecuniaria el daño inmaterial vía un reconocimiento público del agravio generado u otras alternativas contempladas en la sentencia como son la entrega de beca de estudio para la prole y la asignación del nombre de los fallecidos a una escuela en Perú. Y, todo ello se genera con la intención de recuperar el honor, la dignidad de las personas fallecidas y sus familiares.

La siguiente sentencia mantiene vivo el artículo 11 de la Convención Americana. Nos referimos al caso *Escué Zapata vs. Colombia*. Parte de una demanda interpuesta por la Comisión Interamericana de Derechos Humanos a raíz de la denuncia de la señora Etelvina Zapata Escué sumándose a ésta el colectivo de abogados “José Alvear Restrepo”. La Comisión decidió someter la demanda ante ausencia de avances de cumplimiento por parte de la República de Colombia en el caso de la ejecución del indígena Germán Escué Zapata, Cabildo Gobernador de Jambaló (Colombia). Estamos, pues, ante un hecho representativo de la violencia sobrevenida a los pueblos indígenas y sus líderes y ante una responsabilidad reconocida y asumida por el Estado colombiano a pesar de cuestionar determinados preceptos contenidos en los articulados de la Convención como el artículo 11.2 referido a la honra y la dignidad¹⁵⁸.

La Comisión no presentó alegaciones respecto al artículo 11.2 de la Convención Americana, a pesar de ser interpuesta por los representantes del afectado, fundamentado en la violación de la honra y la dignidad de las

¹⁵⁸ Cfr. Corte IDH. *Caso Escué Zapata Vs. Colombia*, Fondo, Reparaciones y Costas, Sentencia de 4 de julio de 2007, pp. 1 y ss. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_165_esp.pdf. (Última consulta en línea 5 de febrero 2019).

personas producto a la invasión arbitraria de la morada. Sin embargo, la Corte reconoce estar delante de un concepto más amplio, el cual no sólo se aboca en la protección de la dignidad y el honor sino que alberga la protección de otros derechos como son el derecho al domicilio, la vida privada, la familia y la correspondencia, contenido en el referido artículo y logrando su protección. Con la referida sentencia, el Tribunal acepta, reconoce y otorga responsabilidades materiales e inmateriales a la República de Colombia.

En los casos presentados, los alegatos a la violación del artículo 11 llegan de la mano de los representantes de las víctimas, sus familiares o ambas, siendo aceptadas y reconocidas por la Corte Interamericana de Derechos Humanos como si se tratara de un artículo no entendido o aceptado por la Comisión, ya que las alegaciones se someten luego de iniciado el proceso y pasado el inicio de la demanda por parte de la Comisión.

La Convención Americana contempla la protección de otros derechos no reconocidos en el artículo 11 de la protección de la honra y la dignidad. Nos referimos al derecho a la propiedad privada contemplado en el artículo 21 y el derecho a la protección de la familia contenido en el artículo 17, formando parte del derecho a la protección de la vida privada, la familia y la correspondencia.

En ese sentido, a pesar de que las comunicaciones telefónicas no forman parte del artículo 11¹⁵⁹ del Convenio, reciben el amparo de la Corte

¹⁵⁹ Cfr. “El artículo 11 protege las conversaciones realizadas a través de las líneas telefónicas instaladas en las residencias particulares o en las oficinas, sea su contenido relacionado con asuntos privados del interlocutor, sea con el negocio o actividad profesional que desarrolla. De ese modo, el artículo 11 se aplica a las conversaciones telefónicas independientemente de su contenido e incluso, puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones. En definitiva, la protección a la vida privada se concreta en el derecho a que sujetos distintos de los interlocutores no conozcan ilícitamente el contenido de las conversaciones telefónicas o de otros aspectos, como los ya mencionados, propios del proceso de comunicación”. STEINER, C. y URIBE, P. (Coordinadores), *Convención Americana sobre Derechos Humanos*, comentada, 1ª ed. D. R. Konrad Adenauer Stiftung, República Federal de Alemania, p. 279. Disponible en: <http://www.corteidh.or.cr/tablas/30237.pdf>. (Última consulta en línea 5 de febrero 2019).

Interamericana de los Derechos Humanos, vía la evacuación de sus sentencias, haciendo posible la inviolabilidad de la comunicación telefónica, su interceptación, grabación, considerada una injerencia a la vida privada (Escher y otros) ¹⁶⁰.

La Convención Americana de Derechos Humanos contempla la protección de la correspondencia, evitando cualquier tipo de injerencia que pueda colocar en peligro la información contenida en la misma. Se trata de una protección que va más allá de la tutela de la correspondencia, albergando la protección de otros derechos, como el derecho a la comunicación telefónica amparado en las Sentencias del Tribunal Interamericano de los Derechos Humanos. Muestra de ello es el caso *Tristán Donoso vs. Panamá*¹⁶¹.

Este caso nos permite pensar ya en un primer acercamiento que nos permite pensar en una aproximación con las normas legislativas conectadas con el desarrollo tecnológico. Con la decisión, se observa y persigue un acercamiento a las normativas internacionales, en especial, las conectadas con el desarrollo tecnológico.

Con este acercamiento se vislumbra la protección de otros derechos conectados con la tecnología, como es el caso de la protección de la inviolabilidad de la imagen, videovigilancia, datos almacenados en las nubes, medios electrónicos desprovistos del consentimiento de su titular, consumando la protección del honor y la dignidad de las personas.

¹⁶⁰ Cfr. “.....Ese mismo año, la Corte Interamericana...emitió la sentencia Escher y otros. En el caso, la CIDH alegó la violación del derecho a la vida privada de las presuntas víctimas al atribuir al Estado la responsabilidad por la interceptación, grabación y divulgación de una serie de conversaciones telefónicas”. STEINER, C. y URIBE, P. (Coordinadores), *Convención Americana sobre Derechos Humanos*, comentada, 1ª ed. D. R. Konrad Adenauer Stiftung, República Federal de Alemania, p. 279. Disponible en: <http://www.corteidh.or.cr/tablas/30237.pdf>. (Última consulta en línea 5 de febrero 2019).

¹⁶¹ Cfr. Corte IDH. *Caso Tristán Donoso vs. Panamá*. Excepción preliminar, fondo, reparaciones y costas. Sentencia de 27 de enero de 2009 Serie C N.º 193. pp. 1 y ss. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_193_esp.pdf. (Última consulta en línea 5 de febrero 2019).

La convención estará sometida a un proceso de actualización constante en la medida que se generen nuevas jurisprudencias conectadas con las sentencias emitidas por la Corte Interamericana de Derechos Humanos. Conforme a lo anterior se protegen nuevos derechos que empapan las normas europeas e internacionales.

Tras estas reflexiones, pasamos de nuevo al escenario europeo, y en concreto, al conformado por la Unión Europea y por la anterior Comunidad Económica Europea (CEE)¹⁶². Como veremos en el próximo epígrafe, gran parte del proceso de consolidación y conformación del mencionado derecho se ha venido y se viene realizando en las distintas instituciones pertinentes de dicho ámbito.

6. La construcción del derecho a la protección de datos en el ámbito de la Unión Europea

6.1. La protección de datos en la Carta de Derechos Fundamentales de la Unión Europea. Artículo 8

La protección de datos encuentra su espacio o acomodo en la Carta de los Derechos Fundamentales de la Unión Europea¹⁶³, materializando la protección

¹⁶² CISNAL DE UGARTE, E. S., FERNÁNDEZ LIESA, C. R. y MOREIRA GONZÁLEZ, C., *Descripción, análisis y comentarios al Tratado de la Unión Europea*, 1ª ed. McGRAW-HILL / INTERAMERICANA DE ESPAÑA, S. A., Madrid, 1993, pp. 23 y ss.

¹⁶³ En 1999 el Consejo Europeo se encarga de recoger en una Carta los derechos fundamentales vigentes en la UE t la Carta queda formalmente proclamada por las tres Instituciones de la Unión en Niza en diciembre de 2000, pero no será jurídicamente vinculante hasta el Tratado de Lisboa y su entrada en vigor el 1 de diciembre de 2009, estando ya equiparada a los postulados de los Tratados. La Carta de Derechos Fundamentales además de su preámbulo contiene 54 artículos en 7 capítulos: El capítulo I sobre la dignidad, el capítulo II sobre la libertad (en el que está ubicado el derecho a la protección de los datos de carácter personal), el capítulo III sobre la igualdad, el capítulo IV referido a la solidaridad, el capítulo V sobre ciudadanía, el capítulo VI relativo a la Justicia, y por último, unas disposiciones generales en el capítulo VII. PÉREZ MIRAS, J., *El derecho a la protección de datos y a la privacidad...op, cit.*, p. 284, nota 565.

de datos a lo interno de la Unión Europea¹⁶⁴ vía lo dispuesto en el Tratado de la Unión Europea (TUE)¹⁶⁵.

El TUE no le otorga capacidad a la Carta para ampliar en modo alguno las competencias de los Tratados a lo interno de la Unión Europea, es decir, el TUE permite adoptar lo dispuesto de la Carta en la Unión, no así otorgar más poder o autoridad que lo habilitado o permitido en los Tratados. Los Tratados se convierten en los límites de la Carta a lo interno de la Unión. Con la decisión, la Carta nunca puede superar, dar o asignar más prerrogativas en materia de protección de datos¹⁶⁶ que las asignadas en los Tratados, aunque sea contemplado en la Carta.

Por su parte, el artículo 8¹⁶⁷ de la Carta acuña el término *protección de datos de carácter personal*, no siendo considerado un derecho absoluto¹⁶⁸, tratado de

¹⁶⁴ Artículo 1 Tercer párrafo TUE “.....La Unión sustituirá y sucederá a la Comunidad Europea.”

¹⁶⁵ Artículo 6

1. La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados.

Las disposiciones de la Carta no ampliarán en modo alguno las competencias de la Unión tal como se definen en los Tratados. Versión consolidada del Tratado de la Unión Europea. Disponible en: <https://www.boe.es/doue/2010/083/Z00013-00046.pdf>. (última verificación en línea 8 de marzo 2018).

¹⁶⁶ Caso que nos compete.

¹⁶⁷ Artículo 8 Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

Carta de los Derechos Fundamentales de la Unión Europea, 2010. Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003>. (Última verificación en línea 21 de abril 2018).

¹⁶⁸ PIÑAR MAÑAS, J. L. y RECIO GAYO, M., *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, 1ª ed. Wolters Kluwer España, S. A., Madrid, 2018, pp. 30-31.

manera leal y legítima previo al consentimiento otorgado, dirigido a las personas que se encuentren en el espacio de la Unión Europea, permitiendo el acceso del interesado. La norma en sí estará bajo el amparo de una autoridad que goce de independencia.

En ese sentido, el Tratado de Funcionamiento de la Unión Europea reconoce y ampara el mencionado derecho¹⁶⁹, es decir, tenemos un *derecho a la protección de datos de carácter personal* reconocido en: a) la Carta de Derechos Fundamentales de la Unión Europea y su artículo 8; b) el Tratado de Funcionamiento de la Unión Europea mediante su artículo 16 ; y c) con el Tratado de la Unión Europea y su artículo 6, permite una rápida trasposición, asimilación o reconocimiento de los derechos contemplados en la Carta incluido el mencionado *derecho a la protección de datos de carácter personal*, sin menoscabo de las competencias de la Unión tal como se erige en los Tratados, *contemplando el mismo valor jurídico que los Tratados*. Formando parte de los considerandos¹⁷⁰ utilizados en la elaboración del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

La Carta aboga por derechos vinculados con la personalidad, permitiendo proteger aquellos derechos relacionados con el individuo y su espacio privado, nos referimos a la vida privada, familiar, domicilio y las comunicaciones¹⁷¹, unos derechos contemplados en el numeral primero del artículo 8 del Convenio del Consejo de Europa. La Carta presenta un concepto más general y global, al

¹⁶⁹ Artículo 16, numeral 1.

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

Versión consolidada del tratado de funcionamiento de la unión europea, Diario Oficial de la Unión Europea, 2010. Disponible en: <https://www.boe.es/doue/2010/083/Z00047-00199.pdf>. (última verificación en línea 8 de marzo 2018).

¹⁷⁰ Cfr. Considerando 1, 2, 3 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

¹⁷¹ Artículo 7 Respeto de la vida privada y familiar.

“Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones”. *Carta de los Derechos Fundamentales de la Unión Europea, 2010*. Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003>. (Última verificación en línea 21 de abril 2018).

emplear el término comunicaciones¹⁷² en lugar de correspondencia, siendo un criterio más amplio e inclusivo, permitiendo desde su génesis la incorporación o entrada de nuevos servicios tales como email, correspondencias íntimas y comercial¹⁷³, llamadas telefónicas u otros nuevos servicios que engloben el concepto de las comunicaciones.

6.2. Directiva 95/46/CE relativa la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Antes de dar inicio a la norma, reproducimos el instrumento jurídico N.º 8¹⁷⁴ de la Sentencia núm. 292/2000 por considerar su conexión e incidencia con a)

¹⁷² (...) En este sentido, Coudhry (2014, 153), nos ilustra sobre la sustitución de la palabra comunicación a la habitual de correspondencia, debido al desarrollo tecnológico en comparación con el artículo 8 del CEDH. Hace un recorrido de análisis sobre el artículo parándose en la sentencia del TJUE en el caso Nexaus France SAS and Nexaus SA contra la Comisión Europea de 14 Noviembre de 2014 (Asunto 135/09), en el que nos dice el tribunal que "la necesidad de protección contra la intervención arbitraria o desproporcionada por las autoridades públicas (...) constituye un Principio General del Derecho de la UE". Coincide ello con la Cuarta Enmienda americana y su conexión con el artículo 7 de la CDFUE y el 8 del CEDH, y conectado al artículo 17 de la Convención Internacional de Derechos civiles y políticos. PÉREZ MIRAS, J., *El derecho a la protección de datos y a la privacidad...*op, cit., p. 286.

¹⁷³ Coudhry, S., *Commentary to article 7: Right to respect for Private and Family life (Family Life Aspects)*. En Peers S., Harvey, T., Kenner, J. & Ward, A. (Eds.). *The EU Charter of Fundamental Rights. A Commentary*. Oxford and Portland: Hart Publishing, 2014.

¹⁷⁴ *Instrumento jurídico N.º 8 de la sentencia 292/2000.*

8. Estas conclusiones sobre el significado y el contenido el derecho a la protección de datos personales se corrobora, atendiendo al mandato del art. 10.2 CE, por lo dispuesto en los instrumentos internacionales que se refieren a dicho derecho fundamental. Como es el caso de la Resolución 45/95 de la Asamblea General de las Naciones Unidas donde se recoge la versión revisada de los Principios Rectores aplicables a los Ficheros Computadorizados de Datos Personales. En el ámbito europeo, del Convenio para la Protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal hecho en Estrasburgo el 28 de enero de 1981, del que hemos dicho en la STC 254/1993, FJ 4, que no se limita "a establecer los principios básicos para la protección de los datos tratados automáticamente, especialmente en sus arts. 5, 6, 7 y 11", sino que los completa "con unas garantías para las personas concernidas, que formula detalladamente su art. 8", al que han seguido diversas recomendaciones de la Asamblea del Consejo de Europa..... en el ámbito comunitario, con la Directiva 95/46, sobre Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y la Libre Circulación de estos datos, así como con la Carta de Derechos Fundamentales de la Unión Europea del presente año, cuyo art. 8 reconoce este derecho, precisa su contenido y establece la necesidad de una autoridad que vele por su respeto. Pues todos estos textos internacionales coinciden en el establecimiento de

la Sentencia núm. 254/1993 en materia de protección de datos personales; b) el Convenio para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal conocido como el Convenio 108, c) la Carta de Derechos Fundamentales de la Unión Europea; d) la Directiva 95/46/CE, resaltando la necesidad de creación de una autoridad que vele por el respeto de la misma.

El proceso de conexión, adopción, interacción y reconocimiento de la protección de datos en el espacio de la Unión Europea¹⁷⁵ se encuentra matizado por acciones tendentes a la incorporación de este derechos en las normas legislativas de sus Estados miembros, pero no fue, si no después del Convenio 108 del Consejo de Europa, cuando la Comisión por medio a la Recomendación 81/679/EEC¹⁷⁶ del 29 de Julio de 1981, exhorta a sus Estados miembros firmar y ratificar el Convenio antes de finales de 1982, lo que a su vez no garantiza un nivel equivalente en los Estados europeos.

En materia de protección de datos personales, la Comisión presentó su primera propuesta el 13 de septiembre de 1990 en forma de Directiva, con la intención de obtener una protección equivalente en los Estados miembros de la Comunidad Europea y disminuir posibles obstáculos que pudieran frenar el intercambio de datos, y con ello, el flujo de datos necesarios para el funcionamiento del mercado interior¹⁷⁷, una propuesta llena de críticas,

un régimen jurídico para la protección de datos personales en el que se regula el ejercicio de este derecho fundamental en cuanto a la recogida de tales datos, la información de los interesados sobre su origen y destino, la facultad de rectificación y cancelación, así como el consentimiento respecto para su uso o cesión. Esto es, como antes se ha visto, un haz de garantías cuyo contenido hace posible el respeto de este derecho fundamental.

¹⁷⁵ CISNAL DE UGARTE, E. S., FERNÁNDEZ LIESA, C. R. y MOREIRA GONZÁLEZ, C., *Descripción, análisis y comentarios al Tratado de la Unión Europea*, 1ª ed. McGRAW-HILL / INTERAMERICANA DE ESPAÑA, S. A., Madrid, 1993, pp. 1 y ss.

¹⁷⁶ O.J. 1981, L 246/31, ESTADELLA YUSTE, O., *La Protección de la Intimidad frente a la Transmisión Internacional...* op. cit., pp. 69.-70; BRIAT., *Personal Data and the Free Flow of Información*, en P. HANSEN, et al. (eds) *Freedom of Data Flows and EEC Law*, 2ª Conferencia de CELIM, Kluwer, Computer /Law series, 1998, p 47. Citado por ESTADELLA YUSTE, O, ibid, p, 70, nota 54.

¹⁷⁷ ULL PONT, E., *Derecho público de la informática, protección de datos...* op. cit. p. 67.

razones que crearon el escenario para la presentación de una segunda propuesta en 1992; la Directiva busca vincular a los Estados en materia de protección de datos, armonizando las leyes nacionales.

A diferencia de la Comisión y el Consejo¹⁷⁸, el Parlamento ha realizado ingentes esfuerzos encaminados a la salvaguarda de los derechos de los individuos respecto a los avances de las tecnologías de la información y con ello, motivar a la Comisión en el establecimiento de una Directiva Comunitaria. En 1975 se presenta la primera resolución del Parlamento 60/48¹⁷⁹ solicitando a la Comisión la redacción de una Directiva sobre la libertad del individuo contra la evolución técnica de la informática, una segunda propuesta del Parlamento fue presentada en 1979, solución basada en el Bayerl Report¹⁸⁰ donde se solicita a la Comisión una armonización de las leyes nacionales de protección de datos para los fines de evitar problemas con las transmisiones internacionales de datos, un segundo Report fue presentado sobre los derechos del individuo frente al desarrollo técnico y procesamiento de datos¹⁸¹, sustentado en las debilidades del Convenio por lo que solicitaba de nuevo a la Comisión la creación de una Directiva¹⁸².

¹⁷⁸ CISNAL DE UGARTE, E. S., FERNÁNDEZ LIESA, C. R. y MOREIRA GONZÁLEZ, C., *Descripción, análisis y comentarios al Tratado de la Unión Europea*, 1ª ed. McGRAW-HILL / INTERAMERICANA DE ESPAÑA, S. A., Madrid, 1993, pp. 27 - 32.

¹⁷⁹ Cfr.O.J.1975, C 60/48 citado por ESTADELLA YUSTE, O., *ibid.*, p, 70, nota 57.

¹⁸⁰ “Entre los puntos más destacados del Bayerl Report se encuentran: a) recomendación a la Comisión para que hiciera un borrador de directiva sobre el sistema de comunicaciones europeo; b) que se armonizaran las leyes nacionales a fin de dar una cierta seguridad a la intimidad de los ciudadanos; c) que se realizara esta labor independientemente de otras organizaciones internacionales; y d) que la directiva que se adoptara estuviera inspirada con otros principios similares a lo de las sociedades occidentales. PARLAMENTO EUROPEO, *Report on the protection of the rights of the individual in the face of Technical Developments in Data Processing Bayerl Report, Doc. núm. 100/79, 1979-1980*”. Citado por ESTADELLA YUSTE, O., *ibid.*, p, 71, nota 60.

¹⁸¹ Doc. PE 70. 166/Ann.I/Fin, Doc. 1-548/81, 12 de octubre de 1981. Citado por ESTADELLA YUSTE, O., *ibid.*, p, 71, nota 62.

¹⁸² “Entre otras cosas también se solicitaba que se armonizaran las leyes nacionales de protección de datos de los estados miembros, y que la directiva que la Comisión adoptara se dirigiera al sector público y privado; la protección se debiera extender a todas las transmisiones personales a través de las fronteras; la notificación a la persona concernida debía ser obligatoria; responsabilidad por daño causado; la operatividad de los bancos de datos debía estar sujeta a previa ratificación y autorización de las autoridades. Sieglerschmidt Report, *ibid.*

El 18 de julio de 1990, la Comisión presentó al Consejo la primera propuesta de Directiva, una segunda propuesta fue presentada en septiembre de 1992, previo a grandes esfuerzos realizados por las autoridades de protección de datos de los Estados miembros, y la imposibilidad de llegar a común acuerdo, pero ya para el 1995, se alcanza una posición común, procediendo con la aprobación del documento; la Directiva asigna un plazo de 3 años¹⁸³ para que los Estados miembros transpongan en sus normas nacionales todas aquellas medidas que afectan los ficheros de datos de carácter personal automatizados, a diferencia de los ficheros manuales, quienes tienen un plazo de 12 años¹⁸⁴, ampliando el principio del respecto a la intimidad, incluido en el Convenio de 1981 del Consejo de Europa.

La creación de la Directiva, permitirá armonizar las legislaciones nacionales en materia de protección de datos, posibilitando la libre circulación de los datos personales entre los Estados miembros de la Unión Europea; el reporte argumentaba que la Directiva sería el único mecanismo capaz de lograr la libre circulación¹⁸⁵.

La pasada Directiva 95/46 (CE)¹⁸⁶ (derogada por el Reglamento) pertenece a la estructura de pilares existente antes del Tratado de Lisboa, con el Tratado

La importancia de este report reside, entre otras cosas, en que hace un llamamiento para examinar la compatibilidad de las disposiciones del Convenio 108 con las necesidades comunitarias que se han subrayado por el PE en otras resoluciones sobre el tema". Citado por ESTADELLA YUSTE, O, *ibid.*, p, 71, nota 63.

¹⁸³ El plazo para la transición de la normativa finalizaba el 25 de octubre de 1998, en el caso de España, la normativa fue presentada fuera del tiempo establecido por la Directiva.

¹⁸⁴ ALMAZARA ALMAIDA, C. (Coordinador), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. LEX NOVA, S. L., Valladolid, 2007, pp. 36-37.

¹⁸⁵ La creación de la directiva no impedirá los posibles obstáculos en materia de protección de datos entre los estados miembros, razones que conducirán a la conformación del Reglamento 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46 (Reglamento general de protección de datos). Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807>. (Última consulta en línea 8 de marzo 2018).

¹⁸⁶ *Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos*. Disponible en:

de Lisboa¹⁸⁷ desaparece la estructura de Pilares¹⁸⁸, el Reglamento forma parte de las modificaciones introducidas por el Tratado de Lisboa, el Reglamento entró en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea, siendo aplicable a partir del 25 de mayo de 2018¹⁸⁹.

La protección de datos¹⁹⁰ de la Unión Europea, anteriormente conocida como Comunidad Europea¹⁹¹, se fundamenta en el artículo 7¹⁹² y 8¹⁹³ de la

<https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678>. (Última consulta en línea 8 de marzo 2018).

¹⁸⁷ *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*. Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807>. (Última consulta en línea 8 de marzo 2018).

¹⁸⁸ CISNAL DE UGARTE, E. S., FERNÁNDEZ LIESA, C. R. y MOREIRA GONZÁLEZ, C., *Descripción, análisis y comentarios al Tratado de la Unión Europea*, 1ª ed. McGRAW-HILL / INTERAMERICANA DE ESPAÑA, S. A., Madrid, 1993, p. 17.

¹⁸⁹ *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*. Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807>. (Última consulta en línea 8 de marzo 2018).

¹⁹⁰ El tema se trató previamente, pero debido a su relevancia ha sido necesario su refrescamiento.

¹⁹¹ Artículo 1. Tercer párrafo TUE "...La Unión sustituirá y sucederá a la Comunidad Europea."

¹⁹² Artículo 7. Respeto de la vida privada y familiar. "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones". *Carta de los Derechos Fundamentales de la Unión Europea, 2010*. Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003>. (Última verificación en línea 21 de abril 2018).

¹⁹³ Artículo 8. *Protección de datos de carácter personal*
1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.
3. El respeto de estas normas estará sujeto al control de una autoridad independiente. *Carta de los Derechos Fundamentales de la Unión Europea, 2010*. Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003>. (Última consulta en línea 21 de abril 2018).

Carta¹⁹⁴ de los Derechos Fundamentales de la Unión Europea y el artículo 16¹⁹⁵ del Tratado de Funcionamiento de la Unión Europea (TFUE)¹⁹⁶.

El artículo 16 en su numeral 2, contempla la figura de autoridades independientes para mantener el respeto de las normas sobre protección de las personas físicas en relación al tratamiento de datos de carácter personal establecidas por el Parlamento Europeo y el Consejo.

Parte del derecho de la Unión estará formado por los Derechos fundamentales del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales unido a las tradiciones constitucionales de los Estados miembros según lo conforma el 6,3 del Tratado de la Unión Europea.

6.3. Reglamento (UE) 2016/679 relativa la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

6.3.1. Etapas previas en la implementación del Reglamento

¹⁹⁴ Artículo 6

1. La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados.

Las disposiciones de la Carta no ampliarán en modo alguno las competencias de la Unión tal como se definen en los Tratados. Versión consolidada del Tratado de la Unión Europea. Disponible en: <https://www.boe.es/doue/2010/083/Z00013-00046.pdf>. (Última consulta en línea 8 de marzo 2018).

¹⁹⁵ Artículo 16, numeral 1.

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

Versión consolidada del Tratado de Funcionamiento de la Unión Europea, Diario Oficial de la Unión Europea, 2010. Disponible en: <https://www.boe.es/doue/2010/083/Z00047-00199.pdf>. (Última consulta en línea 8 de marzo 2018).

¹⁹⁶ *Código Unión Europea*, la Ley-Actualidad, S. A., Edición septiembre 2005, Madrid, 2005, pp. 1-ss.

A continuación, presentamos las etapas previas por las que ha transcurrido el proceso evolutivo de las normas legislativas en materia de protección de datos en España antes de la entrada del Reglamento.

- Artículo 18.4 de la Constitución Española, protege el tratamiento de datos personales reconocido como un derecho fundamental en la Constitución.
- Sentencia núm. 94/1998 del 4 de mayo, garantiza a las personas el control, uso y destino sobre sus datos, configurándolo como un derecho de oposición ante el uso distinto al justificado.
- Sentencia núm. 292/2000 de 30 de noviembre, considera la protección de datos como un derecho autónomo e independiente¹⁹⁷.
- Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD).
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD) (deroga Ley Orgánica 5/1992).

Ante la necesidad de lograr uniformidad¹⁹⁸ en las regulaciones en materia de derecho fundamental a la protección de datos en un entorno cada vez más

¹⁹⁷ ARENAS RAMIRO, M. y ORTEGA GIMÉNEZ, A. (Directores), Protección de Datos, 1ª ed. Sepín, S. L. Madrid, 2019, p. 35.

¹⁹⁸ Cfr. “El Reglamento general de protección de datos pretende con su eficacia directa superar los obstáculos que impidieron la finalidad armonizadora de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.... La transposición de la Directiva por los Estados miembros se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la Unión Europea lo que, en último extremo, ha conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos. Congreso

global, diversas instancias internacionales realizaron esfuerzos para establecer mejoras a las normativas existentes en materia de protección de datos, entre ellas, la Comisión vía su primera comunicación correspondiente al 4 de noviembre de 2010 bajo el título “*un enfoque global de la protección de los datos personales en la Unión Europea*”, considerado el primer documento encaminado a materializar el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, siendo la seguridad jurídica un elemento muy importante en el proceso de su conformación.

6.3.2. Seguridad jurídica en el Reglamento

Como ya hemos comentado, la seguridad jurídica¹⁹⁹ forma parte integral de los argumentos²⁰⁰ que dieron pautas al establecimiento del Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, el cual persigue garantizar la coherencia en materia de protección de datos de las personas físicas en territorio de la Unión Europea, evitando divergencias que pudieran dificultar el desplazamiento de los datos personales en el espacio de la Unión Europea, en ese orden, a pesar de la aplicabilidad directa de los reglamentos en los Estado, se considera la posibilidad de desarrollar una normativa de adaptación, adecuando el Reglamento de protección de datos en los

de los diputados”, *Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal*, XII Legislatura, Boletín oficial de las cortes generales, 24 de noviembre de 2017, p. 6.

Disponible en: http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF. (Última consulta en línea 22 de mayo 2018).

¹⁹⁹ Cfr. “...el principio de seguridad jurídica, en su vertiente positiva, obliga a los Estados miembros a integrar el ordenamiento europeo en el interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos, en tanto que, en su vertiente negativa, implica la obligación para tales Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo...” Congreso de los diputados., *Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal*, XII Legislatura, Boletín oficial de las cortes generales, 24 de noviembre de 2017, p. 7.

Disponible en: http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF. (Última consulta en línea 22 de mayo 2018).

²⁰⁰ Cfr. Considerando 13 Reglamento (UE) 2016/679.

Estados²⁰¹, de ahí la creación de una ley orgánica sustituta de la actual (Ley Orgánica 15/1999 LOPD), una ley que busca adaptar la normativa española²⁰² y completar las disposiciones del Reglamento, garantizando la seguridad jurídica y esclareciendo las disposiciones contempladas en el Reglamento.

A pesar de ello, el Reglamento forma parte de las normativas existentes en materia de protección de las personas físicas en relación a la protección de datos de la Unión Europea; debido a su relevancia abordamos su norma previa (la Directiva 95/46 CE) seguida de la incursión de los nuevos términos contemplados en el Reglamento.

6.3.3. Disposiciones del Reglamento (UE) 2016/679

El Diario Oficial de la Unión Europea mejor conocido por sus siglas en español (DOUE), publicó en fecha 27/04/2016 el *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, derogando en su artículo 94 a la *Directiva 95/46 CE del Parlamento Europeo y Consejo del 24 de Octubre de 1995, relativa a la*

²⁰¹ “En los casos en que el presente Reglamento establece que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros, estos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos del presente Reglamento” *Considerando 8*, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

²⁰² Artículo 1 Objeto de la Ley.

1. La presente ley orgánica tiene por objeto adaptar el ordenamiento jurídico español al Reglamento (UE) del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.
2. El derecho fundamental de las personas físicas a la protección de datos de carácter personal, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica.

Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, XII Legislatura, Boletín oficial de las cortes generales, 24 de noviembre de 2017, p. 7.

Disponible en: http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF. (Última consulta en línea 22 de mayo 2018).

protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, siendo efectivo a partir del 25 de mayo del 2018.

La protección de las personas físicas detentaba una Directiva (la Directiva 95/46) y una Decisión (Decisión Marco 2008/977/JAI del Consejo) ambas derogadas por:

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Y el Reglamento

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Ambos, constituyen el nuevo marco legislativo relativo a la protección de datos personales de la Unión Europea, es importante acotar los nuevos cambios experimentados de Directiva a Reglamento y de Decisión a Directiva, confiriendo desde sus inicios la intención manifiesta del Parlamento y el Consejo de formular nuevas propuestas, con la intención de fortalecer el alcance de la pasada Directiva²⁰³, y al mismo tiempo, lograr adaptarla a los

²⁰³ “...cabe afirmar que fueron un conjunto amplio de motivos —unos con mayor intensidad que otros—los que operaron este asombroso cambio en la posición de la Comisión Europea. Y, de entre ellos, podemos resaltar los siguientes factores: a) La deficiente transposición de la Directiva y, en consecuencia, una débil armonización europea; b) las limitaciones de las

nuevos avances tecnológicos e informáticos que nos ofrecen las TIC en un mundo conectado y globalizado veintiún año²⁰⁴ después de la pasada Directiva²⁰⁵.

El nuevo Reglamento de protección de datos personales tiene su génesis en el numeral 2²⁰⁶ del artículo 16 del Tratado de Funcionamiento de La Unión

Autoridades nacionales de protección de datos en la garantía efectiva y similar del derecho a la protección de datos en el conjunto del territorio europeo; c) la incesante presión de las empresas multinacionales europeas y, particularmente, norteamericanas quejas ante los obstáculos burocráticos a las transferencias internacionales y la heterogeneidad de reglas nacionales; d) el extraordinario impacto tecnológico de servicios *on line* (como las redes sociales) de titularidad estadounidense y ajenos a las exigencias europeas; e) el enorme alcance mediático de la protección de la privacidad y el singular incremento en la sensibilización social; f) el dificultoso diálogo trasatlántico EU - USA sobre las transferencias de dato con fines de seguridad (Casos Swift y PNR); g) la propia agenda europea en seguridad que intensificaba las exigencias de intercambios de datos personales; h) el impulso político de la Comisión personificado en el Comisario de Justicia saliente Barrot y, singularmente, en su sucesora Reding; i) y, ... la entrada en vigor del Tratado de Lisboala garantía efectiva del derecho a la protección de datos personales...todos estos factores crearon el ambiente necesario para que en apenas dos años la Comisión Europea diera un golpe de timón de ciento ochenta grados y propugnara una revisión general del marco jurídico europeo de protección de datos”, RALLO LOMBARTE, A., “Hacia un nuevo sistema Europeo de protección de datos: las claves de la reforma”, UNED, *Revista de Derecho político*, núm. 85, septiembre-diciembre 2012, pp. 25-26.

²⁰⁴ 2 “...La Directiva 95/46/CE.....fue adoptada hace 21 años cuando Internet se encontraba en su etapa inicial de desarrollo.....La propuesta del Reglamento moderniza los principios de la Directiva de 1995, adaptándola a la era digital y armonizando la legislación sobre protección de datos en Europa. Son necesarias unas solidas normas de protección de datos.....” *Comunicación de la comisión del Parlamento Europeo*, Bruselas, 11.4.2006 COM (216) 214 final; página 2, Disponible en: <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016PC0214&from=ES>. (Última consulta en línea 14 octubre de 2016).

²⁰⁵ Posición del eurodiputado verde alemán Jan Philipp Albrecht responsable de la tramitación del texto legislativo “El tiempo vuela y más deprisa aún en el campo de Internet, la tecnología, las redes sociales y la nube informática. El reciente escándalo del ciber espionaje realizado por las autoridades estadounidenses ha enfatizado lo necesario que es reformar la legislación europea de protección de datos, que ya tiene veinte años”. Albrecht y Droutsas: *La reforma de la protección de datos entra en la recta final*. Disponible en: <http://www.europarl.europa.eu/news/es/news-room/20140310STO38525/albrecht-y-droutsas-la-reforma-de-protecci%C3%B3n-de-datos-entra-en-la-recta-final>. (Última consulta en línea 01 octubre de 2016).

²⁰⁶ Tratado de Funcionamiento de la Unión Europea
Artículo 16 (antiguo artículo 286 TCE), Numeral 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

Europea, el cual, para dar cumplimiento a lo expresado en el numeral 1²⁰⁷ del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, bajo el título de protección de datos de carácter personal, entiende que el Parlamento Europeo y el Consejo establecerán con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal, dando cumplimiento al mismo tiempo, al artículo 39²⁰⁸ del Tratado de la Unión Europea; la Comisión Europea presenta su propuesta de reforma del Sistema Europeo de Protección de Datos el 25 de enero de 2012, amparado en el crecimiento de Internet y en el aumento de la velocidad de las transacciones internacionales de datos entre los continentes, aspirando a robustecer la confianza de los ciudadanos en lo que respecta a sus datos personales²⁰⁹. El proceso legislativo ha sido largo, controvertido, vinculado en dar solución a los problemas existentes en la sociedad digital²¹⁰

El Reglamento, compuesto por cuatro vistas, ciento setenta y tres considerandos y 99 artículos, se diferencia de su antecesora la Directiva 95/46/CE por disponer de dos vistas, setenta y dos considerandos y 34 artículos,

Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea.

²⁰⁷ Carta de los Derechos Fundamentales de la Unión Europea.

Artículo 8 Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

²⁰⁸ *Artículo 39, Tratado de la Unión Europea*

De conformidad con el artículo 16 del Tratado de Funcionamiento de la Unión Europea, y no obstante lo dispuesto en su apartado 2, el Consejo adoptará una decisión que fije las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del presente capítulo, y sobre la libre circulación de dichos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

²⁰⁹ RALLO LOMBARTE, A., "Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", UNED, *Revista de Derecho político*, núm. 85, septiembre-diciembre 2012, pp. 15-16.

²¹⁰ DURÁN CARDO, B., *El Delegado de Protección de Datos...op. cit.*, p. 24.

dejando entrever su alcance cuando la comparamos con el Reglamento, este a su vez, entró en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea, siendo aplicable a partir del 25 de mayo del 2018, 2 años después de su publicación, tal como lo expresa el artículo 99²¹¹ del referido Reglamento.

A su vez, se apoya en unas series de considerandos que tienen como objetivo crear las bases para solucionar las divergencias de ejecución y aplicación de la Directiva 95/46/CE en los temas económicos, tecnológicos, jurídicos, etc. asegurando la libre circulación de los datos personales en el mercado interior, por medio a la implementación de mecanismos que generen transparencia y seguridad jurídica en los Estados miembros²¹².

Todo ello sin dejar a un lado las consecuencias del rápido crecimiento tecnológico, muy de la mano con la globalización en un mundo conectado, generando e intercambiando grandes volúmenes de datos personales, en una total convivencia con los sectores públicos, privados y las personas físicas.

De entrada, podemos ver como el Reglamento implementa términos novedosos no existentes en las definiciones de la Directiva 95/46 CE, como son los datos genéticos²¹³, biométricos²¹⁴ y otros presentados a continuación en las novedades que trae consigo el nuevo Reglamento²¹⁵.

²¹¹ *Artículo 99* entrada en vigor y aplicación

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.
2. Será aplicable a partir del 25 de mayo de 2018.

²¹² *Comunicación de la Comisión del Parlamento Europeo*, Bruselas, 11.4.206 COM (216) 214 final; página 3, “la propuesta del Reglamento se centra en: ...el fortalecimiento del mercado interior de la UE...y el establecimiento de Normas Internacionales de Protección de Datos”. Disponible en: <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016PC0214&from=ES>. (Última consulta en línea 14 octubre 2016).

²¹³ «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

Transparencia

El Reglamento incorpora el tema de la transparencia²¹⁶ como principios relativo al tratamiento de los datos personales²¹⁷. En la misma línea, el Reglamento fortalece los temas de seguridad jurídica mediante la implementación de la ventanilla única, no siendo necesario involucrar diferentes autoridades de control, un tema muy importante para las compañías con sucursales distribuidas en Estados de la Unión Europea y otros temas transfronterizos que afectan el sector.

Consentimiento

El consentimiento en el Reglamento toma un nuevo giro, no solo basta con consentir, sino que hay que ser capaz de tener las informaciones necesarias que demuestren el consentimiento, materializándose en un consentimiento inequívoco, explícito, siendo este claro y afirmativo, en ese mismo contexto, el Reglamento contempla el retiro del consentimiento por parte del interesado.

Supresión de Datos (derecho al Olvido)

El tema de la supresión de datos (derecho al olvido)²¹⁸, reconocido en la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) caso Mario

²¹⁴ «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

²¹⁵ DÍA DÍAZ, E., “El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones”, *Revista Aranzadi doctrinal*, núm. 6, 2016, p. 17.

²¹⁶ Artículo 12, numeral 1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información..... relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño..., la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

²¹⁷ Comunicación de la comisión del Parlamento Europeo, Bruselas, 11.4.2016 COM (2016) 214 final; página 3, “los cambios darán a los ciudadanos más control sobre sus datos personales y facilitarán un acceso a los mismos...un acceso más fácil a los propios datos – las personas físicas dispondrán de más información, de modo claro y comprensible, sobre la forma en que se tratan sus datos”. Disponible en: <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016PC0214&from=ES>. (Última consulta en línea 14 octubre 2016).

²¹⁸ Cfr. Artículo 17, Derecho de supresión (<<el derecho al olvido>>).

Costeja Vs. Google²¹⁹, presentados durante la exposición de las jurisprudencias europeas en el trabajo, establece las bases del desarrollo normativo del derecho al olvido²²⁰, instaurando los derechos del interesado ante el responsable del tratamiento, el cual deberá suprimir aquellos datos revestidos de las siguientes circunstancias a) no sean necesario para los fines tratados o recolectados; b) retiro del consentimiento por parte del interesado al cual otorgó su consentimiento²²¹ ya sean estas categorías especiales exceptuando la prohibición del derecho de la Unión o los Estados miembros²²²; c) datos usados en mercadotecnia directa incluida la construcción de perfiles sustentados en esta; d) situación particular; e) datos tratados ilícitamente; f) obligación legal; g) ofertas a menores sin el consentimiento de sus padres, el responsable del tratamiento adoptará todas las medidas necesarias para proveer y satisfacer el requerimiento del interesado, siempre y cuando aquella supresión no afecte a) el derecho a la libertad de expresión e información; b) una obligación legal; c) cumplimiento de una misión de interés público ya sean estos de la salud pública como medicina preventiva o laboral; d) diagnóstico médico; e) tratamiento sanitario o social; f) servicios de asistencia sanitaria y social²²³; g) amenazas fronterizas graves para la salud; h) aumento de niveles de calidad y seguridad en la salud pública²²⁴; i) investigación científica; j) histórica; k) estadísticas o el ejercicio de reclamaciones.

Portabilidad de los datos

²¹⁹ PLAZA PENADÉS, J., “El nuevo modelo de protección de datos personales europeos y el modo de obtener un consentimiento lícito”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 44, Mayo-Agosto 2017, p. 18.

²²⁰ VÁZQUEZ DE CASTRO, E., “Derecho al honor en Internet, Anonimato y Responsabilidades de los Prestadores de Servicios: ¿Evolución e Involución?”, *Revista Aranzadi de Derecho y Nuevas Tecnologías* 44, Mayo-Agosto 2017, p. 213.

²²¹ Cfr. Artículo 6, apartado 1, letra a.

²²² Cfr. Artículo 9, apartado 2, letra a.

²²³ Cfr. Artículo 9, apartado 2, letra h, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

²²⁴ Cfr. Artículo 9, apartado 2, letra i, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

El derecho a la portabilidad de los datos²²⁵ permite al interesado recibir los datos personales del responsable al cual le haya facilitado los datos y transmitirlo a otro responsable, la operación, si es permitido llamarla contará con la aceptación del primer responsable facultando su entrega bajo un formato estructurado, de uso común y lectura mecánica siempre y cuando el interesado entregue su consentimiento para uno u otros fines²²⁶, cuando el interesado otorgue su consentimiento excepto cuando no pueda ser realizado el tratamiento, ya sea esto por ser considerados tratamientos de categorías especiales como etnia, religión, opiniones políticas, convicciones religiosas o filosóficas etc., capaces de identificar a una persona física²²⁷, elaboración de un contrato donde el interesado forma parte de él, o en la elaboración de medidas precontractuales²²⁸, la utilización de medios automáticos en la elaboración del tratamiento, a raíz de ello, aplicará una tramitación de datos personales de responsable a responsable siempre y cuando las condiciones técnicas lo permitan; el derecho a la portabilidad no puede ser ejercido cuando exista de por medio un interés público o un ejercicio de poderes públicos en manos del responsable del tratamiento.

Delegado de protección de datos-DPP (Data Protection Officer (DPO))

El proceso de integración de la Unión Europea devino en un aumento de las transacciones comerciales, la intensificación e intercambio de los datos personales entre los Estados miembros bajo el amparo de las TIC; partiendo de esos considerandos, el Reglamento introduce la figura del Delegado de Protección de Datos siempre que a) se lleve a cabo por una autoridad o un organismo público, b) las operaciones requieran observación habitual y sistemática a gran escala, c) existan características especiales o datos relativos

²²⁵ Cfr. Artículo 20, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 3016.

²²⁶ Cfr. Artículo 6, apartado 1, letra a, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 3016.

²²⁷ Cfr. Artículo 9, apartado 2, letra a, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 3016.

²²⁸ Cfr. Artículo 6, apartado, letra b, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 3016.

a condenas e infracciones penales, d) un grupo empresarial, e) varias autoridades u organismos, f) asociaciones u organismos que representen al responsables o encargados; el delegado de protección de datos debe tener competencias en derecho, protección de datos y en las funciones²²⁹ aplicadas en el Reglamento para los delegados de protección de datos, formando parte de la plantilla del responsable o del encargado fungiendo de enlace y comunicación de la autoridad de control²³⁰.

El delegado participará de las cuestiones relacionadas con la protección de datos, siendo respaldado en sus funciones por el responsable y el encargado del tratamiento, rindiendo cuenta al más alto nivel de la cadena, con la posibilidad de ser contactado por los interesados, velando por el secreto o la confidencialidad, y desempeñando las funciones establecidas en el Reglamento²³¹, entre ellas, las funciones de informar, asesorar, supervisar, cooperar y actuar de punto de contacto con la autoridad de control.

Ante tal situación, entendemos que el responsable de protección de datos debe ser escogido y seleccionado por el más alto nivel de la empresa cumpliendo con los requisitos requeridos, de esta manera evitamos vínculos entre el delegado de protección de datos con el responsable o el encargado del tratamiento. La figura del DPD no es nueva²³² y tiende a convertirse en una figura independiente, protegiendo los derechos del interesado o su titular²³³.

Sistema de accountability

²²⁹ Cfr. Artículo 39, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

²³⁰ Cfr. Artículo 37, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

²³¹ Cfr. Artículo 39, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

²³² “El DPD no es una figura de nueva aparición. Tiene su antecedente directo en el denominado “encargado de protección de los datos personales de la Directiva 95/46/CE....”. DURÁN CARDO, B., *La figura del responsable en el derecho a la protección de datos*, La Ley, Wolters Kluwer, Las Rozas (Madrid), 20016, pp. 326-329.

²³³ DURÁN CARDO, B., *El Delegado de Protección de Datos...* op. cit., p. 24.

El Reglamento, implementa en sus novedades la protección de datos desde el diseño y por defecto, formulando el principio de responsabilidad proactiva o accountability, realizando evaluaciones periódicas de impacto.

Las novedades no cesan en el nuevo proyecto, el Reglamento, implementa en sus novedades la protección de datos desde el diseño y por defecto, formulando el principio de responsabilidad proactiva, realizando evaluaciones periódicas de impacto, a tal punto que implementa una protección de datos desde el mismo momento en que se piensa en el tratamiento, nos referimos a la protección de datos desde el diseño, ya sea al momento de escoger los medios para el tratamiento como al momento de ejecutarlo, tal como lo menciona el artículo 25 del Reglamento.

Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados²³⁴.

De acuerdo al Reglamento, solo por defecto serán utilizados los datos correspondientes a los fines específicos para el cual fueron designados los datos, quedando plasmado en el numeral segundo²³⁵ del correspondiente

²³⁴ Cfr. Artículo 37, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

²³⁵ Artículo 25 numeral 2, el responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas

artículo. El sistema de accountability se conecta con el DPD, siendo realidades en el Reglamento, materializando y haciendo efectiva la protección de datos por defecto y por diseño, estableciendo un sistema de responsabilidades proactivas y con ello, la protección de los derechos de las personas.

Derecho de oposición

El artículo 21 numeral 2, introduce el derecho de oposición del interesado a presentar oposición al uso de sus datos personales para fines mercadológicos acrecentados por las TIC.

Comité de Protección de Datos

Se crea un Comité²³⁶ de Protección de Datos (artículo 68) compuesto por cada uno de los directores de las autoridades de control, un presidente y por un representante del Supervisor Europeo de Protección de Datos; el Comité gozará de amplias competencias e independencia en sus funciones, al mismo tiempo, asesorará a la Comisión en temas relacionados con la protección de datos, y otras funciones específicas de su conformación tal cual se detalla en los artículos del 68 al 76 del Reglamento. Al mismo tiempo, se plantea la creación de una Secretaría bajo el cargo del Supervisor Europeo de Protección de Datos, siguiendo los lineamientos y funciones del Comité de Protección de Datos.

El Comité sustituye al Grupo de Protección de Datos (Grupo 29) contemplado en la Directiva 95/46/CE, formando parte importante del proceso de implementación del Reglamento, promoviendo la colaboración de las autoridades de control en el espacio de la Unión Europea; las decisiones

garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

²³⁶ Comunicación de la comisión del Parlamento Europeo, Bruselas, 11.4.2016 COM (2016) 214 final; página 3, el establecimiento de una “ventanilla única” para las empresas: de forma que las empresas tengan como interlocutor a una sola autoridad de control, no a 28, lo que les simplificará y abarcará operar en la UE. Disponible en: <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016PC0214&from=ES>. (Última consulta en línea 14 octubre 2016).

emanadas del Comité son jurídicamente vinculantes, a diferencia del Grupo de Protección de Datos, contemplando funciones y responsabilidades pertenecientes a otros órganos como el Supervisor Europeo de Protección de Datos o formando parte de órganos no existentes como el Grupo de Protección siendo asumidas por el Comité, con la diferencia de adoptar el carácter vinculante y como no, las nuevas responsabilidades creadas, es decir, estamos delante de un órgano nuevo, por ello será necesario esperar su entrada y ver su accionar con el objetivo de despejar las dudas y preguntas relacionadas hacia el Comité²³⁷.

Las directrices del nuevo Reglamento buscan realizar acciones tendentes en asegurar no solo una correcta implementación del Reglamento, si no, corregir y soportar el proceso post implementación, vislumbrando corregir las debilidades de la pasada Directiva²³⁸, mediante una uniformidad en el tratamiento de los datos personales en todos los Estados miembros²³⁹.

Por tanto, con la intención de adecuar el Reglamento (UE) 2016/679 a los nuevos cambios y transformaciones tecnológicas que impactan a los individuos, empresas, gobierno, el Reglamento inserta un período de verificación de cada 4 años, contribuyendo con su actualización ante los nuevos cambios y transformaciones tecnológicas que impactan la sociedad en todos sus ámbitos.

²³⁷ GONZÁLEZ FUSTER, G., *El Comité Europeo de Protección de Datos*, exponencia en la mesa redonda *Autoridades de control e implementación de la normativa en materia de protección de datos*, Congreso Internacional sobre el impacto del Reglamento europeo de protección de datos: análisis nacional y comparado, Castellón de la Plana, Universitat Jaume I, 17 y 18 de mayo 2018.

²³⁸ “Aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de los datos en el territorio de la Unión se aplique de manera fragmentada...”. Esta diferencia en los niveles de protección se debe a la existencia de divergencias en la ejecución y aplicación de la Directiva 95/46/CE. *Considerando 09, Reglamento (UE) 2016/679 Reglamento Europeo y del Consejo de 27 de abril de 2016.*

²³⁹ “Para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección... debe ser equivalente en todos los Estados miembros...”. *Considerando 10, Reglamento (UE) 2016/679 Reglamento Europeo y del Consejo de 27 de abril de 2016.*

No solo la Unión Europea ha realizado y realiza ingentes esfuerzos legislativos en proteger a las personas físicas mediante la tutela de la privacidad, Intimidad y la protección de sus datos personales, sino, que sus Estados han formado parte de este proceso transformacional, situación reflejada a continuación en la construcción de las normas españolas en materia de privacidad, protección y transferencia internacional de datos personales vinculados desde su nacimiento con la Constitución española y su memorable artículo 18,4.

7. La construcción del derecho a la protección de datos en España.

7.1. El artículo 18.4 de la Constitución española de 1978

Los derechos fundamentales en España van a la par con el nacimiento de la democracia. Es por ello que, a partir del año 1976 durante el momento de la transición hacia la democracia, comienza a producirse un cambio cualitativo, llegando a generarse un ordenamiento jurídico donde los derechos humanos van a tener una tutela más eficaz. Iniciada la democracia, comienza el fortalecimiento y la distinción de los nuevos derechos, a partir del año 1977 se empieza a distinguir entre los derechos de la personalidad, el derecho a la intimidad personal, familiar y social, así como el derecho a la información²⁴⁰.

La Constitución del 27 de diciembre de 1978²⁴¹ se inspira en muchos aspectos de la Constitución alemana, de la cual consigue aportes a los derechos y deberes fundamentales como lo son sus artículos 10.1 y 10.2 (derechos de la persona)²⁴².

²⁴⁰ MOLINERO, C., *La Información y los derechos personales*, Col. Técnico-Universitario núm. 6, Diosa, Barcelona, 1977, pp. 37-39.

²⁴¹ Sobre el origen y las características e influencias véase por todo LÓPEZ GUERRA, L., *El Derecho Constitucional español. Origen y características de la Constitución*, visto en *Derecho Constitucional*, volumen I, 8ª ed. Tirant Lo Blanch, 2010, pp. 19-31.

²⁴² Artículo 10. Título I

Un antecedente cercano del texto constitucional relacionado con el uso de la informática es el artículo 35 de la Constitución de Portugal de 1976²⁴³, siendo una de las primeras constituciones que reconoce ciertos derechos al ciudadano sobre las informaciones contenidas en ficheros automatizados²⁴⁴. De ahí que quepa afirmar que este país aprovechó el momento histórico para ofrecer “la singularidad de ser el primer Estado democrático europeo que constitucionaliza la protección frente a la informática”²⁴⁵.

Sucede, sin embargo, que como señala la doctrina esa incorporación ha de valorarse en su justa medida, pues se produce en un momento de cambio político y será en el proceso de elaboración de las nuevas constituciones cuando, con el eco de los debates generados en otros países, se procede a recoger en las constituciones estas referencias; sirva de ejemplo, que el rechazo público a la atribución de un único número personal informatizado, que

1. La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social.

2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España. *Constitución española de 1978*, Agencia Estatal Boletín Oficial del Estado, Madrid. Disponible en: www.boe.es. <https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf>. (Última consulta en línea 19 de junio 2018).

²⁴³ El artículo 35 de la Constitución usa bajo el encabezamiento *Utilización de la informática* establecía en su redacción original:

1. Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización.

2. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos.

3. Se prohíbe atribuir un número nacional único a los ciudadanos.

Sobre este particular GOMES CANOTILHO, J. J. & MOREIRA, V., *Constituição da República Portuguesa. Anotada*, Coimbra editora, 1980, pp. 103-104.

²⁴⁴ ESTADELLA YUSTE, O., *La Protección de la Intimidad frente a la Transmisión Internacional...* op. cit., p. 39.

²⁴⁵ LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación...*, op. cit., p. 135.

tuvo su relevancia a comienzos de los 70, estuvo también presente en Portugal y propició su incorporación al texto constitucional²⁴⁶.

Este artículo 35 de la Constitución portuguesa de 1976²⁴⁷, que ha sido reformado en numerosas ocasiones, es considerado por la doctrina española como uno de los factores más determinantes para la incorporación del apartado 4 del artículo 18 de la Constitución de 1978. Este apartado -que prevé que “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”- es mucho menos ambicioso que el texto de Portugal, afirmándose que era más imperfecto y menos detallado, incluso en esa época algunos lo consideraban innecesario²⁴⁸. Sin embargo, ciertos grupos parlamentarios pujaron por el mismo²⁴⁹ y la doctrina más especializada, ya en años posteriores ha sabido

²⁴⁶ GONZÁLEZ MURUA, A. R., *La Agencia Vasca de Protección de Datos y el Estado de las Autonomías...* op. cit., p. 35.

²⁴⁷ La constitución fue aprobada por la Asamblea Constituyente en sesión de 2 de abril de 1976. Edición oficial, imprenta Nacional-Casa da Moeda, Lisboa, 1976. Así se expresa en Central de Informática.; *Informática Leyes de Protección de Datos, Documentación Informática núm. 2, serie Verde /Legislación*, 1ª ed. Presidencia del gobierno, Madrid, 1977. nota p. 15.

²⁴⁸ SEMPERE RODRÍGUEZ, C. “Artículo 18 CE”, visto en ALZAGA VILLAAMIL (Director), *Comentarios a la Constitución española de 1978*, Tomo II, Edersa, Madrid, 1997.

²⁴⁹ La enmienda núm. 716 del señor Sancho Rof y la enmienda núm. 779 perteneciente también a la UCD, tendían a la supresión del apartado 4 del entonces artículo 17 puesto que se entendía que ya en el apartado 1 al referirse al honor y a la intimidad se prevenía globalmente cualquier tipo de atentado contra tales facultades; entendiéndose por tanto tal mención redundante (intervención del señor Sancho Rof, en *Diario de Sesiones del Congreso*, de 19 de mayo de 1978, núm. 70, p. 2526). Sin embargo, desde otras posiciones se mantenía que no sólo era necesaria la alusión expresa a la informática, sino que además su tutela se debería de extender frente al uso indebido del ejercicio de todos los derechos, en lugar de restringirlo al derecho al honor y a la intimidad. Esta tesis fue sustentada por el señor Gastan Sanz en nombre del Grupo Mixto (intervención del señor Gastón Sanz, *ibid.*, p. 2527). En parecido sentido, pero finalmente la enmienda que prosperó fue la núm. 117, propuesta por el señor Roca Junyent en nombre de la Minoría Catalana en la Ponencia Constitucional (intervención del señor Roca Junyent, *ibid.*, p. 2527). En otro extremo también se defendió extender la garantía frente a su uso indebido a todos los derechos, pero además ampliar la cobertura a todos los procedimientos o medios técnicos que pudieran afectar al ejercicio de la libertad (intervención del señor Zarazaga Burillo, en *Diario de Sesiones del Congreso* de 27 de septiembre de 1978, núm. 60, p. 2981). Sobre estas diferentes posturas véase por todos PÉREZ LUÑO, A. E., “Informática y libertad. Comentario al artículo 18.4 de la Constitución española...” *op. cit.*, pp. 41-45.

desprender del mismo toda la virtualidad necesaria, como a continuación expondremos²⁵⁰.

Con todo, “estas incorporaciones no pueden interpretarse en el sentido de que estos países asumen una posición vanguardista en la regulación del uso de la informática. Muestra de ello es -además del escaso desarrollo tecnológico que comparativamente con otros países tenían en ese momento- el hecho de que ninguno de ellos procedió a desarrollar legislativamente el contenido del texto constitucional hasta la siguiente de las generaciones (tercera generación)”²⁵¹. En Portugal, esto se produjo con la *Lei de Proteção de dados pessoais face à informática* de 29 de abril de 1991. En el caso de España, hubo que esperar al 29 de octubre del 1992 que es cuando ve la luz la Ley Orgánica 5/1992 (LORTAD), que regula el tratamiento automatizado de datos de carácter personal.

7.2. Corrientes doctrinales más significativas

Como acabamos de señalar, la doctrina española más destacada ha ido intentando desentrañar la previsión del artículo 18.4 de la Constitución española de 1978.

En este sentido, cabe reseñar a Pérez Luño quien bajo la denominación de libertad informática, ha venido considerando una concepción avanzada y de debate actual. Para este autor, este nuevo derecho autónomo va más allá del derecho de la personalidad y, aunque se relaciona con la intimidad, no sólo lo hace con ésta sino también con otros derechos como la identidad, libertad o la igualdad. Asimismo, propugna una lectura conjunta del artículo 18.4 CE y del artículo 105 CE (derecho de acceso a los registros administrativos) conforme al

²⁵¹ GONZÁLEZ MURUA, A. R., *La Agencia Vasca de Protección de Datos y el Estado de las Autonomías...* op. cit., p. 36.

cual se halla la base constitucional para que cualquier persona (individual o colectiva) pueda conocer, acceder, controlar, corregir o destruir los datos personales, todo ello con un apoyo estructural y unas garantías específicas que permiten su existencia efectiva²⁵². Además, este autor basa su construcción en la nueva generación de derechos humanos²⁵³: los de tercera generación²⁵⁴. Influenciado, sin duda, por la Sentencia del Censo de 1983, distingue tres conceptos diferentes: a) libertad informática (facultad de conocimiento, acceso y control de las personas sobre la información que le concierne); b) autodeterminación informativa -*Recht auf informationelle Selbstbestimmung*- (facultad sobre lo que se ha revelado y el uso de los datos); y c) *habeas data*²⁵⁵ (facultad de las personas a conocer y acceder a las informaciones en los bancos de datos, en definitiva, como cauce procesal de salvaguarda de la libertad de las persona en la esfera informática)²⁵⁶. Por último, mientras que el derecho a la libertad informática haría alusión a la esfera subjetiva de la protección de datos, el derecho a la protección de datos correspondería a un marco organizativo del mismo. Para él, ambos son complementarios y necesarios como doble función de los derechos (visión objetiva y subjetiva).

Desde la doctrina, se han señalado algunos problemas de esta teoría tales como su “dependencia” del concepto de intimidad o la disección del nuevo

²⁵² PÉREZ- LUÑO, A. E., “La protección de la intimidad frente a la informática en la Constitución Española de 1978”, *op. cit.*, pp. 69-72.

²⁵³ MARTÍNEZ DE PISÓN, J., *Las generaciones de Derechos Humanos*, Visto en BETEGÓN, J., LAPORTA, F. J., RAMÓN DE PÁRAMO, J. y PRIETO SANCHÍS, L. (Coordinadores), *Constitución y derechos fundamentales*, Ministerio de la Presidencia, Secretaría General Técnica, Centro de Estudios Políticos y Constitucionales, Madrid, 2004, pp. 409-412.

²⁵⁴ PÉREZ LUÑO, A. E., “Las Generaciones de Derechos Humanos”, *Revista del Centro de Estudios Constitucionales*, núm. 10, Septiembre – Diciembre, 1991, pp. 206-210.

²⁵⁵ “En la terminología anglosajona estos derechos son conocidos como *right to know*, *right to access* y *right to correct*. El trío de estos derechos es conocido con el nombre de <<derechos del afectado>>. Niblett ya ha denominado este derecho como *habeas scriptum*. Kirby los ha denominado *golden rule*. G.B.F NIBLETT, *Digital Information and the Privacy Problem*, OECD/ICC series núm.. 2, Paris, 1971, p. 37. Citado por ESTADELLA YUSTE, O, *ibid.*, p, 129, nota 1

²⁵⁶ PÉREZ LUÑO, A. E., “Intimidad y protección de datos personales: Del *habeas corpus* al *habeas data*”. Edición a cargo de Luís García San Miguel Rodríguez-Arango, *Estudios sobre el derecho a la intimidad*, Tecnos, Madrid, 1992, pp. 36-39.

derecho que tiende a subdividirlo. Esta corriente, además, impregnará el derecho latinoamericano permitiendo aflorar al *habeas data*, separándolo del derecho a la protección de datos o colocándolos al mismo nivel²⁵⁷.

Posteriormente, la mayor defensa de la virtualidad de este derecho y su previsión “implícita” de un derecho a la autodeterminación informativa fue defendida por Lucas Murillo de la Cueva. Este autor considera que se trata de un nuevo derecho fundamental que deriva del progreso tecnológico, el cual supera además los derechos previstos en el apartado 18.1 CE (intimidad, honor e imagen) y tutela el pleno ejercicio de los derechos de los ciudadanos. En el año 1990 este autor, y ante la ausencia de desarrollo legislativo en España, sostiene que merced al artículo 10.2 CE, el artículo 18.4 puede ser interpretado conforme al Convenio 108 Y -como hemos podido comprobar anteriormente- en él ya se contienen los principales rasgos del régimen jurídico de este derecho.

Diez años más tarde, la Sentencia núm. 292/2000, del 30 de noviembre -a la que haremos alusión a continuación, recoge la tesis de esta corriente doctrinal, aunque como también a continuación veremos, en posteriores sentencias hay una vuelta a la intimidad.

7.3. Los hitos en la jurisprudencia constitucional en torno al artículo 18.4 de la Constitución española

Tras unas primeras sentencias iniciales en donde el Tribunal Constitucional aborda la cuestión desde la perspectiva única del derecho a la intimidad (Sentencia núm. 110/1984, del 26 de noviembre, Sentencia núm. 142/1993, del 28 de mayo) por primera vez la Sentencia núm. 254/1993, del 18 de agosto alude al concepto de libertad informática. Sin duda alguna, la Sentencia del

²⁵⁷ RODRÍGUEZ MARCANO, E. R., *El derecho a la autodeterminación informativa en Venezuela...*op.cit., pp. 53-61.

Censo alemana y la corriente doctrinal de Pérez-Luño tuvieron un peso decisivo en la argumentación de la misma.

"De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la CE llama "la informática". (F.J 6)

Como se observa, la sentencia no es nada clara. A pesar de que indica esta doble dimensión y contempla la expresión de "libertad informática", luego vuelve de nuevo a la intimidad (la segunda vez como facultad de control de los datos personales de los ciudadanos ante la administración) y acepta las nociones de libertad informática y *habeas data* como garantías de la intimidad frente a la informática²⁵⁸.

En ese sentido, el fundamento jurídico 7 de la Sentencia núm. 254/1993, de 20 de julio de 1993, recoge que La llamada <<libertad informática>> es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*)²⁵⁹, la misma sentencia convierte al Convenio 108 en fuente de interpretación de derecho, específicamente lo

²⁵⁸ Esta sentencia ha sido analizada y criticada dada su poca claridad por la doctrina. Así entre otros: GONZÁLEZ MURUA, A. R., "Comentarios a la STC 254/1993, de 20 de julio. Algunas reflexiones en torno al art. 18.4 de la Constitución y la protección de datos personales", *Revista Vasca de Administración Pública*, núm. 37, pp. 231-270; VILLAVARDE MENÉNDEZ, I., "Protección de datos personales, derecho a ser informado y autodeterminación informática a propósito de la STC 254/1993", *Revista de Derecho Constitucional*, mayo-agosto 1994, pp. 189 a 223.

²⁵⁹ Sentencia núm. 254/1993 del 20 de Julio de 1993.
Disponible en: <https://www.boe.es/boe/dias/1993/08/18/pdfs/T00028-00034.pdf>. (Última consulta en línea 19 de junio 2018).

relacionado al artículo 18.4 de la Constitución donde se establecen límites a la informática para proteger la privacidad²⁶⁰.

Sin ningún tipo de duda la sentencia de mayor calado en materia de protección de datos lo ha constituido la Sentencia núm. 292/2000. Es la primera vez que se reconoce de manera expresa la existencia de un derecho autónomo a la protección de datos que encuentra su sede constitucional en el artículo 18.4 de la Constitución española.

En este sentido su fundamento jurídico quinto recoge:

“La llamada libertad informática” es así derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención...

... Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 C.E., con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 C.E debe limitar el uso de la informática, bien desarrollado el derecho fundamental a la protección de datos (art. 81.1 C.E.), bien regulando su ejercicio (art. 53.1 C.E.). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.”

En este sentido, se podría concluir que se asume la corriente doctrinal de Lucas Murillo de la Cueva. Es más, el propio autor señala años más tarde que, más allá de una disputa conceptual, el derecho a la protección de datos y el derecho a la autodeterminación informativa se identifican en la misma figura y en el mismo contenido²⁶¹.

²⁶⁰ HERNANDO COLLAZOS, I., *Contratos informáticos, derecho informático legislación y práctica*, 1ª ed. Librería Carmelo, San Sebastián, 2009, p. 269.

²⁶¹ LUCAS MURILLO DE LA CUEVA, P., *La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad, en el derecho a la autodeterminación informativa*, dirigido por LUCAS MURILLO DE LA CUEVA, P., y PIÑAR MAÑAS, J. L., Fundación Coloquio Jurídico Europeo, Madrid, 2009, pp. 11-77.

Cuando ya parecía que el derecho a la protección de datos se configuraba como un derecho desvinculado de los derechos de la personalidad -centrado sobre dos piedras angulares: el consentimiento de los titulares y las facultades relativas al acceso y como correlativo la rectificación, cancelación y oposición-, los últimos pronunciamientos del Tribunal Constitucional no han seguido una línea tan sostenida. Es más, las Sentencias núm. 159/2009, de 29 de junio y la Sentencias núm. 173/2011, de 7 de noviembre dan un salto hacia atrás. Las mismas “evidencian la vuelta del TC al tronco común de la intimidad y la confusión nuevamente de ella con el derecho a la protección de datos de carácter personal”²⁶².

Por su parte y más allá del aspecto doctrinal, normativas, sentencias y jurisprudencias españolas en materia de intimidad, protección de datos personales, la Unión Europea (UE) y su predecesora la Comunidad Económica Europea (CEE)²⁶³, realizan ingentes esfuerzos en tejer disposiciones conectadas con sus jurisprudencias, encaminadas a la protección de las personas físicas concerniente al tratamiento de datos personales y su libre circulación, muestra de ello queda expuesto en las próximas líneas.

7.4. Ley Orgánica 5/1992, de regulación del tratamiento automatizado de datos de carácter Personal (LORTAD)

A raíz de la ratificación, firma y publicación en el BOE del Convenio 108 el 15 de noviembre de 1985 por parte de España²⁶⁴ y cumpliendo con las

²⁶² Así lo expresa RODRÍGUEZ MARCANO, E. R., *El derecho a la autodeterminación informativa en Venezuela*. op.cit., p. 107 quién analiza con detención dichas sentencias.

²⁶³ BELLAMY, C. y CHILD, G., *Derecho de la competencia en el mercado común*, 1ª ed. Civitas, S. A., Madrid, 1992, pp. 23-73.

²⁶⁴ “...España ha ratificado el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa. Dicho texto normativo tras su publicación en el BOE de 15 de noviembre de 1985, ha pasado a formar parte de nuestro ordenamiento jurídico. Esta incorporación lejos de suplir el desarrollo legislativo, por vía de Ley Orgánica, del art.18.4 lo hace más apremiante. Ya que con la firma del Convenio europeo nuestro país se comprometía a establecer en su derecho interno los

especificaciones del artículo 22 del Convenio en lo que respeta a la entrada en vigor, España se encaminó a formular o crear una ley que le permitiera asumir el compromiso²⁶⁵ generado a raíz de la ratificación y firma del Convenio; a pesar del compromiso asumido por la ratificación del Convenio 108, no es sino hasta el año 1991 con la adhesión²⁶⁶ al Convenio Schengen cuando España se ve abocada en abordar el tema por sus legisladores tras 14 años de letargos, períodos de incertidumbres y vacíos normativos²⁶⁷ desde la Constitución de 1978²⁶⁸, un proceso tomado sin prisa a pesar del mandato expreso entregado al legislador para que legisle²⁶⁹ en función de lo estipulado en la Constitución y de esta forma regular el uso de la informática, asegurando y garantizando los derechos personales²⁷⁰, es el momento en el cual España se ve obligada a consumir la aprobación de la *Ley Orgánica 5/1992, de 29 de octubre, sobre*

mecanismos jurídicos precisos para hacer efectivos los derechos consagrados en el texto del Consejo de Europa...” PÉREZ LUÑO, A. E., *Panorama general de la legislación española sobre protección de datos*, 1991, p. 25, tomado de IX encuentro implicaciones socio-jurídicas de las tecnologías de la información, CITEMA, España, 1991.

²⁶⁵ Artículo 4. Compromisos de las Partes

1. Cada Parte tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.

2. Dichas medidas deberán adoptarse a más tardar en el momento de la entrada en vigor del presente Convenio con respecto a dicha Parte.

Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447>. (Última consulta en línea 20 de septiembre 2018).

²⁶⁶ MANGAS MARTÍN, A. y LIÑAN NOGUERAS, D. J., *Instituciones y Derecho de la Unión Europea*, 4ª ed. Tecnos, S. A., Madrid, 2004, pp. 82-83.

²⁶⁷ PÉREZ-LUÑO, A. E., *La LORTAD: Entre las luces y las sombras (Conferencia impartida del 14 al 16 de julio de 1993, durante el XXII Curso de Informática y Derecho, celebrado en el Centro Regional de la UNED) visto en CARRASCOSA LÓPEZ, V. (Director), Informática y Derecho 6-7*, 1ª ed. Universidad Nacional de Educación a Distancia, Mérida, Sevilla, 1994, p. 83.

²⁶⁸ FERNÁNDEZ ESTEBAN, M. L., *Nuevas tecnologías, Internet y Derechos Fundamentales*, 1ª ed. Susana Santos Prieto, Madrid, 1998, pp. 127-135

²⁶⁹ LÓPEZ MUÑIZ, M. G., *Los derechos de la persona en la ley de protección de datos personales*, visto en CARRASCOSA LÓPEZ, V. (Director), *Informática y Derecho, II Congreso internacional de Informática y Derecho*, 1ª ed. Universidad Nacional de Educación a Distancia, Mérida, Sevilla, 1996, p. 1305.

²⁷⁰ ULL PONT, E., *Derecho público de la informática, protección de datos...* op. cit., p. 79.

regulación del tratamiento automatizado de datos de carácter personal, conocida por su acrónimo <<LORTAD>>²⁷¹, como hemos comentado, tras el Convenio se obliga a los Estados a crear normas nacionales que garanticen un nivel de protección de datos de carácter personal equivalente a éste, teniendo como último plazo la entrada del Convenio de Schengen²⁷². <<Convenio de aplicación del Acuerdo de Schengen, de 14 de junio de 1985, relativo a la supresión gradual de controles en las fronteras comunes>>, el 19 de junio de 1990 se exige a cada uno de los Estados miembros, que al igual que el Convenio del Consejo de Europa se conserve el mismo nivel requerido y exigido por el Convenio del Consejo de Europa en lo que respecta a la existencia de normas internas sobre protección de datos desprendido de los principios del Convenio del Consejo de Europa²⁷³.

La construcción de la nueva legislación, está llamada a cumplir lo referente al artículo 4 de la Convención (principios básicos) y el artículo 18-4 de la Constitución o ambas propuestas a la vez, el artículo 1 reproduce el artículo 18.4 de la Constitución²⁷⁴, previo a esta.

Es así como la *Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD)* derogada y sustituida por la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)*, fue fruto de un amplio proceso de iniciativas y promoción legislativa iniciadas en el 1976 y culminada

²⁷¹ "...La LORTAD era, en líneas generales, una ley muy proteccionista", visto en BEL MALLÉN, I., CORREDORA y ALFONSO, L. (Coordinadores), *Derecho de la Información*, 1ª ed. ARIEL, S. A., Barcelona, 2003, p. 169.

²⁷² ALMAZARA ALMAIDA, C. (Coordinador), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. LEX NOVA, S. L., Valladolid, 2007, pp. 34-39.

²⁷³ SANTIAGO RIPOL, C. (Coordinador), *La protección de los datos personales: regulación nacional e internacional de la seguridad informática (jornadas organizadas por la Universidad Pompeu Fabra)*, 1ª ed. Generalitat de Catalunya, Catalunya, 1993, p. 60.

²⁷⁴ Con la sentencia 254/93, de 20 de julio el tribunal constitucional, fruto del recurso de amparo 1827/1990, la constitución incorpora una nueva garantía constitucional de otros derechos, fundamentalmente el honor y la intimidad frente a las potenciales agresiones a la dignidad y a la libertad de la persona proveniente de un uso ilegítimo del tratamiento mecanizado de los datos, lo que la constitución llama "la informática".

con la derogación de la ley²⁷⁵ después de varios proyectos, desarrollando por medio al Decreto 1332/1994 de 20 de junio determinados aspectos de la ley²⁷⁶, entre los que se destaca la armonización legislativa estipulada en el Convenio de 1990 (Schengen)²⁷⁷; siendo la primera norma dictada en España en materia de protección de datos, implementando principios y obligaciones en materia de protección de datos²⁷⁸, previo a esta, existía la *Ley Orgánica de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen del 5 de mayo*²⁷⁹, una ley sustituida por la LORTAD en sus aspectos específicos.

Los conceptos de protección de datos de carácter personal, ficheros y tratamientos, se encuentran vivos en la legislación, siguiendo lo estipulado en el Convenio 108, al mismo tiempo, en la exposición de motivos, se presenta una distinción entre la intimidad y la privacidad que transpone de la noción angloamericana de *privacy* americana, derecho a disponer de cualquier aspecto de la personalidad, incluida la información o datos de la persona y de su actividad en cualquier escena²⁸⁰.

²⁷⁵ "...una ley compleja tanto por la variedad de sus contenidos cuanto por la tecnología específica que utiliza", así lo expresa LUCAS MURILLO DE LA CUEVA, P., *Informática y Protección de Datos Personales*, cuadernos y debates, Madrid, 1993, p. 12.

²⁷⁶ Art. 2 Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, "La remisión al Derecho nacional, contenida en los Títulos IV y VI del Convenio de 19 de junio de 1990, de aplicación del Acuerdo de Schengen de 14 de junio de 1985, así como cualquier otra remisión hecha a disposiciones nacionales de protección de datos personales contenida en convenios internacionales, se entenderá referida a la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, y a las disposiciones reglamentarias de desarrollo". Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1994-14121>. (Última consulta en línea 18 de junio 2017).

²⁷⁷ HERNANDO, I., *Contratos informáticos, derecho informático legislación y práctica*, 1ª. ed. Librería Carmelo, San Sebastián, 20009, pp. 257 y 274.

²⁷⁸ CASTAÑEDA GONZÁLEZ, A. (Coordinador), *Derecho tecnológico respuesta legales a nuevos retos*, 1ª ed. Experiencias, S. L, Barcelona, 2004, p. 30.

²⁷⁹ *Ley Orgánica de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen del 5 de mayo*, BOE-A-1982-11196. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-1982-11196>. (Última consulta en línea 23 de agosto 2018).

²⁸⁰ RECALDE DIEZ, J. R., (Presentación), *Informática Judicial y Protección de Datos Personales*, 1ª ed. Servicio Central de Publicaciones del Gobierno Vasco, Vitoria- Gasteiz, 1994, p. 17

Antes y después de la promulgación de la ley, fueron emitidas varias sentencias²⁸¹ relacionadas con aspectos relativos a la protección de datos, infringiendo las disposiciones del Convenio 108 ratificado por España en 1985, sentencias que sirvieron de base para apoyar la promulgación de la actual ley.

La ley contempla ocho exposiciones de motivos, que soportan sus cuarenta y ocho artículos dando origen a la implementación de la ley.

En la misma tesitura, durante el proceso de conformación de la legislación, existieron varias opciones tendentes a la creación de una autoridad capaz de ejercer el control del sistema protector determinado por la ley, entre las alternativas propuestas tenemos a) la creación de una autoridad independiente de los poderes, b) la creación de una autoridad dependiente del Parlamento o del Ejecutivo, c) la autoridad de control estaría bajo el ejercicio de los jueces y los tribunales del Estado, el escenario planteado acarrearía un aumento o carga en los tribunales del Estado u órganos jurisdiccionales, debido a los reclamos existentes en los ficheros privados los archivos públicos utilizarán los procedimientos administrativos, contencioso administrativo; Los órganos jurisdiccionales, serán utilizados al momento de la generación de un daño o perjuicio o una lesión en los derechos del afectado por incumplimiento de la ley; se crea la Agencia de Protección de Datos Personales como órgano de control, fungiendo como filtro de las denuncias realizadas, revestida de capacidad sancionadora.

En el título VI de la LORTAD, se presenta la Agencia de Protección de Datos, con la Sentencia núm. 254/1993 se establece que *“la creación del Registro General de Protección de Datos, y el establecimiento de la Agencia de Protección de Datos, facilitarán y garantizarán el ejercicio de los derechos de información y acceso de los ciudadanos a los ficheros de titularidad pública, y*

²⁸¹ Sentencia del Tribunal Superior de Justicia de Madrid, sala de lo Contencioso-Administrativo, de 13 noviembre de 1991, sentencia núm. 789, Así lo expresa ESTADELLA YUSTE, O., *La Protección de la Intimidad frente a la Transmisión Internacional...op. cit.*, p. 53. nota 48.

además extienden su alcance a los de titularidad privada”; en tal sentido, la protección de datos personales se encuentra resguardada en la Constitución de 1978, recibiendo la influencia de otras normas europeas creadas previamente a la Constitución española de 1978, cuya finalidad es la protección de los datos personales frente a los peligros arrojados por la era informática de ese entonces; Estados como Suecia con su Ley del 11 de mayo de 1973, Alemania con la Ley del 22 de enero de 1977, Francia con su Ley de 1978, y Noruega con su Ley del 8 de junio de 1978, en cada una de ellas se establecieron instituciones especializadas de Derecho público con funciones de control sobre los ficheros de datos personales con posibilidades de ser tocado por los tratamientos automatizados ya sean estos públicos, como privados ²⁸².

La ley a la cual hacemos referencia, deroga la disposición transitoria primera (1) de la Ley Orgánica 1/1982, de 5 de mayo²⁸³ referida a la protección Civil del derecho al honor, la intimidad personal y familiar y a la propia imagen; una ley dispuesta a partir del 29 de noviembre del año 1992, con fecha de publicación del 31 del mismo mes, puesta en vigor a partir del 31 de enero del 1993, tres meses posteriores a su publicación, siendo derogada el 14 de enero del año 2000 por la Ley Orgánica 15/1999 del 13 de diciembre²⁸⁴, de Protección de Datos de Carácter Personal reglamentada en base al Real Decreto 994/1999 del 11 de Junio²⁸⁵, estableciendo el estatuto de la Agencia de Protección de

²⁸² Así lo podemos ver en el Fundamento jurídicos número 8 de la Sentencia núm. 290/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Donde se establecen recursos de inconstitucionalidad contra diversos artículos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_constitucional/common/pdfs/Sentencia290.pdf. (Última consulta en línea 25 de agosto de 2017).

²⁸³ *Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.* Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-1982-11196>. (Última consulta en línea 23 de agosto de 2017).

²⁸⁴ *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.* Disponible en: Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750>. (Última consulta en línea 21 de septiembre 2017).

²⁸⁵ *Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.* Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1999-13967>. (Última consulta en línea 25 de septiembre 2017).

Datos fundamentada en el Real Decreto 428/1993 del 26 de marzo.²⁸⁶ Por su parte, con el Real Decreto 1720/2007, de 21 de diciembre, se aprueba el Reglamento de desarrollo de la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal²⁸⁷.

7.5. Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD)

*La Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal*²⁸⁸, conocida por su acrónimo como <<LOPD>> entró en vigor el 14 de enero de 2000²⁸⁹, es una ley que desde su implementación carece de exposición de motivos, no así el primer proyecto de Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) visto previamente, el cual contiene una breve declaración de motivos referenciado o transpuesto con la Directiva 95/46/CE²⁹⁰; la ausencia de razones o motivos de la referida *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* no

²⁸⁶ *Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.* Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1993-11252>. (Última consulta en línea 23 de agosto 2017).

²⁸⁷ *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.* Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2008-979>. (Última consulta en línea 23 de agosto 2018),

²⁸⁸ *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.* Disponible en: <https://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf>. BOE 298/1999 DE 14-12-1999. (Última consulta en línea 21 de septiembre 2017).

²⁸⁹ VIZCAÍNO CALDERÓN, M., *Comentarios a la ley orgánica de protección de datos de carácter personal*, 1ª ed. Cívitas Ediciones, S. L., Madrid, 2001, p. 37, también ALMAZARA ALMAIDA, C. (Coordinador), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. LEX NOVA, S.L, Valladolid, 2007, p. 44

²⁹⁰ Proyecto de Ley 121/000135 publicado en el BOCG de 31 de agosto de 1999, serie A, n.º 135.1, referenciado por FREIXAS GUTIÉRREZ, G., *La protección de los datos de carácter personal en el derecho español*, 1ª ed., Bosch, Barcelona, 2001, p.83, nota 140. Igual opinión presenta VIZCAÍNO CALDERÓN, M., *Comentarios a la ley orgánica de protección de datos de carácter personal*, 1ª ed. Cívitas Ediciones, S.L, Madrid, 2001, p. 37.

permite asumir las pautas que dieron origen al legislador para su elaboración, en sus inicios la ley fue redactada para reformar la LORTAD sin perseguir la redacción de una nueva norma, pero debido a la gran cantidad de enmiendas fue necesario crear o proponer un nuevo marco legal cuyo objetivo sería la derogación de la norma anterior²⁹¹; por su parte, la ley reconoce como datos de carácter personal a cualquier información concerniente a personas físicas identificadas o identificables²⁹².

Es importante tener en consideración que la Ley 15/1999 (LOPD) es una ley nacional del Estado español, originada luego de la promulgada *Directiva 95/46 (CE), de 28 de enero de 1981, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos de la comunidad europea*, que ha justificado la publicación de la LOPDCP, derogando la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal²⁹³; la Ley 15/1999 contiene la mayoría de los preceptos de la derogada LORTAD, debido a que su propuesta de creación data de fecha 18 de julio de 1990²⁹⁴, ajustándose a un alto porcentaje los aspectos de la Directiva, sin descartar las modificaciones sustanciales que ofrece la LOPDCP²⁹⁵, es importante señalar y acotar que a raíz de la aprobación de la Directiva 95/46 del 24 de octubre de 1995, se hace necesario aportar una nueva reforma al ordenamiento jurídico en

²⁹¹ ALMAZARA ALMAIDA, C. (Coordinador), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. Editora LEX NOVA, S. L., Valladolid, 2007, p. 44. También lo expresa ULL PONT, E., *Derecho público de la informática, protección de datos...* op. cit., p. 115.

²⁹² Artículo 3, apartado a), de la LOPD.

²⁹³ GARCÍA LAJARA, E. C., *Protección de datos de Carácter Personal*, 1ª ed. editorial Comares, Granada, 2000, p. 126. Igual opinión presenta VIZCAÍNO CALDERÓN, M., *Comentarios a la ley orgánica de protección de datos de carácter personal*, 1ª ed. Cívitas Ediciones, S.L, Madrid, 2001, p. 25.

²⁹⁴ FREIXAS GUTIÉRREZ, G., *La protección de los datos de carácter personal en el derecho español*, 1ª ed. Bosch, Barcelona, 2001, p.71.

²⁹⁵ “la Ley Orgánica 5/1992 se promulgó para proteger la privacidad poniendo límites al uso de la informática y otras técnicas de tratamiento automatizado de los datos de carácter personal. La nueva Ley de 1999, que deroga la anterior, extiende la protección frente a cualesquiera ficheros o tratamientos, sean o no automatizados” así lo expresa VIZCAÍNO CALDERÓN, M., *Comentarios a la ley orgánica de protección de datos de carácter personal*, 1ª ed. Cívitas Ediciones, S. L., Madrid, 2001, p. 25.

materia de protección de datos capaz de incluir las disposiciones de la Directiva 95/46 (CE), materializado en la LOPD convirtiendo a España en uno de los países más exigentes y completo que garanticen el derecho a la protección de datos²⁹⁶.

El primer proyecto de la LORTAD fue sometido a varios recursos de inconstitucionalidad²⁹⁷, entre ellos, el Defensor del Pueblo, el Parlamento y el Gobierno de Cataluña y los diputados del Partido Popular; a raíz de la Sentencia STC-290 de 30 de noviembre, se declara la pérdida sobrevenida del objeto del recurso interpuesto de inconstitucionalidad, a raíz de la derogación de la ley, continuando los recursos en la ley que sobreviven, dígase la LOPDCP.

La Ley Orgánica 15/1999, tiene por objeto garantizar y proteger en lo que concierne a tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar como lo expresa su artículo 1, a diferencia del artículo 1 de la LORTAD, que desarrolla el capítulo 18,4 de la Constitución española, limitando el uso de la informática y medios de tratamientos automatizados de los datos de carácter personal para proteger derechos, tales como la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos, modificando su objeto que no es el de limitar²⁹⁸.

²⁹⁶ CASTAÑEDA GONZÁLEZ, A. (Coordinador), *Derecho Tecnológico respuesta legales a nuevos retos*, 1ª ed. Experiencias, S. L, Barcelona, 2004, p. 30.

²⁹⁷ De manera sucinta presentamos los recursos de inconstitucionalidad acumulados y reflejados en la STC 290/2000. Estos son 201/93, 219/93, 226/93 y 236/93, interpuestos respectivamente por el Consejo Ejecutivo de la Generalidad de Cataluña, el Defensor del Pueblo, el Parlamento de Cataluña y por don Federico Trillo-Figueroa Conde, Comisionado por 56 Diputados del Grupo Parlamentario Popular, contra los arts. 6.2, 19.1, 20.3, 22.1 y 2.1, 24, 31, 39.1 y 2, 40.1 y 2, y Disposición final tercera de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Ha comparecido y alegado el Abogado del Estado. Ha sido Ponente el Magistrado don Julio Diego González Campos, quien expresa el parecer del Tribunal. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-T-2001-330>. Publicado en: «BOE» núm. 4, de 4 de enero de 2001. Referencia: BOE-T-2001-330. (Última consulta en línea 25 de agosto 2017).

²⁹⁸ GARCÍA LAJARA, E. C., *Protección de datos de carácter personal*, 1ª ed. Comares, Granada, 2000, p. 4.

La ley está compuesta por cuarenta y nueve artículos, distribuidos en siete títulos, con seis disposiciones adicionales, tres transitorias, una derogada con tres disposiciones finales, sin contar como ya hemos comentado de exposición de motivos o considerandos para su creación.

La Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), presenta aspectos destacables, no contemplados en la Ley Orgánica sobre regulación del tratamiento automatizado de datos de carácter personal (LORTAD), como son la inclusión de los ficheros manuales estructurados, la variación del ámbito de aplicación (ámbito geográfico) el cual incluye a las personas fuera del territorio español, cuando debido al tratamiento de las informaciones utilice medios situados en territorio español y por ende, le sea aplicada la legislación española a raíz del Derecho internacional público, al mismo tiempo, se reduce la cantidad de fichero de cinco a tres, se aumentan el número de definiciones incluyendo el encargado del tratamiento, se inserta el principio de finalidad de forma que sea determinada, explícita y legítima, se amplían el cumplimiento de las obligaciones del responsable del fichero cuando se encuentre fuera del territorio de la Unión Europea, proveyendo un domicilio concreto en territorio español, se refuerza el tema del consentimiento el cual debe ser inequívoco; en el tema de los datos sensibles se incluye la afiliación sindical, se inserta la figura del encargado del tratamiento a diferencia del responsable del tratamiento, se incluye el derecho de oposición como nuevo derecho solicitado por los titulares de los datos, fija un plazo máximo de seis meses para que la Agencia de Protección de Datos²⁹⁹ solucione los planteamientos realizados por los interesados, posibilita la creación de códigos tipos de carácter deontológico, se concretan los requisitos para las transferencias internacionales a terceros países que debe ser considerado por la Agencia Española de Protección de Datos, no significando que las mejoras creadas la conviertan en una norma exenta de errores y deficiencias

²⁹⁹ Actualmente Agencia Española de Protección de Datos.

consideradas por las doctrinas y los expertos en la materia que la han analizado³⁰⁰.

Las normas analizadas reciben los influjos de los reales decretos emitido por el Estado español, modificando y adaptando las normas legislativas, una especie de *mutatis mutandis*, es así como el Decreto 1332/1994 desarrolla aspectos de la Ley Orgánica 5/1992 del 29 de octubre, el Decreto 428/1993 aprueba el estatuto de la Agencia Española de Protección de Datos³⁰¹ y el Real Decreto 994/1999 del 11 de junio, que establece el Reglamento de medidas de seguridad de los ficheros automatizados que posean datos de carácter personal, para evitar <<el acceso, la modificación o la difusión no autorizadas>> como su destrucción accidental³⁰², el mismo decreto es aplicable a los archivos no automatizados³⁰³.

7.6. Proyecto y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)

Se ha de señalar, que a pesar de estar delante de un Reglamento que no necesita trasposición³⁰⁴, se observa en los Estados de la Unión la creación de

³⁰⁰ ALMAZARA ALMAIDA, C. (Coordinador), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. LEX NOVA, S.L, Valladolid, 2007, pp. 45-49.

³⁰¹ La Agencia de Protección de Datos de la Comunidad de Madrid fue creada en el año 2001, seguida de Cataluña en el año 2002 y la del País Vasco en el año 2004 tomado de PÉREZ GÓMEZ, E. y CRESPO LÓPEZ, A., *La protección de datos en los centros de...* op. cit., p. 30.

³⁰² ULL PONT, E., *Derecho público de la informática, protección de datos...* op. cit., p. 57.

³⁰³ PÉREZ GÓMEZ, E. y CRESPO LÓPEZ, A., *la protección de datos en los centros de...* op. cit., p. 29.

³⁰⁴ "...debe entenderse en el marco del Derecho comunitario en el que el Reglamento es norma de alcance general, obligatoria en todos sus elementos y directamente aplicable en cada Estado miembro. Es una norma que se integra en el ordenamiento jurídico nacional sin necesidad de transposición alguna desplegando su eficacia directa...en base a esta eficacia directa.....lejos de garantizar una regulación uniforme del derecho fundamental a la protección de datos.....condujo a una enorme fragmentación normativa que acarreó diferencias sostenibles en el nivel de protección de los datos de carácter personal entre los distintos Estados. Deficiencias e insuficiencias que ...no permitieron hacer frente a los nuevos retos que planteaba la imparable e incisiva evolución tecnológica y la globalizaciónlos ciudadanos y los operadores jurídicos no pueden interpretar y aplicar el contenido de la nueva LOPDyGDD si

normas legislativas internas al Reglamento, ejemplo de ello queda expuesto en España con el proyecto de Ley Orgánica de Protección de Datos de Carácter Personal publicado en el Boletín Oficial de las Cortes Generales de 24 de noviembre de 2017 (actual Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales)³⁰⁵; estamos delante de una ley sustituta de la vigente 15/1999 de 13 de diciembre, fruto de la dificultad de aplicación del Reglamento, conduciendo a los Estados a crear sus propias leyes nacionales de adecuación³⁰⁶ e interpretación de las normas del Reglamento, a raíz de tales decisiones, algunos autores consideran que tenemos de frente a una normativa localizada entre un Reglamento y una Directiva³⁰⁷, otros entienden como un error la instauración de leyes nacionales o más bien, la creación de normativas de adaptación del Reglamento, situación del caso español³⁰⁸, ya que la nueva legislación nacional española en materia de protección de datos, no debe bajo ninguna circunstancias reemplazar un Reglamento y más en el caso español, cuya nueva ley entraría en vigor meses posteriores a la implementación del Reglamento, a pesar de ser concebida su entrada antes del 25 de mayo de 2018, propuesta definitiva de la entrada del

no se tiene presente que..... adapta y complementa lo que el propio RGPD les exige...el RGPD ha dejado a los Estados un considerable margen de actuaciónel RGP es una norma que revista de gran complejidad.....tiene 56 remisiones.....para los Estados miembros.....". visto en ARENAS RAMIRO, M., ORTEGA GIMÉNEZ, A. (Directores), *Protección de Datos...op, cit., pp. 11-13.*

³⁰⁵ *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-16673. (Última verificación en línea 26 de julio 2019).

³⁰⁶ "...los reglamentos, pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de "desarrollo" o complemento de la Unión Europea". ARENAS RAMIRO, M., ORTEGA GIMÉNEZ, A. (Directores), *Protección de Datos...op, cit., p. 38.*

³⁰⁷ RALLO, A., *El impacto del Reglamento Europeo de Protección de datos en España*, mesa redonda Análisis comparado del impacto del RGPD en los Estados miembros, Congreso Internacional sobre el Impacto del Reglamento Europeo de Protección de Datos: análisis nacional y comparado, Universitat Jaume I, Castellon, 17 y 18 de mayo de 2018.

³⁰⁸ GARCÍA MAHAMUT, R., *discurso Inaugural, Congreso Internacional sobre el Impacto del Reglamento Europeo de Protección de Datos: análisis nacional y comparado*, Universitat Jaume I, Castellon, 17 y 18 de mayo de 2018.

Reglamento³⁰⁹ restándoles sentido a la propia ley, ya que al momento de su implementación, el Reglamento habrá creado jurisprudencias y transformaciones internas en los Estados.

Por su parte, estamos al frente de una doble regulación³¹⁰, dos disposiciones garantista de la protección de datos de carácter personal reconocida en el artículo 18.4 de la Constitución española, una de ella compuesta por el *Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos*, como lo establece el apartado 2 del artículo uno de la Ley Orgánica que adapta el ordenamiento jurídico español al Reglamento y la otra, conformada por el proyecto de *Ley Orgánica Española de Protección de Datos* convertido en ley.

El proyecto de *Ley Orgánica Española de Protección de Datos*³¹¹ antesala de la Ley Orgánica 3/2018, la componen setenta y ocho artículos, distribuidos en nueve títulos con trece disposiciones adicionales, cinco transitorias, una derogatoria y cuatro finales, planificada para entrar en vigencia a partir del 25 de mayo de 2018, fecha de entrada del *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 24 de octubre de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. El proyecto de ley tiene como autor al Gobierno español, contemplado en la XII legislatura del 24 de noviembre de 2017 existente en el Boletín Oficial de las Cortes Generales del

³⁰⁹ Consejo de ministros., *Informe sobre el anteproyecto de ley de protección de datos para adaptarla al reglamento comunitario*, Secretaria de Estado de Comunicación, 23 de junio de 2017, p. 12. Disponible en: <http://www.lamoncloa.gob.es/consejodeministros/referencias/documents/2017/refc20170623.pdf#page=12>. (Última consulta en línea 15 de Julio 2018).

³¹⁰ PLAZA PENADÉS, J., “El proyecto de la nueva ley orgánica de protección de datos de carácter personal”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, Enero-Abril, p. 15.

³¹¹ Cfr. “...consta de setenta y ocho artículos estructurados en nueve títulos, diecisiete disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y cinco disposiciones finales”, Congreso de los diputados., *Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal*, XII Legislatura, Boletín oficial de las cortes generales, 24 de noviembre de 2017, p. 7.

Congreso de los Diputados, adoptando la mesa de la Cámara, el acuerdo del proyecto de *Ley Orgánica de Protección de Datos de Carácter Personal* encomienda el dictamen a la Comisión de Justicia y ordena su publicación.

El proyecto fue sometido a cambios y transformaciones en el Congreso de los Diputados, inserta la garantía de los derechos digitales³¹² incorporadas a finales de septiembre de 2018 y adiciona los artículos 79 a 97³¹³ cambiando el nombre del proyecto de *Ley Orgánica Española de Protección de Datos* por el de *Ley Orgánica de Protección de Datos y garantía de derechos digitales* conocida como LOPDyGDD. En igual contexto, incrementa las disposiciones adicionales del proyecto de 13 a 22, las transitorias de 5 a 6, las finales de 4 a 16, y mantiene igual las disposiciones derogatorias.

Ante esa situación, la Ley Orgánica 3/2018 procura garantizar derechos digitales en la esfera del Internet, las comunicaciones, el ámbito laboral, la seguridad, la educación, los menores, la negociación colectiva, olvido, portabilidad, testamento y las políticas de impulso entre otros³¹⁴. Una situación que escapa la esfera de la protección de datos comúnmente contemplada en el Reglamento y las pasadas normas españolas LOPD y LORTAD. Incluye aquellas garantías conectadas con los derechos digitales, jugando un rol más global y preponderante haciendo suya las tecnologías digitales. Complementando el Reglamento de acuerdo a lo dispuesto en el artículo 1 de la ley.

En tal sentido, el Reglamento tutela los datos personales, situación no limitativa en la Ley Orgánica 3/2018, ampliando su rango de acción con la garantía de

³¹² Artículo 1, literal b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución. *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-16673. (Última verificación en línea 26 de julio 2019).

³¹³ ARENAS RAMIRO, M., ORTEGA GIMÉNEZ, A. (Directores), *Protección de Datos...op, cit.*, p. 13.

³¹⁴ ARENAS RAMIRO, M., ORTEGA GIMÉNEZ, A. (Directores), *Protección de Datos...op, cit.*, pp. 337-409.

los derechos digitales, más allá de la tutela de la protección de datos contemplada en las pasadas leyes españolas y el Reglamento, aumentando su espectro, acogiendo una cantera o catálogo de derechos digitales.

8. Jurisprudencias europeas en materia de protección de datos

8.1. Preámbulo

La Unión Europea y la pasada Comunidad Europea contemplan sentencias conectados con la protección de datos³¹⁵, a pesar de ello es importante aclarar que, durante el período de la comunidad europea, no existía un derecho autóctono de la protección de datos, pero si se daban los primeros pasos conectados con el derecho a la vida privada. En este acápite, presentamos dos de las principales sentencias a nivel de la Unión Europea³¹⁶ que impactan y revolucionan las normas existentes en materia de protección de datos y transferencias internacionales, sentencias novedosas y con altos niveles de

³¹⁵ “STJCE de 12 de noviembre de 1969, caso *Stauder*. En este caso, el ciudadano alemán argumentaba que revelar su nombre y su condición económica iba en contra de la dignidad personal, además de señalar que revelar el nombre a vendedores no era compatible con los principios generales del derecho comunitario. El TJCE desestima la demanda argumentando que los Estados tenían cierto “margen de apreciación” para interpretar en este caso la Decisión cuestionada y en este supuesto no se perjudicaba ningún derecho fundamental..... STJCE de 7 de noviembre de 1985, caso *Stanley George Adams* donde el TJCE desestima una demanda, en la que se solicitaba la anulación de una Decisión sobre prácticas anticompetencia en las que se desvelaba el nombre del demandante –cesión y divulgación de datos-, pues no queda probada una relación directa entre el perjuicio y lo previsto en la Decisión)..... o la STJCE de 7 de octubre de 1987, caso *Strack*, donde el TJCE desestima la demanda -sin entrar sobre el acceso a los datos personales- en la que se había denegado a la viuda de un funcionario el acceso al expediente personal del mismo, por encontrarse en él datos médicos que para solicitarlos se tenía que haber seguido un procedimiento especial que no se siguió....la STJCE de 26 de junio de 1980, caso *National Panasonic*, donde por primera vez se reconoce el derecho a la vida privada y la STJCE de 21 de noviembre de 1989, caso *Hoechst*, en el que se cuestiona que las personas jurídicas puedan ser titulares del derecho a la vida privada.... STJCE de 27 de abril de 1994, caso *X. vs. Comisión, y Conclusiones del Abogado General van Gerven*, donde el TJCE tuvo por primera vez en cuenta el consentimiento del titular de los datos”. GONZÁLEZ MURUA, A. R., *Unión Europea y protección de datos personales*, Grupo de Investigación G1184 "Derechos Fundamentales y Unión Europea", 2010, pp. 20-30.

³¹⁶ Sentencia C-131/12 *Google Spain, S.L., Google Inc./ Agencia Española de Protección de Datos, Mario Costeja González*, Sentencia C-362/14 *Maximiliano Schrems/Data Protection Commissionery*.

impacto en Europa y el mundo³¹⁷, con incidencia y alcance a escala global producto a 1) los actores envueltos, 2) resultados de la sentencia, 3) impacto en los Estados y 4) la magnitud económica envuelta en los casos cuyos resultados contribuyen y formarán parte de las nuevas normativas jurídicas Internacionales.

Ambas sentencias (Unión Europea) contienen las conclusiones del Abogado General y las opiniones del Tribunal de Justicia (Gran Sala) no siendo vinculantes las decisiones entre ellas³¹⁸, los casos mencionados son el producto de las remisiones prejudiciales planteadas³¹⁹ por la Audiencia Nacional al órgano instituido por el Derecho Comunitario para conocer estas cuestiones, tal como lo establece el Tratado de Funcionamiento de la Unión Europea (TFU)³²⁰, asignándole competencia al Tribunal de Justicia de la Unión Europea para conocer esos tipos de cuestiones, permitiendo al Tribunal de Justicia interpretar el Derecho de la Unión o la posibilidad de validar un acto de la Unión ante las dudas interpretativas de los artículos de su Directiva 95/46/CE

³¹⁷ “esta sentencia sobre derecho al olvido marca un hito en la historia de la jurisprudencia del Tribunal de Justicia de la UE en materia de derecho de protección de datos personales. Marcará sin duda un antes y un después...Google ha formado un Comité de expertos para valorar las cuestiones sobre derecho al olvido, habiendo recibido más de 40.000 peticiones relativas a la cancelación de datos en el buscador en cuestión de semanas”, ÁLVAREZ CARO, M., “Reflexiones sobre la sentencia del TJUE en el asunto Mario Costeja (C-131/12) sobre derecho al olvido”, *Revista española de Derecho Europeo*, Thomson Reuters, núm. 51, Julio-Septiembre 2014, p. 186.

³¹⁸ PIÑAR MAÑAS, J. L. y RECIO GAYO, M., *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, 1ª ed. Wolters Kluwer España, S. A., Madrid, 2018., p. 201.

³¹⁹ La primera remisión prejudicial corresponde al caso C-131/12 surge a raíz de la interposición de recursos ante la Audiencia Nacional por Google Spain y Google Inc., solicitando nulidad de la resolución de la AEPD, planteando el tribunal unas series de cuestiones prejudiciales al Tribunal de Justicia. La segunda remisión prejudicial corresponde al caso C-362/14 surge a raíz de la interposición de recursos ante la Audiencia Nacional por la High Court of Ireland (Tribunal Supremo Irlandés) planteando el tribunal unas series de cuestiones prejudiciales al Tribunal de Justicia.

³²⁰ Artículo 267, Tratado de Funcionamiento de la Unión Europea (TFU), Versión consolidada del tratado de Funcionamiento de la Unión Europea, 2010. Disponible en: <https://www.boe.es/doue/2010/083/Z00047-00199.pdf>. (Última consulta en línea 8 de marzo 2018).

y la Carta de los Derechos Fundamentales de la Unión Europea, en especial, el destinado a la protección de datos de carácter personal³²¹.

8.2. Google Spain, SL y Google Inc., STJUE de 13 de mayo 2014 C-131/12)³²²

Los actores envueltos en la sentencia son el Sr. Mario Costeja González de nacionalidad española, la Agencia Española de Protección de Datos (AEPD), La *Vanguardia Ediciones* S. L, Google Spain, S. L, Google Inc., y el Abogado General Jaaskinen³²³.

Todo inicia con una reclamación³²⁴ del Sr. Mario Costeja González a raíz de una versión electrónica del periódico online, donde afirmaba que al colocar sus datos en la red aparecía una referencia a un embargo ya solucionado, carente de relevancia y resuelto desde hace años, la editora argumentó que debido a ser autorizada por el Ministerio de Trabajo y Asuntos Sociales español no se cancelaría, el Sr. Mario Costeja González solicitó un escrito a Google Spain para que no aparecieran los resultados de la búsqueda e Interpuso una reclamación ante la Agencia Española de Protección de Datos (AEPD), la AEPD vía resolución del 30 de Julio de 2010³²⁵ desestima la reclamación por entender que se había realizado vía y conforme al Ministerio de Trabajos y Asuntos Sociales, y a su vez, estima la reclamación contra Google Spain y

³²¹ Artículo 8, de la Carta de los Derechos Fundamentales de la Unión Europea. Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003>. (Última consulta en línea 21 de abril 2018).

³²² PIÑAR MAÑAS, J. L. y RECIO GAYO, M., *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, 1ª ed. Wolters Kluwer España, S. A., Madrid, 2018, pp. 125-134.

³²³ PLAZA PENADÉS, J., “El nuevo modelo de protección de datos personales europeos y el modo de obtener un consentimiento lícito,” *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 44, Mayo-Agosto 2017, p. 18.

³²⁴ Se remonta al 5 de marzo de 2010.

³²⁵ PLAZA PENADÉS, J., “Doctrina del Tribunal de Justicia de la Unión Europea sobre protección de datos y derecho al olvido”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 35, Mayo-Agosto 2014, p. 18.

Google Inc. Interponiendo estos un recurso de nulidad de la resolución de la AEPD ante la Audiencia Nacional, la cual interpone una acción prejudicial planteando diversas preguntas al Tribunal de Justicia.

A raíz de la remisión, el Abogado General después de analizar el asunto presenta sus conclusiones el 25 de junio del 2013 donde por medio a ella, *entiende que:*

“1) la normativa nacional en materia de protección de datos es de aplicación a un proveedor de un motor de búsqueda cuando este establece en un estado miembro, a fines de proveer y vender espacios publicitarios en su motor de búsqueda, una oficina que orienta su actividad hacia los habitantes de dicho estado. 2) una autoridad nacional de protección de datos no puede requerir a un proveedor de servicios de motor de búsqueda en Internet que retire información de su índice, salvo en los presupuestos en que el proveedor de servicios no ha respetado los códigos de exclusión o en los que no se ha dado cumplimiento a una solicitud emanada de la página Web relativa a la actualización de la memoria oculta. 3) la Directiva no establece ningún <<derecho al olvido>> generalizado, por tanto, no puede invocarse tal derecho frente a proveedores de servicios de motor de búsqueda sobre la base de la Directiva, aun cuando ésta se interpreta con arreglo a la Carta de los Derechos Fundamentales de la Unión Europea.”³²⁶.

El Abogado General entiende que debido a la Directiva no se puede restringir o colocar fin a la difusión de datos personales que pudieran considerarse lesivos o contrarios a sus intereses, como también solicitar la eliminación de información legítima a los proveedores de motores de búsquedas, convirtiéndose en una injerencia a la libertad de expresión del editor, siendo considerado como una censura del contenido publicado realizada por un particular.

Por su lado, el Tribunal de Justicia dicta sentencia el 13 de mayo de 2014, entendiendo:

³²⁶ *Comunicado de prensa n.º 106/15*, Luxemburgo, 23 de septiembre de 2015. Disponible en: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077es.pdf>. (Última consulta en línea 20 de octubre 2017).

“que el gestor de un motor de búsqueda en Internet es responsable del tratamiento que aplique a los datos de carácter personal que aparecen en las páginas Web publicadas por terceros”³²⁷. La sentencia aplica para todas aquellas plataformas tecnológicas que realizan actividades de tratamiento de datos personales³²⁸.

8.3. SCHREMS, STJUE de 6 de octubre de 2015 (C-362/14)

Antes de abordar la Sentencia SCHREMS, nos interesa de sobremanera dar una pincelada a la Sentencia Lindqvist³²⁹ del TJUE de 6 de noviembre³³⁰ de 2003 relacionada con el caso Bodil Lindqvist, donde se acusa a la Sra. Lindqvist de publicar datos en Internet correspondientes a los integrantes de una parroquia de Suecia. Situación por la que se elevó una cuestión prejudicial ante el TJUE para conocer si la acción ejecutada por la Sra. Lindqvist puede ser considerada una transferencia de datos a países terceros, el TJUE después de analizar el caso emite su sentencia no considerándolo como tal³³¹, la decisión es muy preponderante en estos tiempos y más cuando las personas utilizan las nubes como medio de almacenamiento, ubicadas en servidores localizados en diferentes Estados, incluidos los terceros países, la decisión permite no considerar esos almacenamientos como transferencias internacionales de datos, haciendo más expedito el proceso de almacenamiento en las nubes y

³²⁷ Comunicado de prensa n.º 117/15, Luxemburgo, 6 de octubre de 2015. Disponible en: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070es.pdf>. (Última consulta en línea 24 de octubre 2017).

³²⁸ PLAZA PENADÉS, J., “Doctrina del Tribunal de Justicia de la Unión Europea sobre protección de datos y derecho al olvido”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 35, Mayo-Agosto 2014, p. 19.

³²⁹ PIÑAR MAÑAS, J. L. y RECIO GAYO, M., *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, 1ª ed. Wolters Kluwer España, S. A., Madrid, 2018, pp. 39-40.

³³⁰ Sentencia del TJUE de 6 de noviembre de 2003, Bodil Lindqvist, C-101/01, EU: C:2003:596. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN> (Última consulta en línea 24 de octubre 2019).

³³¹ DURÁN CARDO, B., *La figura del responsable en el derecho a la protección de datos...* op. cit., pp. 382-383.

empleo del Internet, contribuyendo con la masificación de los servicios utilizados en el Internet situación de la World Wild Web.

El próximo caso se refiere a la Sentencia Schrems del 6 de octubre de 2015, donde se anula la decisión 2000/520 de la Comisión por medio a la cual se reconoce y declara a los Estados Unidos de Norte América como puerto seguro (Safe Harbour) facultando las transferencias internacionales a EEUU, con capacidad de proteger los datos de los ciudadanos europeos transferidos al espacio de los Estados Unidos³³².

Los actores envueltos en la sentencia son el Sr. Maximillian Schrems, la High Court of Ireland (Tribunal Supremo Irlandés), Data Protection Commissioner Facebook, Edward Snowden, Estados Unidos, Servicios de Información de Estados Unidos como la National Security Agency (NSA).

Producto a las revelaciones de las actividades de los Servicios de Información (la National Security Agency o <<NSA>>³³³) de los Estados Unidos por el Sr. Edward Snowden, incluida las informaciones que el Sr. Maximillian Schrems ciudadano australiano había proporcionado a Facebook y estos datos transferidos a Estados Unidos desde la filial irlandesa para su conservación, las revelaciones de los datos confirman que Estados Unidos no garantiza u ofrece una supervisión real de los datos transferidos a sus servidores desde otros Estados, el Estado Irlandés, sustentado en la Decisión de la Comisión del 26 de Julio de 2000 donde designa y reconoce a los Estados Unidos como país signatario y garante de un nivel adecuado de protección de los datos personales trasferidos hacia su territorio, decide a través de la High Court of Ireland (Tribunal Supremo Irlandés), elevar una cuestión prejudicial para determinar si es posible suspender la transferencia de datos denunciada.

³³² Cfr. GARCÍA DE PABLOS, J. F., "La transferencia de datos fuera de la Unión Europea", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 40, Enero-Abril 2016, pp. 27-49.

³³³ Las empresas ligadas con el programa de espionaje PRISM, eran poseedoras de la certificación Safe Harbour reforzando con el hecho la sentencia de SCHREMS y por ende la decisión tomada por la Comisión en base a la solicitud del Parlamento.

A raíz de la consulta planteada, *el Abogado General Yves Bot*.

“considera la decisión de la Comisión por la cual declara que un país tercero garantiza un nivel adecuado de los datos personales transferidos por lo que no puede anular, ni tan siquiera reducir las facultades que tienen las autoridades nacionales de control en virtud de Directiva sobre el tratamiento de datos personales es nula; por lo que la decisión de la Comisión en por la que se declara el carácter adecuado de la protección de los datos personales en Estados Unidos, no impide que las autoridades nacionales suspendan la transferencia de datos de los usuarios europeos de Facebook a servidores situados en Estados Unidos”³³⁴.

En ese sentido, el Tribunal de Justicia de la Unión Europea.

“Declara inválida la Decisión de la Comisión que a su vez declaró que Estados Unidos garantiza un nivel de protección adecuado de los datos personales transferidos, estableciendo que la Comisión carecía de competencia para restringir de este modo las facultades de las autoridades nacionales de control”³³⁵.

Con la sentencia.

“la autoridad de control irlandesa está obligada a examinar la reclamación del Sr. Schrems con toda la diligencia exigible y, al término de su investigación, deberá decidir si, en virtud de la Directiva, debe suspenderse la transferencia de los datos de los usuarios europeos de Facebook a Estados Unidos porque ese país no ofrece un nivel de protección adecuado de los datos personales”³³⁶.

En ese sentido, las empresas ligadas con el programa de espionaje PRISM³³⁷, eran poseedoras de la certificación Safe Harbour, reforzando con el hecho el fallo de la

³³⁴ *Comunicado de prensa n.º 77/13*, Luxemburgo, 25 de junio de 2013. Disponible en: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077es.pdf>. (Última consulta en línea 21 de octubre 2017).

³³⁵ *Comunicado de prensa n.º 70/14*, Luxemburgo, 13 de mayo de 2014. Disponible en: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf>. (Última consulta en línea 30 de octubre 2017).

³³⁶ *Comunicado de prensa n.º 70/14*, Luxemburgo, 13 de mayo de 2014. Disponible en: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf>. (Última consulta en línea 30 de octubre 2017).

³³⁷ MÁRQUEZ, W., *Lo que Snowden ha revelado hasta ahora del espionaje de EE.UU.*, BBC NEWS, 2 JULIO 2013. Disponible en: https://www.bbc.com/mundo/noticias/2013/07/130702_eeuu_snowden_revelaciones_espionaje_wbm. (Última consulta en línea 29 de octubre 2019).

Sentencia de SCHREMS y por ende la decisión tomada por la Comisión en base a la solicitud del Parlamento.

Por tanto, la sentencia deja en evidencia las facultades asignadas y otorgadas a los Estados vía sus autoridades internas, al considerar o decidir acerca de la viabilidad o posibilidad de que sus autoridades nacionales puedan ejecutar transferencia de datos a terceros Estados, independiente de las decisiones establecidas previamente por la Comisión para esos Estados, sustentados en las facultades establecidas en la Carta, la Directiva o su actual Reglamento, en definitiva, sus normas comunitarias para con sus autoridades nacionales, estableciendo para ello la posibilidad de solicitar una cuestión prejudicial vía sus tribunales³³⁸.

La sentencia suscitó la posibilidad de riesgos en las relaciones comerciales entre Estados Unidos y la Unión Europea, propiciando un desasosiego en sus vínculos políticos. Una situación que a nuestro entender se aboca en la decisión de una salida política entre la Comisión y el Gobierno de EEUU vía la creación o el establecimiento de un marco regulatorio, nos referimos al UE-EEUU Privacy Shield aprobado el 12 de Julio de 2016³³⁹, sustentado en la Decisión (UE) 2016/1250 de la Comisión, instaurando un sistema de autocertificación apoyado en principios y compromisos asumidos vía sus cartas, situación ampliada en próximos capítulos. Por el momento pasamos a

³³⁸ “El TJUE estima que la existencia de una Decisión de la Comisión Europea que declara que un país tercero garantiza un nivel de protección adecuado de los datos personales transferidos no puede dejar sin efecto ni limitar las facultades de las que disponen las autoridades nacionales de control en virtud de la Carta de los Derechos Fundamentales de la UE y de la Directiva 95/46/Ce. Incluso ante una decisión de la CE, las autoridades nacionales de control ante las que se haya presentado una solicitud, deben poder apreciar con toda independencia si la transferencia de los datos de una persona a un país tercero cumple las exigencias establecidas por la Directiva, suspender en su caso la transferencia y dirigirse a los tribunales para que planteen una cuestión prejudicial”, ÁLVARE CARO, M. y RECIO GAYO, M., “La declaración de invalidez del Acuerdo Puerto Seguro entre la UE y los EEUU por el TJUE (C-362/14)”, *Revista española de Derecho Europeo*, editora Thomson Reuters, núm. 57, Enero-Marzo 2016, p. 135.

³³⁹ DURÁN CARDO, B., *La figura del responsable en el derecho a la protección de datos...*op. cit., p. 427.

ver el entorno latinoamericano en materia de protección de datos y *habeas data*, para luego volver a refrescar este tema³⁴⁰.

II. EL DERECHO A LA PROTECCIÓN DE DATOS EN LATINOAMÉRICA Y LA FIGURA DEL *HABEAS DATA*

1. Antecedentes

No sólo Estados Unidos y Europa han mostrado su preocupación por los riesgos de las nuevas tecnologías de la información³⁴¹ para las libertades de la persona sino que, también en Latinoamérica, comenzó a gestarse esta tendencia recogiendo en los textos constitucionales y desarrollándose en los primeros proyectos legislativos.

En ese sentido, tras la segunda guerra mundial³⁴² se da paso en 1948, a la conformación de la Organización de los Estados Americanos reconocidas por sus siglas como (OEA)³⁴³ y con ella, el nacimiento del Sistema Interamericano

³⁴⁰ 5.3.1 Niveles de protección de datos, Capítulo IV.

³⁴¹ (...) la importancia de la informática como factor de conocimiento y de poder es la ofrecida por su estrecha conexión con el desarrollo de la tecnología americana en la segunda mitad de este siglo. En la Unión Soviética, en la cual, en sus comienzos, la informática fue condenada y combatida como ciencia burguesa, después de la muerte de Stalin, se consiente y favorece su estudio y aplicación como factor indispensable del desarrollo de la sociedad soviética. Este nuevo poder puede ser concentrado o difundido en una sociedad, confiado a la iniciativa privada o reservado al monopolio estatal, concebido como un nuevo tejido cohesionador de la sociedad civil o como un instrumento de sumisión universal, y sobre esta alternativa de empleo de la nueva técnica de conocimiento y de poder se juega el destino social del hombre de hoy. FROSINI, V., *cibernética, derecho y sociedad*, editora Tecnos, S. A., Fuenlabrada, Madrid, 1982, p. 175.

³⁴² PINTO, M., *Las fuentes del Derecho Internacional en la era de la Globalización*, 1ª ed. Universitaria de Buenos Aires, 2009, p. 16.

³⁴³ (...) Esta organización, creada en 1948 por la Conferencia de Bogotá, tiene unos objetivos políticos (garantizar la paz y la seguridad del continente), pero se propone también <<favorecer por medio de una acción concertada el desarrollo económico, social y cultural>> (artículo 4 de la Carta de Bogotá). Con este fin, reúne a todos los Estados americanos (pero únicamente ellos), salvo Cuba y Canadá. Varias de sus instituciones están consagradas al desarrollo, y el presidente Kennedy lanzó *la Alianza para el progreso* dentro de su marco. Visto en LUCHAIRE, F., *La ayuda a los países subdesarrollados*, 1ª. ed. (En lengua castellana) Oikos-Tau, Barcelona, 1971, pp. 64-65.

de Derechos Humanos, colaborador de la protección y conformación de los derechos fundamentales en la región, el Sistema se desarrolló en tiempos convulsos en la región, protagonizado por dictaduras. A tal punto, que su nacimiento surge en momentos de franca proporción entre los gobiernos autoritarios y los democráticos, situación distinta al surgimiento del sistema europeo compuesto por gobiernos estables. Un escenario idóneo para la creación del organismo en la región³⁴⁴.

En ese mismo orden, la democracia y la polarización de fuerzas políticas se convierte en un escenario propicio para la incursión de la tecnología en la sociedad y con él, los desarrollos normativos de la época, tal como lo expresa LOSANO.

(...) la construcción de los grandes sistemas de Estado del Bienestar (Welfare State). Ahora, tanto la guerra fría como el Welfare State tienen necesidad de conocer todo sobre los ciudadanos (naturalmente por razones muy diversas) y encuentran en la informática el instrumento ideal...nacen las primeras propuestas de ley sobre la protección de los datos personales. A partir de finales de los años 60 se suceden las propuestas de imponer límites y controles a quienes gestionan bancos de datos personales...las leyes que entran en vigor en el curso de los años 70 están todas ellas inspiradas en esta versión técnica de la informática³⁴⁵

En este mismo sentido, poco después –como hemos visto- las constituciones de España y Portugal regularon esta cuestión. En Latinoamérica, por su parte también, un buen número de constituciones es

³⁴⁴ “No deja de construir una paradoja, que el nacimiento del sistema Interamericano de derechos humanos haya surgido en una época donde el número de los regímenes democráticos existentes en América haya sido equivalente a los gobiernos autoritarios. Este rasgo diferencia al sistema americano con el europeo conformado por democracias estables y con alto desarrollo político y económico, lo que hace sino realzar la importancia de poseer una organización supranacional como la existente en el continente americano para la observancia y el respeto de los derechos fundamentales” visto en BEL MALLÉN, I., CORREDORA y ALFONSO, L. (Coordinadores), *Derecho de la Información*, 1ª. ed. ARIEL, S. A., Barcelona, 2003, p. 141

³⁴⁵ LOSANO, M. G., *Para una teoría general de las leyes sobre la protección de los datos personales*, CITEMA, visto en IX encuentro, *implicaciones socio-jurídicas de las tecnologías de la información*, CITEMA, España, 1991.

reformado, con el auge de ese fenómeno de “redemocratización” y en donde se procura una mayor tutela de los derechos fundamentales³⁴⁶.

Los constituyentes latinoamericanos de los 80 si bien consagraron inicialmente las reglas de estos textos constitucionales, luego fueron dotándolas de rasgos autóctonos que distinguieron a sus cartas constitucionales³⁴⁷. Por tales razones, se observa una marcada diferencia en Latinoamérica y el debate no será en principio el del derecho a la autodeterminación informativa o el de la libertad informática ni el del derecho a la protección de datos sino que en origen el proceso de reformas va a definir dos versiones principales en función del “... *habeas data*: aquella que se ocupará de otorgar una garantía procesal al derecho a la autodeterminación informativa (*habeas data* propio o tradicional) y aquella que pretenderá garantizar el acceso a la información pública (*habeas data* impropio)”³⁴⁸.

Por ello, como se señala desde la doctrina, las referencias en el contexto latinoamericano se centran sobre todo en esta garantía del *habeas data*, pero más tarde se confundirá con el propio derecho a la protección de datos personales³⁴⁹.

2. El origen del *habeas data*

El concepto de *habeas data* proviene de la locución latina que significa para que tengas tu dato o bien tráigame la información³⁵⁰.

³⁴⁶ PUCCINELLI, O., *El Habeas data en Indoiberoamérica*, Temis, Bogotá, 1999, p. 193.

³⁴⁷ PUCCINELLI, O., “Versiones, tipos, subtipos y subespecies de *habeas data* en el derecho latinoamericano (Un intento clasificador con fines didácticos)”. *Revista Iberoamericana de derecho procesal constitucional* (Proceso y Constitución, núm. 1), Editorial Porrúa / Instituto Iberoamericano de Derecho procesal Constitucional, México, 2004, p. 97.

³⁴⁸ PUCCINELLI, O., *El Habeas data en Indoiberoamérica*, op. cit., p. 193.

³⁴⁹ RODRÍGUEZ MARCANO, E. R., *El derecho a la autodeterminación informativa en Venezuela...op.cit.*, p. 110.

³⁵⁰ CABANELLAS DE TORRES, G., *Diccionario Jurídico Universitario*, editorial Heliasta S.R.L, 2000, p. 461.

Como se señala desde la doctrina, su nombre se ha tomado parcialmente del antiguo instituto del *habeas corpus*, pero es una de las garantías constitucionales más modernas, aunque se denomine mitad en latín y mitad en inglés. Su traducción literal sería “conserva o guarda tus datos”³⁵¹.

En consecuencia, respecto de la locución latina que le da nombre propio al Instituto, se podría referir alguna crítica en su elección, pero hay que reconocer que la expresión es feliz como composición latina para un derecho de fin del siglo de la información. “*habeas*”, segunda persona del presente subjuntivo de *habeo...habere*, significa aquí “conservas tu posesión”, que es una de las acepciones del verbo, y “*data*” es el acusativo plural de *datum*, que los diccionarios más modernos definen como representación convencional de hechos, conceptos e instrucciones de forma apropiada para la comunicación y procesamiento por medios automáticos. En definitiva, que conserves los registros, los datos”³⁵², “tengas los datos”³⁵³.

En Latinoamérica el *habeas data* nace en Brasil en la Constitución de 1988, si bien su existencia ya había sido plasmada, no con esa denominación, en versiones locales³⁵⁴. Con todo, desde la doctrina se señala que Brasil, tras veinte años de dictaduras militares³⁵⁵ busca a Portugal como modelo de

³⁵¹ EKMEKDJIAN, M. y PIZZOLO, C., *Habeas Data (El derecho a la intimidad frente a la revolución informática)*, De palma, Buenos Aires, 1998, p. 1.

³⁵² OTHON SIDOU, J. M., *Las nuevas figuras del derecho procesal constitucional brasileño: mandato de injucao y habeas data*, Boletín Mexicano de Derecho Comparado (Traducción de Flx Zamudio, H.). núm. 70, UNAM, México, 1991, pp. 180-181.

³⁵³ NOGUEIRA ALCALÁ, H., *Autodeterminación informativa y habeas data en Chile e información comparativa*, Anuario de Derecho Constitucional Latinoamericano, 2005, p. 458.

³⁵⁴ PUCCINELLI, O., *El Habeas data en Indoiberoamérica*, op, cit., p. 295.

³⁵⁵ “...el *habeas data* llegó a Brasil a través de la constitución de Portugal. Portugal hizo una constitución en 1976, después de una revolución que puso término a cuarenta años de dictadura. Y esta constitución portuguesa fue fuertemente influenciada por los pactos de derechos humanos. Pasó algo muy crítico: cuando Brasil consiguió cerrar el período de más de veinte años de dictaduras militares, fue a buscar en Portugal el modelo de constitución. Es muy fuerte la influencia de la constitución portuguesa en la constitución de Brasil de 1988. Evidentemente hay peculiaridades, que derivan de condiciones que son típicas y específicas de Brasil, pero sin duda hay una influencia de esta constitución. Y el *habeas data* {sic}, está en la constitución de Portugal, de este modo llegó a Brasil” (De Abreau Dallari, 1997). Tomado de

Constitución. El *habeas data* se introduce en este país como vía para acceder a la información que se encontraba en manos de la policía³⁵⁶ en los registros de todos los ciudadanos que se consideraban enemigos del gobierno³⁵⁷. Se incorpora en una disposición bastante escueta en el artículo quinto inc. LXXII de la Constitución de 1988 y su fin es sólo “asegurar el conocimiento de informaciones” cuando sean personales y que consten en bancos de datos gubernamentales o de carácter público. En cualquier caso, se ha señalado que su construcción es bastante limitada. Su norma de desarrollo se produjo 10 años después (Ley 9.507 del 12 de noviembre de 1997) y cercenada a aspectos procesales³⁵⁸.

3. Tipos y subtipos de *habeas data*

La visión individual de cada país del *habeas data* ha dado lugar a una riqueza tal que desde la doctrina se ha realizado una clasificación de la misma para su mejor comprensión³⁵⁹, 4 años antes se observa una clasificación previa impulsada por Nestor Pedro Sagüés³⁶⁰.

QUESADA RODRÍGUEZ, A., *Protección de datos y telecomunicaciones convergentes*, 1ª ed. Agencia Española de protección de datos, Madrid, 2014, p. 316.

³⁵⁶ “(...) en las realidades latinoamericanas la institución policial tiene imperfecciones muy agudas. Su debilidad en términos de profesionalidad, carrera, sueldos adecuados, entrenamiento, la ha convertido con frecuencia en <<policías malditas>> con serios problemas de corrupción, captación por los grupos de la droga y, hasta en diversas dictaduras como las del Cono Sur en los años setenta y parte de los años ochenta, se convirtió en un apéndice más del sistema brutal de represión instituido” visto en SEN, A. y KLIKSBURG, B., *Primero la gente*, 1ª ed. Deusto, Barcelona, 2007, p. 233.

³⁵⁷ DE ABREU DALLARI, D., “*El Habeas data en Brasil*”, *Ius ET Praxis* (año 3 núm.1), Facultad de Ciencias Jurídicas y Sociales (Universidad de Taica), Chile, 1997, pp. 71-80.

³⁵⁸ Véase RODRÍGUEZ MARCANO, E. R., *El derecho a la autodeterminación informativa en Venezuela...op.cit.*, pp. 112-118.

³⁵⁹ Esta clasificación es realizada por PUCCINELLI, O., “*Versiones, tipos, subtipos y subespecies de habeas data en el derecho latinoamericano (Un intento clasificador con fines didácticos)*” op. cit., p. 106 y ss.

³⁶⁰ SAGÜÉS, N. P., *Subtipos de habeas data*, en jurisprudencia argentina, 1995, pp. 31 y ss; tomado de NOGUEIRA ALCALÁ, H., *Autodeterminación informativa y habeas data en Chile e información comparativa*, Anuario de Derecho Constitucional Latinoamericano, 2005, p. 459.

Como premisa básica se ha de señalar que los tipos de *habeas data* no son únicos; es decir que en ciertos momentos cuando se incoa la acción pueden estar relacionados más de uno.

Como primera gran clasificación cabe distinguir el *habeas data* propio y el impropio. El primero está dirigido a prevenir o reparar lesiones que pudieran producirse en el tratamiento de datos de carácter personal realizado en bases y bancos de datos mientras que el segundo correspondiente al *habeas data* impropio está diseñado a fin de a) obtener información pública que le es negada al legitimado activo o b) replicar información de carácter personal difundida a través de los medios de difusión tradicionales.

El *habeas data* propio presenta unas series de tipo y subtipos. Entre ellos cabe mencionar.

a) el *habeas data* informativo destinado a la mera obtención de información, es preventivo y puede servir de base para eventuales reclamos de operación sobre los datos. Los subtipos correspondientes son: a) el localizador (puede utilizarse para indagar respecto de la localización de los bancos de datos; esta posibilidad se prevé en la ley española y en la ley argentina); b) el finalista (su fin es determinar para qué se creó el registro); c) el exhibitorio; y d) el autoral (puede inquirir de las fuentes de las cuales se obtuvo la información almacenada). Las constituciones de Argentina, Brasil, Colombia, Ecuador, Guatemala, Paraguay, Perú y Venezuela y las leyes de Argentina y Chile han recogido los rasgos de finalistas, exhibitorias y autorales.

b) el *habeas data* reparador, está dirigido a producir modificaciones sobre los datos colectados en el sistema de información o sobre éste, con la finalidad de prevenir tratamientos técnicamente. Los subtipos correspondientes son:

- El aditivo, su finalidad es agregar al sistema de información datos de carácter personal no asentados en este; dentro de él cabe mencionar el actualizador (actualizar datos vertidos pero ciertos, lo vienen incluyendo en los textos constitucionales de Argentina, Brasil, Colombia, Ecuador,

Paraguay, Venezuela y las ciudades autónomas de Argentina, así como las leyes de Argentina y Chile);

- El aclaratorio, destinado a aclarar situaciones ciertas pero que pueden ser incorrectamente interpretadas;
- El inclusorio, cuyo fin es incluir una información ya que la omisión de la misma produce un perjuicio;
- El rectificador o correctivo, al objeto de corregir datos falsos, inexactos e imprecisos; viene siendo regulado en las constituciones de Argentina, Brasil, Colombia, Ecuador, Paraguay, Venezuela, Portugal, Buenos Aires y sus ciudades Autónomas, así como en las leyes generales de Argentina y Chile;
- El exclutorio o cancelatorio: diseñado para eliminar total o parcialmente los datos almacenados respecto de determinada persona, cuando por algún motivo no deben mantenerse incluidos en el sistema de información de que se trate. La figura ha sido regulado en las constituciones de Argentina, Ecuador, Paraguay y Venezuela, las cartas de Portugal, Ciudad Autónoma y provincia de Buenos Aires, Chaco y Chubut, así como en las leyes generales de Argentina y Chile;
- El disociador, permite y asegura que el dato sea sometido a las técnicas correctas de disociación, desvinculando el dato para que quien opera el dato no tenga acceso a conocer la identidad de la persona. Guarda similitud con los *habeas data* reservador y exclutorio ya que apuntan a que los datos en cuestión puedan ser valorados dentro de determinados parámetros, sin conocer la identidad del registrado como por ejemplo contrarrestar violaciones a las normas que autorizan a recoger datos anónimos con fines epidemiológico. Se encuentra en las leyes generales argentina y chilena;
- El encriptador: busca lograr mayor seguridad y agilidad a la operación sobre determinados datos por lo que puede ser necesario acudir a técnicas de encriptación, donde el dato está oculto y solo puede ser conocido por quien tenga en su haber la llave para descifrarlo;
- El bloqueador: emparentado con el reservador y el exclutorio trabaja la transmisión de los datos asentados en un registro, el impedimento a

tercero puede o no puede ser temporal según la circunstancia. Se prevé en las leyes generales de Argentina y Chile;

- El asegurador: por medio de él se logra la constatación judicial de las condiciones en que opera el sistema de información que contiene los datos y en su caso la imposición de condiciones técnicas mínimas de seguridad para que se pueda proseguir con tratamiento de datos de carácter personal. Guarda relación con el reservador, pero es más amplio en el sentido de que no opera solo respecto de datos confidenciales, sino de cualquier tipo de datos. Se encuentra en las leyes generales de Argentina y Chile;
- El impugnativo: tiene como objetivo establecer una conclusión distinta a la que aparece en el registro mediante la impugnación. Las normas sobre protección de datos suelen prever el derecho del registrado a impugnar las valoraciones que de sus datos realice el registrador, así como de las decisiones judiciales o administrativas con único fundamento en el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado. Presenta similitud con el rectificador o correctivo. Se prevé en la ley argentina;
- El resarcitorio (denominado también reparador): tiende, precisamente a lograr la satisfacción de indemnizaciones, y donde ello es factible, la constitución del Ecuador lo ha previsto de manera expresa al regular el *habeas data* y en Colombia se han admitido regularmente *habeas data* donde se pretendían indemnizaciones (cabe recordar que la acción de tutela colombiana, por la que se visualiza el derecho del *habeas data* permite incluir el reclamo de ellas). También lo prevén las leyes españolas, argentinas y chilenas.

Por su parte, el *habeas data* impropio no está dirigido a la protección de datos de carácter personal asentados en bases o bancos de datos, sino a obtener información pública que le es indebidamente negada al legitimado activo o replicar información de carácter personal difundida a través de los medios de difusión tradicionales. Se distinguen entre:

- *Habeas data* de acceso a información pública (*habeas data* público) tiene como objetivo permitir el acceso a la información pública estableciendo para ellas acciones procesales constitucionales específicas. Está prevista en Perú;
- *Habeas data* replicador permite que toda persona afectada por informaciones o agraviada en cualquier medio de comunicación social, tiene derecho que éste se rectifique en forma gratuita, inmediata y proporcional. Se encuentra en la constitución peruana de 1993, fue modificado y no existe en la actualidad.

Como se señala desde la doctrina³⁶¹, con todo ello se muestra que esta figura del *habeas data* con sus correspondientes haces de facultades parte de un mismo derecho, el derecho a la protección de datos de carácter personal, pero que ante las confusiones han seguido el camino del *habeas data* o de la garantía olvidando la existencia del derecho a la protección de datos. Evidentemente que la afirmación de que en Latinoamérica existe un nuevo derecho fundamental, llamado el *habeas data* en lugar del derecho fundamental a la protección de datos obedece a unas razones que pasamos a exponer.

4. Razones de la asunción del *habeas data* en Latinoamérica frente al derecho a la protección de datos

Vamos a ofrecer en este apartado siguiendo a la doctrina³⁶² las razones por las que el *habeas data* durante su momento se ha venido alzando como un derecho fundamental en detrimento del derecho a la protección de datos de carácter personal.

³⁶¹ RODRÍGUEZ MARCANO, E. R., *El derecho a la autodeterminación informativa en Venezuela...op.cit.*, pp. 132-135.

³⁶² *Ibidem*, p. 135 y ss.

Cabe afirmar que la incorporación del derecho a la protección de datos se inicia en Latinoamérica en la década de los 80 como consecuencia de la oleada democrática que conlleva, por tanto, la reforma de sus constituciones e influenciadas especialmente por las constituciones portuguesas y españolas de finales de los 70. Así cabría citar, la constitución de Guatemala que realiza la implementación y reforma constitucional en el año 1985, la de Nicaragua en el 1987 y la de Brasil en el 1988. Es ésta -como hemos visto- la primera que incorpora el término del *habeas data*.

¿Por qué en Latinoamérica la garantía judicial (*habeas data*) se ha incorporado conjuntamente con el derecho (en la mayoría de los países) confundiéndole con éste o asumiéndose como tal ?

Obedece a las siguientes justificaciones:

En primer lugar, la visión que tiene Latinoamérica con respecto al derecho a la protección de datos debido a su realidad política, jurídica y social y que es fruto de las siguientes razones:

a) Su inestabilidad política y jurídica. Se tratan de jóvenes democracias y donde la lucha por el poder y las pugnas políticas son una constante. Ello no facilita la progresividad de los derechos fundamentales, siendo sus incorporaciones incompletas y apresuradas³⁶³. Esto también ha afectado al derecho a la protección de datos, produciendo un desarrollo confuso y lento unido a la génesis basada en la búsqueda de obtención del simple acceso a la información ante el poder y el uso indebido de la informática.

b) La inexistencia de tratados internacionales preexistentes que contribuyan a una regulación y unificación del derecho a la protección de datos. En el

³⁶³ ARGÜELLO TELLEZ, F., "Protección de datos personales: La Directiva Comunitaria, su influencia y repercusiones en Latinoamérica", *Protección de datos de carácter personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala 2-6 de junio de 2003)*, Tirant Lo Blanch, Agencia de Protección de Datos, Valencia 2006, p. 80.

contexto europeo, tanto el Consejo de Europa como la Unión Europea desde fechas tempranas (Convenio 108 de 1981 y Directiva del 95, si bien han existido otros textos unificadores incluso antes) han marcado un cauce que ha permitido que cada país asuma y modifique su regulación de la materia si no quiere quedar fuera del espacio común. No ocurre así en Latinoamérica. Si bien se ha tratado de avanzar hacia el reconocimiento internacional del derecho a la protección de datos personales. Así, cabe citar la Declaración de Santa Cruz de la Sierra, realizada en el 15 de noviembre del 2003, donde 21 Estados lograron aceptar y manifestar a la vez que la protección de datos personales es un derecho fundamental y en donde se presenta³⁶⁴ la Red Iberoamericana de Protección de Datos³⁶⁵. Por otra parte, la Organización de Estados Americanos (OEA)³⁶⁶ también debe continuar con los esfuerzos de contribuir con la expansión y homogenización de la protección de datos, mediante la realización de pactos internos entre los Estados que conforman la Organización, considerando entre otros al modelo europeo cuyos acuerdos benefician a la ciudadanía mediante un comercio más seguro e instauración de normas que permiten asegurar los procesos comerciales en toda la región. Como se expresa desde la doctrina, “si la OEA adopta medidas estratégicas, beneficiará a todos los países latinoamericanos y logrará que nos convirtamos en un lugar en donde se pueda invertir sin reserva en negocios que involucran transferencia de datos personales desde diversas partes del mundo. Esto hará que América Latina sea más competitiva frente a otros sitios del globo terráqueo respecto de nuevos y más significativos negocios en TIC e información personal”³⁶⁷.

³⁶⁴ La Red Iberoamericana de Protección de Datos nace en Junio de 2003 con la Declaración de la Antigua, Guatemala; siendo presentada en noviembre durante la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno de ese mismo año.

³⁶⁵ PIÑAR MAÑAS, J. L., *La Red Iberoamericana de Protección de Datos: Declaraciones y Documentos*, Tirant Lo Blanch, Valencia, 2006, pp. 17-18.

³⁶⁶ PASTOR RIDRUEJO, J. A., *Curso de Derecho Internacional Público y Organizaciones Internacionales*, Tecnos, Madrid, 2009, p. 799.

³⁶⁷ REMOLINA ANGARITA, A., *Ámbito Jurídico*, núm. 326, julio-agosto de 2011, p. 12.

c) La incorporación aislada de disposiciones constitucionales y legales frente al uso de la informática. Como ya se ha ido desprendiendo a lo largo de este trabajo las regulaciones en el contexto latinoamericano se han realizado de manera aislada en cada país. Además, se ha destacar que si repasamos los distintos textos constitucionales observaremos que, tras la constitucionalización en los años 80 de este derecho en Guatemala, Nicaragua y Brasil, en los 90 se abre una segunda etapa con los Estados de Colombia, Paraguay, Perú, Argentina, Ecuador y Venezuela finalizando en el 2000 con países como Bolivia, Honduras, México y la República Dominicana con su reforma Constitucional del 2010 ampliamente vista y presentada en el capítulo III. Pero no todo se queda en el despliegue constitucional, sino que los Estados se abocan en la construcción de leyes generales y específicas, situación de Argentina, Colombia, y Perú. En cambio otros, poseedores de Constituciones de la era pre informática, no contemplan desarrollos constitucionales en materia de protección de datos o habeas data, pero sí han implementado interesantes leyes de protección de datos, situación de Chile, Costa Rica, Uruguay, un proceso que no se detiene en los Estados Latinoamericanos.

En segundo término, la visión pragmática de Latinoamérica que ha aceptado una visión del Derecho Constitucional en términos de Derecho Procesal Constitucional, asumiendo figuras tales como el amparo, el habeas corpus y por último el *habeas data*, pero configurándolas como nuevos derechos constitucionales. Cabe deducir esto de las siguientes razones:

a) Se han creado figuras procesales en el ámbito del Derecho Constitucional. Latinoamérica plantea su salida elevando a nivel constitucional el remedio procesal constitucional. En este sentido, se señala que “el *habeas data* es un proceso constitucional que se instala en la órbita del derecho de acceso a la justicia sin restricciones, salvando cuestiones de legitimación que en la especie son ineludibles por tratarse de afecciones de carácter

personalísimo”³⁶⁸. Es decir, se sitúa en el camino del *habeas data* en lugar de en el del derecho a la protección de datos personales.

b) Asunción del *habeas data* como nuevo derecho o garantía, parte del Derecho Procesal Constitucional. Para la doctrina ha sido muy difícil ofrecer algo de luz en este panorama³⁶⁹. Al referirse al *habeas data* se habla tanto de derecho, de garantía, de proceso o de acción. Por ello, en muchas ocasiones la doctrina le otorga una naturaleza mixta (acción y derecho) o planteada como acción o proceso. Esto origina confusión al establecerlo de este modo, pero también complica el esquema³⁷⁰.

5. Habeas data en las constituciones latinoamericanas

5.1. Puntualizaciones

El *habeas data* y la protección de datos personales incluida sus leyes generales y específicas han sido objeto de numerosos estudios, entre ellos, el premiado con el Accésit otorgado en la XVIII edición de los premios de investigación de la Agencia Española de Protección de Datos, con el tema *Protección de datos y habeas data: una visión desde Iberoamérica*³⁷¹, bajo la coordinación de LÓPEZ CARBALLO soportado por 21 especialistas de distintos países iberoamericanos. El estudio agrupa a los Estados Iberoamericanos

³⁶⁸ GOZAINI, O., *El derecho de amparo*, 2ª ed. De Palma, Buenos Aires, 1998, p. 250.

³⁶⁹ Véase entre otros EKMEKDJIAN, M. A. y PIZZOLO, C., *Habeas Data (El derecho a la intimidad frente a la revolución informática)*, op, cit., p 1; ZAMBRANO, F., *El procedimiento de amparo constitucional* (Colección de textos legislativos venezolanos, núm. 2), Caracas, Atenea, 2001, pp. 49-97; SAGÜÉS, N. P., *Derecho Procesal Constitucional. Acción de Amparo*, Buenos Aires, Astrea, 1995, p. 652. Se agradece el esfuerzo de sistematización, en este sentido sobre la teoría de estos autores y otros en RODRÍGUEZ MARCANO, E. R., *El derecho a la autodeterminación informativa en Venezuela...op.cit.*, pp. 163-170.

³⁷⁰ PUCCINELLI, O., *El Habeas data en Indoiberoamérica*, op, cit., pp. 218-219.

³⁷¹ LÓPEZ CARBALLO, D. (Coordinador), *Protección de datos y habeas data: una visión desde Iberoamérica*, imprenta nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2015, pp. 1 y ss.

alrededor de sus legislaciones específicas, tales como protección de datos, privacidad, *habeas data*. En las siguientes líneas, vamos a analizar la conexión del *habeas data* con los plexos constitucionales y legislativos de los Estados Iberoamericanos, analizando sus normas y procesos de conexión que van desde el orden constitucional al legislativo y viceversa.

La protección de datos y el *habeas data* forman parte de los modelos de protección de datos existentes. El primer modelo se fundamenta en instrumentos legales, referente a técnicas y herramientas de orden jurídico e informático, orientado a materializar la autodeterminación informativa referenciada como un derecho humano. El segundo modelo es considerado el más nuevo mecanismo procesal de corte constitucional abordado en las constituciones latinoamericanas siendo representativo de Sudamérica³⁷².

Como ya hemos venido comentando, la incursión del *habeas data* en Latinoamérica obedece a factores sociales, históricos y políticos ocurridos en el siglo pasado y concluidos a finales de los años 70, conectados con el fin de las dictaduras y el surgimiento de jóvenes democracias en los Estados Latinoamericanos, dando origen a procesos de reformas constitucionales. Si bien, la figura se matiza por enmiendas o redacciones constitucionales, incorporando el modelo europeo en auge, adaptando la autodeterminación informativa a los procesos de reforma, en una especie de tropicalización³⁷³ de la norma.

La presencia del *habeas data* crece en Latinoamérica siendo de uso frecuente y relevante³⁷⁴, materializándose y formando parte integral de varias

³⁷² QUESADA RODRÍGUEZ, A., *Protección de datos y telecomunicaciones convergentes*, 1ª ed. Agencia Española de protección de datos, Madrid, 2014, pp. 314-315.

³⁷³ "...los países de la zona, los cuales adoptaron y <<tropicalizaron>> dentro de sus nuevos textos fundamentales un derecho que, para la fecha, se encontraba en boga en Europa: el derecho de autodeterminación informativa (Martínez-Herrera, 2011, p. 2, visto en QUESADA, A., *Protección de datos y telecomunicaciones convergentes*, 1ª ed. Agencia Española de protección de datos, Madrid, 2014, p. 315.

³⁷⁴ REMOLINA ANGARITA, N., *Recolección internacional de datos personales: un reto del mundo...*op. cit., pp. 106 y 107.

de sus constituciones y sus normas locales sobre protección de datos³⁷⁵; Fundamentado en tales cuestiones en este lugar pasamos a identificar y conocer su relevancia en los distintos países del escenario latinoamericano. enfocado en sus normas constitucionales y legislativas incidiendo en el accionar de los mismos.

5.2. Consideraciones del *habeas data* en el escenario latinoamericano

Con el devenir de los años, el *habeas data* continúa permeando los textos fundamentales de las naciones iberoamericanas³⁷⁶, siguiendo las particularidades léxico-jurídica de cada país³⁷⁷, impregnando en sus textos constitucionales una acción de acceso, garantía³⁷⁸ nueva, un procedimiento jurisdiccional, un proceso constitucional o recurso de protección a la autodeterminación informativa para la protección de los datos personales de las personas. Con ello se salvaguarda y protege a las personas físicas mediante su incorporación en los textos constitucionales, sirviendo de instrumento garantista; esta tendencia es seguida por América Latina desde la Constitución de Brasil y extendiéndose a los demás países del área, entre ellos, Argentina, Colombia, República Dominicana, Perú, Paraguay y Venezuela³⁷⁹.

³⁷⁵ Formando parte Brasil, Paraguay, Perú, Venezuela, Panamá, Honduras, República dominicana, honduras y otros más.

³⁷⁶ “En Iberoamérica, la Constitución de Brasil de 1988, al parecer, fue la primera que estableció el *habeas data* en la región, seguida por las de Colombia, Paraguay, Argentina y Perú, entre otras; toda ellas con la idea común de proteger, fundamentalmente, el *derecho a la intimidad personal y familiar*, además de otros derechos, como “el buen nombre” (Colombia), el derecho al honor, la buena reputación, la voz y la imagen propia (Perú)”. DURÁN RIBERA, W. R., *Contenido y alcances del habeas data en Bolivia*, Anuario de Derecho Constitucional Latinoamericano, 2006, p. 904.

³⁷⁷ BAZÁN, V., *El habeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado*, Estudios constitucionales, vol. 3, núm. 2, Universidad de Talca, Centro de Estudios Constitucionales de Chile 2005, p. 90.

³⁷⁸ “El resto de los países indoiberoamericanos que lo ha regulado, llama de tal manera a una garantía procesal constitucional nacida...en el Brasil”. PUCCINELLI, O., *El Habeas data en Indoiberoamérica*, Temis, Bogotá, 1999, p.102.

³⁷⁹ BEL MALLÉN, I., CORREDORA y ALFONSO, L. (Coordinadores), *Derecho de la Información*, 1ª ed. ARIEL, S. A., Barcelona, 2003, p. 134.

El *habeas data* tutela los derechos de su titular y no aplica para los datos de terceros. Faculta al dueño del dato del acceso a sus datos personales ubicados en archivos, registros, bancos de datos u otros medios técnicos de almacenamiento. En tal sentido, la acción de *habeas data* faculta la supresión, rectificación, actualización u oposición de los datos en caso de ser requerido. Por otra parte y, como hemos externado, el *habeas data* impropio, permite el acceso a los datos públicos, siendo representativo de los Estados democráticos o en vía de democracia, tanto en países europeo como latinoamericanos.

En ese sentido, el *habeas data* evoluciona, se afianza, siguiendo un proceso de estandarización en los Estados Latinoamericanos, proceso reflejado en las constituciones y leyes generales de los Estados conocidas como leyes ómnibus³⁸⁰. Dichas leyes son capaces de ejercer amplios derechos sobre la protección de datos personales conectado con sus mecanismos de tutela y garantía; los Estados europeos son parte de este gran grupo, a diferencia de los Estados Unidos de América conformado por leyes sectoriales³⁸¹ en materia de protección de datos.

A raíz de las diferencias léxico-jurídicas de cada país, el *habeas data* incursiona en las constituciones latinoamericanas, no permeando a todas las constituciones por igual. En unos casos, se reconoce la figura del *habeas data* en su plexo constitucional, típico del modelo constitucional³⁸² dominicano y su ley general³⁸³, estableciendo e integrando de manera literal la figura del *habeas*

³⁸⁰ Como leyes Ómnibus europeas podemos reconocer la Ley Sueca de 1973, la Ley Alemana de 1977, continuando con la Ley Francesa de 1978, el caso español con sus leyes ya comentadas LORTAD de 1992 sustituida por la LOPD del 1999, la Ley Italiana de 1996.

³⁸¹ Se reconoce la *Privacy Act* de 1974; una ley que protege a las personas frente a la intromisión realizada por las agencias federales, específicamente en la protección de su intimidad por medio a los bancos de datos de la administración federal.

³⁸² Artículo 70, Constitución de la República Dominicana, Votada y Proclamada por la Asamblea Nacional en fecha trece (13) de junio de 2015, Gaceta Oficial N.º 10805 del 10 de julio de 2015.

³⁸³ Artículo 17 Ley núm. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. Gaceta Oficial N.º 10737 del 15 de diciembre de 2013.

data. En otros, reconocen la acción, más no han literalizado expresamente la denominación del *habeas data*; este es el caso del modelo de la Constitución Argentina de 1994, siendo ampliamente reconocido en el proceso jurisprudencial y doctrinal de Argentina y sus otros Estados.

Tal situación nos permite entender que estamos delante de una no homogenización del *habeas data* en el orden constitucional latinoamericano, careciendo de un proceso de estandarización entre los Estados, influenciado por sus diferencias. En este sentido, hay que destacar la carencia de órganos supranacionales, capaces de dictar o crear normas de estandarización en las constituciones de los Estados Latinoamericanos. A raíz de tales supuestos, la incursión del *habeas data* constitucional latinoamericano debe ser un proceso sencillo capaz de ser adecuado, absorbido e implementado en los Estados Latinoamericanos, dando la posibilidad de adaptarse a los cambios por venir.

En la medida que el *habeas data* ingresa en las constituciones latinoamericanas, los Estados envueltos en sus reformas constitucionales o en fase de transformación se apoyan en las constituciones ya reformadas o en las normativas legislativas previas que contemplan la figura del *habeas data*, siendo el común denominador las reformas precedentes realizadas, ya sean específicas o puntuales como veremos en el caso de Brasil que toma de referencia la Constitucional de Portugal³⁸⁴.

5.3. El proceso constitucional del *habeas data* en Latinoamérica

La Constitución de Brasil es la primera³⁸⁵ en Latinoamérica que esboza el término de *habeas data*, siendo pionera en utilizar la expresión *habeas data*³⁸⁶.

³⁸⁴ “...el *habeas data* llegó a Brasil a través de la constitución de Portugal. Portugal hizo una constitución en 1976...” Visto en QUESADA RODRÍGUEZ, A., *Protección de datos y telecomunicaciones convergentes*, 1ª ed. Agencia Española de protección de datos, Madrid, 2014, p. 316.

³⁸⁵ QUESADA RODRÍGUEZ, A., *Protección de datos y telecomunicaciones convergentes*, 1ª ed. Agencia Española de protección de datos, Madrid, 2014, p. 316.

Se incorpora bajo el título de los derechos y garantías, precedido por los reflejos e influencia de la Ley núm. 824 de diciembre de 1984 correspondiente al Estado de Río de Janeiro. En el capítulo I asignado a los derechos y deberes individuales y colectivos de la Constitución Federativa de Brasil (artículo 5/LXXII)³⁸⁷ se crea un recurso especial de *habeas data*. Este instituto reconocido constitucionalmente se contempla para las siguientes razones 1) *asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público*; 2) *para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo*; contemplando una naturaleza de acción constitucional y al mismo tiempo, tiene la capacidad de amparar el derecho por una garantía³⁸⁸.

No es sino hasta el 12 de noviembre del 1997, cuando se establece el reglamento del *habeas data* mediante Ley núm. 9.507³⁸⁹, contemplando la asignación de tribunales de acuerdo a la identidad del accionante. Esta Ley que

³⁸⁶ BAZÁN, V., "El habeas data, su autonomía respecto del amparo", *Anuario de Derecho Constitucional Latinoamericano* año XVIII, Bogotá, 2012, p. 44. Disponible en: <http://www.corteidh.or.cr/tablas/r29666.pdf>. (Última consulta en línea 23 de marzo 2019).

³⁸⁷ *Constitución Política de Brasil de 1988*. Disponible en: <http://www.wipo.int/edocs/lexdocs/laws/es/br/br117es.pdf>. (última verificación en línea 19 de marzo 2018). Al mismo tiempo también se observa en HERRERO HIGUERAS, M., *Panorama General de la Legislación Mundial sobre protección de datos*, CITEMA, p. 43, tomado de IX encuentro implicaciones socio-jurídicas de las tecnologías de la información, CITEMA, 1991.

³⁸⁸ Da Silva afirma que el *habeas data* es un remedio Constitucional, un medio dirigido a provocar la actividad jurisdiccional y que, por ese motivo, tienen naturaleza de acción (acción constitucional); aunque añade que, paralelamente, contiene un derecho que, en vez de ser reconocido en forma independiente, se encuentra contenido en la garantía que lo ampara. DA SILVA, J. A., *Curso de Direito Constitucional Positivo*, 8ª ed. Malheiros, Sao Paulo, 1992, pp. 386 y ss. ; BAZÁN, V., *El habeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado op. cit.* p. 97.

³⁸⁹ RODRÍGUEZ VILLAR, P., "La protección de datos personales y la esfera de actuación de las autoridades de control", en , J. A. TRAVIESO (Director), *Régimen Jurídico de los Datos Personales*, tomo I, 1ª ed. Abeledo Perrot. S.A. Buenos Aires, 2014, p. 180.

llega 10 después se limita a regular aspectos procesales del *habeas data* y se obvia todo lo relativo al tratamiento de datos personales.³⁹⁰

Con la protección de datos personales se asegura la protección de la privacidad, el buen nombre y el debido proceso mediante el *habeas data* como garantía procesal usada frecuentemente en Latinoamérica. En este lugar ha ido adquiriendo importancia y relevancia, siendo en algunos casos un derecho y en otros una acción, ya sea judicial o administrativa capaz de exigir respeto de las personas sobre sus datos. Pasamos a exponer, sucintamente, como se prevé el *habeas data* en las diferentes constituciones latinoamericanas.

- Paraguay

La Constitución de Paraguay de 1992 contempla en su artículo 135 la nomenclatura del *habeas data* como una garantía constitucional³⁹¹, fruto de la propuesta de la comisión la cual contó con la participación de investigadores, magistrados y docentes, apoyados en anteriores propuestas normativas³⁹², manifestando que:

“Toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos”³⁹³.

³⁹⁰ PUCCINELLI, O., “Versiones, tipos, subtipos y subespecies de *habeas data* en el derecho latinoamericano...op cit., p. 100.

³⁹¹ REMOLINA ANGARITA, N., *Recolección Internacional de datos personales: un reto del mundo...*op. cit., p. 108.

³⁹² En este sentido basada en la Carta brasileña de 1988, la Constitución colombiana de 1991 y el artículo 31 de la Constitución guatemalteca de 1985, PUCCINELLI, O., *El Habeas data en Indoiberoamérica*, Temis, Bogotá, 1999, p. 551.

³⁹³ Constitución de Paraguay Asunción 1992.
Disponible en: https://www.oas.org/juridico/spanish/par_res3.htm. (Última consulta en línea 20 de marzo 2018).

La Constitución paraguaya reconoce el derecho de todos los paraguayos de contar con el acceso a las informaciones ubicadas en sus archivos privados y oficiales de carácter público. Al mismo tiempo, no sólo otorga el tan llamado derecho de acceso sino que asigna prerrogativas o derechos de actualización, rectificación, destrucción de los datos. Todo ello conecta muy de la mano con los órganos judiciales encargados de recibir dichas solicitudes bajo la representación de sus magistrados, ampliando las prerrogativas del modelo brasileño³⁹⁴.

A diferencia del modelo brasileño, el modelo paraguayo contempla la asignación de un magistrado competente perteneciente al Tribunal de Primera Instancias de lo Civil y Comercial de Turno, conformado por múltiples tribunales y un proceso complejo. Más allá de esas diferencias, solo cuentan con dos leyes relacionadas en materia de protección de datos. Nos referimos a las núm. 1682/01 y 1969/02 orientadas al sector financiero.

En ese sentido, la Ley N.º 1969 del 3 de septiembre de 2002 modifica, amplía y deroga varios artículos de la Ley N.º 1682 del 16 de enero del 2001. Por ello algunos autores, entre ellos, Mario Arrúa de León mantiene la tesis de inexistencia de una *política de protección global sobre las personas* en Paraguay, a raíz de la ausencia de una ley general y existencia de leyes sectoriales³⁹⁵ en la materia³⁹⁶.

³⁹⁴ “...el texto constitucional paraguayo no solamente copia el brasileño, sino que lo amplía, adoptando una mejor definición del *habeas data* y ampliando la tutela de éste al proteger “además de derechos personalísimos (privacidad, no discriminación) y no patrimoniales (convicciones religiosas, ideas políticas, etcétera); áreas de tipo patrimonial, ya que se lo plantea, también para atacar información equivocada sobre los bienes de un individuo o corporación”. QUESADA RODRÍGUEZ, A., *Protección de datos y telecomunicaciones convergentes*, 1ª ed. Agencia Española de protección de datos, Madrid, 2014, pp. 314-315.

³⁹⁵ Normativas relacionadas con la Protección de Datos “Ley N.º 3440, de 16 de julio de 2008, que modifica varias disposiciones de la Ley N.º 1160/97, Código Penal. Ley N.º 4439, de 3 de octubre de 2011, que modifica y amplía varios artículos de la Ley N.º 1160/97, Código Penal. Artículos 146 b; 146 c; 146 d; 174; 174 b; 175; 175 b y 188. Ley N.º 1682, de 16 de enero de 2001, que reglamenta la información de carácter privado. Ley N.º 4017, de 23 de diciembre de 2010, de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico. Ley N.º 4868, de 26 de febrero de 2013, de Comercio electrónico. Ley N.º 4868, de 26 de febrero de 2013, de Comercio electrónico. Decreto N.º 7369, de 23 de septiembre de 2011, por el que se aprueba el Reglamento de la Ley N.º 4017/10. Decreto N.º 1165, de 27 de enero de 2014, por el que se aprueba el Reglamento de la Ley N.º 4868, de

La interposición de la acción de *habeas data* en Paraguay ha permitido la obtención de los archivos de la policía considerados como archivos del terror, revelando la nefasta noticia de personas muertas en las cárceles consideradas desaparecidas durante el período de la dictadura. La revelación fue originada a raíz de la acción de *habeas data* ante el juzgado de Primera Instancia por el Sr. Martín Almada³⁹⁷.

- Perú

La Constitución política del Perú de 1993³⁹⁸ reconoce la acción de *habeas data* estableciendo, en su Título V, artículo 200 numeral 3, las garantías constitucionales que proceden contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos contemplados en el artículo 2 numeral 5 y 6 de la Constitución; de acuerdo al numeral 5: las personas tienen derecho a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional, mediante pedido del juez, del fiscal de la nación o de una comisión investigadora del congreso con arreglo a la ley y siempre que se refieran al caso investigado pueden ser levantados; asimismo, también tienen derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que

Comercio electrónico. Ley N.º 4989, de 9 de agosto de 2013, que crea el marco de aplicación de las tecnologías de la información y comunicación en el sector público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)”.

³⁹⁶ MAYORGA JÁCOME, T. C., GARCÍA JIMÉNEZ, M., CARRIÓN JUMBO, J. L., YARAD JEADA, P. V. y DURET GUTIÉRREZ, J. F., “Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos”, *Revista científica*, dominio de la ciencia, vol. 5, núm. 1, 2019, p. 530. Disponible en: [file:///C:/Users/pc/Dropbox/Documentos/Dialnet-HistoriaDeLaNormativaReguladoraDeLaProteccionDeDat-6869937-1%20\(1\).pdf](file:///C:/Users/pc/Dropbox/Documentos/Dialnet-HistoriaDeLaNormativaReguladoraDeLaProteccionDeDat-6869937-1%20(1).pdf). (Última consulta en línea 23 de Octubre 2019).

³⁹⁷ BAZÁN, V., *El habeas data, su autonomía respecto del amparo*, Anuario de Derecho Constitucional Latinoamericano año XVIII, p. 47.

³⁹⁸ Constitución política de Perú de 1993, *Diario Oficial el Peruano*, 31 de diciembre de 1993. Disponible en: <http://pdba.georgetown.edu/Parties/Peru/Leyes/constitucion.pdf>. (Última consulta en línea 20 de marzo 2018).

afecten la intimidad personal y familiar. De esta manera, conecta con el numeral 7, donde las personas tienen derecho al honor, a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias.

El desarrollo normativo de Perú no se detiene con el plexo constitucional, sino que ha mantenido un progresivo despliegue de legislaciones de carácter sectorial y general. Tales son los casos de: la Ley Orgánica núm. 26,301 del Tribunal Constitucional del 18 de abril de 1994 que regula la tramitación procesal del *habeas data*, modificada por la Ley núm. 26.545 del 10 de noviembre de 1995 y completamente abrogada por la Ley núm. 28.237 que aprueba el Código Procesal Penal del 2004; la Ley núm. 26.470³⁹⁹ orientada a producir transformaciones al proceso constitucional de la acción de *habeas data* y la Ley núm. 27.806 relativa a la Transparencia y Acceso a la Información Pública entre otras. En ese sentido, el proceso transformacional del sistema legislativo peruano continúa su avance, aprobando en el 2011 la Ley núm. 29.733 de protección de datos personales y 2 años después su reglamento, la

³⁹⁹ Cfr. “El *habeas data* establecido por la constitución en su artículo 200, es un procedimiento como lo es un juicio sumario o un juicio ejecutivo, es un trámite rápido que se sigue para proteger determinados derechos, protegiendo los derechos que establece el propio artículo 200 referido al artículo 2º de la constitución en sus incisos 5), 6) y 7), siendo un procedimiento ágil para defender los derechos fundamentales...mediante el *habeas data* cualquier persona tiene derecho a acceder a las informaciones ubicadas en cualquier oficina del Estado. Cambiando el concepto de que la información que estaba en poder del Estado era del Estado, de acuerdo al nuevo concepto de la constitución, donde la información que está en poder del estado es de la población, de los ciudadanos, siendo el estado él solo administrador de esa información, es decir el *habeas data* es un procedimiento de carácter judicial cuyo objeto es proceder determinados derechos mediante un proceso rápido siendo el primer derecho Obtener Información.

El segundo derecho del artículo 200 es proteger la intimidad de las personas dentro del proceso de informatización de la vida moderna...la información que está en poder del estado es de la población, de los ciudadano, el Estado sólo es administrador de esa información, el *habeas data*, en segundo lugar, sirve para impedir que alguien negocie información privada a través de cualquier sistema de cómputo...garantizando los derechos fundamentales en la vida moderna; ...pero no existe consenso en el tercer derecho donde cualquier ciudadano puede pedir una rectificación sobre una información que daña su honorabilidad o que no es correcta o no es cierta.

...en cuanto a la aplicación del procedimiento del *habeas data*, hay acuerdo solo para los dos primeros derechos....para obtener información y para proteger la intimidad, se debate y aprueba el proyecto sustitutorio de reforma constitucional sobre la Acción de *habeas data*, pero no sirve, como procedimiento, para rectificar las informaciones que se dan.....”, Ley N.º 26470, “se debate y aprueba el proyecto sustitutorio de reforma constitucional sobre la Acción de *habeas data*” primera legislatura ordinaria de 1994, 5.ª A Sesión Vespertina, miércoles 17 de agosto de 1994. Disponible en:

<http://www4.congreso.gob.pe/dgp/constitucion/Const93DD/reforconst/Ley26470.pdf>. (Última consulta en línea 24 de abril 2018).

referida ley tiende a regular la materia en cuestión, insertando principios existente en legislaciones anteriores como el consentimiento previo, informado, expreso o inequívoco, sin dejar a un lado la necesidad de información suficiente, garantizando los derechos consagrados en el artículo 2 y 6 de la Constitución.

- Venezuela

El artículo 28 de la Constitución de Venezuela de 1999 otorga a las personas el derecho de acceder a sus datos ubicados en registros oficiales y privados, con la posibilidad de conocer el uso que se haga de los mismos y su finalidad, contemplando medidas para los datos erróneos o que afecten los derechos del dueño. En definitiva estamos delante de la acción de *habeas data*, aunque no contemple su naturaleza léxico jurídica.

La Defensoría del Pueblo⁴⁰⁰ contempla entre sus atribuciones la defensa y vigilancia de los derechos establecidos en la Constitución de la República Bolivariana de Venezuela, interponiendo acciones de inconstitucionalidad, entre ellas el *habeas data* o cualquier otro recurso procedente de conformidad con la ley⁴⁰¹.

En ese sentido. la Constitución Venezolana del 2011⁴⁰² es la carta magna vigente de Venezuela, admitida el 15 de diciembre de 1999, sometida a la enmienda N.º 1 de la Asamblea Nacional, sancionada el 14/12/2009, aprobada en referéndum constitucional el 15/2/2009, siendo promulgada por el Presidente de la República bolivariana de Venezuela Hugo Chávez Frías, el 19 de febrero de 2009, plantea de manera léxico-jurídica la figura del *habeas data*

⁴⁰⁰ Artículo 281, *Constitución de la República Bolivariana de Venezuela*.

⁴⁰¹ República Bolivariana de Venezuela, *Asamblea Nacional Constituyente*. 1999. *Constitución de la República Bolivariana de Venezuela*, Gaceta Oficial Extraordinaria N.º 36.860 de fecha 30 de diciembre de 1.999. Disponible en: https://www.oas.org/dil/esp/constitucion_venezuela.pdf. (Última consulta en línea 23 de marzo 2018).

⁴⁰² Publicada en *Gaceta Oficial* N.º 5.908 extraordinario, de fecha 19 de febrero de 2009. Ediciones de la Asamblea Nacional Impreso en la Imprenta Nacional y Gaceta Oficial. Depósito Legal: Lf78420093401032 Caracas, abril de 2009.

a diferencia de sus antecesoras, reconociendo por vez primera en el constitucionalismo venezolano, el *habeas data*⁴⁰³ o.

“ El derecho de las personas de acceso a la información que sobre sí mismas o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley. El *habeas data* incluye el derecho de las personas de conocer el uso que se haga de tales registros y su finalidad, y de solicitar ante el tribunal competente su actualización, rectificación o destrucción, si fuesen erróneos o afectasen ilegítimamente sus derechos”⁴⁰⁴.

- Panamá

El proceso constitucional del *habeas data* en Latinoamérica no siempre se origina desde la carta magna y su posterior desarrollo legislativo sino que su desarrollo normativo procede e inicia desde la concepción primigenia de sus leyes generales seguido de su constitucionalización. En el caso de Panamá se reconoce de manera léxico-jurídica la figura del *habeas data* de este modo; comienza en la ley para luego pasar a formar parte de su carta magna. Pasamos a exponerlo.

La acción de *habeas data* panameña ubicada en el artículo 44 de la reforma constitucional del 15 de noviembre de 2004 otorga a las personas la capacidad de promover la llamada acción de *habeas data*, garantizando el acceso a sus informaciones personales ubicadas en bancos de datos, registros oficiales o particulares, permitiendo la actualización, rectificación, supresión, o solicitar la confidencialidad de la información o los datos de carácter personal; la acción constitucional fue precedida del precepto legislativo núm. 6 del 22 de enero de 2002⁴⁰⁵, positivándose constitucionalmente.

⁴⁰³ Cursivas nuestras.

⁴⁰⁴ *Constitución de Venezuela 1999*.

Disponible en: <http://www.minci.gob.ve/wp-content/uploads/2011/04/CONSTITUCION.pdf> (Última consulta en línea 23 de marzo 2018).

⁴⁰⁵ Publicada en *Gaceta Oficial*, n.º 24476 de 23 de enero 2002.

La Constitución panameña⁴⁰⁶ ha recibido importantes reformas constitucionales pautadas por el acto legislativo núm. 1 de 2004.

El artículo 43 de la Constitución permite las solicitudes de información de acceso público o de interés colectivo, ya sean estos almacenados en archivos de servidores públicos o personas privadas que presten servicios públicos, con la salvedad de que no se encuentren limitados por disposición escrita o mandato de la ley. Al mismo tiempo, como expresa el artículo 44, por medio de la acción de *habeas data* la persona puede solicitar la actualización, corrección, rectificación o supresión de los datos.

- Honduras

La Constitución de Honduras del año 1982⁴⁰⁷ incluida sus reformas⁴⁰⁸, actualizada con el Decreto 36 del 4 de Mayo de 2005, contempla en su artículo 182 la figura del *habeas data*, ubicado en el Título IV del capítulo I, bajo la denominación del *habeas corpus*, *habeas data* y el amparo. Esta denominación fue modificada por el Decreto 243 del año 2003 y un desarrollo posterior con el Decreto Legislativo N.º 381-2005⁴⁰⁹

⁴⁰⁶ Aprobada el 11 de octubre de 1972. Dicha constitución ha estado sujeta a diversos actos reformativos como los de 1978, al Acto Constitucional de 1983, a los actos legislativos N.º 1 de 1993 y N.º 2 de 1994, y el acto legislativo N.º 1 de 2004 referenciado al texto único publicado en la *Gaceta Oficial* n.º 25.176 del 15 de noviembre de 2004. *Constitución de Panamá de 1972*. Disponible en: <http://pdba.georgetown.edu/Constitutions/Panama/vigente.pdf> (Última consulta en línea 23 de marzo 2019).

⁴⁰⁷ *Constitución política de la República de Honduras de 1982*. Disponible en: https://www.oas.org/dil/esp/Constitucion_de_Honduras.pdf (Última consulta en línea 25 de marzo 2018).

⁴⁰⁸ La Constitución política de la República de Honduras de 1982, incluye Reformas de 1982, 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 y 2005.

⁴⁰⁹ “se reformó el Capítulo I, del Título IV de la Constitución de la República, donde el Estado de Honduras reconoce la garantía del HABEAS DATA: “Que toda persona tiene el derecho a acceder a la información sobre si misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y /o enmendarla.” Legislación República de Honduras. Disponible en: <http://www.redipd.es/legislacion/honduras-ides-idphp.php> (Última consulta en línea 18 de noviembre 2019).

En ella, el Estado reconoce tanto la figura del *habeas corpus* o exhibición personal, como el *habeas data*, enfatizando que en el caso del *habeas data* solamente puede ser promovida por la persona afectada, evitando todo tipo de poder o formalidades conocida únicamente por la sala de lo constitucional de la Corte Suprema de Justicia; en caso de no admitir la acción constitucional, incurrirían en responsabilidades penales y administrativas, cometiendo delito de detención ilegal para aquellas autoridades o agentes que ejecutasen el ocultamiento, como lo expresa el artículo mencionado.

- República Dominicana

En ese sentido, la Constitución de la República Dominicana recoge la acción del *habeas data* en el artículo 70 de la carta magna del 2010 y también lo hace en el mismo precepto de la actual Constitución del 2015. Se tratan de constituciones garantistas en lo que a materia de derechos fundamentales se refiere, reflejo de la democratización del Estado dominicano bajo los influjos de las constituciones europeas y latinoamericanas. No nos detenemos en este lugar, pues un estudio detallado se presentará en el capítulo III del trabajo, donde abordaremos el *habeas data* desde su contexto doctrinal, constitucional, pasados proyectos y la actual Ley núm. 172-13 concebida para tutelar tales derechos.

- Ecuador

En el caso de Ecuador, el artículo 92 de la Constitución del 2008 reconoce la salvaguarda de la autodeterminación informativa mediante la implementación de la acción de *habeas data* contemplado en la sección quinta del mencionado artículo, donde:

“Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso

que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos⁴¹⁰.”

Conforme a este precepto, las personas tienen el derecho de acceder a sus datos personales y conocer el uso que se haga de los mismos, así como el conocimiento sobre su uso, finalidad, origen, tiempo y destino de la información personal, solicitando la actualización, rectificación, eliminación o anulación de los datos; exigiendo la adopción de medidas necesarias de seguridad cuando se refiera a datos sensibles. La Constitución ecuatoriana (sustituida) contemplaba la acción en el capítulo 94.

La cuarta sección de la Constitución ecuatoriana, contempla en su artículo 91 la acción de acceso a la información pública, garantizando su acceso cuando ha sido denegada o no sea fidedigna.

- Argentina

La actual constitución de la República de Argentina nace con la reforma constitucional del 1994, la cual introduce nuevos derechos y garantías como los derechos de tercera y cuarta generación, contemplando la acción de *habeas data*⁴¹¹. Unos derechos presentes en la constitución en el segundo capítulo de la primera parte y el tercer párrafo del artículo 43. Pero a diferencia de otros textos constitucionales no hace mención de la figura del *habeas data*, es decir, no se ha literalizado la figura⁴¹², pero sí su accionar para tomar conocimiento

⁴¹⁰ *Constitución de la República de Ecuador 1998*. MIRAR 2008

Disponible en: http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf. (Última consulta en línea 13 de abril 2018).

⁴¹¹ “ Se debe caracterizar el caso de Argentina como particular (y ejemplar) en tanto cuenta con un sistema de *habeas data* de gran calidad, al punto que a la fecha es miembro del reducido grupo de países americanos cuyo sistema de protección de datos ha sido formalmente reconocido como adecuado, por la Comisión Europea”. QUESADA RODRÍGUEZ, A., *Protección de datos y telecomunicaciones convergentes*, 1ª ed. Agencia Española de protección de datos, Madrid, 2014, p. 326.

⁴¹² “ Para entender el porqué de la falta de utilización expresa de la denominación *habeas data* se interpone evocar que la ley n.º 24309 que declaró la necesidad de la reforma constitucional Argentina que terminó plasmándose en 1994, habilitaba a la Convención Constituyente a debatir la “consagración expresa del *habeas corpus* y del amparo” ...sin mencionar al *habeas data*...en los artículos 6 y 7 de la ley se estableció una fuerte proscrición y una no menos dura sanción consecuente prefigurada para toda transgresión a las pautas que el Congreso fijaba a la Convención en cuanto a lo que esta podía modificar y al modo como debía hacerlo,

de los datos a ellas referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística. El mismo artículo contempla el amparo y el habeas corpus, dando posibilidad a las personas de interponer ambas acciones de forma rápida y expedita, tutelando derechos de intimidad. Es decir, se presenta como una variable del amparo.⁴¹³

La Ley núm. 25.326 de protección de datos personales del 4 de octubre del 2000, reconoce bajo el capítulo VII, artículo 33, la acción de protección de los datos personales o mejor conocida como *habeas data*. Se trata de una acción destinada al conocimiento de los datos personales e implementación de medidas tendentes en asegurar la correcta información⁴¹⁴. El fundamento de la protección de datos en Argentina se ancla en esta ley y en el Decreto regulatorio núm. 1558/2001 y sus normas. La ley reglamenta el *habeas data*, permitiendo la posibilidad a su titular de interponer dos procesos, uno prejudicial y otro judicial. El Decreto aprueba la reglamentación de la ley y crea la Dirección Nacional de Protección de Datos Personales como órgano de control.

bajo pena de nulidad de lo reformado en violación a dichos lineamientos.” BAZÁN, V., *El habeas data, su autonomía respecto del amparo*, Anuario de Derecho Constitucional Latinoamericano año XVIII, Bogotá Colombia, 2012, p. 51.

⁴¹³ Sobre esta cuestión, RODRÍGUEZ MARCANO, E. R., *El derecho a la autodeterminación informativa en Venezuela*. Universidad nacional de educación a distancia, Madrid, 2013, pp. 121-126.

⁴¹⁴ Artículo 33, *Ley núm. 25.326 Protección de los datos personales Argentina*

1. La acción de protección de los datos personales o de *habeas data* procederá:

a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;

b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/iberoamerica/leyes_nacionales/common/pdfs/LEY-25.326-Proteccion-de-los-datos-personales.pdf. (Última consulta en línea 23 de marzo 2018).

La acción de *habeas data* contemplada en la Ley núm. 25.326 procederá cuando sea necesario tomar conocimiento de los datos personales, siendo ejercida por los afectados, tutores, sucesores, representantes legales o coadyuvados por el Defensor del Pueblo en caso de posible falsedad, inexactitud, desactualización, siendo competente el juez del domicilio del actor del demandado o el del lugar del hecho, tramitado por las disposiciones de la presente ley, siendo interpuesta por medio escrito, alegando las razones de la acción y con un plazo de respuesta de 5 días⁴¹⁵.

La acción de *habeas data* es de la competencia tanto del juez del domicilio del actor del demandado o el lugar del hecho.

Es así como, al unísono de los cambios constitucionales ocurridos en las naciones latinoamericanas, se teje un movimiento legislativo en franca evolución y constante desarrollo, con transformaciones necesarias para adaptar nuestras normas legislativas a los procesos de democratización y transformación legislativa, conectados con los cambios tecnológicos que impactan y repercuten en nuestras naciones. Ante tal realidad, presentamos las siguientes legislaciones que debido a su influencia impactan los Estados iberoamericanos.

5.4. Incorporación del *habeas data* en normas generales de protección de datos

Estados que no contemplan la figura del habeas data en sus normas constitucionales

Las reformas constitucionales en América Latina durante los años 80 y siguientes han contribuido con la inserción de la figura del *habeas data* en sus cartas magnas. Sin embargo, la incursión del *habeas data* en Latinoamérica no

⁴¹⁵ Capítulo VII, artículo 33 al 43 Ley 25, 326. *Protección de los Datos Personales*.

solo se materializa vía sus normas constitucionales, sino, que existen Estados Latinoamericanos cuya entrada del *habeas data* se configura vía sus leyes generales y sectoriales.

Como ya hemos mencionado, en esta ocasión presentamos los Estados que no contemplan en su acervo constitucional la figura del *habeas data*, más si en sus legislaciones internas, sectorial o jurisprudencial.

A continuación, presentamos la incursión del *habeas data* en las normas generales o específicas de los Estados Latinoamericanos.

- Bolivia

La Constitución de Bolivia del 2009⁴¹⁶ contempla la acción de protección de privacidad, una especie de símil de la acción de *habeas data*. La acción se presenta en el artículo 130⁴¹⁷ de la Constitución política del Estado, aprobada mediante referéndum del 25 de enero de 2009. Con ella, se deroga la constitución de 1967 y también la del 2004. Esta última consideraba en el artículo 23⁴¹⁸ la disposición léxico-jurídica del *habeas data*.

⁴¹⁶ Constitución de Bolivia 2009.

Disponible en: https://www.oas.org/dil/esp/Constitucion_Bolivia.pdf (Última consulta en línea 21 de marzo 2018).

⁴¹⁷ SECCIÓN III ACCIÓN DE PROTECCIÓN DE PRIVACIDAD Artículo 130. I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad. Disponible en: https://www.oas.org/dil/esp/Constitucion_Bolivia.pdf. (Última consulta en línea 23 de marzo 2017).

⁴¹⁸ Artículo 23. Constitución de Bolivia 2004.

- I. Toda persona que creyere estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos, de datos públicos o privados que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de "*Habeas Data*" ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección suya.
- II. Si el Tribunal o Juez competente declara procedente el recurso, ordenará la revelación, eliminación o rectificación de los datos personales cuyo registro fue impugnado.

Por tanto, vemos como tras la reforma de la Constitución del 2009, la acción de *habeas data* se transforma o más bien se cambia por una acción de protección de privacidad, reconociendo la autodeterminación informativa a través de la acción de protección de la privacidad, logrando realizar una tendencia de aproximación a la autodeterminación informativa, pero alejándose de su carácter autóctono reconocida como *habeas data*. A pesar de ello, la acción apunta a la imagen y reputación, no centrando sus esfuerzos en los datos, creando con ello una situación confusa no comprendida a su totalidad, por no dejar claridad respecto al objetivo protegido⁴¹⁹.

- México

Las leyes mexicanas conectadas con la materia de protección de datos⁴²⁰ tienen su génesis en las disposiciones y normas estatutarias contempladas en la carta magna mexicana del 2017, incluido su proceso de reforma del 2009⁴²¹,

-
- III. La decisión que se pronuncie se elevará en revisión, de oficio ante el Tribunal Constitucional, en el plazo de veinticuatro horas, sin que por ello se suspenda la ejecución del fallo.
 - IV. El recurso de "*Habeas Data*" no procederá para levantar el secreto en materia de prensa.
 - V. El recurso de "*Habeas Data*" se tramitará conforme al procedimiento establecido para el Recurso de Amparo Constitucional previsto en el Artículo 19º de esta Constitución.

Disponible en: <https://www.lexivox.org/norms/BO-CPE-20040413.html#idm4333904>. (Última consulta en línea 19 de marzo 2019).

⁴¹⁹ LÓPEZ CARBALLO, D. (Coordinador), *Protección de datos y habeas data: una visión desde Iberoamérica*, imprenta nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2015, p. 133.

⁴²⁰ "La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (Cámara de Diputados de H. Congreso de la Unión, 2002), la Ley Federal de las Entidades Paraestatales (Cámara de Diputados del H. Congreso de la Unión, 1986), la Ley Federal de Procedimiento Administrativo (Cámara de Diputados del H. Congreso de la Unión, 1994), la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos Cámara de Diputados del H. Congreso de la Unión, 2002) y especialmente las disposiciones de la Ley Federal de Protección de datos Personales en posesión de los Particulares (Cámara de Diputados de H. Congreso de la Unión, 2010). QUESADA RODRÍGUEZ, A., *Protección de datos y telecomunicaciones convergentes*, 1ª ed. Agencia Española de protección de datos, Madrid, 2014, p. 338.

⁴²¹ "...en el 2009 se establece expresamente en el art. 16 de la Constitución Federal el derecho a la protección de datos personales, como lo son aquellos de acceso, rectificación, cancelación y oposición (denominados por su acrónimo como derechos ARCO), MUÑOZ FRANCO, G., *La Protección de Datos Personales en México*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, op.cit., p. 1046.

destacando la Ley Federal de Transparencia del 2002 y la Ley de Acceso a la Información Pública del 2012.

México forma parte de los países no certificados por la Comisión Europea en materia de protección de datos, siendo un sistema robusto, que no cuenta con los votos suficientes para ser acreedor de la certificación. No obstante, continúan los esfuerzos en modificar sus normas y adaptarlas a los cambios jurídicos y tecnológicos que inciden en el escenario mundial.

No obstante, México pasa a formar parte de los Estados que se adhieren al Convenio 108 del Consejo de Europa, y en esa misma línea integra bajo un mismo órgano de control las normas de transparencia, acceso a la información pública y protección de datos personales, convirtiéndose en referente internacional.

- Costa Rica

La Constitución de Costa Rica no contempla la figura del *habeas data* propio o tradicional; el artículo 30 contempla el *habeas data* impropio, permitiendo el acceso a los departamentos administrativos, siendo reconocidos los principios del *habeas data* mediante su jurisprudencia constitucional, permitiendo el acceso a los departamentos administrativos y proveyendo a los costarricenses de una garantía procesal.

En 1996 se presentó un proyecto de reforma con la intención de incluir el *habeas data*. Los resultados no fueron satisfactorios por no llegar a una conclusión, siendo desestimado por la sala de lo constitucional de la Corte Suprema, a pesar de ello, persisten los esfuerzos para constitucionalizar el *habeas data*.

El marco regulatorio de Costa Rica es muy amplio, incluida su Ley núm. 8.968 de Protección de la Persona frente al Tratamiento de sus Datos Personales del 7 de julio del 2011 incluido su Reglamento instituido con el Decreto N.º. 37554-JP y su Ley General de Telecomunicaciones núm. 8.642.

En igual sentido mediante la Directriz 046-H-MICITT, de 9 de abril de 2013 se tejen las normas vinculadas con la computación en las nubes en el sector de las instituciones públicas, y con el Decreto Ejecutivo 40008⁴²² se reforma el pasado reglamento instituido con el Decreto N.º. 37554-JP⁴²³.

- Uruguay

El proceso legislativo de Uruguay se enmarca en una serie de normas legislativas, cuyos resultados se concretizan con el reconocimiento de Uruguay como Estado adecuado en materia de protección de datos⁴²⁴. Iniciamos con la Ley núm. 18.331 de Protección de Datos y *Habeas Data* del 11 de agosto del 2008, una ley sustituta de la Ley núm. 17.838 de 24 de septiembre de 2005 que le asigna a la protección de datos el rango de derecho fundamental e inserta la acción del *habeas data* en la norma legislativa núm. 18.331⁴²⁵; además se complementa con lo reglamentado por los decretos 664/008 de 22 de diciembre de 2008 y 414/09 de 31 de agosto de 2009⁴²⁶, regulando a su vez los caracteres generales del *habeas data* e incorporando sus principios tomando en cuenta los derechos asignados a los titulares de los datos⁴²⁷.

⁴²²Legislación República de Costa Rica. Disponible en: <http://www.redipd.org/legislacion/costarica-ides-idphp.php>. (Última consulta en línea 18 de noviembre 2019).

⁴²³Legislación República de Costa Rica. Disponible en: <http://www.redipd.org/legislacion/costarica-ides-idphp.php>. (Última consulta en línea 18 de noviembre 2019).

⁴²⁴ Considerando II, Decreto núm. 414/009, Protección de Datos Personales – Acción de Hábeas Data, Disponible en: https://www.agesic.gub.uy/innovaportal/v/295/1/agesic/decreto-n%C2%B0-414_009-de-31-agosto-de-2009.html. (Última consulta en línea 5 de abril 2018).

⁴²⁵ Capítulo VIII, Ley núm. 18.331 de Protección de datos personales y acción de *habeas data*. Disponible en: <https://www.agesic.gub.uy/innovaportal/v/302/1/agesic/ley-n%C2%B0-18331-de-11-de-agosto-de-2008.html>. (Última consulta en línea 18 de abril 2018).

⁴²⁶ ROTONDO, F., *Protección de Datos Personales en la República de Uruguay*, en J. A. TRAVIESO, (Director), *Régimen Jurídico de los Datos Personales*, op.cit., p. 1131.

⁴²⁷ GAIERO GUADAGNA, B, y SOBA BRACESCO, I. M., *El proceso de habeas data en Uruguay (protección de datos personales y acceso a la información pública)*, Anuario de Derecho Constitucional Latinoamericano, año XVI, Konrad Adenauer Stiftung, Montevideo, Uruguay, 2010, p. 339.

La ley incorpora la acción de protección de datos personales a través de la cual los ciudadanos uruguayos tienen la posibilidad de conocer sus datos personales emprendiendo una acción judicial sin importar su ubicación, ya sea que se encuentren en una base pública o privada, exigiendo su rectificación, inclusión o supresión cuando estos presenten falsedad o error. La acción podrá ejecutarse cuando los datos hayan sido denegados fuera de los plazos previstos por la ley, o en caso de haber sido solicitados al responsable de la base de datos y éste se haya denegado, siendo competentes para conocer de la acción los Juzgados de Primera Instancia en lo Contencioso Administrativo cuando el sujeto incumplidor le corresponde al Estado o los Juzgados de Primera Instancia en lo Civil.

Al mismo tiempo, la acción puede interponerse por el afectado o su representante, siendo aplicable para las personas jurídicas. La ley contempla la legitimación, los tramites empleados en primera instancia, las medidas provisionales correspondiente al amparo, así como los recursos de apelación y segunda instancia empleado, dejando claro que éste solo podrá ser apelado cuando se trate de sentencia definitiva o aquellas rechazadas por ser improcedentes, dando la oportunidad de plantear acciones de inconstitucionalidad ya sean esta por vía de excepción u oficio⁴²⁸.

Seis meses después de la promulgada Ley núm. 18.331 del 11 de agosto de 2008, ve la luz la Ley núm. 18.381 de Acceso a la Información Pública del 17 de octubre de 2008 regulando el derecho a la información pública. En esta ocasión, estamos ante un *habeas data* impropio tal y como vimos cuando nos referimos al tema de los tipos de *habeas data*. Por tanto, el *habeas data* de la Ley núm. 18.331 obedece al reconocido y ya externado *habeas data* propio o referenciado a las personas físicas mientras que al igual que lo externado en la Ley núm. 18.381 (de Acceso a la Información Pública) su legitimación aplica tanto para personas físicas como jurídicas en el ejercicio del acceso a la información pública.

⁴²⁸ Artículos 38-45 de la Ley núm. 18.331.

La iniciativa legislativa permite un acercamiento y alineación con la Directiva 95/46/CE, instaurando la Unidad Reguladora y de Control de Datos Personales como órgano de control, separada de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), bajo la dirección de un Consejo conformado por tres miembros, dos de los cuales son asignados por el Poder Ejecutivo y un tercero reservado para el director de la AGESIC. El órgano estará revestido de capacidad sancionadora y de suspensión⁴²⁹.

- Colombia

El *habeas data* en Colombia ostenta la condición de derecho fundamental⁴³⁰ al igual que la intimidad⁴³¹, a pesar de no ser reconocido constitucionalmente. La Constitución de 1991 recoge en su artículo 15 “el derecho de las personas a su intimidad personal y familiar... derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas”. El mismo artículo respeta la libertad y otras garantías por medio a la recolección, el tratamiento y la circulación de datos, solicitando en algunos casos, la presentación de libros o documentos privados de acuerdo a lo señalado en la ley y consagrado en la Constitución Colombiana.

El término de *habeas data* brillaba por su ausencia en la regulación colombiana si bien, fue introducido el 19 de noviembre de 1991 mediante el Decreto 2591, antes del período mencionado⁴³², después de pasar por

⁴²⁹ PÉREZ PONTE, M., *Facultades y atribuciones del órgano de control de la ley nacional de protección de datos personales 25.326*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo I, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, Argentina, 2014, p. 182.

⁴³⁰ Así lo expresa CIFUENTES MUÑOZ, E., “El Habeas data en Colombia, en Derecho PUC”, *Revista de la Facultad de Derecho de la Pontificia Universidad Católica del Perú*, núm. 51, diciembre de 1997, publicado en 199, Lima, p, 122

⁴³¹ BEATRIZ CALLE, S., *Apuntes jurídicos sobre la protección de datos personales a la luz de la actual norma de habeas data en Colombia 2009*, p. 126.

⁴³² “...los intentos de regulación del derecho a la intimidad. Antes de la expedición de la Constitución Política de 1991, cabe destacar el proyecto de Ley N.º 73 de 1986...Después de la expedición de la Constitución Política a través de proyectos como el número 070 de 1997.de

múltiples discusiones internas en la Asamblea Constituyente vía su comisión, y motivadas por la necesidad de proteger al individuo de la publicación de bases de datos morosas y crediticias, a raíz de la existencia y desarrollo de tecnologías capaces de colocar en riesgo la intimidad y aquellos derechos protegidos en el individuo ante su posible publicación y la necesidad de inversión extranjera, se consiguió bajo el amparo y apoyo de los congresistas muy larga en la legislación del 2006, dando luz al proyecto de Ley núm. 027 de 2006 y la Ley núm. 1.266 de 2008.

Bajo la Ley estatutaria núm. 1.266 del 31 de diciembre del 2008, compuesta de 7 capítulos y 22 artículos se dictan las disposiciones generales del *habeas data*, regulando el manejo de la información contenida en bases de datos personales con especial interés en la financiera, crediticia, comercial, de servicios y la proveniente de terceros países dictando otras disposiciones.

La ley, desarrolla el plexo constitucional, estableciendo la capacidad que tienen las personas de:

“... conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personal esa que se refiere el artículo 15 de la Constitución Política.....particularmente en relación con la información financiera y crediticia, comercial de servicios y la proveniente de terceros países”⁴³³.

Aplicable a todos los datos de información personal ya sean estos de naturaleza pública o privada, contemplado en su artículo 2.

protección de la intimidad personal y el buen nombre frente a los sistemas de información y los bancos de datos...la ley estatutaria números 115 de 1997, N.º 52 de 2000 y 124 de 2001...pretendía desarrollar el artículo 15 de la Carta...la ley estatutaria N.º.64 de agosto de 2003 y 143 de 2003...” BEATRIZ CALLE, S., *Apuntes jurídicos sobre la protección de datos personales a la luz de la actual norma de habeas data en Colombia*, Apuntes jurídicos sobre la protección de datos personales a la luz de la actual norma de *habeas data* en Colombia, Colombia, 2009, pp. 126-128.

⁴³³ Art. 1, Ley estatutaria N.º 1266 del 31 de diciembre de 2008 por la cual se dictan las disposiciones generales del *habeas data* y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Disponible en: <http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/Ley%201266%20de%2031%20de%20diciembre%202008.pdf>. (Última consulta en línea 23 de marzo 2018).

En esta norma no se contempla el acceso a las bases de datos para fines de inteligencia del Estado del Departamento Administrativo de Seguridad (DAS) y de la fuerza pública para garantizar la seguridad nacional interna y externa; igualmente se excluyen los datos pertenecientes al ámbito personal, doméstico o a los usados internamente.

El *habeas data* ha sido ratificado y confirmado en varias sentencias emanadas por el Tribunal Constitucional colombiano, entre ellas la C-993/04⁴³⁴ del 12 de octubre de 2001 y la Sentencia del 26 de septiembre bajo el número C-981/05, donde se establece el objeto de instauración del *habeas data* siendo el de:

“Evitar que el individuo perdiera la posibilidad de controlar su propia información y no saber quién pudiera hacer uso de ella. De esta manera, se encontró que la forma de subsanar esto era otorgarle la posibilidad a la persona natural o jurídica de rectificar, actualizar o corregir los datos que sobre ella existan; esto a través del *habeas data*”⁴³⁵.

Más allá de la Ley núm. 1.266 del 2008, el Congreso de la República ha desarrollado diferentes normas jurídicas tendentes a fomentar el *habeas data* y la protección de datos personales, tales son los casos de la Ley núm. 1.273 de 2009, la Ley núm. 1.581 de 2012, la Ley núm. 1.621 de 2013 y el proyecto de Ley núm. 090 de 2014 que establece modificaciones a la Ley núm. 1.266 relacionada con el sistema financiero, crediticio, comercial, y terceros países, convirtiéndose en un sistema robusto, a pesar de no ser considerado entre los países certificados por la Comisión Europea⁴³⁶.

⁴³⁴ Sentencia núm. C-993/04 *Habeas data*.

Disponible en: <http://www.corteconstitucional.gov.co/relatoria/2004/C-993-04.htm>. (Última consulta en línea 24 de marzo 2018).

⁴³⁵ Sentencia núm. C-981/05 *Reserva de Ley estatutaria - Criterios para su determinación respecto de derechos fundamentales*. Disponible en: <http://www.corteconstitucional.gov.co/relatoria/2005/c-981-05.htm>. (Última consulta en línea 24 de marzo 2018).

⁴³⁶ QUESADA RODRÍGUEZ, A., *Protección de datos y telecomunicaciones convergentes*, 1ª. ed. Agencia Española de protección de datos, Madrid, 2014, pp. 330-332.

- Chile

La República de Chile no cuenta en su haber con un reconocimiento constitucional de la acción del *habeas data*, o de disposiciones de protección de datos. Ante tales cuestiones, ha iniciado un proceso de adecuación y mejoras constitucionales mediante la modificación constitucional, con la intención de adecuar la carta magna a los nuevos estándares internacionales en materia de protección de datos existente en Europa y organismos internacionales⁴³⁷.

En ese sentido, el 11 de junio del 2002 se promulgó la Ley núm. 19.812, introduciendo modificaciones a la Ley núm. 19.628 sobre protección de la vida privada para favorecer la reinserción laboral de las personas desempleadas, .siendo publicada la pieza legislativa dos días después de su promulgación, dígase el 13 de junio del 2002⁴³⁸. El reglamento de la Ley núm. 19.628 instituye el Registro de Bancos de Datos Personales a cargo de la inscripción de todos los bancos de datos personales empleados por las autoridades u organismos. El Registro estará bajo la administración de los organismos públicos⁴³⁹, sujetando a la propia ley el tratamiento de los datos personales ubicados en registros públicos o privados.

Con el Decreto 779. La Ley 20.575 implementa el principio de finalidad para aquellos datos personales de índole económica, financiera, bancaria, comercial; con responsabilidad de implementar los principios de legitimidad,

⁴³⁷ “El Ministerio de Economía de Chile elaboró una propuesta de ley con el fin de avanzar en la legislación de datos para cumplir con los estándares Internacionales....para elaborar el anteproyecto de ley se consideró la legislación internacional, en especial la Resolución de Madrid, las Directrices de la Unión Europea y la OCDE y la experiencia de países como México, Costa Rica y Uruguay” LÓPEZ CARBALLO, D. (Coordinador), *Protección de datos y habeas data: una visión desde Iberoamérica*, imprenta nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2015, p. 32.

⁴³⁸ Biblioteca del Congreso Nacional de Chile., *Historia de la Ley núm. 19.812*. Disponible en: <https://www.bcn.cl/historiadelaley/historia-de-la-ley/vista-expandida/5947/>. (Última consulta en línea 3 de abril 2018).

⁴³⁹ PÉREZ PONTE, M., *Facultades y atribuciones del órgano de control de la ley nacional de protección de datos personales 25.326*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo I, 1ª ed., ABELEDOPERROT S. A., Buenos Aires, Argentina, 2014, p. 180.

acceso, oposición, información, calidad de los datos, finalidad, proporcionalidad, transparencia, no discriminación, limitación de uso y seguridad en el tratamiento para los responsables de los datos y sus distribuidores, si bien la propia Ley núm. 19.628 contempla en el título V la responsabilidad de las personas naturales, jurídicas, organismos públicos de indemnizar ante cualquier daño ocasionado por un tratamiento indebido de los datos, o proceder de acuerdo a lo ordenado por un tribunal o el titular de los datos con su eliminación, modificación, bloqueo. El monto acordado será dispuesto por el juez en base a la gravedad y las circunstancias del caso.

- Nicaragua

En igual contexto, el *habeas data* nicaragüense no se encuentra reconocido en la Constitución de Nicaragua de 1987, pero sí es contemplado en su ley de amparo n.º 49, reconocida por medio de la Ley núm. 831 del 30 de enero del 2013, garantizando y tutelando los datos personales. A través de esta reforma se realiza un acercamiento de la figura del *habeas data*, permitiendo a los ciudadanos la posibilidad de interponer el recurso a través de la sala constitucional de la Corte Suprema de Justicia, en caso de que sus derechos de privacidad sean vulnerados⁴⁴⁰.

- Guatemala

La Constitución del 1985, contempla las disposiciones establecidas en su reforma del 1993, presentada previamente.

La Constitución política de la República de Guatemala del 17 de noviembre de 1993 no contempla en su plexo constitucional la figura del *habeas data* o la protección de datos personales en su forma léxico-jurídica. A pesar de ello, conserva el derecho de las personas de acceder y corregir informaciones registradas en archivos estatales, tal como se muestra a continuación en el artículo 31.

⁴⁴⁰ LÓPEZ CARBALLO, D. (Coordinador), *Protección de datos y habeas data: una visión desde Iberoamérica*, imprenta nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2015, pp. 91-92.

“Acceso a archivos y registros estatales. Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización.....”⁴⁴¹

El Estado Libre Asociado de Puerto Rico⁴⁴², la República del Salvador y Cuba no reconocen la acción o figura del *habeas data* en su Constitución,

A pesar de lo anterior, el Salvador contempla un marco regulatorio en materia de garantía a la intimidad vía constitucional (Art. 2), acceso a la información pública por medio al Decreto núm. 534 de 2011 que instituye la ley⁴⁴³.

Después de presentar la conformación del *habeas data* en los plexos constitucionales y legislaciones de los Estados Latinoamericanos, pasamos a exponer a manera de conclusión el desarrollo doctrinal del concepto que bebe de las corrientes doctrinales españoles antes expuestas.

5.5. Perspectivas del derecho a la protección de datos en Latinoamérica

Como hemos comentando y para ir concluyendo, se ha de poner de manifiesto que la tesis mantenida por Pérez Luño del trinomio (libertad informática-autodeterminación informativa-*habeas data*) es asumido por la gran mayoría de la doctrina. Esa procesalización ocurrida en Latinoamérica se debe -como señala el propio autor- a que “los países subdesarrollados que carecen

⁴⁴¹ Artículo 31, Constitución de la República de Guatemala de 1993. Disponible en: https://www.oas.org/juridico/mla/sp/gtm/sp_gtm-int-text-const.pdf. (Última consulta en línea 7 de octubre 2019).

⁴⁴² LÓPEZ CARBALLO, D. (Coordinador), *Protección de datos y habeas data: una visión desde Iberoamérica*, imprenta nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2015, p. 132.

⁴⁴³ Salvadoreños serán multados si no cumplen nueva ley de protección de datos de la UE, [elsalvador.com](https://www.elsalvador.com/noticias/negocios/salvadorenos-seran-multados-si-no-cumplen-nueva-ley-de-proteccion-de-datos-de-la-ue/484160/2018/), 2018. <https://www.elsalvador.com/noticias/negocios/salvadorenos-seran-multados-si-no-cumplen-nueva-ley-de-proteccion-de-datos-de-la-ue/484160/2018/>. (Última consulta en línea 18 de noviembre 2019).

de una tecnología informática propia exigen que se reconozca la facultad de ejercer un control sobre los datos que pueden recogerse en su territorio; siendo considerado un cauce procesal para preservar en el mundo informático la libertad de las personas”⁴⁴⁴. Y ese camino es por el que ha optado Latinoamérica con el *habeas data* para que se reflejara constitucionalmente y poder acceder a los datos dado el abuso del poder informático.

El *habeas data* no debe ser considerado como un derecho fundamental⁴⁴⁵, sino ser un instrumento o garantía procesal abocada en la defensa de los derechos de las libertades Informáticas, El mismo presenta coincidencias jurídicas con el *habeas corpus* el cual se enfoca en la defensa de los derechos a la libertad de las personas, en una dimensión física y externa de la libertad: Pero en el caso del *habeas data* se centra en proteger aspectos internos de la libertad, como son la intimidad, autodeterminación, libertad de las personas. Por tanto, las garantías están dirigidas a la protección de objetivos distintos. El *habeas data* no es una sustitución del *habeas corpus*⁴⁴⁶.

No parece, -a priori- por tanto, que la tesis de Lucas Murillo de la Cueva, del derecho a la autodeterminación informativa o del derecho a la protección de datos (tras la sentencia 292/2000) ni como ya a nivel europeo se consolida (conforme a la Carta de Derechos Fundamentales de la Unión Europea del 2000 y del Tratado de Lisboa del 2007 donde ya se reconoce expresamente en

⁴⁴⁴ PÉREZ LUÑO, A. E., *Del Habeas Corpus al Habeas Data (Conferencia impartida el 11 de mayo de 1990, durante el XIV Curso de Informática y Derecho, celebrado en el Centro Regional de la UNED) visto en CARRASCOSA LÓPEZ, V. (Director), Informática y Derecho 1, 1ª ed. Universidad Nacional de Educación a Distancia, Mérida, Sevilla, 1992, p. 154.*

⁴⁴⁵ “Es necesario precisar que algunos textos constitucionales latinoamericanos, además de considerar el *habeas data* como una acción o proceso constitucional (Argentina, Bolivia, Brasil, Ecuador, Paraguay, Perú), también la consideran como un derecho fundamental (Colombia y Venezuela)”, NOGUEIRA ALCALÁ, H., *Autodeterminación informativa y habeas data en Chile e información comparativa*, Anuario de Derecho Constitucional Latinoamericano, 2005, p. 458.

⁴⁴⁶ PÉREZ-LUÑO, A.E., *Del Habeas Corpus al Habeas Data (Conferencia impartida el 11 de mayo de 1990, durante el XIV Curso de Informática y Derecho, celebrado en el Centro Regional de la UNED) visto en CARRASCOSA LÓPEZ, V. (Director), Informática y Derecho 1, 1ª ed. Universidad Nacional de Educación a Distancia, Mérida, Sevilla, 1992, pp. 156-160.*

el artículo 8 el derecho a la protección de datos) haya sido quien ha triunfado en el contexto latinoamericano.

En cambio, entendemos que a pesar de la incursión del *habeas data* en los plexos constitucionales latinoamericanos; el acercamiento de las legislaciones latinoamericanas con las normas europeas ha permitido la desaceleración del *habeas data* y la entrada, fortalecimiento y consolidación de la protección de datos en Latinoamérica. Tal es el caso de la norma de Bolivia la cual inserta el *habeas data* en la constitución del 2004 y trascurrido 5 años con la reforma constitucional del 2009 desaparece la figura e inserta la acción de privacidad reconociendo la autodeterminación informativa por medio a dicha acción.

Con todo se ha de decir que autores como Casal o Rodríguez Marcano apuestan por el mismo o realizan importantes precisiones. Así, el primero señala que se han de aclarar conceptos básicos para poder definir el *habeas data*; en este sentido se ha de señalar que la libertad informática es un “derecho fundamental” y dentro del mismo se encuentran otros derechos como son el derecho a la autodeterminación informativa, el derecho de información y acceso, el derecho de rectificar y cancelación, el derecho a la indemnización por daños y el derecho a garantías suficientes; es precisamente el *habeas data* una de esas garantías⁴⁴⁷. Por su parte, el segundo autor defiende una postura innovadora al defender el derecho a la protección de datos personales y encontrar su sede constitucional ex arts. 60 y 28 de la Constitución venezolana de 1999⁴⁴⁸.

Como observamos, el escenario latinoamericano planteado se reviste de normas constitucionales, generales y específicas en materia de *habeas data* y protección de datos personales previamente vistas, siguiendo un proceso de

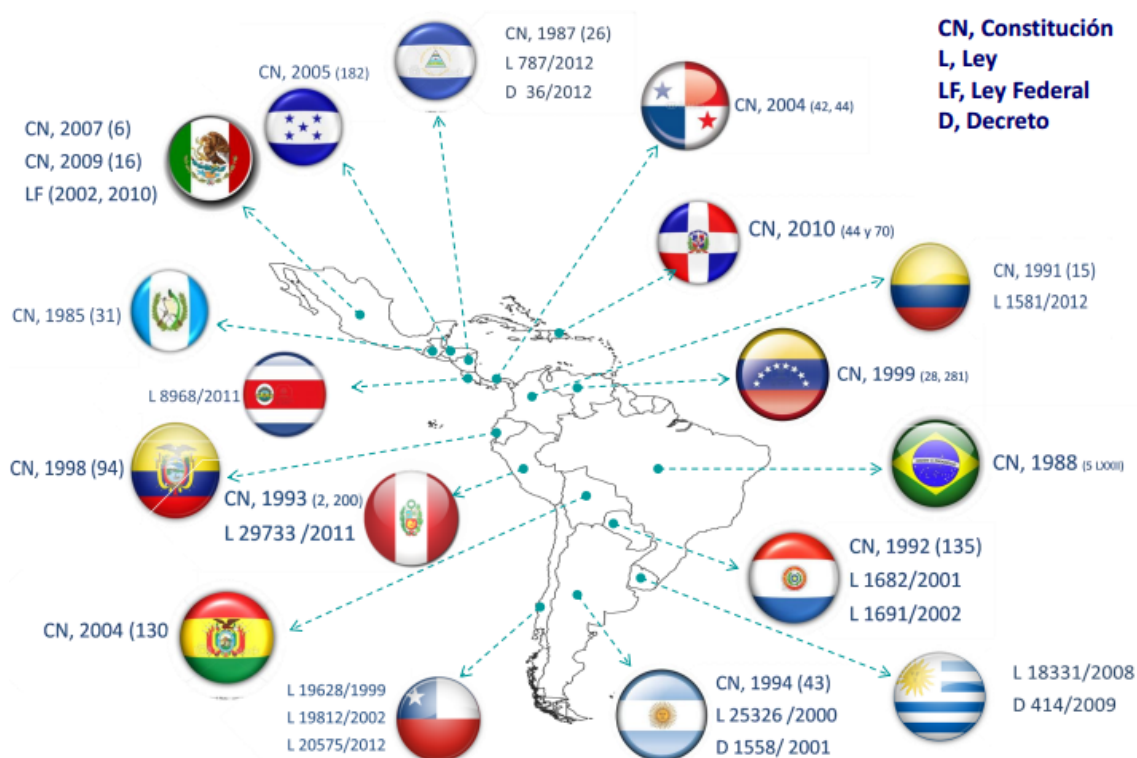
⁴⁴⁷CASAL, J., “El nuevo Derecho Constitucional venezolano” (*IV Congreso de Derecho Constitucional en Homenaje al Doctor Humberto La Roche*), Caracas, UCAB, 2001, p. 209.

⁴⁴⁸ RODRÍGUEZ MARCANO, E. R., *El derecho a la autodeterminación informativa en Venezuela...* op. cit., pp. 168-169.

transformación y actualización, situación de la República Dominicana con su actual Ley núm. 172-13 en materia de protección de datos y *habeas data*. A continuación, presentamos una muestra del panorama de la protección de datos personales y *habeas data* en las normas constitucionales, generales y específicas de los países latinoamericanos durante el período comprendido entre 1985 al 2012⁴⁴⁹. Con todo, se puede considerar un escenario vigente a pesar del tiempo transcurrido, reflejando a grandes rasgos la configuración del escenario latinoamericano vinculado con esos derechos y su acercamiento al modelo europeo.

⁴⁴⁹ Se observa un posterior desarrollo del mapa latinoamericano sobre protección de datos personales correspondiente al 2014. Debido a los pocos cambios que presenta entre los que se encuentra la actual Ley núm. 172-13, hemos decidido mantener el que se presenta.

Fig. 1. Mapa latinoamericano sobre la protección de datos personales, constituciones y normas generales (1985-2012)⁴⁵⁰.



Mapa Latinoamericano sobre la protección de datos personales: Constituciones y normas generales (1985-2012)
Nelson Remolina Angarita©, Universidad de los Andes, Bogotá, Colombia

En un mismo sentido, cabría situar las leyes uruguay y argentina, pues como se señala desde la doctrina de Troncoso Reigada, “esta aproximación de los países iberoamericanos al modelo europeo de protección de datos personales está siendo valorada positivamente por la Comisión Europea, a través del reconocimiento de que estos países tienen un nivel adecuado de protección -que ha obtenido hasta ahora Argentina en 2003 y muy recientemente Uruguay en agosto de 2012⁴⁵¹. Otro dato que cabe señalar es

⁴⁵⁰ TRONCOSO REIGADA, A., *Latinoamérica y protección de datos personales en cifras (1985-2012)*. Disponible en: <https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Latinoamerica-proteccion-datos-en-cifras-1985-2012-Remolina.pdf>. (Última consulta en línea 24 de febrero 2017).

⁴⁵¹ TRONCOSO REIGADA, A., “El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio en los modelos de protección de datos a nivel internacional”, *Revista Internacional de Protección de Datos Personales*, Universidad de los Andes, Bogotá, núm.1., julio-diciembre 2012, pp. 1-2 y pp. 30-31.

el importante papel que el Convenio 108 del Consejo de Europa está jugando en ausencia de un instrumento internacional. México es parte del Convenio 108 y su Protocolo Adicional desde el 12 de junio de 2018 convirtiéndose en el segundo Estado Latinoamericano que adopta el Tratado. Uruguay es el primer Estado Latinoamericano y no europeo que forma parte del Convenio desde el 7 de enero del 2013.

6. Ley Modelo Iberoamericana en materia de Protección de Datos

6.1. Consideraciones generales

Los Jefes de Estado y de Gobierno de los países iberoamericanos, la Red Iberoamericana de Protección de Datos (RIPD), la Organización de Estados Americanos (OEA) y los Comisionados de Protección de Datos aúnan sus esfuerzos de cara a contribuir con la normalización de leyes en materias de protección de datos, mediante propuestas de creación de estándares iberoamericanos de protección de datos.

En ese sentido, se presentan diferentes propuestas de armonización, la primera, impulsada por los acuerdos de Madrid dirigidos por la Agencia Española de Protección de Datos (2002). La segunda, bajo la relatoría de la Organización de los Estados Americanos (OEA) en colaboración con la Red Iberoamericana de Protección de Datos (RIPD) a sugerencia de los Jefes de Estado y de Gobierno, (2010). Y en junio del 2017 se presentó una tercera propuesta con el lema “un nuevo marco normativo para la protección de los datos personales en Iberoamérica”, bajo la dirección del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI) de México, reconociendo los estrechos lazos de colaboración entre la Red Iberoamericana de Protección de Datos (RIPD)⁴⁵², la OEA, las Cumbres de

⁴⁵² España ostenta la secretaría permanente de la Red Iberoamericana de Protección de Datos, asistiendo a cada una de las reuniones.

Jefes de Estado y de Gobierno y la Unión Europea (UE) representada por Bruselas⁴⁵³.

Es importante resaltar que la Red Iberoamericana de Protección de Datos (RIPDP) y la Organización de Estados Americanos (OEA) forman parte de los organismos supranacionales de cooperación exentos de normativas jurídicas de corte internacional, es decir, no revisten de capacidad para producir o crear normas jurídicas de rápida implementación en los Estados, pero si, son mecanismos para externar recomendaciones de tipo político a los gobiernos⁴⁵⁴. En ese sentido, entendemos que a pesar de no producir normativas jurídicas de rápida implementación en los Estados, cuentan con la capacidad de influir en los cambios normativos orquestados en los Estados, mediante la preparación de normativas modelos que fungen como recomendaciones normativas a seguir en los Estados adscritos a la organización.

De igual modo, por medio a la implementación de conferencias y talleres, los Comisionados de Protección de Datos contribuyen con el proceso de estandarización de los principios de protección de datos, recomendando a sus miembros la incorporación al Convenio 108, previo a transitar por un proceso de aprobación, estando incluidos los Estados pertenecientes a la Red Iberoamericana de Protección de Datos (RIPD).

Por su parte, los Estados miembros de la Red Iberoamericana de Protección de Datos (RIPD), materializan sus esfuerzos de colaboración utilizando diversas herramientas de protección de datos como el proyecto *Corpus Iuris*, un proyecto originario de la Red, creado para tener acceso a una base de

⁴⁵³ Cfr. "...hay dos espacios de concertación entre Europa y Latinoamérica: uno, las Cumbres Iberoamericanas de Jefes de Estado y de Gobierno, promovidas por España, y dos, las Cumbres de jefes de Estado y Gobiernos de la Comunidad Europea, América Latina y el Caribe (ALC-UE)" ROCHA VALENCIA, A. y PRECIADO CORONADO, J. (Coordinadores), *Proyectos y Estrategias de Integración, América Latina y el Caribe en el contexto de América del Norte y Europa*, 1ª ed, CUCSH-UdeG, Guadalajara, 2008, p. 20.

⁴⁵⁴ LÓPEZ JIMÉNEZ, D. y VARGAS, P., "La autorregulación del comercio electrónico en el ámbito de América Latina", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 40, Enero-Abril 2016, pp. 84.

información conformada por documentos y normas dispuestas de forma sencilla. La herramienta permite el acceso de los documentos nacionales de los Estados que componen la Red y aquellas normas internacionales en materia de protección de datos y derechos fundamentales procedentes de los Estados y organismos internacionales⁴⁵⁵, situando el desarrollo y alcance de la protección de datos personales a la altura y nivel de los derechos humanos.

En las próximas líneas, abordamos las propuestas de conformación del Estándar Iberoamericano en materia de protección de datos. Las propuestas incluyen principios, mecanismos de control e iniciativas encaminadas a la protección de datos, a raíz del esfuerzo conjunto de los Jefes de Estados, organizaciones internacionales, Grupo de Viabilidad, convenciones; presentando una estrecha vinculación y coincidencia de tiempo y espacio entre ellas; realizando sinergias de cooperación, fundiendo e interconectando sus esfuerzos, situación observada en cada uno de los escenarios planteados.

6.2. Iniciativas de los Jefes de Estado y de Gobierno Iberoamericano en el proceso de normalización de la protección de datos en los Estados Iberoamericanos

Desde sus inicios, las Cumbres Iberoamericanas de Jefes de Estado forman parte de los mecanismos instituidos en los Estados para fortalecer la comunidad iberoamericana. Las cumbres se apoyan en propuestas e implementación de iniciativas en materia de protección de datos, asumiendo con ello, el derecho internacional humanitario y la protección de los derechos humanos⁴⁵⁶.

⁴⁵⁵ *Corpus Iuris Internacional y Nacional*.

Disponible en: <http://corpusiurispdp.inai.org.mx/Pages/home.aspx>. (Última verificación en línea 25 de mayo 2019).

⁴⁵⁶ *XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, Declaración de Santa Cruz de la Sierra*, 14 y 15 de noviembre, 2003, página 3.

Disponible en: <http://www.oei.es/historico/xiiicumbredece.htm>. (Última consulta en línea 11 de abril 2017).

En ese sentido, consciente de la importancia de la protección de datos personales como un derecho fundamental, los Jefes de Estado y de Gobierno Iberoamericano externan su apoyo a la creación de la Red Iberoamericana de Protección de Datos⁴⁵⁷, afirmando su compromiso al mencionado derecho fundamental y en especial, a las iniciativas regulatorias en materia de protección de datos en los Estados Iberoamericanos.

Los acercamientos⁴⁵⁸ entre la Unión Europea y América-Latina sustentado en su profunda herencia cultural⁴⁵⁹ aseguran la transferencia de conocimientos en diferentes campos (político, económico, justicia), mediante la asociación estratégica birregional, destacando la protección de todos los derechos humanos y las libertades fundamentales, profundizando en el respecto de los derechos humanos.

Es así que, por medio a la convocatoria de la Agencia de Protección de Datos Española (encuentros iberoamericanos)⁴⁶⁰, se observa el vínculo o

⁴⁵⁷ *XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, Santa Cruz de la Sierra, Bolivia*, 14 y 15 de Noviembre, declaración final pagina 5, punto 45, el cual expresa "Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad".
Disponible en: <http://www.oei.es/historico/xiiicumbreddec.htm>. (Última consulta en línea 11 de abril 2017).

⁴⁵⁸ El acercamiento de Europa con Latinoamérica vía sus cumbres y reuniones de Jefes de Estado, se puede ventilar en dos fases o ámbitos. El primero se materializa con la participación de España y los Estados Iberoamericanos, situación observada en la I Cumbre Iberoamericana de Jefes de Estado y de Gobierno celebrada en Guadalajara durante los días 18 y 19 de 1991; más tarde se observa la participación de la Unión Europea como bloque en el escenario latinoamericano, ejemplo de ello se plasma en la Primera Cumbre entre los Jefes de Estado y de Gobierno de América Latina y el Caribe y la Unión Europea, declaración de Río de Janeiro, 28 y 29 de junio de 1999.

⁴⁵⁹ *Primera Cumbre entre los Jefes de Estado y de Gobierno de América Latina y el Caribe y la Unión Europea, declaración de Río de Janeiro*, 28 y 29 de junio de 1999, página 2. Disponible en: <http://www.oei.es/historico/cumbrerio.htm>. (Última consulta en línea 03 de abril 2017).

⁴⁶⁰ I Encuentro Iberoamericano de Protección de datos, declaración de San Lorenzo del Escorial-España, 2002., *27 International Conference of Data protection and Privacy Commissioners, declaración de Montreux*, 14 y 16 de septiembre 2005.
Disponible en: https://icdppc.org/wp-content/uploads/2015/06/montreux_declaration-Spanish.pdf. (Última consulta en línea 17 de mayo 2017).

conexión de los Estados Iberoamericanos⁴⁶¹ y España en materia de protección de datos, asignando a la intimidad y a la privacidad la categoría de derecho fundamental de las personas, resaltando la importancia del tratamiento leal y respetuoso de los datos personales, eje fundamental en la expansión del comercio electrónico⁴⁶².

En tal sentido, los Estados Iberoamericanos valoran, reiteran, declaran, ponen de manifiesto que, a pesar de su interés en la protección de los datos personales como derecho fundamental, existen dificultades en Iberoamérica de hacerlo efectivo, viendo la necesidad de contar con marcos normativos nacionales⁴⁶³.

Ante tal necesidad, se plantea la implantación de una “cultura”⁴⁶⁴ de protección de datos en los Estados Iberoamericanos, garantizando con ello una protección “adecuada”, sustentada en regulaciones nacionales y el establecimiento de mecanismos de control⁴⁶⁵ independientes en los Estados

⁴⁶¹ Entre los participantes al primer encuentro Iberoamericano tenemos: Argentina, Brasil, Costa Rica, España, México, Paraguay, Perú y Uruguay.

⁴⁶² Discurso de toma de posesión del director de la Agencia española (APD) Dr. José Piñar Mañas el cual aboga por la cooperación con América Latina y la contribución a la implantación en dichos países de un marco jurídico que garantice un nivel de protección de datos adecuado en los mismos, en uno de los ejes vertebradores de la acción Internacional de la ADP. / *Encuentro Iberoamericano de Protección de datos, declaración de San Lorenzo del Escorial-España*, 2002. Disponible en: http://www.redipd.es/documentacion/common/declaracion_2002_I_encuentro.pdf. (Última consulta en línea 03 de abril 2017).

⁴⁶³ *II Encuentro Iberoamericano de Protección de Datos, Declaración de San Lorenzo del Escorial-España*, 2003, p. 1-2 Disponible en: http://www.redipd.es/documentacion/common/declaracion_2003_II_encuentro_es.pdf. (Última consulta en línea 18 de mayo 2017).

⁴⁶⁴ “(...) la UNESCO (1996) define la cultura como “la manera de vivir juntos, que moldea nuestros pensamientos, nuestras imágenes y nuestros valores” en SEN, A. y KLIKSBERG, B., *Primero la gente*, 1ª ed. editora Deusto, Barcelona, 2007, p. 263.

⁴⁶⁵ En el III Encuentro Iberoamericano de Protección de Datos, se crea un subgrupo para realizar un estudio analítico de la Viabilidad de creación de Autoridades de Control en el entorno Iberoamericano, a iniciativa de El Salvador y coordinado por la representación de Argentina. Disponible en: <http://www.redipd.es/actividades/encuentros/III/index-ides-idphp.php>. (Última consulta en línea 18 de mayo 2017).

Iberoamericanos, facilitando el libre flujo de datos personales entre los Estados⁴⁶⁶.

6.3. Propuesta de viabilidad de creación de autoridades de control en los Estados Latinoamericanos

Producto a las dificultades económicas y sociales existente en los países iberoamericanos, el *Grupo de Trabajo de Viabilidad de Creación de Autoridades de Control en el entorno Latinoamericano* mejor conocido como “*Grupo de Viabilidad*”, a raíz del III Encuentro Iberoamericano de Protección de Datos, propone un Modelo Marco de autoridad con amplios poderes de control y otros posibles modelos alternativos, con la flexibilidad necesaria para ser adaptados a las circunstancias jurídicas y sociales de cada Estado.

En ese orden, el desarrollo económico, judicial, social y económico de la Unión Europea presenta diferencias con el resto de Europa, y también al mismo tiempo, el avance tecnológico y crecimiento de los flujos transfronterizos de datos aumentan entre Europa e Iberoamérica, generando con ello la necesidad de homogeneizar y crear organismos capaces de regular y asegurar una real protección de datos al amparo del crecimiento tecnológico existente en Iberoamérica. Para ello, deben crearse reglas claras y organismos independientes con la capacidad necesaria para ejercer tal proceso regulatorio. De ahí, la importancia que le asigna la Cumbre a la creación de autoridades de control en el entorno latinoamericano, apostando por reglas claras entre los Estados por medio de la existencia de órganos imparciales, que velen y aseguren una real protección de datos personales en un mundo cambiante.

Es por ello que, sustentado en la no homogeneización de un marco regulatorio en materia de protección de datos en los Estados Iberoamericanos y, ante la dificultad económica que subyace en la creación del órgano

⁴⁶⁶ *III Encuentro Iberoamericano de Protección de Datos, Declaración de Cartagena de Indias – Colombia 2004*, página 1. Disponible en: <http://www.redipd.es/actividades/encuentros/III/index-ides-idphp.php>. (Última consulta en línea 18 de mayo 2017).

regulador, el Grupo de Viabilidad plantea la formación de órganos de control adaptados en cada uno de los Estados Latinoamericanos; tales diferencias representan un obstáculo en el ejercicio de las actividades económicas y la libre circulación de mercancías, personas, servicios y capitales que exigen constantes flujos de información⁴⁶⁷.

Se observa como la misma declaración conecta la protección de datos personales con el desarrollo social y económico de los Estados Iberoamericanos; es decir, que, ante un eventual desarrollo del marco regulatorio en materia de protección de datos en los Estados Iberoamericanos, se contribuye con un mayor crecimiento de la economía en los Estados, repercutiendo en la mejora del ciudadano iberoamericano, caso que nos compete.

De igual forma, con el fin de asegurar niveles equivalentes de protección de datos en Latinoamérica, es de vital importancia la homogeneización de sus normas mediante la creación de legislaciones nacionales y órganos capaces de velar por el cumplimiento del proceso⁴⁶⁸, propugnando por el establecimiento de órganos reguladores independientes, asegurando la fiel ejecución de las medidas necesarias que contribuyan a la homologación de las normas en materia de protección de datos en los Estados Iberoamericanos.

A raíz de ello, el Grupo de Viabilidad presenta las siguientes propuestas de modelos de autoridades de control de protección de datos.

⁴⁶⁷ *IV Encuentro Iberoamericano de Protección de Datos., Informe de Viabilidad de creación de Autoridades de Control en el entorno Iberoamericano, Huixquilucan (Estado de México)*, 4 de noviembre de 2005. Disponible en: <http://www.redipd.es/actividades/encuentros/IV/index-ides-idphp.php>. (Última consulta en línea 6 de mayo 2017)

⁴⁶⁸ *IV Encuentro Iberoamericano de Protección de Datos., Informe de Viabilidad de creación de Autoridades de Control en el entorno Iberoamericano, Huixquilucan (Estado de México)*, 4 de noviembre de 2005, pp. 1y ss. Disponible en: <http://www.redipd.es/actividades/encuentros/IV/index-ides-idphp.php>. (Última consulta en línea 6 de mayo 2017)

a) Iniciaremos con el modelo europeo, un modelo matizado por las previsiones del Convenio 108 y sus protocolos anexos⁴⁶⁹, reflejando ser un órgano imparcial, manifestando su completa independencia, constituyendo un elemento de protección efectiva de las personas con respecto al tratamiento de sus datos personales. Así lo expresa en el preámbulo y el numeral 3 del artículo 1 de su Protocolo Adicional, ratificado en el párrafo 2 del artículo 28 de la Directiva 95/46/CE, donde se contemplan una total independencia⁴⁷⁰ entre sus funciones. En este sentido, la Agencia de Protección de Datos Española⁴⁷¹ y sus homólogas autonómicas (la Agencia Vasca de Protección de Datos o la Agencia Catalana de Protección de Datos), entre otras, son fruto del modelo europeo⁴⁷².

b) Este modelo se propone a raíz de la situación latinoamericana, rodeada y compuesta por diferentes escenarios. Entre ellos, nos referimos a Estados con normativas generales en materia de protección de datos y órganos de control independientes (caso Argentino) o a otros, ausentes de normativas generales en materia de protección de datos personales. A expensas del contexto normativo, la situación económica de los Estados Latinoamericanos no permite la existencia o proliferación de órganos de control independientes, ya que su

⁴⁶⁹ *Protocolo Adicional de Convenio n.º 108 para la protección de las personas con respecto al tratamiento de datos de carácter personal y relativo a transferencias de datos.*

⁴⁷⁰ PIÑAR MAÑAS, J. L. y RECIO GAYO, M., *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, 1ª ed. Wolters Kluwer España, S. A., España, 2018, pp. 252-265.

⁴⁷¹ *Real Decreto 156/1996*, de 2 de febrero, por el que se modifica el Estatuto de la Agencia de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo, para designar a la Agencia de Protección de Datos como representante español en el grupo de protección de personas previsto en la Directiva 95/46/ce, de 24 de octubre. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1996-2991>. (Última consulta en línea 25 de junio del 2017)

⁴⁷² Responde a este modelo entre otras las siguientes *autoridades de protección de datos* que podemos encontrar en estas direcciones: Alemania: www.datenschutz.de; Austria: www.dsk.gv.at; Bélgica: www.privacy.fgov.be; Chipre: www.dataprotection.gov.cy; Dinamarca: www.datatilsynet.dk; Eslovaquia: www.dataproyection.gov.sk ; Eslovenia: www.varuh-rs.si; Estonia: www.dp.gov.ee; Finlandia: www.tietosuoja.fi; Francia: www.cnil.fr; Grecia: www.dpa.gr; Holanda: www.chpweb.nl; Hungría: www.abiweb.obh.hu/abi; Irlanda: www.dataprivacy.ie; Islandia: www.personuvernd.is; Italia: www.garanteprivacy.it; Letonia: www.dvi.gov.lv; Lituania: www.ada.lt; Malta: www.dataprotection.gov.mt; Noruega: www.datatilsynet.no; Polonia: www.giodo.gov.pl; Portugal: www.cnpd.pt; Reino Unido: www.dataprotection.gov.uk; República Checa: www.uouu.cz; Suecia: www.datainspektionen.se.

instauración prevé una reestructuración económica y un aumento de empleados en el sector público y privado.

El Grupo de Viabilidad, selecciona en sus conclusiones el modelo europeo, siendo el más representativo; a pesar de ello, el proyecto presenta alternativas complementarias y no excluyentes entre sí, que preceden a los órganos de control.

Es así como producto a la realidad de los Estados Latinoamericanos, el Grupo de Viabilidad propone tres alternativas de implementación del órgano regulador, alineadas y conectadas con las realidades de los Estados Iberoamericanos.

La primera de las alternativas se centra en utilizar las estructuras existentes, como es el caso de las administrativas, constitucionales (defensorías del pueblo, ministerios públicos, etc.), tratando siempre de crear mecanismos de control o, arbitral la independencia.

La segunda alternativa se orienta en la creación de órganos y mecanismos complementarios de protección en el ámbito público, sopesando la instauración de supervisores o encargados de protección de datos o reestructurando los organismos internacionales localizados en los Estados.

La tercera alternativa va de la mano del sector privado, promoviendo una mayor colaboración e integración, mediante el funcionamiento de expertos, incentivando la autorregulación ya sea por la implementación de códigos de conductas.

Es así como la carencia o ausencia de leyes especiales en materia de protección de datos conectadas con el aspecto económico dificulta la creación de órganos independientes en temas de protección de datos en los Estados Latinoamericanos.

Tal situación genera la necesidad de crear normativas⁴⁷³ encaminadas a la protección de datos. Por ello, son estas las razones que motivan a organismos internacionales a establecer modelos normativos relacionados con la protección de datos, las cuales sirvan de base para instaurar leyes especiales y, así, aportan un grano de arena al proceso de creación e institucionalización del órgano de control en los Estados Latinoamericanos.

Al unísono de las alternativas propuestas por los diferentes modelos de órganos de control y las normativas de leyes especiales en materia de protección de datos, la creación de autoridades de control en el entorno latinoamericano continúa el mismo camino o trayectoria, plasmado por las diferencias existentes en los Estados Latinoamericanos sin dejar de lado su desarrollo normativo⁴⁷⁴. Como sabemos, algunos Estados cuentan con normas constitucionales en materia de privacidad e intimidad pero no poseen leyes especiales de protección de datos. Sin embargo, esta situación irá en descenso en la medida que los Estados Latinoamericanos prosigan con su acercamiento⁴⁷⁵ a los procesos regionales y transnacionales del mundo globalizado y, con ello, se contribuirá activamente con los flujos internacionales de datos personales, salvaguardando las garantías del derecho fundamental a

⁴⁷³ En el V Encuentro Iberoamericano de Protección de Datos, Declaración de Lisboa 2007, se aprueban las Directivas de Armonización de Protección de Datos en la Comunidad Iberoamericana, cuya finalidad busca la creación de iniciativas legislativas referentes para otros países en otras áreas geográficas. Al mismo tiempo, en la declaración del VI encuentro de la Red Iberoamericana de protección de datos en el documento “Un compromiso para alcanzar estándares internacionales de protección de datos y privacidad” se realiza un llamado a las conferencias Internacionales en materia de protección de datos a que se avoquen en la adopción de un instrumento jurídico común en materia de protección de datos., *V Encuentro Iberoamericano de Protección de Datos, Declaración de Lisboa 2007* Disponible en: <http://www.redipd.es/actividades/encuentros/V/index-ides-idphp.php>. (última verificación en línea 08 de junio 2017).

⁴⁷⁴ *V Encuentro Iberoamericano de Protección de Datos, Declaración de Lisboa, 2007*. Disponible en: <http://www.redipd.es/actividades/encuentros/V/index-ides-idphp.php>. (Última consulta en línea 08 de junio 2017).

⁴⁷⁵ *En el V Encuentro Iberoamericano de Protección de Datos, Declaración de Lisboa 2007*, se plantearon iniciativas de adhesión al Convenio para la Protección de Datos Personales relativo al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa, de 1981 (Convenio 108), como instrumento regulador internacional abierto a los Estados no Miembros de esa organización. Disponible en: <http://www.redipd.es/actividades/encuentros/V/index-ides-idphp.php>. (Última consulta en línea 08 de junio 2017).

la protección de datos por medio a la fijación de patrones internacionales que permitan proteger la información personal en un mundo globalizado⁴⁷⁶.

El desarrollo tecnológico acorta distancia, aumenta los flujos de información, incentivando el comercio de la mano con la globalización, haciendo que nuestros datos personales se trasladen de un lugar a otro, razones necesarias para su regulación⁴⁷⁷, creación de normas claras y homogéneas logrando así una real protección de las personas.

En la medida que la tecnología⁴⁷⁸ se aproxima e impacta a Latinoamérica de igual modo deben iniciarse los procesos de protección de las personas físicas en relación a los tratamientos automatizados o no automatizados de sus datos personales para -con ello- lograr materializar una eficiente, efectiva y real protección de los datos personales.

⁴⁷⁶ V *Encuentro Iberoamericano de Protección de Datos, Declaración de Lisboa, 2007*. Disponible en: <http://www.redipd.es/actividades/encuentros/V/index-ides-idphp.php>. (Última consulta en línea 06 de abril 2017).

⁴⁷⁷ En la declaración del VI encuentro de la Red Iberoamericana de protección de datos en el documento “Un compromiso para alcanzar estándares internacionales de protección de datos y privacidad”, presenta las garantías que deben contener los estándares Internacionales en materia de protección de datos.

1. Los datos personales deben ser obtenidos y tratados de modo leal y lícito, respetando, como regla general, el poder de decisión de la persona sobre la información que le afecta.
2. Las personas han de ser educadas en la protección de sus datos y estar informadas sobre quién y para qué fines se tratan sus datos.
3. Los fines del tratamiento de datos serán específicos y concretos.
4. El tratamiento de datos ha de ser proporcionado a los fines que lo justifican.
5. Los datos personales deben ser exactos y veraces.
6. Es preciso identificar categorías de datos que por su mayor sensibilidad exijan una protección reforzada.
7. Es preciso garantizar la confidencialidad y la seguridad de la información personal.
8. Las personas deben tener la posibilidad de conocer que información se trata, rectificarla si es inexacta, obtener su cancelación si es innecesaria y oponerse a su tratamiento.
9. Las limitaciones a las anteriores garantías han de fundarse en razones de interés público.
10. Debe prevverse una autoridad que permita que estas garantías sean efectivas.

⁴⁷⁸ “Frente al vertiginoso avance de las tecnologías de la información, los riesgos a los derechos fundamentales y en especial a la vida privada de las personas se han multiplicado”, “la protección de los datos de las personas por parte de los Estados se dificulta, si se carece del marco legal indispensable y los órganos responsables de su aplicación no cuentan con las condiciones óptimas para el cabal cumplimiento de sus funciones”, segundo considerando del VIII encuentro Iberoamericano de Protección de Datos., *Declaración de México, México 2010*. Disponible en: <http://www.redipd.es/actividades/encuentros/VIII/index-ides-idphp.php>. (Última consulta en línea 12 de junio 2017).

A nivel de tendencias tecnológicas y, guardando las distancias, si bien Latinoamérica se encuentra a la altura de los Estados europeos en materia tecnológica, en esa misma medida debe contemplar su proceso regulatorio, a pesar de que en la actualidad no cuente con idénticas realidades económicas, sociales y políticas con respecto a los Estados europeos o Estados pertenecientes a la Unión Europea, los cuales son poseedores de estándares legislativos vanguardistas en materia de protección de datos⁴⁷⁹. En ese sentido, es de vital importancia disponer de autoridades de control independientes en los Estados Iberoamericanos, organizados y direccionados por una autoridad general de control a nivel supranacional. Dicha autoridad deberá ser sustentada económicamente por el aporte de los Estados, producto a los beneficios obtenidos por el aumento de las transacciones comerciales generadas por el movimiento internacional de datos fruto de la cooperación entre los mismos. Con todo lo expuesto, se constata la necesidad de poseer un órgano de control regional o supranacional capaz de agrupar a la región, soportado por un organismo supranacional como es el caso de la Organización de Estados Americanos (OEA), considerado de vocación regional⁴⁸⁰, el cual ha de ejercer un rol similar al del Comité⁴⁸¹ contemplado en el Reglamento (UE) 2016/679, a fin de lograr la homogeneización de una normativa general en materia de protección de las personas físicas en lo que respecta al tratamiento de datos personales y su libre circulación.

6.4. Planteamiento de Estándares internacionales para la protección de la privacidad, en relación con el tratamiento de datos de carácter personal

⁴⁷⁹ *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016*. Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807>. (Última consulta en línea 8 de marzo 2018).

⁴⁸⁰ LUCHAIRE, F., *La ayuda a los países subdesarrollados*, 1ª ed. (en lengua castellana) Oikos-Tau, Barcelona, 1971, p. 49.

⁴⁸¹ Manteniendo la distancia.

Cimentado en el interés de los Estados Iberoamericanos impulsados por España⁴⁸² vía solicitud realizada por los Jefes de Estado y de Gobierno, se realizaron trabajos de cooperación en favor de la estandarización de la protección de datos. Este compromiso fue asumido por organismos, asociaciones, y redes internacionales de protección de datos, entre ellos, la Red Iberoamericana de Protección de Datos, la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad⁴⁸³, la Asociación Francófona de Autoridades de Datos Personales (Association Francophone des Autorités de Protection des Personnelles)⁴⁸⁴ y la Organización de Estados Americanos (OEA) en colaboración con la Red Iberoamericana de Protección de Datos.

La propuesta de Estándares Internacionales de Privacidad contenida en la Resolución de Madrid fue puesta a la luz pública durante la inauguración⁴⁸⁵ oficial de la 31 Conferencia Internacional de Protección de Datos y Privacidad, celebrada el 4 de noviembre del 2009.

⁴⁸² La Agencia de Protección de Datos Española convocó a los países de América Latina procedentes de Argentina, Brasil, Costa Rica, España, México, Paraguay, Perú y Uruguay, al primer encuentro Iberoamericano de protección de datos celebrado en San Lorenzo del Escorial (España), los días 20, 21 de mayo de 2002. Disponible en: https://icdppc.org/wp-content/uploads/2015/06/montreux_declaration-Spanish.pdf. (Última consulta en línea 17 de mayo 2017).

⁴⁸³ Proponentes: Agencia Española de Protección de Datos, Comisario Federal de Protección de Datos y la transparencia (Suiza), Supervisor Europeo de Protección de Datos, Comisión Nacional de la Informática y de las Libertades (Francia), Comisión de Protección de Datos de Irlanda, Oficina del Comisario de Privacidad de Canadá, Oficina para la Protección de los Datos Personales (República Checa), Comisario Federal para la Protección de Datos (Alemania), Garante para la Protección de Datos Personales (Italia), Autoridad Holandesa de Protección de Datos, Comisario de Privacidad de Nueva Zelanda, Oficina del Comisario de Información (Reino Unido).

⁴⁸⁴ *Declaración conjunta de Madrid sobre la Protección de Datos Personales*, (Association Francophone des Autorités de Protection des Personnelles), Madrid, 3 de noviembre de 2009, pp. 1 y ss. Disponible en: http://www.redipd.es/documentacion/common/declaracion_2009_VII_encuentro_es.pdf. (Última consulta en línea 08 de junio 2017).

⁴⁸⁵ Su Alteza Real, el Príncipe Felipe, durante la inauguración oficial de la 31 Conferencia Internacional de Protección de Datos y Privacidad, celebrada en el Palacio del Congreso del Paseo de la Castellana elogió “por avanzar en la elaboración de unos estándares internacionales de protección que permitan dar ese salto fundamental que consiste en pasar de declarar que son necesario, a conseguir que sean una realidad”. Disponible en: <http://www.privacyconference2009.org/home/index-ides-idweb.html>. (Última consulta en línea 16 de julio 2017).

La propuesta conjunta de redacción de *Estándares internacionales para la protección de la privacidad, en relación con el tratamiento de datos de carácter personal* integra legislaciones de cinco continentes, constituyendo uno de sus valores el de avanzar hacia un documento internacionalmente vinculante, y protegiendo los derechos y libertades en un mundo globalizado, caracterizado por las transferencias internacionales⁴⁸⁶.

Este documento es una propuesta conjunta de redacción de Estándares Internacionales. La iniciativa, formada por principios, derechos, obligaciones y procedimientos, está compuesta de 25 puntos distribuidos en 6 partes. Comenzando por la primera, ésta comprende las disposiciones generales, donde se observa como objetivo el de facilitar los flujos internacionales de datos de carácter personal, necesarios en un mundo globalizado, con un carácter de aplicación total o parcial, teniendo los Estados la posibilidad de completar el nivel de protección con medidas adicionales que protejan la privacidad a nivel internacional con relación a la protección de datos personales. El documento se aplica a los tratamientos automatizados o parcialmente automatizados, pertenecientes al sector público o privado.

La segunda parte contiene los principios básicos de lealtad, legalidad, finalidad, proporcionalidad, calidad, transparencia y responsabilidad, bajo los principios de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos⁴⁸⁷.

En la tercera se aborda la legitimación para el tratamiento, la cual está compuesta por 4 puntos, y se detiene en los supuestos necesarios para la legitimación, los datos sensibles y las transferencias internacionales, con respecto a estas últimas, se permite el flujo entre Estados cuando se den los

⁴⁸⁶ RALLO LOMBARTE, A., *Estándares Internacionales sobre Protección de Datos Personales y Privacidad*, Resolución de Madrid, 5 de noviembre de 2009, Madrid, p. 12.

⁴⁸⁷ *Pacto Internacional de Derechos Civiles y Políticos*. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1977-10733>. (Última consulta en línea 23 de junio 2017).

siguientes requisitos: a) el destinatario ofrezca el nivel de protección previsto en el documento; b) mediante cláusulas contractuales; c) normas internas de privacidad cuya observancia resulte vinculante; d) protección de un interés vital; o e) cumplimiento de una obligación legal para salvaguarda de un interés público. De modo, que toda transferencia internacional de datos de carácter personal deberá acreditar que la transferencia cumpla con las garantías establecidas en el documento o cuando esta sea requerida por las autoridades de supervisión.

Al mismo tiempo, la cuarta parte corresponde a los derechos del interesado, reconocidos en los llamados derechos ARCO, formado por los derechos de acceso, rectificación, cancelación y oposición.

La quinta contiene los derechos de oposición y confidencialidad. Ambos engloban el tema de seguridad de modo que las personas responsables y quienes intervengan en cualquier fase del tratamiento deben respetar la confidencialidad.

Por último, la sexta parte corresponde al tema de cumplimiento y supervisión distribuida en 4 puntos en la que se destaca la existencia de autoridades de supervisión imparciales e independientes en los Estados, responsables de supervisar los principios establecidos en el documento, así como de mantener mecanismos de cooperación nacional e internacional entre los órganos de supervisión.

Las autoridades de supervisión tendrán la responsabilidad de conocer de las reclamaciones y de realizar investigaciones e intervenciones que resulten necesarias para garantizar el cumplimiento de la legislación nacional aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal.

6.5. Iniciativas de los Estados en materia de protección de datos

Los *Estándares Internacionales sobre Protección de Datos Personales y Privacidad* representan una muestra de la intención y el deseo de los Estados en contar con una regulación internacional en materia de protección de datos, como se observa en las reuniones sostenidas entre los Jefes de Estado y de Gobierno de los Estados Iberoamericanos.

Las iniciativas de los Estados en lograr una regulación o estandarización de la protección de datos personales no concluyen con el Estándar propuesto sino que hay que continuar con el esfuerzo⁴⁸⁸ de promoción⁴⁸⁹ del Estándar y de crear leyes generales y constitucionales de protección de datos en Estados que no cuentan con desarrollos normativos en la materia; es ahí la necesidad y el esfuerzo de las organizaciones y los Estados en concretizar e impulsar la estandarización.

6.6. Organizaciones internacionales y estandarización

Las iniciativas de estandarización reciben el apoyo de los reguladores y encargados de protección de datos del mundo, representados en las Conferencias Internacionales de Comisarios de Protección de Datos (ICDPPC, por sus siglas en inglés), quienes mantienen la visión de crear espacios de

⁴⁸⁸ “Impulsar la adopción de estándares regionales e Internacionales, a fin de ofrecer un modelo de regulación que garantice un alto nivel de protección y facilite un eficiente intercambio Internacional de datos personales...facilitar el fluido intercambio Internacional de datos personales a efecto de dotar de mayores garantías.....de un mundo globalizado”, VIII Encuentro Iberoamericano de Protección de Datos., *Declaración de México*, México 2010. Disponible en: <http://www.redipd.es/actividades/encuentros/VIII/index-ides-idphp.php>. (Última consulta en línea 12 de junio 2017).

⁴⁸⁹ Los Integrantes de la Red asumen el compromiso de intensificar la promoción de la normativa de protección de datos personales en el ámbito Iberoamericano, así como la creación de autoridades con competencias adecuadas para garantizar su aplicación, *declaración del X encuentro de la Red Iberoamericana de Protección de Datos*, 22 de octubre, Punta del Este, Uruguay, 2012. Disponible en: www.redipd.es/documentacion/common/declaracion_2012_X_encuentro_es.pdf. (Última consulta en línea 16 de julio 2017).

sinergias que permitan promover de una manera universal la protección de datos personales⁴⁹⁰ a la luz de la no homogeneización de los regímenes jurídicos en el mundo. En efecto, tal disparidad contribuye, con la ausencia de garantías, a debilitar la protección de datos.

Los Comisionados abogan por la obtención de un Convenio internacional de protección de datos y autoridades de protección de datos independientes con poderes de control, promoviendo la cooperación con aquellos países que no disponen por el momento de autoridades de protección de datos, sin dejar de lado, las organizaciones no gubernamentales relacionadas con los temas de protección de datos y la intimidad, razones que permiten la realización de reuniones conjuntas con otras organizaciones, con el objetivo de globalizar el tema de la protección de datos.

La Conferencia de Montreux⁴⁹¹ permitió a los Comisarios de Protección de Datos, solicitar a las Naciones Unidas la preparación de un instrumento jurídico vinculante, estableciendo de forma clara y detallada los derechos a la protección de datos y de la intimidad como derechos humanos de obligado cumplimiento; al mismo tiempo, apelaban a que el Convenio de Europa invitara a los Estados con legislaciones de protección de datos a adherirse al Convenio 108 conforme lo expresa su propio artículo 23⁴⁹².

⁴⁹⁰ 27ª Conferencia Internacional de Comisionados de Protección de Datos; *La Protección de Datos Personales y de la Intimidad en un Mundo Globalizado: un Derecho Universal que respeta Diversidades*”, Declaración de Montreux, 14-16 de septiembre de 2005, Suiza. Disponible en: https://icdppc.org/wp-content/uploads/2015/06/montreux_declaration-Spanish.pdf. (Última consulta en línea 17 de mayo 2017).

⁴⁹¹ Ciudad perteneciente a Suiza, donde fue efectuada la 27ª Conferencia Internacional de Comisionados de Protección de Datos; *La Protección de Datos Personales y de la Intimidad en un Mundo Globalizado: un Derecho Universal que respeta Diversidades*”, Declaración de Montreux, 14-16 de septiembre de 2005, Suiza. Disponible en: https://icdppc.org/wp-content/uploads/2015/06/montreux_declaration-Spanish.pdf. (Última consulta en línea 17 de mayo 2017).

⁴⁹² Artículo 23 Convenio 108. Adhesión de Estados no miembros

1. Después de la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa podrá invitar a cualquier Estado no miembro del Consejo de Europa a que se adhiera al presente Convenio mediante un acuerdo adoptado por la mayoría prevista en el

La misma declaración apela por el establecimiento de autoridades de supervisión independientes, la promoción de cooperación con aquellos Estados que en los momentos actuales del Convenio no cuenten con autoridades de protección de datos y supervisión. Asimismo, es importante recalcar que más allá del establecimiento de autoridades de supervisión, se apuesta por aquellas autoridades de Supervisión que gocen de independencia, al tiempo, que apelan incentivar los trabajos de intercambio de información con las organizaciones gubernamentales y no gubernamentales de carácter internacional que traten la protección de datos e intimidad.

La intimidad y la privacidad forman parte de los temas tratados en las conferencias internacionales. A continuación, pasamos a examinar la posición asumida por las conferencias respecto a tan importantes derechos.

6.7. Derecho a la intimidad/privacidad desde la óptica de los Comisionados de Protección de Datos y Privacidad

La intimidad y la protección de datos jugaron un papel protagónico en la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad realizada en la ciudad de Montreux (Suiza) bajo el lema *La protección de datos personales y de la intimidad en un mundo globalizado: un derecho universal que respeta diversidades*.

En ese sentido en la *35 Conferencias Internacionales de Comisionados de Protección de Datos y Privacidad* se retomó el concepto de privacidad, conectando y haciendo alusión a *la 27 Conferencia Internacional de*

artículo 20, d), del Estatuto del Consejo de Europa y por unanimidad de los representantes de los Estados contratantes que tengan el derecho a formar parte del Comité.

2. Para cualquier Estado adherido, el Convenio entrará en vigor el día primero del mes siguiente a la expiración de un período de tres meses después de la fecha del depósito del instrumento.

Comisionados de Protección de Datos, se trabajó indistintamente los conceptos de privacidad e intimidad, no existiendo límites entre estos, siendo considerados conceptos iguales y evitando distinción al momento de referirse a la privacidad y la intimidad.

Vista la posición fijada, seguimos con las Propuestas de Estándares.

6.8. Convención internacional vinculante para los Estados

La propuesta de *Estándares Internacionales para la Protección de la Privacidad y Datos de Carácter Personal*, presentada en párrafos anteriores, representa una de las vías conjuntas en la internacionalización de la protección de datos, a raíz de la necesidad de proteger la privacidad en un mundo sin fronteras, presentado en la resolución llevada a cabo en la *30 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad*.

La misma conferencia de Madrid resuelve que la propuesta del Estándar es un paso previo al desarrollo de un instrumento internacional vinculante. Es por ello que entre las resoluciones de la conferencia se encomienda a las autoridades de protección de datos y privacidad para que en las próximas conferencias (#31 y #32) se responsabilicen de los esfuerzos encaminados a la promoción y difusión de propuestas que sirvan de base para la elaboración del convenio universal vinculante, con la participación de instituciones públicas, privadas y organismos relacionados con la protección de datos y la privacidad.

Por tanto, con la globalización de la tecnología de información -incluidos los desarrollos tecnológicos como los teléfonos móviles, Internet, etc.- se persigue la instauración de una comunidad capaz de hacer frente a los avances tecnológicos, por medio a la creación de normas y estándares, más allá de las posibles barreras culturales, actores involucrados, enfoques locales y

regionales⁴⁹³. Siendo partícipes de la presencia global de la protección de datos y el crecimiento de las autoridades de protección de datos⁴⁹⁴ así como su expansión en América Latina, Asia y África⁴⁹⁵, se torna global el movimiento de estandarización de la protección de datos.

En la *33 Conferencia Internacional de Comisionados de Privacidad y Protección de Datos*⁴⁹⁶, correspondiente a la *IX Conferencia Iberoamericana*, llamada declaración de la ciudad de México se manifiesta la necesidad de comprometerse a compartir el conocimiento entre los Estados, autoridades y organizaciones de expertos en materia de privacidad.

En el mismo sentido y, ante la existencia de un convenio internacional de protección de datos -el Convenio 108-, reconocido en las conferencias internacionales, se invita al Consejo de Europa a solicitar su adhesión a los países que no cuentan con legislaciones en materia de protección de datos⁴⁹⁷.

⁴⁹³ 2do. considerando *33 Conferencia Internacional de Comisionados de Privacidad y Protección de Datos., Declaración de la ciudad de México*, Instituto Federal de Acceso a la Información y Protección de Datos, México, 2011. Disponible en: http://www.redipd.es/documentacion/common/declaracion_2011_IX_encuentro_es.pdf. (Última consulta en línea 09 de mayo 2017).

⁴⁹⁴ “Intensificar...la normativa de protección de datos personales en el ámbito Iberoamericano...la creación de autoridades...” *Declaración del X Encuentro de la Red Iberoamericana de Protección de Datos, 22 de octubre, Punta del Este, Uruguay, 2012*. Disponible en: <http://www.redipd.es/actividades/encuentros/X/common/pdfs/DeclaracionXEIPD.pdf>. (Última consulta en línea 12 de junio 2017).

⁴⁹⁵ *33 Conferencia Internacional de Comisionados de Privacidad y Protección de Datos., Declaración de la ciudad de México*, Instituto Federal de Acceso a la Información y Protección de Datos, México, 2011. Disponible en: http://www.redipd.es/documentacion/common/declaracion_2011_IX_encuentro_es.pdf. (Última consulta en línea 13 de junio 2017).

⁴⁹⁶ Se convirtió en la primera reunión de Autoridades de Protección de Datos celebrada en América Latina...logrando un reconocimiento mayor de los Estándares Internacionales sobre Protección de Datos y Privacidad de Madrid., *Declaración del X encuentro de la Red Iberoamericana de Protección de Datos, 22 de octubre, Punta del Este, Uruguay, 2012*. Disponible en: <http://www.redipd.es/actividades/encuentros/X/common/pdfs/DeclaracionXEIPD.pdf>. (Última consulta en línea 12 de junio 2017).

⁴⁹⁷ La propuesta quedó reflejada en el segundo párrafo de la página 133.

A raíz de la inexistencia en el 2013 de una convención internacional vinculante sobre protección de datos, se le hace un llamado a los gobiernos en la 35 Conferencia Internacional, para que aboguen por la adopción de un protocolo adicional al artículo 17⁴⁹⁸ del Pacto de Derechos Civiles y Políticos (ICCPR, por sus siglas en Inglés), debiendo consolidar los estándares que han sido desarrollados y apoyados por la conferencia internacional y por las disposiciones del comentario general n.º 16 a ese pacto, con la finalidad de conformar unos estándares de aplicación global para la protección de datos y la protección de la privacidad de conformidad con el Estado de derecho.

La conformación del Estándar en materia de protección de datos no se hace esperar en Iberoamérica, recibiendo el apoyo de diferentes organismos, entre ellos, la OEA, sus órganos internos y los Estados miembros de la organización. Por ello, a continuación, pasamos a dar una mirada a la siguiente propuesta de estandarización.

6.9 Estandarización de la protección de datos latinoamericana

La Asamblea General de la OEA, en su Cuadragésimo Primer Período Ordinario de Sesiones⁴⁹⁹, celebrado en San Salvador durante los días 5 al 7 de junio de 2011⁵⁰⁰, presentó el *Proyecto de Resolución de Acceso a la Información Pública y Protección de Datos Personales*, previo a recordar en la Asamblea General: a) las Resoluciones de Acceso a la Información Pública; b)

⁴⁹⁸ Como recordamos, este precepto reza lo siguiente: Artículo 17

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y su reputación.
2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

⁴⁹⁹ AG/doc. 5176/11, *Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas*, 26 mayo San Salvador, El Salvador, 2011; AG/RES.2661 (XLI-O/11), aprobada en la cuarta sesión plenaria, celebrada el 7 de junio de 2011. Disponible en: http://www.oas.org/es/sla/cji/docs/CJI-doc_402_12_rev2.pdf. (Última consulta en línea 12 de agosto 2017).

⁵⁰⁰ Acordado por el Consejo Permanente en la sesión celebrada el 25 de mayo de 2011;

el fortalecimiento de la democracia y c) la *Ley Modelo Interamericana*⁵⁰¹ sobre *Acceso a la Información Pública*, encomendando al Departamento de Derecho Internacional la elaboración de un estudio comparativo sobre los distintos regímenes jurídicos, políticos y mecanismos de aplicación existentes para la protección de datos personales, el cual incluye leyes, reglamentos y auto regulaciones nacionales, con miras a explorar la posibilidad de un marco regional en esta área.

La propuesta del modelo a la *Ley Interamericana de Protección de Datos Iberoamericana* fue precedida de diversos estudios y documentos⁵⁰² presentados por el Comité Jurídico Interamericano a solicitud de la Asamblea General, sin dejar de lado las propias resoluciones de la Asamblea⁵⁰³.

El esfuerzo de la Organización de los Estados Americanos⁵⁰⁴ por contar con una Ley Estándar de Protección de Datos Personales se sustenta en una serie de propuestas preliminares entre ellas “*Comentarios Preliminares sobre una Declaración de Principios para la Protección de la Privacidad y de los Datos*

⁵⁰¹ *Ley Modelo Interamericana sobre Acceso a la Información Pública*, Resolución AG/RES. 2607 (XL-O/10). Disponible en: www.oas.org/dil/esp/ag-res_2607-2010.pdf. (Última consulta en línea 12 de junio 2017).

⁵⁰² Consejo Permanente de la Organización de los Estados Americanos, Comisión de Asuntos Jurídicos y Políticos., *Proyecto de Principios y Recomendaciones Preliminares sobre la Protección de Datos (la protección de datos personales)*, CP/CAJP-2921/10 rev.1 corr.1, 17 octubre 2011, p. 2. Disponible en: http://www.oas.org/dil/esp/cp-cajp-2921-10_rev1_corr1_esp.pdf. (Última consulta en línea 13 de agosto 2017).

⁵⁰³ Consejo permanente de la Organización de los Estados Americanos, Comisión de Asuntos Jurídicos y Políticos., *Proyecto de Principios y Recomendaciones Preliminares Sobre la Protección de Datos (la protección de datos personales)*, CP/CAJP-2932/11 Rev.1, 13 de abril 2011, p. 2. Disponible en: http://www.oas.org/es/sla/ddi/docs/CP-CAJP-2921-10_rev1_corr1.pdf. (Última consulta en línea 13 de agosto 2017).

⁵⁰⁴ “.....del año 1997 la Organización de Estados Americanos viene estudiando en distintas instancias la protección de datos personales...comité jurídico Interamericano...elabora un Anteproyecto de Convención Americana sobre Autodeterminación Americana en septiembre del año 2000, que se basa fundamentalmente en el Convenio 108 para la Protección de las personas con respecto al tratamiento de datos de carácter personal de 1981, y la Directiva europea”, PALAZZI, P, *Transmisión Internacional de Datos Personales y Protección de la Privacidad en América Latina*. Trabajo publicado por la Agencia Protección de Datos en CD-ROM, Catálogo de Ficheros, 2001, visto en “BEL MALLÉN, I. CORREDORA y ALFONSO, L. (Coordinadores), *Derecho de la Información*, 1ª ed. ARIEL, S. A., Barcelona, España, 2003, p. 135.

*Personales en las Américas*⁵⁰⁵, “*Principios y Recomendaciones Preliminares sobre la Protección de Datos (La Protección de Datos Personales)*”⁵⁰⁶, documento presentado por el Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos, conforme al párrafo 11 de la parte dispositiva de la resolución AG/RES.2514 (XXXIX-O/09).

El estudio preliminar de *Principios y Recomendaciones sobre la Protección de Datos (La Protección de Datos Personales)*⁵⁰⁷ fue sometido a modificación por las observaciones planteadas por los Estados miembros, generando una versión revisada de este documento⁵⁰⁸. Dicho proyecto⁵⁰⁹ consta de 6 capítulos e incluye los tres criterios de tratamiento de datos personales: el europeo, el de Estados Unidos y el latinoamericano, siendo el criterio europeo el más estructurado, conformado por regulaciones estatales.

El segundo capítulo nos presenta un panorama de la protección de datos en Europa, Estados Unidos y Canadá, desde la perspectiva de sus orígenes,

⁵⁰⁵ David P. Stewart, *Comentarios Preliminares sobre una Declaración de Principios para la Protección de la Privacidad y de los Datos Personales en las Américas, Documento CJI/doc.382/11*. Disponible en: http://www.oas.org/es/sla/cji/docs/CJI-doc_382-11.pdf. (Última consulta en línea 12 de agosto 2017).

⁵⁰⁶ Comisión de Asuntos Jurídicos y Políticos, OEA/Ser.G, CP/CAJP-2921/10 REV. 1 corr. 1, 17 octubre 2011. Disponible en: http://www.oas.org/dil/esp/cp-cajp-2921-10_rev1_corr1_esp.pdf. (Última consulta en línea 12 de agosto 2017).

⁵⁰⁷ Consejo Permanente de la Organización de los Estados Americanos., *Principios y Recomendaciones Preliminares sobre la Protección de Datos (La Protección de Datos Personales)*, OEA/Ser.G, CP/CAJP-2921/10 rev.1 corr.1, 17 de octubre 2011. Disponible en: http://www.oas.org/dil/esp/cp-cajp-2921-10_rev1_corr1_esp.pdf. (Última consulta en línea 12 de agosto 2017).

⁵⁰⁸ *Principios y Recomendaciones Preliminares sobre la Protección de Datos*, OEA/Ser.G, CP/CAJP-2932/11 rev.1, 13 abril 2011. Disponible en: http://www.oas.org/es/sla/ddi/docs/CP-CAJP-2921-10_rev1_corr1.pdf. (Última consulta en línea 11 de agosto 2017).

⁵⁰⁹ El Departamento de Derecho Internacional previamente presentó el proyecto de Principios y Recomendaciones Preliminares sobre la Protección de Datos Personales CP/CAJP-2921 Rev.1, agradecido en el cuadragésimo primer periodo ordinario de sesiones,

⁵⁰⁹ AG/RES-2661 (XLI-O/11). *Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas*, 26 mayo San Salvador, El Salvador, 2011. Disponible en: http://www.oas.org/es/sla/cji/docs/CJI-doc_402_12_rev2.pdf. (Última consulta en línea 12 de agosto 2017).

desarrollo y estatus actual de la protección de datos conectado con sus regulaciones.

En relación al tercero, se analiza la protección de datos en América Latina, donde la figura del *habeas data* surge para la protección de los datos y se muestra diferente a los modelos ya mencionados. El *habeas data* es el mecanismo utilizado por los Estados Latinoamericanos en la corrección y actualización de los datos, teniendo más limitaciones que el europeo⁵¹⁰. El capítulo IV no pierde de vista los conceptos básicos relacionados con la protección de datos.

El cuanto al quinto capítulo, éste contiene 15 principios de protección de datos⁵¹¹, siendo el primer principio el de legitimidad y justicia, seguido por propósito específico, limitados y necesarios, transparencia, rendición de cuentas, condiciones para el procesamiento de datos, revelación de información a los procesadores de datos, transferencias internacionales, derecho de la persona al acceso de la información, derecho de la persona a corregir y suprimir sus datos personales, derecho a objetar el procesamiento de datos personales, legitimación para ejercer los derechos sobre el procesamiento de datos personales, medidas de seguridad para proteger los datos personales, deber de confidencialidad, control, cumplimiento y responsabilidad.

A continuación, nos detendremos en dos principios: el principio 8 relacionado con las transferencias internacionales y el principio 15 correspondiente al control, cumplimiento y responsabilidad;

⁵¹⁰ Consejo Permanente de la Organización de los Estados Americanos, *Principios y Recomendaciones Preliminares sobre la Protección de Datos (la protección de datos personales)*, OEA/Ser.G, CP/CAJP-2921/10 rev.1 corr.1, 17 de octubre 2011, p. 7. Disponible en: www.oas.org/dil/esp/cp-cajp-2921-10_rev1_corr1_esp.pdf. (Última consulta en línea 14 de agosto 2017).

⁵¹¹ En el 2009 se presentó la Resolución de Madrid que se constituye en el primer esfuerzo en establecer estándares internacionales.

Como hemos visto previamente, el tema de las transferencias internacionales forma parte de los principios establecidos en el documento preliminar de protección de datos personales presentados por la Comisión de Asuntos Jurídicos y Políticos de la Organización de Estados Americanos (OEA). El principio presenta 5 factores bajo los cuales se permite la transferencia internacional hacia el país receptor, quien debe garantizar normas mínimas de privacidad; la naturaleza de los datos corresponde al primer factor, seguido por; a) el país de origen; b) el país receptor; c) el propósito para el cual se procesan los datos; d) las medidas de seguridad vigentes para la transferencia; y e) el procesamiento de los datos personales. El principio manifiesta que, a pesar del aseguramiento de la protección de datos en las transferencias internacionales, ésta debe continuar siendo flexible en cuanto a la forma de lograrlo.

Sustentado en la protección equivalente⁵¹² en el país receptor, algunos Estados han expresado sus reservas a la regulación de las transferencias internacionales. En los casos donde el país receptor por medio a sus leyes locales no pueda garantizar la protección de los datos personales durante las transferencias internacionales, el exportador será responsable de la protección de los datos personales ejecutados durante la transferencia.

Si el país receptor no cuenta con los mínimos necesarios para asegurar la protección de los datos personales durante las transferencias internacionales, ésta podrá ejecutarse, si cuenta con cláusulas contractuales o si el país cuenta con una legislación nacional que permita la transferencia internacional de los datos, apoyadas en condiciones específicas⁵¹³.

⁵¹² Los Estados contemplan e instituyen en sus normativas nacionales iguales niveles de protección, caso los estados pertenecientes a la Unión Europea.

⁵¹³ 1) la transferencia es necesaria y en beneficio de la persona en una relación contractual; 2) la transferencia es necesaria para proteger un interés vital, como evitar un daño sustancial o la muerte de la persona o de un tercero; 3) la transferencia está autorizada legalmente para proteger un interés público; 4) el exportador de los datos se responsabiliza de la protección de los mismos.

El empleo de Internet en los procesos de transferencias internacionales representa una realidad siendo tomada en cuenta por las normas que rigen las transferencias internacionales entre los Estados, evitando limitaciones en los flujos transfronterizos producto a las innovaciones y desarrollos tecnológicos existentes.

Los Estados miembros de la OEA deberán contar con una autoridad de supervisión imparcial e Independiente, responsable de velar por el cumplimiento de los principios y su legislación nacional aplicable, con capacidad de manejar denuncias, imponer sanciones y prever reparaciones para los afectados.

Con el propósito de cumplir con los objetivos planteados, la autoridad gozará de capacidad técnica con facultades y recursos suficientes para llevar a cabo investigaciones y auditorias para el cumplimiento de las normas. Asimismo, la autoridad supervisora bajo las disposiciones de las leyes nacionales podrá contar con autoridad suficiente para aceptar o denegar transferencias internacionales ocurridas bajo su jurisdicción.

La conformación de la Propuesta de *Ley de Protección de Datos Latinoamericana* se sustenta en antecedentes previos a su presentación entre ellos se destaca:

- La Ley Modelo Interamericana sobre acceso a la información pública y su guía de implementación contenida en la resolución AG/RES. 2607 (XLI-O/10)⁵¹⁴.
- El crecimiento e importancia de la privacidad y la protección de datos personales, el fomento y la protección de los flujos transfronterizos.⁵¹⁵

⁵¹⁴ AG/RES-2661 (XLI-O/11), *Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas*, 26 mayo San Salvador, El Salvador, 2011. Disponible en: http://www.oas.org/es/sla/cji/docs/CJI-doc_402_12_rev2.pdf. (Última consulta en línea 12 de agosto 2017).

⁵¹⁵ AG/RES-2661 (XLI-O/11), *Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas*, 26 mayo San Salvador, El Salvador, 2011.

- El constante esfuerzo realizado por los Estados para garantizar el acceso a la protección de datos personales.
- El esfuerzo de entidades internacionales y regionales⁵¹⁶.

En los próximos pasos presentaremos el estudio comparativo de las normas internas en los Estados americanos realizado por la OEA, con la intención de establecer un marco regional en materia de protección de datos personales. Dicho estudio tiene como finalidad el establecimiento de un marco legislativo contemplando leyes y reglamentos.

Se escogió al Comité Jurídico Interamericano (CJI)⁵¹⁷ como encargado de preparar el documento de *Principios de Privacidad y Protección de Datos Personales en las Américas*, con miras a explorar la posibilidad de un marco regional en esta área (junio de 2011)⁵¹⁸.

El Comité Jurídico entregó un cuestionario⁵¹⁹ de prácticas sobre privacidad y protección de datos a las delegaciones de los países⁵²⁰ miembros, con los fines de proveer los insumos necesarios para la elaboración del documento. Las

Disponible en: http://www.oas.org/es/sla/cji/docs/CJI-doc_402_12_rev2.pdf. (Última consulta en línea 12 de agosto 2017).

⁵¹⁶ La Organización de Cooperación y Desarrollo Económicos (OCDE), el Foro de Cooperación Económica Asia-Pacífico (APEC), La Unión Europea y el Consejo de Europa.

⁵¹⁷ El Doctor David P. Stewart aceptó la relatoría del tema en el XLI Periodo Ordinario de Sesiones de la Asamblea General de la OEA (El Salvador, junio de 2011).

⁵¹⁸ David P. Stewart., 80 Periodo Ordinario de Sesiones., *Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas*, OEAS/Ser. Q, CJI/doc.402/12 rey 2, 9 marzo México, 2012. Presentación Verbal hecha por Dante Negro, director del Departamento de Derecho Internacional, ante la Comisión de Asuntos Jurídicos y Políticos sobre el documento, *Protección de Datos en las Américas*, 13 de noviembre de 2012.

⁵¹⁹ Comisión de Asuntos Jurídicos y Políticos, Consejo Permanente de la Organización de los Estados Americanos, *Cuestionario de Legislación y Prácticas sobre Privacidad y Protección de Datos*, CP/CAJP-3026/11, 31 octubre 2011. Disponible en: www.oas.org/dil/esp/CP-CAJP-3026-11_esp.pdf. (Última consulta en línea 11 de agosto 2017).

⁵²⁰ Los once países que respondieron al cuestionario fueron, Argentina, Canadá, Colombia, Costa Rica, El Salvador, Estados Unidos, México, Panamá, Perú, República Dominicana y Uruguay. Presentación Verbal hecha por Dante Negro, director del Departamento de Derecho Internacional, ante la Comisión de Asuntos Jurídicos y Políticos sobre el documento, *Protección de Datos en las Américas*, 13 de noviembre de 2012.

preguntas del cuestionario están relacionadas con los temas de legislación, normatividad y cumplimiento, jurisprudencia, cooperación transfronteriza, *habeas data*, desafíos tecnológicos y empresariales.

En base a las informaciones aportadas por los Estados miembros se elaboró el estudio comparativo de *Protección de Datos en las Américas*, compuesto de diversos regímenes jurídicos, políticos y mecanismos de aplicación existentes para la protección de datos personales, incluidas leyes, reglamentos y autorregulaciones nacionales⁵²¹, guardando una estrecha relación con el cuestionario suministrado a los Estados miembros.

El documento, compuesto por 4 capítulos, donde el primer capítulo es a manera de introducción y donde explica las razones que dieron origen al documento, entre ellas, la Resolución AG/RES 2661 (XLI-O/11) que -como hemos reiterado- encomienda al Departamento de Derecho Internacional la preparación del documento.

El segundo capítulo corresponde a los marcos jurídicos generales en materia de protección de datos y privacidad, presentando una comparación de los marcos jurídicos europeos, Estados Unidos y América Latina. Además, resalta en las constituciones iberoamericanas la figura del *habeas data*⁵²² correspondiente a 6 de los 11 Estados miembros consultados y que, a su vez, respondieron al cuestionario entregado a las delegaciones de los países.

Por su parte, el tercero se refiere a los instrumentos internacionales sobre privacidad / protección de datos de diversas organizaciones multilaterales como la OCDE, el Consejo de Europa, la Unión Europea y el APEC y la coincidencia

⁵²¹ Consejo Permanente de la Organización de los Estados Americanos, Comisión de Asuntos Jurídicos y Políticos, OEA/Ser.G, CP/CAJP-3063/12, 3 abril 2012. Disponible en: www.oas.org/es/sla/ddi/docs/cp-cajp-3063-12.pdf. (Última consulta en línea el 13 de agosto 2017).

⁵²² 8 de los 11 Estados miembros que respondieron al cuestionario conservan en sus constituciones la figura de *habeas data* entre ellos Argentina, Colombia, República Dominicana, México, Panamá, Perú.

en algunos puntos con los Estados miembros permite emplear sus experiencias y normas legislativas hacia los mismos.

El cuarto capítulo está compuesto por 3 secciones; la primera sección se refiere a la constitucionalización de la protección de datos, la existencia o no de leyes generales y sectoriales en el Estado; la segunda sección apunta a los mecanismos de supervisión empleados para asegurar la supervisión y aplicación de las leyes en materia de protección de datos y su conexión con el Estados sin dejar de lado su independencia, la tercera sección corresponde a las transferencias internacionales, determinando si el Estado cuenta con sistemas de aseguramiento y normas de protección de los datos; la cuarta sección está dedicada a las jurisprudencias y normas especiales en materia de privacidad/protección de datos.

El documento sirve de base para analizar el mejor escenario para América Latina en cuestión de privacidad/protección de datos, tomando como base los modelos existentes e implementados en Europa, Estados Unidos y las organizaciones internacionales. Por tanto, la necesidad es clara. Ahora el tema es determinar el camino a seguir, fundamentado en las informaciones del documento⁵²³ y ser aceptado por los Estados miembros partiendo de sus diferencias⁵²⁴.

⁵²³ “El instrumento adecuado y las estrategias para llevar a dicho objetivo es lo que debe ser determinado por el mejor saber y entender de los estados miembros, ya sea a través de una declaración de principios, la elaboración de una ley modelo, la adopción de una convención Interamericana, o la implementación de esfuerzos para intercambiar mejores prácticas y experiencias que lleven gradualmente a una armonización de las leyes internas de los Estados miembros.....” presentación verbal hecha por Dante Negro, Director del Departamento de Derecho Internacional, ante la comisión de asuntos jurídicos y políticos sobre el documento, Estudio Comparativo: protección de Datos en las Américas, 13 de Noviembre, 2012.

⁵²⁴ “por el momento es necesario concluir que no existe una talla única. Un intento de describir o imponer un solo enfoque normativo detallado tiene pocas posibilidades de lograr aprobación amplia a corto plazo”, *Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas*, CJI/doc. 402/12 rev.2, 9 de marzo 2012. Disponible en: www.oas.org/es/sla/cji/docs/CJI-doc_402_12_rev2.pdf. (Última consulta en línea 13 de agosto 2017).

La Asamblea General de la OEA, en su Cuadragésimo Tercer Período Ordinario de Sesiones⁵²⁵ teniendo en cuenta la importancia de la privacidad y la protección de datos personales y la necesidad de fomentar y proteger el flujo transfronterizo de información en las Américas, y -sin dejar de lado a) el estudio comparativo sobre los distintos regímenes jurídicos, políticos y mecanismos de aplicación existente para la protección de datos personales, inclusive las leyes, reglamentos y autorregulaciones nacionales⁵²⁶, b) la Propuesta de Declaración de Principios de Privacidad y c) la Protección de Datos Personales en las Américas⁵²⁷ con sus 12 principios propuestos⁵²⁸ aprobados en la sesión del 9 de marzo de 2012- encomienda la formulación de propuestas sobre las distintas formas de regular la protección de datos personales incluyendo un proyecto de *Ley Modelo sobre Protección de Datos Personales* sin dejar de lado los Estándares Internacionales existentes en la materia.

Luego de realizar varias consultas, el relator del tema decidió presentar una propuesta ampliada de los 12 principios, considerando las directrices existentes en materia de privacidad/protección de datos, con el fin de ser utilizados en la elaboración de leyes nacionales. Se optó por dejar a un lado, la idea de creación de un texto legislativo común producto a la inexistencia de un enfoque

⁵²⁵ Asamblea General, Cuadragésimo Tercer Período Ordinario de Sesiones, OEA/Ser.P, AG/RES. 2811 (XLIII-O/13), 6 de junio 2013, La Antigua, Guatemala. Disponible en: www.oas.org/es/sla/docs/ag06222s04.pdf. (Última consulta en línea 11 de agosto 2017).

⁵²⁶ Consejo Permanente de la Organización de los Estados Americanos, comisión de asuntos jurídicos y políticos, OEA/Ser.G, CP/CAJP-3063/12, 3 abril 2012. Disponible en: www.oas.org/es/sla/ddi/docs/cp-cajp-3063-12.pdf. (Última consulta en línea 13 de agosto 2017).

⁵²⁷ 80 periodo ordinario de sesiones., *Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas*, OEA/Ser. Q/CJI/RES.186 (LXXX-O/12), 9 MARZO 2012. México, D. F., México. David P. Stewart, 80 Período Ordinario de Sesiones., *Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas* OEA/Ser.Q, CJI/doc.402/12 rev.2, 9 marzo 2012, México, D.F., México. Disponible en: www.oas.org/es/sla/cji/docs/CJI-RES_186_LXXX-O-12.pdf. (Última consulta en línea 12 de agosto 2017).

⁵²⁸ Los 12 principios propuestos fueron: propósitos Legítimos y Justos, Claridad y Consentimiento, Pertinencia y Necesidad, Uso Limitado y Retención, Deber de Confidencialidad, Protección y Seguridad, Fidelidad de la Información, Acceso y Corrección, Información Sensible, Responsabilidad, Flujo Transfronterizo de Información y Responsabilidad, Publicidad de las Excepciones.

regional común, pues el doctor David P. Stewart entendió ser muy prematuro dedicar tiempo a la redacción de leyes y disposiciones de códigos, siendo lo más fundamental la interacción con los Estados miembros⁵²⁹.

Para ello, fue presentado un anteproyecto, conteniendo los cuatro primeros principios⁵³⁰ de manera ampliada y a modo de guía en el proceso de elaboración de leyes nacionales.

Presentada la propuesta del anteproyecto y consultados los expertos en el ámbito de la Unión Europea, grupos regionales y representantes de instituciones gubernamentales, académicas, empresariales, no gubernamentales, y con informaciones procedente de los Estados miembros, el relator del tema concluye de forma ampliada con la presentación de los 12 principios, considerando las directrices de la Unión Europea, OCDE, APEC, etc.⁵³¹. De este modo, el Comité Jurídico Interamericano da por concluido el mandato acordado por la Asamblea General.

Reconociendo el interés manifestado de los Estados Latinoamericanos en realizar esfuerzos de cooperación más allá de sus fronteras⁵³² por medio a las Conferencias Iberoamericanas de Jefes de Estado y Presidentes de

⁵²⁹ 84 Períodos Ordinarios de Sesiones, Privacidad y Protección de Datos, OEA/Ser.Q, CJI/doc.450/14, 25 de febrero de 2014, Río de Janeiro, Brasil. Disponible en: http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_documentos_referencia_CJI_doc_450-14.pdf. (Última consulta en línea 14 de agosto 2017).

⁵³⁰ Los principios ampliados son: Ámbito de aplicación, Propósitos Legítimos y Justos, Claridad y Consentimiento, Pertinencia y Necesidad, Uso Limitado y Retención.

⁵³¹ 86 periodo ordinario de sesiones, OEA/Ser.Q. CJI/doc. 474/15 rev.2, 26 marzo 2015, Río de Janeiro, Brasil. Disponible en: http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf (Última consulta en línea 15 de agosto 2017).

⁵³² “consideramos fundamental reforzar las relaciones económicas y comerciales.....así como promover mayores corrientes de comercio e inversión entre Latinoamérica y la Unión Europea, siendo España y Portugal puntos privilegiados de enlace entre los dos continentes”. , *IV Cumbre Iberoamericana de Jefes de Estados y Presidentes de Gobierno.*, 14 y 15 de junio 1994, Disponible en: <http://www.oei.es/histórico/ivcumbre.htm>. (Última consulta en línea 9 de abril 2017).

Gobierno⁵³³, sin dejar de lado los esquemas de integraciones regionales y subregionales⁵³⁴ de sus Estados, conectados por sus afinidades⁵³⁵ de orígenes, fundamentado en una cultura de credos, creencias y sangre, lenguas comunes (español y el portugués), cercanías culturales y educativas⁵³⁶, manifiestan su interés en procurar el bienestar de sus pueblos por medio al desarrollo económico, comprometidos con la promoción, protección y defensa de los derechos humanos en un mundo globalizado.

En ese sentido, la cooperación entre los países del área debe reducir las diferencias de los países desarrollados con los países en desarrollo⁵³⁷, sin dejar de lado los vínculos de cooperación con España, Portugal y la Unión Europea, por medio a las Conferencias de Jefes de Estado y de Gobierno de América Latina, el Caribe y la Unión Europea⁵³⁸, recibiendo los beneficios de la integración.

A raíz de ello, los Jefes de Estado y de Gobierno, reconocen en la protección de datos personales el grado de derecho fundamental, apoyando las iniciativas

⁵³³ *Cumbres Iberoamericanas de Jefes de Estado y Presidentes de Gobierno*. Disponible en: <http://www.oei.es/histórico/cumbres2.htm>. (Última consulta en línea 6 de abril 2017)

⁵³⁴ *I Cumbre Iberoamericana de Jefes de Estados y Presidentes de Gobierno, Declaración de Guadalajara*, 18 y 19 de julio 1991, México. Disponible en: <http://www.oei.es/histórico/icumbr.htm>. (Última consulta en línea 7 de abril 2017).

⁵³⁵ *II Cumbre Iberoamericana de Jefes de Estados y Presidentes de Gobierno, Declaración de Madrid*, 23 y 24 de julio 1992, Madrid. Disponible en: <http://www.oei.es/histórico/iicumbre.htm>. (Última consulta en línea 7 de abril 2017).

⁵³⁶ *V Cumbre Iberoamericana de Jefes de Estado y de Gobierno*, 16 y 17 de octubre 1995, San Carlos Bariloche (Argentina). Disponible en: <http://www.oei.es/histórico/ivcumbre.htm>. (Última consulta en línea 9 de abril 2017).

⁵³⁷ *II Cumbre Iberoamericana de Jefes de Estado y de Gobierno*, 15 y 16 de Julio 1993. Disponible en: <http://www.oei.es/histórico/iicumbr.htm>. (Última consulta en línea 7 de abril 2017).

⁵³⁸ *VII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, Declaración de Margarita*, 08 y 09 de Noviembre 1997, Margarita, República de Venezuela, p. 14, Disponible en: <http://www.oei.es/histórico/iviicumbre.htm>. (Última consulta en línea 9 de abril 2017) también se puede observar en la Primera cumbre entre los Jefes de Estado y de Gobierno de América Latina, el Caribe y la Unión Europea., *Declaración de Río de Janeiro*, 28 y 29 de junio de 1999, Río de Janeiro, Brasil, Disponible en: <http://www.oei.es/histórico/cumbrerio.htm>. (Última consulta en línea 3 de abril 2017).

regulatorias iberoamericanas en los Estados⁵³⁹, sin obviar las políticas de acceso a las tecnologías de la información y de la comunicación (TICs) por parte de los jóvenes⁵⁴⁰, mediante el impulso de estrategias para universalizar las TICs⁵⁴¹.

Por último, en la XXII Cumbre Iberoamericana se reconoce la importancia de la Constitución Gaditana de 1812 en los procesos independentista de los Estados Iberoamericanos, estableciendo la noción de ciudadanía, formas libres de elección de autoridades etc., enriqueciendo y consolidando los procesos de formación de las constituciones iberoamericanas⁵⁴².

6.10. Nuevos estándares de protección de datos latinoamericana

En el *XV Encuentro Iberoamericano de Protección de Datos* celebrado en Santiago de Chile durante los días 20, 21 y 22 de junio del año 2017 fueron presentados los *Nuevos Estándares Iberoamericanos de Protección de Datos*⁵⁴³. A raíz de la *XXV Cumbre de Jefes de Estado y de Gobierno* celebrado en Colombia en el 2016, la RIPD dio inicio a los trabajos⁵⁴⁴, para ello

⁵³⁹ *XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno.*, 14 y 15 de noviembre 2003, San Carlos Bariloche (Argentina). Disponible en: <http://www.oei.es/histórico/ixiiicumbredeec.htm>. (Última consulta en línea 11 de abril 2017).

⁵⁴⁰ *XVIII Cumbre Iberoamericana, Declaración de El Salvador*, 29 a 31 de octubre, San Salvador, El Salvador. Disponible en: <http://www.oei.es/histórico/ixiiicumbredeec.htm>. (Última consulta en línea 11 de abril 2017).

⁵⁴¹ *XIX Cumbre Iberoamericana, Declaración de Lisboa*, 30 de noviembre y 1 de diciembre de 2009. Disponible en: <http://www.oei.es/histórico/ixiiicumbredeec.htm>. (Última consulta en línea 11 de abril 2017).

⁵⁴² *XXII Conferencia Internacional de Jefes de Estados, declaración de Cádiz*, 16 y 17 de noviembre 2012, Colombia. Disponible en: <http://www.oei.es/histórico/xxiicumbredeec.htm>. (Última consulta en línea 12 de abril 2017).

⁵⁴³ Los nuevos estándares de protección de datos surgen durante el XIV Encuentro Iberoamericano de protección de datos, celebrado el 8 de junio en Santa Marta, Colombia, en la reunión fue acordado la elaboración de los Estándares Iberoamericanos.

⁵⁴⁴ Los trabajos de los nuevos estándares estuvieron liderados por el Instituto Nacional de Transparencia y Acceso a la Información Pública (INAI) quien ocupaba la presidencia de la RIPD para ese entonces.

fue efectuado un taller de *Estándares Iberoamericanos de Protección de Datos* los días 9, 10 y 11 de mayo⁵⁴⁵.

El documento⁵⁴⁶-como su nombre indica y hemos reseñado con anterioridad- ha sido preparado tomando en cuenta los Estados Iberoamericanos pues son los destinatarios de los estándares. El texto está compuesto por 45 artículos distribuidos en 10 capítulos. En su parte inicial, se observan las razones y motivos que originan la conformación del documento, seguido de las disposiciones generales, definiciones de conceptos, ámbitos de aplicación, clasificados en ámbitos de aplicación subjetivo, objetivo y territorial; asimismo, el documento contempla las excepciones generales al derecho a la protección de datos, la ponderación del derecho a la protección de datos personales, el tratamiento de datos personales de niñas, niños y adolescentes, finalizando el capítulo I con el tratamiento de datos personales de carácter sensible.

En ese sentido, el capítulo II presenta 12 principios de protección de datos personales. El primer principio corresponde al de legitimación, seguidos de licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad.

Los derechos ARCO son contemplados en el capítulo III, iniciando con el derecho de acceso, seguido por el de rectificación, cancelación, oposición; continuando con el derecho a no ser objeto de decisiones individuales automatizadas, el derecho a la portabilidad de los datos personales y el derecho a la limitación del tratamiento de los datos personales.

⁵⁴⁵ El taller tiene como nombre un nuevo marco normativo para la protección de los datos personales: *Los Estándares Iberoamericanos*, formando parte de Ellos España, México, Uruguay, Argentina, Colombia, El Salvador, EEUU, Unión Europea, Bruselas, 2017. Disponible en: http://www.redipd.es/actividades/talleres/CartagenadeIndias_2017/index-ides-idphp.php. (Última consulta en línea 14 de junio 2017).

⁵⁴⁶ *Red Iberoamericana de Protección de Datos, Estándares de Protección de Datos personales para los Estados Iberoamericanos*, Santiago de Chile, 20 de junio 2017. Disponible en: http://inicio.inai.org.mx/nuevo/Estandares%20PDP_lbero.pdf. (Última consulta en línea 29 de junio 2017).

El capítulo IV va dirigido al encargado, su alcance, cláusulas y subcontratación de servicios seguido por el capítulo V dirigido a las transferencias internacionales de datos personales; continuando en el capítulo VI con la privacidad por diseño y por defecto, incluyendo los mecanismos de autorregulación.

La autoridad de control y supervisión tienen su espacio en la normativa, siendo integrada en el capítulo VII, seguido por las reclamaciones y sanciones dispuestas en el capítulo VIII; los temas de reparación del daño bajo la sombrilla del derecho de indemnización se ubican en el capítulo IX, cerrando el capítulo con la cooperación internacional mediante el establecimiento de mecanismos de cooperación internacional.

Las razones de creación del Estándar y las acciones a tomar pueden observarse en las informaciones iniciales del documento, señaladas unas veces como considerando y otras como acciones a tomar en cuenta por los Estados miembros. El documento resalta el reconocimiento del grado constitucional que han otorgado la mayoría de los Estados Iberoamericanos a la protección de las personas físicas en relación con el tratamiento de sus datos personales, bajo la forma del derecho a la protección de datos personales o *habeas data*, situación reflejada por los tribunales o cortes constitucionales mediante sus jurisprudencias.

Como hemos comentado en el inicio, mediante reunión celebrada en Cartagena (Colombia) los días 28 y 29 de octubre del 2016, contando con el apoyo de los Jefes de Estado y de Gobierno de los Estados Iberoamericanos, más las Directrices de Armonización presentadas a raíz de la reunión celebrada en Santa Cruz de la Sierra Bolivia en el 2006 y tomando en cuenta los marcos normativos de la Unión Europea, han sido creados los *Estándares Iberoamericanos en materia de Protección de Datos*. En esta ocasión, hemos realizado una separación entre las razones del establecimiento del Estándar y las acciones a tomar en cuenta por los Estados Iberoamericanos en la creación

y normalización de sus preceptos legales y constitucionales, una situación puesta en contexto a continuación.

Razones:

- Ausencia de armonización en los Estados Iberoamericanos, respecto al derecho a la protección de datos personales en sus legislaciones nacionales.
- Dificultad en enfrentar los nuevos retos y desafíos que concierne a la protección de datos, producto a la evolución vertiginosa de la tecnología y la globalización en diversos ámbitos.
- Contribución al cimiento de las economías en los Estados Iberoamericanos, por medio al flujo de los datos personales. contribuyendo a erigir las economías en los Estados Iberoamericanos.
- Necesidad de protección de los niños, niñas y adolescentes, debido a su vulnerabilidad ante el riesgo ocasionado por el tratamiento de sus datos personales a gran escala.
- No todo los Estados Iberoamericanos cuentan con legislación en materia de protección de datos personales.

Acciones:

- Elevar y hacer uniforme la protección de las personas físicas en los Estados Iberoamericanos, favoreciendo las actividades comerciales en la región, evitando el establecimiento de barreras a la libre circulación.
- Adoptar los contenidos de los estándares, contando con un marco regulatorio normalizado que ofrezca niveles de protección a las personas físicas respecto a sus datos personales, garantizando el desarrollo comercial y económico de la zona.

- Ofrecer un catálogo de principios que respondan a los estándares nacionales e internacionales en la materia.
- Reconocer los derechos ARCOS y la Portabilidad, como una manera de garantizar el derecho a la protección de datos personales de forma gratuita y bajos costes, mediante la adopción de un marco regulatorio y el ejercicio del derecho a la autodeterminación informativa, en tiempo de los motores de búsqueda en Internet.
- Establecer una base mínima de protección de datos, para la realización de las transferencias internacionales de datos personales, ante el crecimiento de los flujos transfronterizos soportados por el desarrollo de las nuevas técnicas de la información y comunicación.
- Garantizar las reclamaciones de los titulares en materia de protección de datos personales ante la autoridad de control.
- Establecer una base mínima de cooperación internacional, entre autoridades de control latinoamericana y terceros, enfatizando la protección de los titulares.

La Propuesta de *Estándares de Protección para los Estados Iberoamericano* incorpora en su normativa temas latentes en el reciente Reglamento(UE) 2016/679, pues se trata de una normativa dispuesta en armonizar las legislaciones de los Estados Iberoamericanos en materia de protección de datos y como no, acercarla a las nuevas disposiciones normativas existentes en esa materia.

En ese sentido, el Estándar incorpora el derecho a la portabilidad del titular de los datos, pudiendo transferir sus datos a otros responsables, previo recibir la entrega del anterior en un formato con las características adecuadas que le permita transferirlo al responsable para su utilización, a raíz de ello, se entregará en un formato electrónico estructurado, siempre y cuando los datos

sean tratados vía electrónica o utilizando medios automatizados. Se implementa el tema de la evaluación de impacto a la protección de datos personales cuando se entrañe la posibilidad de afectar a su titular señalado en la legislación nacional de los Estados Iberoamericanos, contemplando el derecho de indemnización que tiene el titular. En ese mismo contexto, el Estándar contempla medidas proactivas en el tratamiento de datos personales, incorporando la privacidad por diseño y por defecto, consideradas y aplicadas por el responsable, ante, y durante la obtención de los datos personales.

De igual forma, el Estándar contempla la implementación e instauración de mecanismos de autorregulación vinculante, con la responsabilidad de llevar a cabo la aplicación de la normativa desarrollada, sin dejar de lado, el establecimiento de medios de resolución de conflictos entre los actores involucrados, como son el titular y el responsable. De igual forma, se establece la posibilidad de implementar una o varias autoridades de control con plena independencia, gozando de posibles influencias externas sin estar sujetas a instrucciones u ordenamientos.

El Estándar no coarta a los Estados en la búsqueda de mecanismos que les permitan o les faciliten la incorporación de sus legislaciones nacionales y, para ello, les permite adoptar mecanismos de cooperación internacional, dándoles la posibilidad de recibir ayudas en temas de cooperación, asistencia entre las autoridades de control, intercambio de experiencias en solución de conflictos y protección de datos.

Sin embargo, a pesar de las intenciones del Estándar de acercarse a las últimas tendencias legislativas en materia de protección físicas de las personas relativa a los tratamientos de datos personales como el referido Reglamento (UE) 2016/679, éste no contempla en sus disposiciones el derecho de supresión de los datos del interesado reconocido como *derecho al olvido*, asignándole al interesado el derecho de solicitar la supresión de sus datos ante el responsable del tratamiento; más bien, la normativa conecta el derecho de supresión con el derecho de cancelación, asumiendo en este derecho la

posibilidad que tiene el titular de solicitar la supresión del dato en posesión del responsable y evitar continuar con su uso.

6.11. A considerar

El Estándar presentado persigue por medio a sus 45 artículos, "elevar el nivel de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales, así como entre los Estados Iberoamericanos, el cual responda a las necesidades y exigencias Internacionales..."⁵⁴⁷, garantizando y tutelando tales derechos en el espacio iberoamericano mediante la instauración de reglas comunes capaces de asegurar tales tratamientos, al mismo tiempo, contempla:

"Impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, autoridades de control no pertenecientes a la región y autoridades y entidades internacionales en la materia"⁵⁴⁸

Se tratan de medidas encaminadas a favorecer el movimiento de datos entre los Estados Iberoamericanos y -como no- con los Estados no pertenecientes al entorno iberoamericano.

De acuerdo al objeto perseguido por el Estándar, estamos delante de una normativa dispuesta a situar la protección de datos iberoamericana al nivel de las normativas internacionales, persiguiendo: a) mejorar el establecimiento de los flujos transfronterizos; b) implantar autoridades de control en los Estados; c) crear y agilizar la comunicación; y d) cooperación entre las autoridades de control. Además, ha de ser capaces de lograr e insertar el Estándar en las normativas nacionales de los Estados, integrándose a los principios y

⁵⁴⁷ Capítulo 1, numeral 1, literal b, Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

⁵⁴⁸ Capítulo 1, numeral 1, literal e, Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

disposiciones contempladas en los 45 artículos de la normativa pero ¿cómo logramos instaurar el *nivel de coherencia* de protección de datos en los Estados y obtener la ansiada homologación fruto de la inserción de los principios y disposiciones de la normativa en las leyes existentes en los Estados Iberoamericanos.?, ¿cómo lograr una efectiva cooperación entre las autoridades de control en los Estados obteniendo *niveles equivalentes de protección*?. Por otra parte, ¿cómo establecemos *sanciones equivalentes* en los Estados ante infracciones cometidas por buscadores globales en Internet?, ¿cómo llegamos a obtener marcos sólidos y coherentes en las normativas de protección de las personas físicas, si las anteriores propuestas de estándares y modelos de protección de datos no han formado parte de las normativas iberoamericanas en materia de protección de datos?. Todas estas cuestiones tienen de base que no se ha logrado un nivel uniforme de protección de datos o una homologación en las leyes de protección en los Estados Iberoamericanos, incluyendo la creación de autoridades de control independientes en todos los Estados Iberoamericanos, y, todo ello, a pesar de la disposición y esfuerzo presentado por organizaciones, Jefes de Estado y de Gobierno vía sus cumbres.

Compartimos en parte el argumento sustentado por Artemi Rallo Lombarte, director de la Agencia Española de Protección de Datos durante el período 2007-2011, y Olga Estadella Yuste⁵⁴⁹ en su libro “*La Protección de la Intimidad frente a la Transmisión Internacional de Datos Personales*”. El primero descarga en los Estados la responsabilidad de implementar sus normativas en materia de protección de las personas físicas en relación al tratamiento de los datos personales⁵⁵⁰. La segunda plantea la conveniencia de conformar una autoridad supranacional de control; decimos en parte, porque si observamos el modelo europeo, a pesar de haber contado con la Directiva 95/46/CE, no existe

⁵⁴⁹ ESTADELLA YUSTE, O., *La Protección de la Intimidad frente a la Transmisión Internacional de Datos Personales*, 1ª ed. TECNOS, Madrid, 1995, pp. 147-148.

⁵⁵⁰ RALLO, A., *El impacto del Reglamento Europeo de Protección de datos en España*, mesa redonda análisis comparado del impacto del RGPD en los Estados miembros, Congreso Internacional sobre el Impacto del Reglamento Europeo de Protección de Datos: análisis nacional y comparado, Universitat Jaume I, Castellon, España, 17 y 18 de mayo de 2018.

una alineación de la protección de datos entre los Estados que conforman la Unión Europea, siendo necesario elevar el nivel de protección de datos en los Estados de la Unión mediante la implementación de un Reglamento (sin dejar aún lado los distintos mecanismos instaurados y existentes que lo conduzcan a materializar lo expresado en el mismo, como son los mecanismos de coherencias, cooperación y un Comité sustituto del Grupo 29 o al Supervisor Europeo de Protección de Datos).

Al otro lado del Atlántico, surge la necesidad de crear en los Estados Iberoamericanos mecanismos capaces de ayudar y formar parte de la implementación del Estándar, de lograr la cooperación entre las autoridades de control, de establecer una supervisión coherente y efectiva con poderes equivalentes entre las autoridades, no siendo suficiente la presentación del Estándar mismo, situación planteada en nuestra propuesta de modelo al final del capítulo, no sin antes, presentar la propuesta del Marco de Protección de Datos del Mercosur, cuya génesis se sustenta en el Marco de Protección de Datos de la UE, una situación manifiesta desde el momento mismo de creación de las instituciones⁵⁵¹ del bloque, hundiéndose sus raíces en el modelo⁵⁵² de la UE⁵⁵³.

En la propuesta de un Marco de Protección de Datos para el Mercosur⁵⁵⁴ se observa una marcada tendencia en lograr o dotar a los Estados que

⁵⁵¹ Consejo del Mercado Común, Comisión de Representantes Permanentes del Mercosur, Grupo Mercado Común, Comisión de Comercio del Mercosur, Parlamento del Mercosur, Tribunal Permanente de Revisión, Tribunal Arbitral Ad Hoc, Tribunal Administrativo-Laboral, Foro Consultivo Económico-Social.

⁵⁵² Consejo Europeo, Consejo de la Unión Europea, Comisión Europea, Parlamento Europeo, Tribunal de Cuentas Europeo, Tribunal de Justicia de la Unión Europea, Tribunal General, Tribunal de la Función Pública, Comité Económico y Social Europeo, Banco Central Europeo, Banco Europeo de Inversiones.

⁵⁵³ DE AZEVEDO CUNHA, M. V., *Protección de Datos en el Mercosur: Hacia un Marco Común*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, Argentina, 2014, pp. 1105-1110.

⁵⁵⁴ DE AZEVEDO CUNHA, M. V., *Protección de Datos en el Mercosur: Hacia un Marco Común*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, Argentina, 2014, pp. 1126-1129.

constituyen el Mercosur⁵⁵⁵ de un nivel común de protección de datos, mediante la armonización de sus normas, creando mecanismos capaces de entregar o proporcionar los mínimos requeridos por los Estados, garantizando el trasiego de información entre los países que conforman el bloque, facilitando la circulación de bienes y servicios, aumentando la cooperación entre los Estados. Sin embargo, se trata de una propuesta marcada por la diferencia en sus normas legislativas, como son los casos de Argentina y Uruguay, cuyas normas en materia de protección de datos reciben el reconocimiento de la Comisión Europea, pero que no ocurre con los demás Estados que forman el Mercosur (tal es el caso de Venezuela al margen de la situación convulsa por la que atraviesa la nación Suramericana pues la constitución Venezolana no contempla la protección de datos en su carta magna, a excepción de la figura del *habeas data* dispuesta en el plexo constitucional). La propuesta contempla la creación de una Oficina Consultiva para el Mercosur en materia de protección de datos, a semejanza del Grupo 29 creado bajo la iniciativa europea 95/46/CE del Parlamento y el Consejo. Dicha Oficina Consultiva estará dispuesta por representantes de las autoridades de los Estados, favoreciendo el comercio entre el Mercosur y la UE. Pero, no hemos de olvidar que en el Reglamento (UE) 2016/679 se sustituye el Grupo de Datos del artículo 29 de la Directiva 95/46/CE del Parlamento y el Consejo por el del Comité, cuyas decisiones son vinculantes para los Estados miembros, a diferencia del carácter no vinculante establecido en el Grupo 29.

Por su parte, el proceso de estandarización u homologación de las normas nacionales en materia de protección de datos no termina e inicia con el Estándar sino que -previo a ello y post al Estándar- los Estados Latinoamericanos siguieron y prosiguen con los esfuerzos de actualizar sus normas nacionales en materia de protección de datos y *habeas data*, propio de los Estados Latinoamericanos, siendo materializado vía sus reformas constitucionales y leyes ómnibus, situación puesta en contexto en las próximas líneas.

⁵⁵⁵ Estados miembros: Argentina, Uruguay, Paraguay, Brasil y Venezuela.

6.12. Planteamiento de propuesta de modelos latinoamericanos

A raíz de la inexistencia de homologación de las leyes nacionales en materia de protección de datos entre los Estados Iberoamericanos, y a expensas de ausencia de organismos capaces de realizar tales implementaciones, presentamos la siguiente propuesta, sustentada en lo previamente visto y analizado en el presente capítulo, así como las propuestas presentadas por organismos, Jefes de Estado y de Gobierno, organizaciones internacionales etc.

Como se ha evidenciado y comentado en secciones anteriores, el modelo europeo es parte integral de los modelos más representativos tomados en cuenta por los Estados Iberoamericanos a la hora de crear nuevas normas legislativas u homologar sus normas existentes en materia de protección de datos. A pesar de ello, no forman parte de nuestro análisis debido a que, independiente de su gran fortaleza, no todos los Estados Iberoamericanos presentan las estructuras adecuadas y viables que conducen a la implementación u homologación de la norma europea, como son: a) el apoyo económico necesario para crear, implementar y llevar a cabo la normativa europea; b) la cultura existente en los Estados; c) el desarrollo, e influencia tecnológica que impacta a los Estados; d) La intención o voluntad de los gobiernos; e) la infraestructura jurídica existente; f) la ausencia de una Unión de Estados Iberoamericanos con pleno derechos y deberes como los existentes en los Estados que conforman la Unión Europea; y g) la capacidad de materializar tal implementación, son algunos de los requisitos necesarios para completar tales fines. No es ésta la realidad. Al momento, no más de dos Estados Iberoamericanos han sido reconocidos por decisiones de la Comisión como Estados con normativas adecuadas en materia de protección de las personas físicas en lo que respecta a la protección de datos personales, permitiendo el flujo de datos desde la Unión Europea hacia esos denominados terceros países declarados adecuados.

En la actualidad, no han sido posibles las propuestas de modelos y estándares de implementación de una Ley Iberoamericana en materia de protección de datos en los Estados Iberoamericanos, a pesar de los constantes esfuerzos empleados por organizaciones internacionales, tal es el caso de la Organización de los Estados Americanos (OEA). Para hacer efectiva la norma, los Estados deben realizar su implementación y crear mecanismos de controles independientes con el objetivo de realizar tales adecuaciones. Por tanto, estamos delante de dos situaciones: la primera es el reconocimiento, aporte y colaboración de los Estados en el establecimiento y creación de una *Ley de Protección de Datos Personales* Iberoamericana como es el caso de la creación de los *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*; y la segunda es asegurar su implementación mediante la creación de mecanismos de controles. Además, pasada la implementación, se necesita garantizar la colaboración entre los organismos instituidos en los Estados (órganos de control), solucionando posibles desavenencias entre los organismos, maximizando la colaboración entre ellos. En consecuencia, y, en resumen, estamos delante de tres situaciones: La primera se ampara en la creación de la norma o el Estándar a ser implementado en los Estados, seguido (segundo) por la instauración de organismos o instituciones en los Estados capaces de realizar las adecuaciones necesarias para cumplir con la implementación y, en una tercera fase, instaurar un mecanismo dispuesto a coordinar y colaborar con los organismos instituidos en los Estados.

Con la normativa a implementar en los Estados, se dispone de leyes equivalentes en los mismos, uniformando el nivel de protección de datos, elevando la protección existente; En ese sentido, con la creación de organismos independientes en los Estados se aspira por una supervisión coherente al momento de realizar tales implementaciones, evitando divergencias. De esa manera, se crearán marcos sólidos y coherentes en lo que a materia de protección de las personas físicas se refiere en relación al tratamiento automatizado de datos personales, elevando el nivel de protección en la región, reforzando la seguridad jurídica y la transparencia en la zona,

aumentando el nivel de confianza, imprescindible y necesario para los operadores económicos en el área conformada por los países iberoamericanos.

En tal sentido, se contempla la creación de un organismo coordinador de los órganos de control, el cual asegure la cooperación efectiva entre las autoridades de control, otorgue poderes equivalentes entre las autoridades, aplicando sanciones equivalentes a las infracciones cometidas en el espacio iberoamericano. Además, este órgano coordinador debe ser capaz de solucionar posibles desavenencias entre los órganos de los Estados, y, por tanto, su conformación deberá estar constituida por un representante de los Estados Iberoamericanos con amplios poderes para tomar decisiones.

En síntesis, más allá del modelo europeo observado, los nuevos modelos deberán estar dirigidos y encausados por un organismo de coordinación capaz de realizar tal agrupación, razones éstas que nos invitan a pensar sobre cual modelo organizativo institucional deberá guiar el proceso de homologación de la ley, más allá del deseo expreso de los Estados en sus múltiples reuniones, acuerdos realizados con organizaciones, congresos, reuniones de Jefes de Estados y propuestas normativas realizadas.

El organismo de coordinación ha de recibir el apoyo económico de los Estados, formando parte de una estructura independiente, o en dicho caso, estar bajo la sombrilla de una organización supranacional instituida, como es el caso de la Organización de los Estados Americanos (OEA) o un organismo con tales capacidades de influencia y reconocimiento.

En la propuesta es necesario y de sumo interés el carácter vinculante y el compromiso asumido por los Estados a la hora de implementar el Estándar en los Estados Iberoamericanos, una situación que nos permite traer a colación que “solo el interés de los Estados Latinoamericanos permitirá realizar cualquier implementación en su territorio”. Así lo externaba el ex director de la Agencia Española de Protección de Datos Artemis Rallo, mediante

conversación realizada luego de su presentación en el *Congreso Internacional sobre el Impacto del Reglamento Europeo de Protección de Datos*⁵⁵⁶.

En conclusión, para lograr este objetivo, hacer efectiva la implementación del Estándar en los Estados Iberoamericanos vamos, en este lugar, a abordar y señalar cuáles serían los requisitos necesarios y suficientes:

- Madurez de los Estados en las normas de protección de datos.
- Intención y voluntad de los Estados.
- Apoyo económico de los Estados.
- Instauración de mecanismos de control en los Estados (órganos de control).
- Instauración de un organismo regional capaz de hacer efectiva y materializar la implementación en los Estados.

Es decir, apelamos por la creación de un Sistema de Mecanismo de Control Supranacional, conformado por órganos de control independientes en los Estados, dirigidos por un Comité u organismo capaz de agrupar y representar a todos los órganos de control y al mismo tiempo, poseer capacidad económica y de decisión para crear, formular, implementar y solucionar conflictos relacionados con la protección de datos personales en los Estados. Además, dada la existencia de vulneraciones internacionales de datos, es necesario la unificación de los Estados bajo una única iniciativa, formando un bloque regional, capaz de protegerlos de las continuas amenazas globales existentes en materia de protección de datos, en un mundo cada vez más tecnológico y ante un aumento de flujos transfronterizos entre los Estados, regiones, de naturaleza y escala global, fruto de la capacidad de los actores envueltos. Es por eso que ante fuerzas globales, redes globales, necesitamos normas globales para su regulación las cuales garanticen la protección de las personas físicas en relación a los tratamientos de datos personales.

⁵⁵⁶ RALLO, A., *El impacto del Reglamento Europeo de Protección de datos en España*, mesa redonda Análisis comparado del impacto del RGPD en los estados miembros, Congreso Internacional sobre el Impacto del Reglamento Europeo de Protección de Datos: análisis nacional y comparado, Universitat Jaume I, Castellon, España, 17 y 18 de mayo de 2018.

Para terminar mostramos un ejemplo donde se observa y refleja esta necesidad. En el caso Cambridge Analytica⁵⁵⁷ varias empresas mexicanas al parecer vulneraron la Ley de Protección de Datos Personales Mexicanas mediante la obtención de datos de Mexicanos y Colombianos por medio a la aplicación Pig.Pigi (usada en la oferta de diversos servicios ofrecido a sus clientes tales como entradas de cine y descuentos). Dicha información fue empleada en las campañas electorales estadounidenses, entre ellas la del candidato Republicano Donald Trump, lo cual evidencia la imposibilidad de establecer penas a las empresas radicadas fuera de los Estados Unidos Mexicanos⁵⁵⁸.

⁵⁵⁷ AMER, K. y NOUJAIM, J., *El gran hackeo*, Netflix, 2019.

⁵⁵⁸ “Estamos en pañales, porque cómo se va a multar a una empresa que no tiene un establecimiento en México, lo que hace muy difícil hacer efectiva la multa. Quedamos en un estado de indefensión. Por ello, es fundamental promover mecanismos de colaboración internacional en este sentido. Porque muchas de las vulneraciones ya se están dando desde afuera”. María Solange Maqueo, profesora investigadora del centro de investigación y Docencia Económica (CIDE) especialista en protección de datos personales, visto en SANTILLAN, O., *Falla Inai en protección de datos personales*, Eje Central, 2018. Disponible en: <http://www.ejecentral.com.mx/falla-inai-en-proteccion-de-datos-personales/>. (Última consulta en línea 26 de mayo 2018).

CAPÍTULO III

EI DERECHO A LA PROTECCIÓN DE DATOS Y *HABEAS DATA* EN LA CONSTITUCIÓN DE LA REPÚBLICA DOMINICANA. SU RELACIÓN CON OTROS DERECHOS

I. ANTECEDENTES CONSTITUCIONALES DEL DERECHO A LA PROTECCIÓN DE DATOS EN REPÚBLICA DOMINICANA

1. Introducción

Como tendremos ocasión de constatar en este Capítulo, República Dominicana no es ni mucho menos ajena sino todo lo contrario a la construcción doctrinal y jurisprudencial que se realiza tanto en Latinoamérica como en el contexto europeo y especialmente, a las contribuciones españolas. Pero para empezar, y en el mismo sentido, se ha de reseñar que el crecimiento tecnológico como fenómeno global articula el desarrollo legislativo de los procesos de reformas que acompañan las normas europeas, americanas y latinoamericanas. De esta situación tampoco escapa sino que forma parte la República Dominicana, conectada con los movimientos tecnológicos y transformaciones legislativas que ocurren a largo y ancho del Atlántico, en especial, las legislaciones latinoamericanas materializada en las cartas magnas de los Estados.

Es evidente que el escenario planteado no era posible en las primeras constituciones. Los cambios tecnológicos e influjo de los derechos fundamentales actuales no eran los que permeaban las estructuras jurídicas de la época, contemplando otros derechos durante su proceso de elaboración; sin embargo, este escenario va evolucionando a medida que los nuevos albores de libertad y reivindicaciones sociales ocurren a lo largo y ancho de los mares.

Es por ello que ante tales informaciones nos interesa, al menos, saber cuál ha sido el origen histórico de la constitucionalización de estos derechos, para contextualizar la Constitución del 2010 y la actual Constitución del 2015, cuyas normas en materia de protección de datos y *habeas data* se mantiene constante tras la carta magna del 2010 pesar de la transformación o reforma constitucional realizada en el 2015⁵⁵⁹.

2. Antecedentes constitucionales. Primeras reflexiones doctrinales sobre protección de datos y Constitución de 2002

La primera Constitución Dominicana data del 1844. En ella ya se reconocían los derechos individuales, entre ellos la dignidad humana. Su catálogo de derechos era muy amplio para su tiempo y enormemente generoso. Era notoria la influencia de la Constitución norteamericana de 1787, francesas de 1799 y 1814, haitianas de 1816 y 1843, y española⁵⁶⁰ (tanto de la Constitución de 1812⁵⁶¹ como la de 1837), siendo considerada una Constitución Derivada por adaptar las experiencias constitucionales de otros países a la nuestra⁵⁶². No existía alusión al derecho a la intimidad, pero sí, desde entonces -como mencionaremos a continuación- a la garantía de la inviolabilidad del domicilio.

⁵⁵⁹ En materia de protección de datos y *habeas data* la Constitución del 2010 y 2015 son indistintas al momento de ser utilizados los referidos términos en cuestión; la constitución del 2010 refleja por primera vez estos derechos, transferidos a la nueva reforma constitucional del 2015.

⁵⁶⁰ RAY GUEVARA, M., *Opinión Constitucional*, 1ª ed. Santo Domingo, República Dominicana, 2014, p. 289

⁵⁶¹ “El texto de la Constitución de Cádiz se recibió en la isla el 13 de Julio del mismo año de su promulgación. Lo llevó la goleta española Intrépido Rovira al mando de don Francisco Puyols. El día 18 se hizo la publicación y hubo fiestas como toque de campanas, salvas de artillería y se enarboló el pabellón nacional, y el día 19 se juró con gran solemnidad en la catedral y en Santa Bárbara. Fiestas parecidas se celebraron en los pueblos” RAY GUEVARA, M., *Opinión Constitucional*, 1ª ed. Santo Domingo, República Dominicana, 2014, p. 288; tomado de; WENCESLAO, V., *Historia del derecho dominicano*. Santo Domingo, 2006. pp. 113 y siguientes.

⁵⁶² BREA FRANCO, J., *El Sistema Constitucional Dominicano*, Tomo I, 1ª ed. UNPHU, Santo Domingo, República Dominicana, 1983, p. 87.

Por su parte, los derechos individuales se transforman en protección efectiva de los derechos humanos a partir de la Constitución del 1955 y ya la Constitución del 1947 mantiene el último epígrafe de derechos individuales.

En la Constitución del 2002 se prevén estos derechos; si bien cabe reseñar que aborda el concepto de manera tácita cuando se refiere a la dignidad humana.

Además, se sostiene que entre los derechos individuales y sociales contempladas en dicha Constitución se encontraba:

“La inviolabilidad de la correspondencia y demás documentos privados, los cuales no podrán ser ocupados ni registrados sino mediante procedimientos legales en la substanciación de asuntos que ventilen en la justicia. Es igualmente inviolable el secreto de la comunicación telegráfica, telefónica y cablegráfica”⁵⁶³. (Art. 8 y 9).

De ahí la doctrina deducía que la expresión “correspondencia y demás documentos privados” utilizada por el constituyente, comprendía una protección amplísima, llegando a afirmar que en dicho texto se salvaguardaban los datos personales en general o los datos vinculados a la vida privada de una persona física.

También señalaba que, merced a las posibilidades de esta previsión “es igualmente inviolable el secreto de la comunicación telegráfica, telefónica y cablegráfica”- se protegían los datos personales que podían ser manejados a través de los mecanismos que modernamente se utilizan para la transmisión de datos⁵⁶⁴.

⁵⁶³ Artículo 8 y 9 Constitución de la República Dominicana del 2002.

⁵⁶⁴ ACOSTA DE LOS SANTOS, H., “Protección de Datos en la República Dominicana”, en *Revista iberIUS*, monográfico dedicado a *La protección de datos personales*, núm.2, agosto, 2006, pp. 83-85. Disponible en: http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnálisisDocumentacionJudicial/revista%20iberius/IberIUS_02.pdf. (Última consulta en línea 24 de agosto 2013). También ver “La protección de datos personales”, *Revista iberIUS*, año 2, núm. 2, Agosto 2006. Disponible en: <http://www.iberius.org/documents/20536/23722/Proteccion.pdf/52245388-464d-450c-ae20-2858950d1c09>. (Última consulta en línea 24 de noviembre de 2019).

Se trata, por tanto, de la interpretación de un constitucionalista avezado que preocupado y conocedor de la realidad constitucional y legislativa de su país y de otros países del contexto latinoamericano⁵⁶⁵, norteamericano y europeo en materia de protección de datos, intenta “sacar el máximo partido” al texto constitucional para proteger este nuevo derecho. Compartimos, por tanto, esta tesis.

En cualquier caso, como el propio autor refiere con la expresión “los datos personales en general o los datos vinculados a la vida privada de una persona física”, en nuestra opinión todavía se es muy deudor de la concepción “vida privada”. Además, todavía este texto constitucional se ancla en posibles invasiones a los derechos de la era preinformática (telegráfica, telefónica y cablegráfica). Cabe añadir, por ejemplo, que el artículo 24 de la Constitución de Guatemala, en un texto muy similar a éste, en 1985, casi dos décadas antes, ya señalaba además de este tipo de comunicaciones las radiofónicas -pero en lo que a nosotros nos interesan- las relativas a “otros productos de la tecnología moderna”.

En definitiva, no aparece en el texto constitucional del 2002 un reconocimiento expreso del derecho a la protección de datos con sustantividad y autonomía propia, lo cual hubiera sido lo deseable en una constitución de principios del siglo XXI.

II. EL DERECHO A LA PROTECCIÓN DE DATOS EN LA CONSTITUCIÓN DEL 2010 y 2015. EL ARTÍCULO 44 NUMERAL 2

La actual Constitución de la República Dominicana proclamada el 26 de enero del 2010 - día en que se conmemoró el 197 del natalicio del patricio Juan

⁵⁶⁵ “... América Latina necesita de una identidad étnico-cultural que nos permita tener más cosas en común, al menos en términos de las constituciones, de nuestras naciones”, visto en CAMPOS FARIAS, F., *Estudio Comparado de las Constituciones Políticas Nacionales Latinoamericanas*, Santo Domingo, República Dominicana, 2002, p. 205.

Pablo Duarte⁵⁶⁶ recoge en el numeral 2 del artículo 44 el derecho a la protección de datos. Pero antes de entrar a analizar más detalladamente la virtualidad de este precepto, es importante avanzar en este lugar que también - y conforme al objeto de todo nuestro estudio- en el epígrafe III y IV nos detendremos en otros derechos que entroncan con éste, como es el derecho a la intimidad (desplegado en el artículo 44 en la constitución dominicana) y el habeas data (previsto en su artículo 70).

El derecho a la intimidad, al honor, al buen nombre y a la propia imagen se ubican en el título II “De los derechos, garantías y deberes fundamentales”, específicamente en el capítulo I, bajo la denominación de “Los derechos fundamentales” de la Sección I perteneciente a los derechos civiles y políticos de la Constitución dominicana del 2010 (e igualmente en la actual Constitución del 2015) desplegado en los artículos del 37 al 49.

Más concretamente estos derechos se consagran en el artículo 44 de la Constitución dominicana. Dicho precepto compuesto de cuatro numerales, contempla en su numeral segundo la posibilidad de tener acceso a las informaciones y datos ubicados en registros oficiales o privados. Así:

“Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos”⁵⁶⁷

Desde la doctrina no se ha dudado en afirmar que es la primera vez que se constitucionaliza la protección de datos personales en la carta magna de la

⁵⁶⁶ RAMÍREZ MORILLO, B., *Derecho Constitucional Dominicano*, editora Centenario, S. A., Santo Domingo, República Dominicana, 2010, p. 35.

⁵⁶⁷ Artículo 44, numeral 2.

República Dominicana y que, por tanto, la misma forma parte de la actual Constitución⁵⁶⁸.

La Constitución de la República Dominicana ha sufrido 39 reformas⁵⁶⁹. Es por ello que se afirma que la Constitución actual es un reflejo de los nuevos tiempos, como respuesta a cambios producidos en la sociedad dominicana⁵⁷⁰ a tal punto de hacer suya e insertar en sus normas internas el tema de la protección de datos personales, obedeciendo con ello, a los nuevos cambios y aires constitucionales que invaden los diferentes Estados Latinoamericanos y europeos⁵⁷¹.

Como podemos apreciar, nuestra carta magna manifiesta un interés especial en la protección de los datos personales⁵⁷², la doctrina afirma que aquí se reside un derecho a la protección de los datos personales que se contrapone a la erosión y degradación que afectan a los derechos fundamentales ante determinados usos de la tecnología. Desde que las personas nacen, la tecnología de la información y su evolución se nutren de sus datos. En este sentido, se garantiza la facultad que tiene toda persona de acceder y decidir por sí misma sobre la utilización de sus datos personales u oficiales y sobre sus bienes y de decidir cuándo y dentro de qué límites procede hacer uso de esa información referente a su vida y a sus bienes. Tiene derecho al acceso a

⁵⁶⁸ RAMÍREZ MORILLO, B., *Derecho Constitucional Dominicano*, editora Centenario, S. A., Santo Domingo, República Dominicana, 2010, p. 15.

⁵⁶⁹ CÉSAR MATOS, J., *Introducción al Estudio del Derecho*, Santo Domingo, República Dominicana, p. 433.

⁵⁷⁰ RAMÍREZ MORILLO, B., *Derecho Constitucional Dominicano*, editora Centenario, S. A., Santo Domingo, República Dominicana, 2010, p. 3.

⁵⁷¹ DÍEZ DE VELASCO, M. A., *Instituciones de Derecho Internacional Público*, 15ª ed. Tecnos, Madrid, 2005, p. 261.

⁵⁷² AMIANA, M., *Notas de Derecho Constitucional*, editora tiempo, S. A., Santo Domingo, República Dominicana, 1995, p. 37.

la información que sobre ella se contenga y -conocida la misma- saber el uso y destino que de ella se haga⁵⁷³.

En ese sentido, la actual Constitución de la República Dominicana integra el tema de la protección de datos, ejerciendo con ello una especie de descubrimiento de derecho, ampliando la base de los derechos fundamentales existentes en la Constitución del 2010, creando de la misma forma derechos fundamentales por el solo hecho de estar inscrito en la Constitución o lo que es lo mismo ser un derecho previamente constitucionalizado⁵⁷⁴. Con esta reforma, la República Dominicana se convierte en “la Constitución más avanzada de Iberoamérica” en pleno siglo XXI⁵⁷⁵.

Es por ello que, en la presente Constitución, el legislador la acerca más a los derechos fundamentales supeditando la democracia al respecto y garantía de los derechos fundamentales⁵⁷⁶. En la carta magna, los derechos se denominan derechos fundamentales ya que son aquellos derechos humanos reconocidos en la legislación vigente de un Estado y bajo la protección de su fuerza coactiva. El reconocimiento de los derechos fundamentales normalmente se hace en el texto constitucional, y supone la legitimación de la democracia del Estado⁵⁷⁷.

Por otra parte, no se puede soslayar la relación de este precepto con otro trascendente para su interpretación, el artículo 74.3. Conforme a este último,

⁵⁷³ SOSA PÉREZ, R., *Constitución Comentada*, editora Fundación Institucionalidad y Justicia Inc. (FINJUS), Santo Domingo, 2011, pp. 91-92.

⁵⁷⁴ JORGE PRATS, E., *Derecho Constitucional*, Volumen II, editora IUSNOVUM, Santo Domingo, República Dominicana, 2012, p. 50.

⁵⁷⁵ RAY GUEVARA, M., *Opinión Constitucional*, 1ª ed. Santo Domingo, República Dominicana, 2014, p. 309.

⁵⁷⁶ RAMÍREZ MORILLO, B., *Derecho Constitucional Dominicano*, op. cit., p. 35.

⁵⁷⁷ CARRERAS SERRA, L., *Régimen jurídico de la información*, Ariel, España, 1996, p. 12.

nuestra constitución les asigna una jerarquía constitucional a los tratados⁵⁷⁸ internacionales cuando expresa que los tratados, pactos y convenios relativos a derechos humanos, suscritos y ratificados por el Estado dominicano, tienen jerarquía constitucional y son de aplicación directa e inmediata por los tribunales y demás órganos del Estado.

Es por ello, que la reforma Constitucional del 2010 puso la ley sustantiva del Estado dominicano al día con los convenios y tratados internacionales⁵⁷⁹, y a la vez, logró que el texto se acercara más a la realidad nacional⁵⁸⁰.

El artículo 179 de la Declaración de Derechos del Hombre y del Ciudadano de 1789 expresa que “toda sociedad en la cual la garantía de los derechos no esté asegurada no existe constitución, porque sin garantía los derechos fundamentales no son derechos”. Siguiendo esta argumentación cabe decir que, en caso de que sean violados los derechos fundamentales, nuestro país puede ser demandado ante la Corte Interamericana de los Derechos Humanos, ya que el Estado dominicano es signatario de “La Convención Americana”. Esto significa que un no cumplimiento de los acuerdos firmados, puede colocar en riesgo la reputación del Estado dominicano con los Estados participantes, afectando con ello la imagen del país con los Estados signatarios de la Convención y con el resto del mundo⁵⁸¹. La República Dominicana es signataria de tratados internacionales relacionados con el tema de los derechos humanos y la protección de datos personales, su “denuncia”⁵⁸², “nulidad”⁵⁸³

⁵⁷⁸ GAMBOA SERAZZI, F., *Manual de Derecho Internacional Público*, 4ª ed. LOM, Chile, 1997, p. 42.

⁵⁷⁹ DÍEZ DE VELASCO, M., *Instituciones de Derecho Internacional Público*, 13ª ed. TECNOS, S. A., Madrid, España, pp. 128-138.

⁵⁸⁰ RAMÍREZ MORILLO, B., *Derecho Constitucional Dominicano*, op.cit., p. 127.

⁵⁸¹ *Ibidem*, p.127.

⁵⁸² GAMBOA SERAZZI, F., *Manual de Derecho Internacional Público*, op. cit. p. 54.

⁵⁸³ *Ibidem*, p.55.

puede acarrear “conflicto Regional o Global”⁵⁸⁴ generados por el incumplimiento de los acuerdos establecidos.

El proceso de reforma⁵⁸⁵ contemplado en la Constitución del 2010 ha sido el producto de los trabajos de una sociedad activa⁵⁸⁶ conformada por una Comisión⁵⁸⁷ de juristas⁵⁸⁸ y la participación de diferentes sectores, - entre ellos el sector económico, político, empresarial, transporte, energético, ambiental, social, religiosos, ONG, transporte etc.- generando con ello, un gran despliegue de propuestas y adecuaciones contemplados en la actual Constitución de la República Dominicana caso de la incursión del *habeas data* y la protección de datos insertado en el artículo 44 numeral 2 y el 70 de la Constitución.

En ese sentido, se ha de señalar que desde la doctrina especializada se ha puesto de relieve dicha situación que se refleja en el tema de la protección de

⁵⁸⁴ PEREIRA, J., *Diccionario de Relaciones Internacionales y Política exterior*, editora Ariel S. A., Barcelona 2008, p. 207.

⁵⁸⁵ El proceso de reforma, se fundamenta en la necesidad de modificar la parte sustancial de la Constitución de la República, una Constitución establecida sin modificaciones o cambios sustanciales desde el año 1966; los cambios constitucionales realizados durante el 1994 y el 2002 no eran suficientes para llenar las expectativas de la sociedad, fundamentos de la creación de la reforma, bajo la inspiración del entonces presidente de la República doctor Leonel Fernández Reyna, reconocido en los considerandos del Decreto. Cfr. *Decreto N.º 323-6*, Artículo 2. Disponible en: http://www.camaradediputados.gob.do/serve/listfile_download.aspx?id=1121&num=1. (Última consulta en línea 11 de marzo 2018).

⁵⁸⁶ RAMÍREZ MORILLO, B., *Derecho Constitucional Dominicano*, op. cit., p.131.

⁵⁸⁷ La Comisión tuvo a su cargo la responsabilidad de preparar el documento de propuesta de reforma, alimentado por las consultas realizadas a los principales actores de la sociedad activa (Sectores Populares, Sociales, Sociedad Civil, Políticos y Religiosos), el documento contiene propuestas y recomendaciones de modificación⁵⁸⁷ debiendo preparar los documentos a emplear en las consultas, incluyendo guías, pautas y orientaciones, así como la organización de los procesos de consulta en amplios sectores de la población, completando el anteproyecto de reforma constitucional. Decreto. N.º 323-06 que crea e integra la Comisión encargada de preparar las consultas que fueren necesarias tendentes a modificar la Constitución de la República.

⁵⁸⁸ Decreto N.º 323-6, Artículo 1, Se designa una Comisión integrada por los juristas señores Dr. Raymundo Amaro Guzmán, Dr. Julio César Castaños Guzmán, Lic. Pelegrín Castillo, Dr. Flavio Darío Espinal Jacobo, Dra. Aura Celeste Fernández, Dr. Luís Gómez Pérez, Dr. Milton Ray Guevara, Lic. Eduardo Jorge Prats, Dra. Licelott Marte, Dr. César Pina Toribio, Lic. Leyda Margarita Piña, Dr. José Darío Suárez y Lic. Adriano Miguel Tejada.

datos personales siendo “el único país que contiene un plexo de principios constitucionales (calidad, licitud, lealtad, seguridad y finalidad) que deben regir el tratamiento de datos personales”⁵⁸⁹ estando al alcance y superando en otros casos, las normas constitucionales en materia de protección de datos en los países que integran la región.

Con respecto a estos principios desde la doctrina dominicana se ha recogido que éstos deben ser entendidos del siguiente modo:

- Los principios de calidad, licitud y lealtad requieren que los datos sean exactos y prohíbe que se adquieran por medios fraudulentos, desleales e ilícitos
- El principio de seguridad requiere la protección debida de los datos personales y de sus bienes que tiene que resguardar el registro de los mismos.
- El principio de finalidad exige que el registro de los datos personales y de los bienes de las personas cumpla con los propósitos que motivan su registro y tratamiento, debiendo ser cancelados cuando no fueran necesarios para tal fin.

La doctrina también deduce que este derecho descansa sobre los principios del consentimiento de la persona -quién manifiesta su voluntad sobre el tratamiento de sus datos- y la proporcionalidad entendida como el registro adecuado, pertinente y no excesivo de los datos, en relación al fin para el que se recaban y procesan.

⁵⁸⁹ REMOLINA ANGARITA, N., *Informe Latinoamérica y Protección de datos personales en cifras*, 1985-2012, Bogotá Colombia, p. 5. Disponible en: http://www.redipd.org/noticias_todas/2013/tribuna/common/Latinoamericaypdencifras19852012_NRemolina.pdf. (Última consulta en línea 14 de agosto 2013).

Del mismo modo, las restricciones que la ley prevea no deben reducir la eficacia del derecho de acceso y protección de los datos personales y de sus bienes, siendo necesaria las debidas garantías⁵⁹⁰.

La República Dominicana, por tanto, merece una valoración positiva conforme al mapa latinoamericano sobre la protección de datos personales, constituciones y normas generales (1985-2012) perteneciente al informe *Latinoamérica y Protección de Datos Personales en Cifras (1985-2012)* por lo anterior citado y expuestos a continuación.

El Estado dominicano forma parte del análisis realizado en materia de protección de datos a 21 países incluyendo Centroamérica, Caribe y Suramérica (Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Uruguay y Venezuela) y de estos países la República Dominicana forma parte de los 14 países que reconocen y contemplan en sus constituciones la protección de datos⁵⁹¹.

Además, la República Dominicana también pertenece al grupo de países con leyes nacionales en materia de protección de datos. Con todo, como se verá en el próximo epígrafe, fuimos partícipes de un interesante proceso de propuestas legislativas al respecto, cuyos resultados son observados en la promulgación de la *Ley núm. 172-13 que tiene por objeto la protección integral de datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados dar informes, sean estos públicos o privados*⁵⁹².

⁵⁹⁰ SOSA PÉREZ, R., *Constitución Comentada*, op.cit., p. 92.

⁵⁹¹ REMOLINA ANGARITA, N., *Informe Latinoamérica y Protección de datos personales en cifras*, op. cit., pp.1-2.

⁵⁹² G.O. N.º 10737 del 15 de diciembre de 2013.

Por último, se ha de reseñar que, además del artículo 44 numeral 2, hay numerosas referencias por las que deduce que el texto actual dominicano es un texto plenamente insertado en la era informática.

Así, frente a las previsiones de Constitución del 2002 que hemos analizado, en esta carta magna se alude ya a:

“...la inviolabilidad de la correspondencia, documentos o mensajes privados en formatos físico, *digital, electrónico o de todo otro tipo*⁵⁹³.....Es inviolable el secreto de la comunicación telegráfica, telefónica, cablegráfica, *electrónica, telemática o la establecida en otro medio*”⁵⁹⁴.

“El *manejo, uso o tratamiento de datos e informaciones* de carácter oficial que recaben las autoridades encargadas de la prevención, persecución y castigo del crimen...”⁵⁹⁵.

En relación al *habeas data* -que después analizaremos-:

“Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en *registros o bancos de datos* públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme a la Ley”⁵⁹⁶.

También en un sentido más general:

“El Estado garantiza servicios públicos de radio, televisión y redes de bibliotecas y de *informática*, con el fin de permitir el *acceso universal a la información*. Los centros educativos incorporarán el conocimiento y aplicación de las *nuevas tecnologías y de sus innovaciones*, según los requisitos que establezca la ley”⁵⁹⁷.

“...El Estado procurará, junto al sector privado, un crecimiento equilibrado y sostenido de la economía...tendente al pleno empleo y

⁵⁹³ Todas las cursivas que a continuación aparecen son nuestras.

⁵⁹⁴ Artículo 44, numeral 3, Constitución de la República Dominicana del 2010.

⁵⁹⁵ Artículo 44, numeral 4, Constitución de la República Dominicana del 2010.

⁵⁹⁶ Artículo 70, Constitución de la República Dominicana del 2010.

⁵⁹⁷ Artículo 63, Constitución de la República Dominicana del 2010.

al incremento del bienestar social, la formación permanente de los recursos humanos y el *desarrollo científico y tecnológico*⁵⁹⁸.

III. EL DERECHO A LA PROTECCIÓN DE DATOS EN LA CONSTITUCIÓN DE 2010 Y SU RELACIÓN, ESPECIALMENTE CON EL DERECHO A LA INTIMIDAD, LA VIDA PRIVADA Y EL LIBRE DESARROLLO DE LA PERSONALIDAD

Ya hemos mencionado que la protección de datos en su numeral 2 del artículo 44 se sitúa dentro del precepto denominado "*Derecho a la intimidad y el honor personal*", disponiendo que.

"Toda persona tiene derecho a la intimidad. Se garantiza el respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo. Se reconoce el derecho al honor, al buen nombre y a la propia imagen. Toda autoridad o particular que los viole está obligado a resarcirlos o repararlos conforme a la Ley"⁵⁹⁹.

En ese sentido, este entronque de la protección de datos con ese conjunto de derechos es bastante similar al texto de la Constitución española de 1978, en donde la orden al legislador para que se regule el uso de la informática (18.4 Constitución española) se encuentra dentro del mismo precepto que trata de un conjunto de derechos como la intimidad, el honor, la propia imagen, la inviolabilidad del domicilio y el secreto de las comunicaciones. Sin embargo, en España se partió del derecho a la intimidad y no se ha asumido el derecho a la vida privada (si bien posteriormente judicialmente se fue desarrollando) mientras que en República Dominicana el concepto de "vida privada" (incluso como hemos visto en la Constitución del 2002 ya se aludía a lo "privado") ha permeado y es más novedosa la incorporación del derecho a la intimidad.

⁵⁹⁸ Artículo 218, Constitución de la República Dominicana del 2010.

⁵⁹⁹ Artículo 44 numeral 2, Constitución de la República Dominicana del 2010.

La referencia a “vida privada” o lo “privado” (nos referimos, en este caso, en exclusiva, a esta acepción de lo privado) se encuentra muy presente en el texto actual. Así además de la referencia expresa a la “vida privada”, se habla de ello en:

“El hogar, el domicilio y todo recinto *privado* de la persona”⁶⁰⁰;

“Se reconoce la inviolabilidad de la correspondencia, documentos o mensajes *privados* en formatos físico... Sólo podrán ser ocupados, interceptados o registrados, por orden de una autoridad judicial competente, preservando el secreto de lo *privado*, que no guarde...”⁶⁰¹;

A menudo, como se comentó en el capítulo I intimidad y vida privada, equivocadamente, se usan como sinónimos. Así, desde la doctrina dominicana se señala que:

“..el derecho a la intimidad es lo que los norteamericanos denominan “the right to privacy”, el derecho a la privacidad...”⁶⁰².

De este modo escrito parece que obedecen a la misma realidad y estos dos conceptos deben ser deslindados. La intimidad se refiere al derecho en virtud del cual excluimos a todas o a determinadas personas del conocimiento de nuestros pensamientos, sentimientos, sensaciones y emociones, exclusión que se realiza en su contenido íntimo o privado⁶⁰³. Sin embargo, cuando nos referimos al término de privacidad se ha de entender el ámbito de su vida familiar, aficiones, bienes particulares, etc. Íntimo se refiera a las cosas profundas del alma humana, así como a lo cercano, mientras que privado alude a lo personal y lo particular, es decir, a aquello que se mantiene alejado del público y que ha de estar libre de intromisión. Todos estos aspectos, además

⁶⁰⁰ Artículo 44, numeral 1, Constitución de la República Dominicana del 2010.

⁶⁰¹ Artículo 44, numeral 3, Constitución de la República Dominicana del 2010.

⁶⁰² JORGE PRATS, E., *Derecho Constitucional*, op. cit., 2012, p.175.

⁶⁰³ ROMERO COLOMA, A, M., *Libertad de Información frente a otros derechos en conflicto, Honor, Intimidad y presunción de Inocencia*, 1ª ed., Civitas, Madrid, 2000, p. 41.

de los íntimos, constituyen una esfera que se debe proteger de la intromisión⁶⁰⁴.

Pero además también se sigue sin romper el binomio entre intimidad y protección de datos Así, desde la doctrina se señala.

“el derecho de acceso a datos personales o derecho a la autodeterminación informativa es una derivación del derecho a la intimidad y del derecho a la información”⁶⁰⁵ o,

“el derecho de acceso a la información sobre sus datos personales, o lo que se ha denominado derecho a la autodeterminación informativa, se construye a partir del derecho a la intimidad personal y familiar y sirve de garantía al honor y al derecho a la imagen y permite el ejercicio de otros derechos del ciudadano”⁶⁰⁶.

Sin lugar a dudas, los conceptos e interpretaciones emitidas de la Constitución del 2010 obedecen a la forma como la *privacy* norteamericana permeó el contexto europeo, entendido como un derecho más de la personalidad (intimidad, honor), siendo mucho más que eso. El derecho a la autodeterminación informativa (relativa a la Sentencia del Censo de 1983 en Alemania) se vinculó a un derecho a la personalidad⁶⁰⁷. Todas estas expresiones y tesis de interpretación después han “viajado” a Latinoamérica y siguen estando -como se puede comprobar- presentes.

Otro precepto que también se suele relacionar, a menudo, con la protección de datos es el relativo al derecho al libre desarrollo de la personalidad. El motivo de enlazar con ese derecho es debido a la construcción del derecho a la autodeterminación alemana que ante la ausencia expresa de derecho recurre

⁶⁰⁴ DÍAZ ROJO, J. A., “Privacidad”, *El cajetín de la lengua*. Disponible en: <http://pendientedemigracion.ucm.es/info/especulo/cajetin/privacid.html>. (Última consulta en línea 14 de agosto 2013).

⁶⁰⁵ *Ibidem*, p. 176.

⁶⁰⁶ SOSA PÉREZ, R., *Constitución Comentada*, op. cit., p. 92.

⁶⁰⁷ RODRÍGUEZ MARCANO, E. R., *El derecho a la autodeterminación informativa en Venezuela...op.cit.*, pp.17-18 y p.385.

al libre desarrollo de la personalidad. En el artículo 43 de la Constitución del 2010 bajo el título *derecho al libre desarrollo de la personalidad* se establece que.

“Toda persona tiene derecho al libre desarrollo de su personalidad sin más limitaciones que las impuestas por el orden jurídico y los derechos de los demás”⁶⁰⁸.

Pero en el caso dominicano, ya no es necesario atender al mismo para derivar el contenido esencial del derecho a la protección de datos, pues conforme al artículo 44 numeral 2 (junto con el 70) podemos encontrar base suficiente.

IV. EL *HABEAS DATA* EN REPÚBLICA DOMINICANA

1. Consideraciones iniciales

La protección de datos, como hemos mencionado, se encuentra inserta en las recientes reformas constitucionales. Al mismo tiempo, el concepto se incluye en el derecho de acceso bajo la sombrilla del *habeas data*, capaz de realizar tal protección y tratamiento de datos. Por tanto, es importante recordar y reconocer que, a pesar de que en los demás numerales la palabra datos no se encuentra inmersa, podemos argumentar que el concepto como tal está inmerso en las correspondencias, informaciones, documentos, mensajes privados, independientemente de su forma de almacenamiento, ya sean estos depositados en registros oficiales o privados.

A diferencia de la protección de datos, el *habeas data* se encuentra definido literalmente a partir de la Constitución del 2010, razones éstas que nos permiten imbuirnos directamente en el concepto reflejado en la Constitución, y presentado a continuación.

⁶⁰⁸ Artículo 43, Constitución de la República Dominicana del 2010.

2. *Habeas data*

La acción de *habeas data* contenido en su artículo 70 perteneciente al capítulo II bajo el epígrafe “de las garantías a los derechos fundamentales expresa:

“Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme a la ley. No podrá afectarse el secreto de las fuentes de información periodística”⁶⁰⁹

Es la primera vez que se constitucionaliza en la República dominicana con un texto muy similar al previsto en el tercer párrafo del artículo 43⁶¹⁰ de la Constitución Argentina. En principio, todo parece indicar que el constituyente dominicano lo ha entendido no como un derecho o un derecho instrumental sino como un cauce procesal, una garantía judicial para materializar el derecho a la protección de datos. Es decir, mientras que el artículo 44 numeral 2 establece el derecho a acceder a la información y a los datos que sobre una persona existan, el *habeas data* responde *a posteriori* cuando judicialmente éste no funciona. De hecho, ya en el artículo 44 también se avanza que:

“...podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos”⁶¹¹.

⁶⁰⁹ Artículo 70 Constitución de la República Dominicana del 2010.

⁶¹⁰ Cfr. “Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística.”, *Constitución de la República Argentina*, 22 de agosto de 1994. Disponible en: <http://pdba.georgetown.edu/Parties/Argentina/Leyes/constitucion.pdf>. (Última consulta en línea 26 de abril 2018).

⁶¹¹ Artículo 44, numeral 2, Constitución de la República Dominicana del 2010.

Aunque luego comentemos algunos aspectos relacionados con la precisión terminológica de ambos preceptos, lo que sí parece es que sitúa al *habeas data* en los términos que -como ya mantuvimos en el *capítulo II* - nos parecen más ajustados.

En este sentido, hay que ver si su interpretación posterior por la doctrina, la jurisprudencia y el desarrollo legislativo sigue entendiendo el *habeas data* como una de las garantías (no la única -como veremos-) que se incardina dentro del derecho fundamental a la protección de datos y no presenta la confusión de otros textos del contexto latinoamericano.

De momento desde la doctrina dominicana no existen demasiados comentarios al respecto. Conocemos su origen brasileño estudiado en el *capítulo II*. Este precepto se ha de regir además por lo pautado en el artículo 64 de la *Ley núm. 137-11*⁶¹², del *tribunal constitucional y de los procedimientos constitucionales en el régimen procesal común del amparo*. Y en este sentido, la doctrina destaca que, si bien a nivel constitucional se ha reglamentado de manera autónoma, la ley que lo desarrolla parece considerarlo un subtipo de amparo al disponer que se rija por ese proceso común. Esto es criticado desde un sector doctrinal que considera que a pesar de esta remisión procesal común el *habeas data* es una “acción”⁶¹³ autónoma con características propias.

En cualquier caso, cuando se comenta este artículo vuelve a reabrirse la cuestión de qué es lo que tutela el *habeas data*, el derecho a la intimidad como género, que caracteriza la defensa de la privacidad, del honor, la imagen, la

⁶¹² BARNICHTA GEARA, E., *Jurisprudencia Constitucional Dominicana*, 1ª ed. Centenario SRL, Santo Domingo, República Dominicana, 2014, p. 32.

⁶¹³ “..... de este modo, nos hemos propuesto presentar al *habeas data* como una acción que viene a llenar un vacío dentro de la legislación dominicana, respecto a salvaguardar derechos fundamentales y por qué no, derechos que en otras latitudes han sido denominados nuevos derechos, como es el caso del derecho a la autodeterminación informativa” Introducción monografía CASTILLO MOTA, S. P., KARINA BELLO, H. y BURÓ GUTIÉRREZ, J., *La acción de habeas data y su aplicación en la República Dominicana*, Santo Domingo, República Dominicana, 2004.

reputación, la identidad entre otros derechos⁶¹⁴ o el derecho de autodeterminación informativa, como derecho de cada persona para determinar por sí y ante sí, qué debe hacer en su relación de ella con el mundo informático⁶¹⁵. Desde la doctrina dominicana se concluye que esta garantía trata de impedir que se lesione el derecho a la intimidad o que los datos estén siendo manejados sin su consentimiento⁶¹⁶.

Nosotros, sin embargo, no consideramos acertada esa reflexión. El *habeas data* protege tanto los datos íntimos como los que no lo son⁶¹⁷ y también con respecto a los datos obtenidos con su consentimiento caben ejercer esta misma acción.

En cualquier caso, lo que es claro es que la Constitución reconoce que el actor tiene derecho a conocer la existencia y acceder a los datos referidos a su persona. Si la información es falsa o le discrimina, puede exigir la rectificación, la actualización y la confidencialidad. De esta manera podemos decir que en nuestra Constitución reside un *habeas data* reparador rectificado o correctivo, aditivo actualizador y reservador, conforme a la clasificación de los tipos y subtipos que analizamos en el *capítulo II*.

Hay otros aspectos del *habeas data* en los que, en nuestra opinión, cabe la duda y es que al poner en relación el último apartado del artículo 44 numeral 2 con el artículo 70 coinciden en que ambos se refieren a que cabe acción judicial para la actualización y rectificación de los datos. Sin embargo, el primero contempla la posibilidad de oposición al tratamiento que el segundo no recoge. El artículo 70, en cambio, sí contempla el *habeas data* reservador (con

⁶¹⁴ GOZAÍNI, O., *Introducción al Derecho Procesal Constitucional*, Buenos Aires, Rubinzal-Culzoni, 2006.

⁶¹⁵ GARCÍA BELAUNDE, D., *Derecho Procesal Constitucional*, Bogotá, Temis, 2001.

⁶¹⁶ BALBUENA BATISTA, P., *Constitución Comentada*, op.cit., p. 165.

⁶¹⁷ Desde siempre lo ha mantenido Lucas Murillo de la Cueva al afirmar que se trata de un derecho cuya idea es preservar el derecho a la información individual, sea íntima o no, ya que no es la intimidad la que se tutela, véase LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, op.cit., pp. 88-124.

respecto a la confidencialidad) que el apartado del numeral 2 del artículo 4 olvida. Por último, el artículo 70 habla de la posibilidad de suspensión y no de destrucción como menciona el otro precepto. Esto puede ser interpretado a) como un error tipográfico de la Constitución que en vez de suspensión quiso decir supresión; así, desde la doctrina se menciona la supresión, pero no la suspensión⁶¹⁸; o b) además del *habeas data* reparador exclutorio o cancelatorio se contempla el *habeas data* bloqueador (referido a la suspensión); c) sólo se contemple el bloqueador. En definitiva, esperemos que los olvidos y discordancias no sean entendidos como una limitación a subtipos de *habeas data* que en su momento puedan ser accionados.

Asimismo, aunque la acción corresponde en exclusiva a la persona titular de los datos, un sector doctrinal aboga por que cuando la actividad afecta a un gran número de personas se reconozca legitimación o “calidad” para accionar a determinadas asociaciones vinculadas a la protección de tales derechos, así como reconocer legitimación activa a cualquier persona que pueda justificar un interés, aún y cuando la información no sea a ella referida. En ese sentido, y según la interpretación del Tribunal Europeo de Derechos Humanos, éste reconoció el derecho a accionar a una persona que vivió en distintos orfanatos a acceder a aquellos registros que le permitieran reconstruir su trayectoria vital y sus conexiones familiares (caso *Gaskin*, al que nos hemos referido en el capítulo II).

Para concluir, también cabe comentar la parte final del texto la cual prevé que “no podrá afectarse el secreto de las fuentes de información periodísticas”. Ello hace referencia a los posibles conflictos entre el tratamiento de datos personales y los eventuales límites del ejercicio del derecho a la información, por parte de los profesionales de la información que podría en determinados

⁶¹⁸ “Así las cosas, si la información mantenida es falsa o si aun siendo verdadera no fue consentida, el titular puede exigir la supresión”. Esta es la interpretación de BALBUENA BATISTA, P., *Constitución Comentada*, op.cit., p. 166.

casos afectar el derecho a la intimidad de las personas y que habrá de resolverse conforme a la ponderación de los derechos ⁶¹⁹.

V. EL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA Y SU RELACIÓN CON EL DERECHO A LA PROTECCIÓN DE DATOS

La Constitución de 2010 reconoce en su artículo 49, numeral 1:

“Toda persona tiene derecho a la información. Este derecho comprende buscar, investigar, recibir y difundir información de todo tipo, de carácter público, Por cualquier medio, canal o vía, conforme determinan la Constitución y la ley”⁶²⁰.

Este precepto hunde sus raíces en el artículo 19 de la Declaración Universal de los Derechos Humanos⁶²¹; el artículo 13 de la Convención Americana sobre Derechos Humanos⁶²²; y el artículo 19 del Pacto Internacional de los Derechos Civiles y Políticos⁶²³, los cuales forman parte del derecho interno dominicano.

Excede el objeto de nuestro estudio detenernos en este derecho. Simplemente se quieren reseñar ciertos datos para situarnos en las coordenadas deseadas.

⁶¹⁹ *Ibidem*, p. 166.

⁶²⁰ Artículo 49, numeral 1, *Constitución de la República Dominicana 2010*.

⁶²¹ Art.19: “Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión”.

⁶²² Art.13. “Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección...”.

⁶²³ Art. 19.” Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección”.

a) A diferencia de Europa que, en términos generales, se comenzó antes con la constitucionalización y desarrollo legislativo de la protección de datos, en muchos países de Latinoamérica la preocupación por la transparencia ha sido debido sobre todo a la instauración de las jóvenes democracias⁶²⁴ que tenían “sed de información” ante la represión de regímenes anteriores. Por eso, muchos países, como República Dominicana, cuentan con una legislación al respecto. Así, Incluso antes de la Constitución del 2010, ya desde 2004 nuestro país se rige por una ley general en la materia y un reglamento de desarrollo del 2005. De esta manera nuestra *Ley General núm. 200-04 sobre Libre Acceso a la Información Pública (LGLAIP)* reconoce que “el acceso a la información es un derecho de todos” y conforme al art. 1 de la LGLAIP “Toda persona tiene derecho a solicitar y a recibir información completa, veraz, adecuada y oportuna, de cualquier órgano del Estado dominicano, y de todas las sociedades anónimas, compañías anónimas o compañías por acciones con participación estatal”⁶²⁵.

b) Este derecho -como veremos a continuación- ya ha sido analizado por la jurisprudencia constitucional. Este derecho tiene una gran relevancia para el fortalecimiento del Estado Social y Democrático de Derecho, pues su ejercicio garantiza la transparencia y permite a la ciudadanía acceder libremente a las informaciones en poder de las instituciones del Estado, y con ello, controlar y fiscalizar a los poderes públicos.

⁶²⁴ “Actualmente los países americanos sólo poseen, con la calificada excepción de Cuba, regímenes democráticos.....la democracia no acaba los conflictos con la libertad de expresión, solo se hacen más sutiles y la discusión más compleja, ése es el desafío que tienen el amplio campo del derecho a la información en los países americanos”, BEL MALLÉN, I., CORREDORA y ALFONSO, L. (Coordinadores), *Derecho de la Información*, 1ª ed. ARIEL, S. A., Barcelona, 2003, p. 141.

⁶²⁵ En torno a estas cuestiones véase BARINAS UBINAS, B., “*Los derechos fundamentales de acceso a la información pública y protección de datos personales: una aproximación a la pertinencia de su vinculación normativa en República Dominicana*”, Congreso Internacional protección internacional de los Derechos Fundamentales: dimensión pública y privada, Globernance, Donostia, 2012. Disponible en: <http://globernance.org/wp-content/uploads/2013/08/BerecineBarinas1.pdf>. (Última consulta en línea 13 de agosto 2013).

c) No se trata de un derecho absoluto. Este derecho en relación a nuestro tema debe ser conectado con el derecho a la protección de los datos personales. En este sentido, y como hito a destacar, el 21 de septiembre del 2012, se falla una sentencia del Tribunal Constitucional -que a continuación analizaremos- y que sienta la posición del Tribunal en el primer recurso de revisión en materia de amparo, el cual dirime el conflicto entre el derecho de acceso a la información pública y el derecho a la protección de los datos personales. Mientras avanzaba la *Ley General de Libre Acceso a la Información Pública*, la falta de una normativa de protección de datos personales provocó muchos desencuentros. Las bases sentadas por la reciente jurisprudencia constitucional y el proceso abierto con distintas propuestas legislativas en materia de protección de datos parecen anunciar situaciones más equilibradas entre ambos derechos. En definitiva, mientras que en las dictaduras se tendían a hacer opaco al poder y transparente a la ciudadanía, ahora, en democracia de lo que se trata es de hacer transparente al poder y opaca a la ciudadanía.

VI. ANÁLISIS DE LA JURISPRUDENCIA CONSTITUCIONAL

1. Antecedentes claves

El Tribunal Constitucional de la República Dominicana ha emanado o evacuado varias sentencias relacionadas con la protección de datos personales, el *habeas data* y el libre acceso a la información pública; de entrada, y antes de conectar con el tema anterior, pasamos a presentar un extracto de las estadísticas generadas en el Tribunal Constitucional durante sus primeros años de creación. Para ello, definiremos en todo su contexto la evolución del Alto Tribunal en lo que a materia de estos derechos fundamentales se trata, reflejados en las sentencias emanadas por el Alto Tribunal y presentadas a continuación.

En el periodo comprendido entre el 2012 al 2015, el Tribunal Constitucional ha evacuado 1427 sentencias distribuidas de la manera siguiente: a) 104 en el 2012; b) 290 en el 2013; c) 407 en el 2014 y d) 626 pertenecen al 2015, observando un crecimiento de un 602 % si comparamos el 2012 con el 2015.

En las sentencias emanadas se contemplan los temas de libre acceso a la información pública, *habeas data*, intimidad, honor y sentencias vinculadas con las fichas policiales, registros relacionados con los antecedentes penales en manos de los organismos de investigación del Estado, entre ellos, de la Policía Nacional, de la Dirección Nacional de Control de Drogas y otros estamentos de seguridad del Estado.

En materia de libre acceso a la información pública, se han evacuado 22 sentencias distribuidas de la manera siguiente, 2 sentencias en el 2012, cuatro en el 2013, 9 en el 2014 y 7 en el 2015, observando un incremento de las sentencias emitidas por el Tribunal Constitucional en materia de libre acceso a la información pública, sustentado en la medida que se consolida el Tribunal Constitucional.

Situación similar se observa en el *habeas data* durante el período planteado, con la salvedad de carecer de sentencias en el 2012, con 2 sentencias para el 2013 y el 2014, y 5 sentencias en el 2015. En ese sentido, el comportamiento se mantiene para el honor y las fichas policiales ligadas a los antecedentes penales, registrando 2 sentencias para el honor en el 2014 y 4 sentencias pertenecientes a las fichas policiales ligadas a los antecedentes penales, notando un incremento en las sentencias emanadas por el Tribunal Constitucional año tras año, específicamente las sentencias de libre acceso a la información pública, donde, como hemos mencionados, pasamos de 2 sentencias en el 2012 a 9 sentencias en el 2014, con una ligera variación en el 2015, una situación muy distinta al período comprendido entre el 2012 al 2015 cuyo incremento oscila desde 0 % en el 2012 a un 5 % en el 2015.

El *habeas data* es considerado constitucionalmente una acción judicial, capaz de proteger derechos fundamentales mediante el acceso de los datos ubicados en archivos o registros, sean estos públicos o privados, con la posibilidad de ejercer los cambios o transformaciones necesarias (suspensión, rectificación, actualización, confidencialidad)⁶²⁶ garantizando tales derechos. Una acción judicial conducida por el *régimen procesal común del amparo*⁶²⁷, lo que nos permite dar una mirada a las sentencias recibidas y emanadas por el Tribunal Constitucional, determinando la carga procesal del Tribunal en materia de amparo, formando parte el *habeas data*.

Con la propuesta de instauración de un órgano de control nacional, dotado de independencia funcional y económica, capaz de accionar en materia de *habeas data*, visualizamos una potencial disminución de los expedientes o sentencias relacionadas con el amparo y su conexión con el *habeas data*, para ello, presentaremos las estadísticas cursadas por el Tribunal Constitucional de la República Dominicana, sustentado en los 5,250 expedientes recibidos por el Tribunal Constitucional desde su formación al 31 de marzo del 2019, de los cuales se han generado 3,786 sentencias y encontrándose 1,464 sentencias pendientes y en proceso⁶²⁸.

El 43% (2,233) de las sentencias recibidas por el Tribunal Constitucional, corresponden a revisiones de sentencias de amparo, mientras que el 57% (3,017) se categorizan como otros⁶²⁹. Por su parte, para las sentencias emitidas por el Alto Tribunal el 44 % (1,648) de las sentencias pertenecen a revisión de sentencias de amparo y el 56 % (2,138) se tipifica como otros. En

⁶²⁶ Artículo 70, Constitución de la República Dominicana del 2015.

⁶²⁷ Artículo 64, Ley núm. 137-11 Orgánica del Tribunal Constitucional y de los procedimientos constitucionales.

⁶²⁸ Tribunal Constitucional. Disponible en: <https://www.tribunalconstitucional.gob.do/transparencia/estad%C3%ADsticas-institucionales/2019/enero-marzo-2019/>. (Última verificación en línea, 22 de mayo 2019).

⁶²⁹ Otros (Acción Directa de Inconstitucionalidad, Control Preventivo Tratado, Conflicto de Competencia, Suspensión, Recurso de Casación Declinado por la SCJ),

conclusión, podemos derivar que la revisión de sentencias de amparo superan el 40% de las sentencias recibidas y emitidas por el Tribunal Constitucional.

Ante tal situación, la instauración de un órgano revestido de independencia funcional y económica, permite agendar una eventual reducción de la acción de *habeas data* encausada por el *régimen procesal común del amparo*, contribuyendo con la disminución de la carga procesal del Tribunal Constitucional vía las sentencias recibidas y emitidas por el Alto Tribunal, situación manifiesta en las próximas gráficas y expuesta a continuación.

Figura 2. Sentencias recibidas Tribunal Constitucional de la República Dominicana (2012-2018).

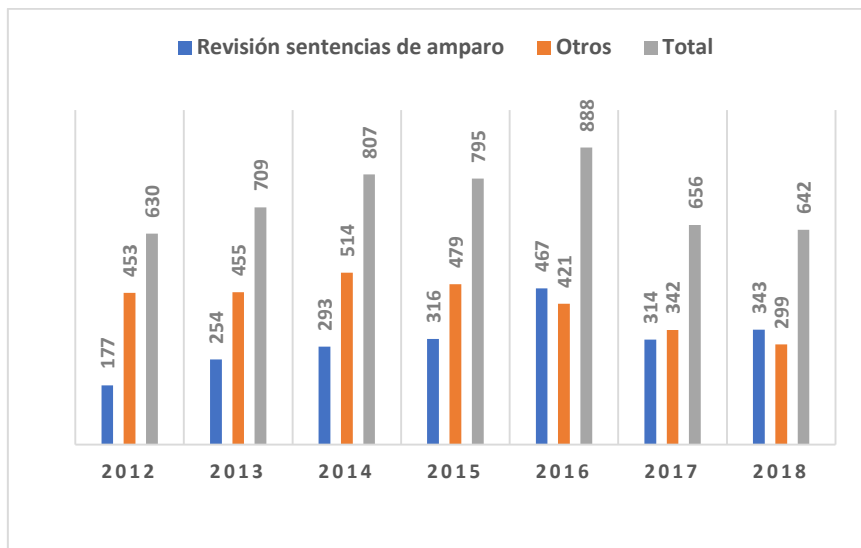
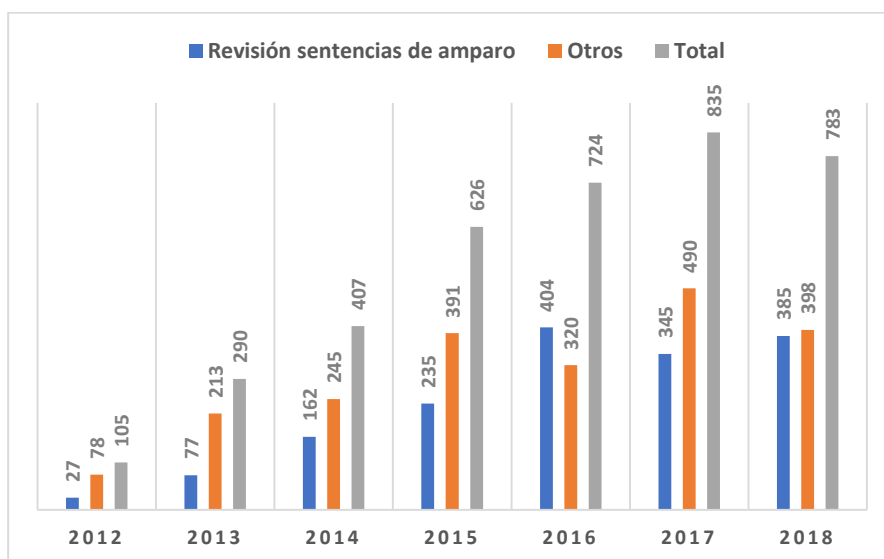


Figura 3. Sentencias emitidas Tribunal Constitucional de la República Dominicana (2012-2018) .



La carga procesal existente en el Tribunal Constitucional es un reflejo de los Tribunales Ordinarios y como no del Tribunal Superior Administrativo. Por tanto, una disminución de las eventuales sentencias recibidas y emitidas por el Tribunal Constitucional en materia de amparo, redundan en una real disminución de las sentencias emitidas y recibidas por el Tribunal Superior Administrativo y los Tribunales Ordinarios. todo ello orquestado a raíz de la creación de un órgano de control dotado de independencia funcional y económica.

2. Hallazgos constitucionales

Antes de proceder con el desarrollo de las principales sentencias emanadas por el Tribunal Constitucional en materia de acceso a la información pública, intimidad, honor, *habeas data*, autodeterminación informativa, nos avocamos a identificar y presentar los hallazgos más representativos en lo que a esos derechos se refiere, formando parte del acervo jurisprudencial constitucional conectado con esos derechos vía las sentencias constitucionales.

El Tribunal Constitucional de la República Dominicana vincula el derecho a la protección de datos con la dignidad, la integridad, el honor e Intimidad, estableciendo en la intimidad y la privacidad los límites al acceso a la información pública (ej. Sentencia núm. TC/0011/12)⁶³⁰. Esto se ampara en el artículo 44 numeral 2⁶³¹ y 49⁶³² de la Constitución de la República Dominicana del 2010 y 2015 que, tal como se ha establecido, encausa los límites del derecho de acceso a la información pública con el honor, la intimidad, la dignidad y la moral de las personas. Con todo, el Tribunal Constitucional de la República Dominicana enfatiza y reconoce con rango constitucional el libre acceso a la información pública, concediéndole el carácter de derecho fundamental. De este modo, lo ha dejado reflejado vía la evacuación de sus sentencias (TC/0011/12, TC/0042/12⁶³³, TC/0052/13⁶³⁴, TC/0062/13⁶³⁵, TC/0084/13⁶³⁶ y TC/0039/14⁶³⁷).

⁶³⁰ Sentencia núm. TC/0011/12. Referencia: Expediente núm. TC-030-12-00003, relativo a la acción de amparo incoada por Gary Gresko, S. A., contra la Dirección General de Migración. Disponible en:

<http://www.tribunalconstitucional.gob.do/sites/default/files/documentos/Sentencia%20TC%200011-12%20C.pdf>. (Última consulta en línea 22 de enero 2016).

⁶³¹ Artículo 44.- Derecho a la intimidad y el honor personal, numeral 2, Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos.

⁶³² Artículo 49.- Libertad de expresión e información. Toda persona tiene derecho a expresar libremente sus pensamientos, ideas y opiniones, por cualquier medio, sin que pueda establecerse censura previa.

⁶³³ Sentencia núm. TC/0042/12. Expediente núm. TC-05-2012-0010, relativo al recurso de revisión en materia de amparo incoado por la Cámara de Diputados de la República Dominicana y el Estado Dominicano contra el señor Manuel Muñoz Hernández. Disponible en: <https://www.tribunalconstitucional.gob.do/node/582>. (Última consulta en línea 25 de enero 2016).

⁶³⁴ Sentencia núm. TC/0052/13. Expediente núm. TC-04-2012-0040, relativo al recurso de revisión constitucional de decisiones jurisdiccionales incoado por la Asociación Nacional de Pilotos, contra la Sentencia núm.130, dictada por la Tercera Sala de la Suprema Corte de Justicia, en fecha siete (07) de marzo de dos mil doce (2012). Disponible en: <https://www.tribunalconstitucional.gob.do/node/1330>. (Última consulta en línea 25 de enero 2016).

⁶³⁵ Sentencia núm. TC/0062/13. Expediente núm. TC-04-2012-0041, relativo al recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Allan de Jesús

Al mismo tiempo, el Tribunal Constitucional declara que los datos de sueldo, nombres, cargos y salarios no deben convertirse en límites para el ejercicio del libre acceso a la información pública otorgado en la Ley núm. 200-04, una ley llamada al fortalecimiento de la democracia y la transparencia en el sector público. Eso sí, excluye aquellos datos relacionados con la seguridad nacional y la investigación (ej. Sentencia núm. TC 0016/14), pero no los datos correspondientes al número de identificación personal y electoral (ej. Sentencia núm. TC 0016/14), protegidos por la *Ley núm. 200-04 de Libre Acceso a la Información Pública*.

Como hemos visto previamente, el tema de acceso referido en el artículo 44 numeral 2 de la Constitución de la República Dominicana del trece (13) de junio de 2015, Gaceta Oficial N.º 10805 del 10 de julio de 2015, representa ser un tema obligado en las sentencias de *habeas data* emitidas por el Tribunal Constitucional, pues conecta el acceso o garantía constitucional del *habeas data* y permite a todo individuo titular de sus datos acceder a los mismos ubicados en los bancos de información, sin explicar sus razones, artículo 70⁶³⁸ de la Constitución.

Tiburcio Andrickson contra la Sentencia núm.60, dictada por la Tercera Sala de la Suprema Corte de Justicia, en fecha quince (15) de febrero de dos mil doce (2012). Disponible en: <https://www.tribunalconstitucional.gob.do/sites/default/files/documentos/Sentencia%20TC%20062-13%20C.pdf>. (Última consulta en línea 27 de enero 2016).

⁶³⁶ *Sentencia núm. TC/0084/13. Expediente núm. TC-04-2012-0045, relativo a recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Alejandro Alberto Paulino Vallejo contra la Sentencia núm.105 dictada por la Tercera Sala de lo Laboral, Tierras, Contencioso Administrativo y Contencioso Tributario de la Suprema Corte de Justicia, en fecha veintinueve (29) de febrero de dos mil doce (2012).* Disponible en: <https://www.tribunalconstitucional.gob.do/node/1544>. (Última consulta en línea 27 de enero 2016).

⁶³⁷ *Sentencia núm. TC/0039/14. Expediente núm. TC-05-2012-0114, relativo al recurso de revisión constitucional en materia de amparo incoado por Reemberto José de Jesús Pichardo Juan contra la Sentencia núm. 114-2012, de fecha treinta y uno (31) de agosto de dos mil doce (2012), dictada por la Segunda Sala del Tribunal Superior Administrativo.* Disponible en: <https://www.tribunalconstitucional.gob.do/content/sentencia-tc003914>. (Última consulta en línea 27 de enero 2016).

⁶³⁸ Artículo 70.- *Habeas data*. Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme a la ley. No podrá afectarse el secreto de las fuentes de información periodística.

Ante esa situación y ,desde el punto de vista del Tribunal Constitucional, se establece y reconoce el *habeas data*, acogiéndolo como una garantía constitucional puesta a disposición de todo individuo⁶³⁹, de igual forma, el Tribunal Constitucional hace referencia al principio de privacidad correspondiente al literal c del artículo 5 de la Ley núm. 172-13, ordenando a las instituciones por medio a la sentencia previa que,

“Procedan a la corrección de los datos erróneos que se contengan en sus bases internas, y en los cuales se expresa que el accionante ha sido deportado desde los Estados Unidos”⁶⁴⁰.

En materia de *habeas data*, las sentencias emitidas por el Tribunal Constitucional conectan la figura con el derecho a la intimidad, el honor, la defensa de la privacidad, la propia imagen; estableciendo una real protección de los derechos fundamentales, creando jurisprudencias por medio a la evacuación de sus sentencias, originadas tras la presentación de recursos de revisión constitucional en materia de *habeas data*, afirmando que:

“ La garantía del *habeas data* “está caracterizada por su doble dimensión:1) una manifestación sustancial, que comporta el derecho a acceder a la información misma que sobre una persona se maneja; y 2) una manifestación de carácter instrumental, en tanto permite que la persona, a través de su ejercicio, proteja otros derechos relacionados a la información, tales como el derecho a la intimidad, a la defensa de la privacidad, a la dignidad humana, la información personal, el honor, la propia imagen, la identidad, la autodeterminación informativa, entre otros”⁶⁴¹.

⁶³⁹ Sentencia núm. TC/0024/13. Expediente núm. TC-05-2012-0036, relativo al recurso de revisión de sentencia de *habeas data* incoado por Fior D'Alisa Recio Tejada, Procuradora Fiscal Adjunta del Distrito Nacional, Coordinadora del Departamento de Investigaciones de la Procuraduría Fiscal del Distrito Nacional, en contra de Mario Pérez García, Agustín Abreu Galván, Manuel Mario Pérez. Disponible en: <https://www.tribunalconstitucional.gob.do/node/1223>. (Última consulta en línea 29 de enero 2016).

⁶⁴⁰ Artículo 5, Ley núm. 172-13

⁶⁴¹ Sentencia núm. TC/0475/18. Expediente núm. TC-05-2016. relativo al recurso de revisión constitucional de sentencia de amparo interpuesto por Ricardo Sosa Filoteo contra la Sentencia núm.00125-2015, dictada por la Tercera Sala del Tribunal Superior Administrativo el veintiocho (28) de septiembre de dos mil quince (2015). Disponible en: <https://www.tribunalconstitucional.gob.do/consultas/secretar%C3%ADa/sentencias/tc047518/>. (Última consulta en línea 14 de noviembre 2018).

El Tribunal Constitucional considera entre sus disposiciones la construcción del concepto del derecho a la autodeterminación informativa contemplado en la evacuación de sus sentencias. A pesar de no ser considerado literalmente en la Constitución del 2010, 2015 o Ley núm. 172-13, este concepto procedente de la autodeterminación informativa Alemana influenciando las corrientes doctrinales europeas (-y más concretamente españolas-, como se ha visto) y latinoamericanas que circundan y empapan la región también ha pasado a formar parte del acervo jurisprudencial dominicano, asumiendo diferentes posturas. Entre ellas cabe resaltar que la acción del *habeas data* permite la protección del derecho a la autodeterminación informativa y, con ello, la protección de los derechos tutelados por ésta como la intimidad, el honor y otros derechos fundamentales conectados con la personalidad del individuo y ampliamente ya comentados.

El Tribunal Constitucional acoge los principios de la nueva Ley núm. 172-13, destacando la Licitud de los datos personales y la calidad de estos, en cuyo literal c⁶⁴² nos presenta las acciones a realizar para aquellos datos que no poseen el nivel de calidad demandado, destacando la supresión o sustitución de los mismos.

Por otra parte y, cómo se ha examinado, el artículo 70 de la Constitución Dominicana y el 64 de la *Ley Orgánica núm. 137-11 del Tribunal Constitucional y de los Procedimientos Constitucionales* prevén la figura del *habeas data*, contemplando la particularidad propia del amparo, asignándole su propia sustantividad con características propias, protegiendo el derecho a la autodeterminación informativa⁶⁴³. En tal sentido, el Tribunal Constitucional

⁶⁴² Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o, en su caso, completados por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular de los datos establecidos en la presente ley.

⁶⁴³ *Sentencia núm. TC/0475/18. Expediente núm. TC-05-2016. relativo al recurso de revisión constitucional de sentencia de amparo interpuesto por Ricardo Sosa Filoteo contra la Sentencia núm.00125-2015, dictada por la Tercera Sala del Tribunal Superior Administrativo el veintiocho (28) de septiembre de dos mil quince (2015).* Disponible en:

mediante la evacuación de sus sentencias y, amparados en el principio de oficiosidad que le otorga la referida Ley núm. 137-11 en su respectivo artículo 7 numeral 11, recalifica la acción de amparo ordinario en un *habeas data*⁶⁴⁴. Por ello, entendemos que desde el punto de vista Constitucional, el Tribunal reconoce, modifica y asume como tal la acción de *habeas data* figurada en el Derecho Procesal Constitucional, una acción capaz de proteger el derecho fundamental a la autodeterminación informativa que posibilita el desarrollo de la legitimación activa. Es decir, podemos categorizar diciendo que *el habeas data*, desde la óptica del Tribunal Constitucional, es una acción de amparo con sustantividad propia, siendo reconocido o tipificado como un amparo con su propio apellido, capaz de proteger aquellos derechos para el cual fue concebido, o llamado a proteger. Así, con tales decisiones, el Tribunal Constitucional hace pleno uso de la tutela efectiva otorgada por la Constitución y el principio rector de efectividad contenido en la *Ley Orgánica núm. 137-11 del Tribunal Constitucional y de los Procedimientos Constitucionales*

En la Sentencia núm. TC-0475-18 se contempla una vulneración de los principios enunciados por el Tribunal Constitucional, el principio de tutela efectiva, en donde, a diferencia del Tribunal Constitucional, el Tribunal Superior Administrativo no ejerce la recalificación mencionada, una recalificación sustentada en el principio de oficiosidad contemplado en la ley, ejercido en la sentencia ya vista y emitida por el Tribunal Constitucional; en el caso de la recalificación, nos referimos a la recalificación del amparo por el de *habeas data*, ejerciendo y manifestando el principio de tutela efectiva.

Con la situación manifiesta, se presenta una desvinculación entre las decisiones del Tribunal Constitucional y del Tribunal Superior Administrativo en

<https://www.tribunalconstitucional.gob.do/consultas/secretar%C3%ADa/sentencias/tc047518/>.
(Última consulta en línea 14 de noviembre 2018).

⁶⁴⁴ Sentencia núm. TC/0050/14. Recurso de revisión constitucional en materia de amparo incoado por el señor Melvin Velázquez Then, contra la Sentencia núm. 088-2011, dictada por la Segunda Sala del Tribunal Superior Administrativo, en fecha diez (10) de agosto de dos mil once (2011). Disponible en:

<https://www.tribunalconstitucional.gob.do/consultas/secretar%C3%ADa/sentencias/tc005014/>.
(Última consulta en línea 14 de noviembre 2018).

materia de análisis del objeto pretendido y la naturaleza de la información solicitada, lo cual no contribuye a su vez con una alineación de la tutela judicial efectiva en materia de amparo y *habeas data*. En este sentido, podemos acotar y señalar que desde el punto de vista jurisprudencial se observan discrepancias y puntos de vistas distintos en materia de amparo, acceso a la información pública, *habeas data*, protección de datos entre el Tribunal Superior Administrativo y el Tribunal Constitucional. Y esto queda reflejado en las sentencias emanadas por el Alto Tribunal y presentadas durante el capítulo.

De su lado, el Tribunal Constitucional extrapola la acción constitucional del *habeas data* con el amparo, una decisión sustentada en los artículos de la Constitución Dominicana y la Ley núm. 137-11, nos referimos al artículo 185.4 dedicado a la competencia del Tribunal Constitucional, esbozando su competencia en única instancia para cualquier tema o materia dispuesta en la ley, con la posibilidad otorgada por el Tribunal de recurrir a todas aquellas sentencias emanadas o dispuestas por el juez de amparo, en ese sentido el *habeas data* se rige por el régimen del amparo⁶⁴⁵ contemplado en la misma ley⁶⁴⁶. Así, estamos ante un procedimiento de carácter gratuito, preferente, sumario, libre de costas, cargas e impuestos y alineados con los principios asumidos en la Constitución⁶⁴⁷ como son el principio de celeridad y economía procesal. De ese modo, se evita recurrir a los tribunales ordinarios para la defensa de los derechos fundamentales, por los costos involucrados y el tiempo empleado en el proceso.

En tanto, sustentado en las sentencias emanadas por el Tribunal Constitucional, destacamos la doble dimensión del *habeas data*. Por un lado, se otorga el derecho de acceso a los datos y, por el otro, protege otros derechos conectados con la información,, como son el derecho a la intimidad, privacidad, honor, imagen y el ya mencionado derecho a la autodeterminación

⁶⁴⁵ Artículo 64, Ley núm. 137-11.

⁶⁴⁶ Capítulo VI, Ley núm. 137-11.

⁶⁴⁷ Artículo 7,4 y 7,5, Constitución dominicana del 2015.

informativa⁶⁴⁸ sirviendo de garantía y mecanismo de protección para los mencionados derechos fundamentales establecidos en la carta magna y reflejado en sentencias jurisdiccionales evacuadas por el Tribunal Constitucional⁶⁴⁹.

Nos referimos a un proceso constitucional, no ordinario, desprovisto del carácter contradictorio, carente de un demandante y un demandado, accionado por el solicitante cuyos derechos fundamentales se encuentran vulnerados, y, en el que se solicita su pronto restablecimiento.

En ese sentido, el *habeas data* no contempla el proveer información relacionada con un tercero⁶⁵⁰ sino que afecta sólo a informaciones sobre sí mismo, establecido desde el orden constitucional⁶⁵¹ y jurisprudencial mediante sentencias emanadas por el Tribunal Constitucional⁶⁵². Por tanto, ante la

⁶⁴⁸ Sentencia núm. TC-0475-18, recurso de revisión constitucional de sentencia de amparo interpuesto por Ricardo Sosa Filoteo contra la Sentencia núm.00125-2015, dictada por la Tercera Sala del Tribunal Superior Administrativo el veintiocho (28) de septiembre de dos mil quince (2015). Disponible en: <https://tribunalsitestorage.blob.core.windows.net/media/17264/tc-0475-18.pdf>. (Última consulta en línea 14 de noviembre 2018).

⁶⁴⁹ Sentencia núm. TC/0204/13, recurso de revisión constitucional en materia de amparo, incoado por Rosa Elena Rijo, contra la Sentencia núm. 404/2012, dictada en fecha veinticuatro (24) de mayo de dos mil doce (2012), por la Cámara Civil y Comercial del Juzgado de Primera Instancia del Distrito Judicial de La Altagracia. Disponible en: <https://www.tribunalconstitucional.gob.do/consultas/secretar%C3%ADa/sentencias/tc020413/>. (Última consulta en línea 29 de enero 2016).

⁶⁵⁰ Sentencia núm. TC/478/15, recurso de revisión constitucional en materia de amparo interpuesto por el señor José Rafael Diloné Estévez contra la Sentencia núm. 365-14-01904, dictada por la Primera Sala de la Cámara Civil y Comercial del Juzgado de Primera Instancia del Distrito Judicial de Santiago el once (11) de noviembre de dos mil catorce (2014). Disponible en: <https://www.tribunalconstitucional.gob.do/consultas/secretar%C3%ADa/sentencias/tc047815/>. (Última consulta en línea 14 de noviembre 2018).

⁶⁵¹ “El *habeas data* es una garantía constitucional que nuestra carta sustantiva pone a disposición de todo individuo, que le permite acceder a cualquier banco de información, registro de datos y referencias sobre sí mismo, sin necesidad de explicar razones. El interesado puede, igualmente, solicitar la corrección de esa información, en caso de que le ocasione algún perjuicio.”, Sentencia TC-0475-18, recurso de revisión constitucional de sentencia de amparo interpuesto por Ricardo Sosa Filoteo contra la Sentencia núm.00125-2015, dictada por la Tercera Sala del Tribunal Superior Administrativo el veintiocho (28) de septiembre de dos mil quince (2015)”. Disponible en: <https://tribunalsitestorage.blob.core.windows.net/media/17264/tc-0475-18.pdf>. (Última consulta en línea 14 de noviembre 2018).

⁶⁵² Sentencia núm. TC/478/15.

oposición o recelo de entrega de datos correspondiente a un tercero se utilizará el amparo.

La legitimación activa acciona el *habeas data* tanto para las personas físicas como para las personas morales o jurídicas⁶⁵³, a diferencia de lo estipulado en la Ley núm. 172-13 que prevé ciertas restricciones a los tratamientos de datos referenciados a las personas físicas o jurídicas⁶⁵⁴. Por ende, las personas jurídicas gozan de derechos fundamentales⁶⁵⁵, al mismo tiempo y, soportado en el artículo 67 de la Ley núm. 137-11, se le otorga a las personas físicas y jurídicas la posibilidad de solicitar, pedir, exigir sus derechos fundamentales mediante la acción de amparo.

Por último y, a manera de cerrar la sección, el Tribunal reconoce vía sus sentencias, los deberes de actualización, rectificación y exclusión de datos cuando sean discordantes con la realidad como se observa en el fondo de la revisión, a fin de proteger los derechos fundamentales de intimidad, privacidad, buen nombre.

A continuación, mostramos las sentencias más representativas en materia de acceso a la información pública, *habeas data*, intimidad, protección de datos personales.

⁶⁵³ Sentencia núm. TC/0404/16, recurso de revisión constitucional en materia de *habeas data* incoado por la sociedad comercial Boreo, S. R. L. contra la Sentencia núm. 052-2014, dictada por la Segunda Sala de la Cámara Penal del Juzgado de Primera Instancia del Distrito Nacional el once (11) de marzo de dos mil catorce (2014), p. 14. Disponible en: <https://www.tribunalconstitucional.gob.do/consultas/secretar%C3%ADa/sentencias/tc040416/>. (Última consulta en línea 16 de noviembre 2018).

⁶⁵⁴ Artículos 4.1 y 4.4 Ley núm. 172-13

⁶⁵⁵ Libertad de empresa, propiedad, debido proceso, intimidad y honor personal, libertad de expresión e información, libertad de asociación.

3. STC/0011/12. El derecho de acceso a la información pública y su conexión con el derecho a la intimidad/privacidad y el derecho a la protección de datos personales

La presente sentencia se orienta al derecho de acceso a la información pública, limitada por el derecho a la intimidad / privacidad.

La Sentencia TC/0011/12 forma parte del Expediente núm. TC-030-12-00003⁶⁵⁶, relativo a la acción de amparo incoada por Gary Gresko, S. A., contra la Dirección General de Migración. En ella, la recurrente, Gary Gresko, S. A. interpuso una acción de amparo con el objeto de obtener protección de los derechos fundamentales a la intimidad y al honor, así como de libre acceso a la información pública consagrados respectivamente por los artículos 44 y 49.1 de la Constitución.

La parte accionante pretende que la Dirección General de Migración le entregue la información relativa a las entradas y salidas del país de los señores Amal Fabiani y Jean Claude Fabiani, desde el año 2004 a la fecha.

La Sentencia objeto del presente recurso de revisión fue dictada por la Segunda Sala del Tribunal Superior Administrativo, con el número 152-2011, en fecha 19 de diciembre de 2011. En ella se rechazaba la acción de amparo incoada por Gary Gresko S. A.

Entre los argumentos de este Tribunal para rechazar el amparo se basaba en:

“Que no procede diferir la solicitud consignada, ya que la misma atenta contra la privacidad de los señores Jean Claude Fabiani y Amal Fabiani, de acuerdo con el artículo 44 de la Constitución de la

⁶⁵⁶ Sentencia núm. TC/0011/12. Referencia: Expediente núm. TC-030-12-00003, relativo a la acción de amparo incoada por Gary Gresko, S. A., contra la Dirección General de Migración. Disponible en: <http://www.tribunalconstitucional.gob.do/sites/default/files/documentos/Sentencia%20TC%200011-12%20C.pdf> (Última consulta en línea 22 de enero 2016).

República Dominicana, que establece el derecho a la intimidad y el honor...”

“Que entre de las limitaciones al acceso a la información pública se encuentran aquellas informaciones y datos que puedan afectar a intereses privados preponderantes, las cuales pueden ser rechazadas cuando afecten los mismos, sobre todo cuando se trate de datos personales cuya publicidad pudiera significar una invasión de la privacidad personal”⁶⁵⁷.

En este apartado parece ser confuso el deslinde entre privacidad e intimidad, pues señala que los datos personales no pueden ser públicos cuando afectan a la privacidad.

El Tribunal Constitucional se ampara, entre otros, en el artículo 44 numeral 2. y lo realiza a través de un circunloquio para hablar del derecho a la protección de datos “Los *derechos que corresponden a toda persona respecto a los datos suyos* contenidos en registros públicos o privados, al igual que el uso y manejo que con ellos pueda efectuarse”⁶⁵⁸..

Finalmente, se confirma la sentencia recurrida por el Tribunal (dictada por la Segunda Sala del Tribunal Superior Administrativo), y, para ello, se apoya en las jurisprudencias del Tribunal Constitucional de España (STC. 171/90 de 12 de noviembre) y la Corte Constitucional de Colombia (Sentencia T-417/96, del 9 de septiembre de 1996). Así, concluye con el siguiente razonamiento:

“La divulgación no consentida de datos contenidos en los registros de la Dirección General de Migración resulta un ejercicio desproporcionado del derecho a la información, que vulnera el núcleo esencial del derecho fundamental a la dignidad, la integridad, la intimidad y el honor de las personas registradas, cuando carezca

⁶⁵⁷ Sentencia núm. TC/0011/12. Referencia: Expediente núm. TC-030-12-00003, relativo a la acción de amparo incoada por Gary Gresko, S. A., contra la Dirección General de Migración. Disponible en:

<http://www.tribunalconstitucional.gob.do/sites/default/files/documentos/Sentencia%20TC%200011-12%20C.pdf> (Última consulta en línea 22 de enero 2016).

⁶⁵⁸ Sentencia núm. TC/0011/12. Referencia: Expediente núm. TC-030-12-00003, relativo a la acción de amparo incoada por Gary Gresko, S. A., contra la Dirección General de Migración. Disponible en:

<http://www.tribunalconstitucional.gob.do/sites/default/files/documentos/Sentencia%20TC%200011-12%20C.pdf> (Última consulta en línea 22 de enero 2016).

de incidencia en asuntos de interés colectivo y concierna personas cuya relevancia pública no haya sido alegada ni tampoco establecida”⁶⁵⁹.

En este fallo se vincula el derecho a la protección de los datos con la dignidad, la integridad, la intimidad y el honor.

4. STC/0042/12. Un hito entre el derecho de acceso a la información pública, derecho a la intimidad y el derecho a la protección de los datos personales

Esta sentencia no aborda específicamente el derecho a la protección de datos personales sino que como consecuencia de un derecho de acceso a la información pública se vierten ciertas reflexiones también sobre el primero. Como hemos establecido y, por tanto, se pronuncia especialmente sobre el derecho de acceso a la información pública y supone un hito por la jurisprudencia presentada.

La Sentencia núm. TC/0042/12 correspondiente al Expediente núm. TC-05-2012-0010⁶⁶⁰, relativo al recurso de revisión en materia de amparo incoado por la Cámara de Diputados de la República Dominicana y el Estado Dominicano contra el señor Manuel Muñoz Hernández, el cual solicitó a la Cámara de Diputados entregar un listado con los nombres de los asesores y el salario devengado por sus asesores. Este requerimiento no fue aceptado por la Cámara de Diputados quienes entregaron en vez de la propuesta un monto global de salario sin los nombres de los asesores.

⁶⁵⁹ Sentencia núm. TC/0011/12. Referencia: Expediente núm. TC 030-12-00003, relativo a la acción de amparo incoada por Gary Gresko, S. A., contra la Dirección General de Migración. Disponible en: <http://www.tribunalconstitucional.gob.do/sites/default/files/documentos/Sentencia%20TC%200011-12%20C.pdf> (Última consulta en línea 22 de enero 2016).

⁶⁶⁰ Sentencia núm. TC/0042/12. Expediente núm. TC-05-2012-0010, relativo al recurso de revisión en materia de amparo incoado por la Cámara de Diputados de la República Dominicana y el Estado Dominicano contra el señor Manuel Muñoz Hernández. Disponible en: <https://www.tribunalconstitucional.gob.do/node/582>. (Última consulta en línea 25 de enero 2016).

La Sentencia a la cual se somete la revisión es la núm. 166-2011 del Tribunal Superior Administrativo, interpuesta por Manuel Muñoz Hernández contra la Cámara de Diputados de La República Dominicana. Dicho Tribunal ordenaba a dicha Cámara de Diputados a entregar toda la información relativa a la nómina de los asesores de la Cámara de Diputados, tal y como lo dispone la Ley núm. 200-04 sobre Libre Acceso a la Información Pública, contentiva de nombres, apellidos, cargos y sueldos.

En ese sentido, el Tribunal se ampara en el derecho de acceso a la información pública, un derecho con rango constitucional sustentado en la *Ley núm. 200-04 de Acceso a la Información Pública*, el cual contempla sus propios límites en los datos personales relativos al individuo como son su domicilio, teléfono, expediente médico, origen étnico o social, características físicas, morales o emocionales, la fotografía y todo aquello relacionado con su persona e intimidad. En este sentido señalaba que:

“Un listado de empleado y funcionario contiene el nombre y apellido de funcionarios o empleados público, y hacerlos público en nada afectan la *privacidad*⁶⁶¹ o *intimidad* de la persona, por ende, el listado o nómina debe incluir nombres y apellidos, cargos y salarios percibidos; otra cosa sería si se les solicitaran números de cédulas, números telefónicos, domicilios de tales personas, pues estos sí forman parte de los *datos personales* de la persona y afectan a su *intimidad*”⁶⁶².

“Que si bien es cierto que el nombre de la persona es lo que lo distingue y lo identifica, no menos cierto es que al tratarse de una nómina de una empresa pública o de poder público, como es el caso que nos ocupa, el nombre de los empleados y funcionarios es una *información pública*, no así sus demás datos tales como cédula, domicilio, entre otros”⁶⁶³ ..

⁶⁶¹ Todas las cursivas que aparezcan en esta sentencia son nuestras.

⁶⁶² *Sentencia núm. TC/0042/12. Expediente núm. TC-05-2012-0010, relativo al recurso de revisión en materia de amparo incoado por la Cámara de Diputados de la República Dominicana y el Estado Dominicano contra el señor Manuel Muñoz Hernández.* Disponible en: <https://www.tribunalconstitucional.gob.do/node/582>. (Última consulta en línea 25 de enero 2016).

⁶⁶³ *Sentencia núm. TC/0042/12. Expediente núm. TC-05-2012-0010, relativo al recurso de revisión en materia de amparo incoado por la Cámara de Diputados de la República Dominicana y el Estado Dominicano contra el señor Manuel Muñoz Hernández.* Disponible en:

Por su parte, los recurrentes consideraban que se violó el derecho a la intimidad y el derecho de sus asesores ya que divulgaron sus datos personales sin su consentimiento. Sin embargo, el recurrido defendía que la información solicitada no significaba peligro para los asesores sino una forma de identificarlos como personas.

Finalmente, el Tribunal Constitucional admite dicho recurso y considera que posee trascendencia o relevancia constitucional ya que supone definir el alcance del derecho de acceso a la información frente al derecho a la intimidad, la protección de datos personales y, en particular, determinar cuáles datos pueden ser divulgados en relación a una persona física. Además, también supone referirse a la ponderación de los derechos en conflictos, asunto sobre lo que el Alto Tribunal no había sentado jurisprudencia.

El Tribunal Constitucional ampara sus consideraciones en el derecho a la información del art. 19 de la Declaración Universal de los Derechos Humanos, el artículo 13 de la Convención Americana sobre Derechos Humanos, el artículo 19 del Pacto Internacional de los Derechos Civiles y Políticos, así como en el artículo 49.1 de la Constitución del 2010.

El Tribunal se refiere al artículo 44 numeral 2 para expresar que el mismo es un límite al derecho de acceso a la información pública y también. como señala el artículo 49, este aparece como límite al derecho al honor, a la intimidad, así como a la dignidad y la moral de las personas.

Posteriormente se refiere a los límites que la Ley núm. 200-04 de Acceso a la Información Pública prevé. En lo que en nuestro caso atañe se establece como límite el derecho a la privacidad e intimidad, señalando como la propia ley en su artículo 8 establece el límite de los datos personales cuya publicidad

<https://www.tribunalconstitucional.gob.do/node/582>. (Última consulta en línea 25 de enero 2016).

podiera significar una invasión de la privacidad personal. Aun así, se destaca que estos datos podrán ser otorgados cuando sean *de interés público*.

Asimismo, “en lo relativo al *derecho a la protección de datos personales*, este se apoya en los derechos fundamentales a la *dignidad* humana y a la *privacidad*”. Se reconoce al ciudadano su derecho a estar informado para consentir expresamente la entrega y uso de sus datos personales.

Haciendo un pequeño inciso, vemos como el Tribunal reconoce la existencia de ese derecho a la protección de los datos personales vinculándolo con la privacidad (en el sentido de la *privacy* norteamericana) y la dignidad (heredera de la sentencia del Censo Alemán).

El Tribunal señala en que en este caso:

“están en conflicto el derecho a la información pública que tienen las personas y los grupos que no pertenecen al sector público, y el derecho a la *intimidad*, en la medida que revelar los nombres, cargos y salarios de los funcionarios y empleados de una determinada institución pública dejaría abierta la posibilidad de que se penetre en la esfera *privada* de esas personas”⁶⁶⁴.

“Cabe destacar que el que los nombres y apellidos de un individuo, aunque constituyen un medio para identificarlo como persona, no son datos que afectan a la esfera más íntima de su titular, ni consideradas informaciones personales sensibles, como sí lo serían, por ejemplo, las cuestiones ideológicas, las características personales, las condiciones de salud, la orientación sexual y el origen”⁶⁶⁵..

⁶⁶⁴ Sentencia núm. TC/0042/12. Expediente núm. TC-05-2012-0010, relativo al recurso de revisión en materia de amparo incoado por la Cámara de Diputados de la República Dominicana y el Estado Dominicano contra el señor Manuel Muñoz Hernández. Disponible en: <https://www.tribunalconstitucional.gob.do/node/582> (Última consulta en línea 25 de enero 2016).

⁶⁶⁵ Sentencia núm. TC/0042/12. Expediente núm. TC-05-2012-0010, relativo al recurso de revisión en materia de amparo incoado por la Cámara de Diputados de la República Dominicana y el Estado Dominicano contra el señor Manuel Muñoz Hernández. Disponible en: <https://www.tribunalconstitucional.gob.do/node/582>. (Última consulta en línea 25 de enero 2016).

En ese sentido, es positivo, que distingue entre datos íntimos y no íntimos e incluso acoge la terminología informaciones personales sensibles, propias del régimen del derecho a la protección de datos.

El Tribunal Constitucional considera que:

“aunque el derecho a la intimidad es un valor fundamental del sistema democrático, al igual que la protección a los datos personales, no pueden, de manera general, aunque sí excepcionalmente, restringir el derecho de libre acceso a la información pública, ya que limitarlo despojaría a la ciudadanía de un mecanismo esencial para el control de la corrupción en la Administración Pública”⁶⁶⁶..

Es clara, por tanto, la distinción entre derecho a la intimidad y protección a los datos personales y ambas pueden limitar excepcionalmente el derecho a libre acceso a la información pública.

Finalmente, el Alto Tribunal rechaza en cuanto al fondo, el recurso interpuesto por la Cámara de Diputados de la República Dominicana, objeto de esta decisión y confirma la anterior (Sentencia núm. 166-2011) del Tribunal Superior Administrativo.

5. STC/0010/13. El derecho de acceso a la información pública y el derecho a la protección de datos personales

La siguiente sentencia corresponde al Expediente núm. TC-04-2012-0040⁶⁶⁷ relativo al recurso de revisión constitucional de decisiones jurisdiccionales

⁶⁶⁶ Sentencia núm. TC/0042/12. Expediente núm. TC-05-2012-0010, relativo al recurso de revisión en materia de amparo incoado por la Cámara de Diputados de la República Dominicana y el Estado Dominicano contra el señor Manuel Muñoz Hernández. Disponible en: <https://www.tribunalconstitucional.gob.do/node/582>. (Última consulta en línea 25 de enero 2016).

⁶⁶⁷ Sentencia núm. TC/0010/13. Expediente núm. TC-04-2012-0039, relativo al recurso de revisión constitucional de decisiones jurisdiccionales incoado por la Asociación Nacional de Pilotos, contra la Sentencia núm. 86, dictada por la Tercera Sala de la Suprema Corte de Justicia, en fecha doce (12) de abril de dos mil doce (2012). Disponible en: <https://tribunalsitestorage.blob.core.windows.net/media/7434/sentencia-tc-0010-13-c.pdf>. (Última consulta en línea 27 de enero 2016).

incoadas por la Asociación Nacional de Pilotos contra la Sentencia núm. 130, dictada por la Tercera Sala de la Suprema Corte de Justicia, el siete (7) de marzo de dos mil doce (2012), mediante un recurso de revisión de decisiones jurisdiccionales.

El recurrente (Asociación Nacional de Pilotos) solicita a la Suprema anular la sentencia que imposibilita entregar las relaciones de entradas y salidas de los aviones, así como entregar la nómina de los funcionarios y empresarios por el Instituto Dominicano de Aviación Civil, fundamentado en la interpretación de los artículos 17 y 18 de la Ley núm. 200-04 (Ley General sobre Libre Acceso a la Información Pública).

El Tribunal Constitucional entiende que procede el recurso constitucional para revisar las decisiones dictadas por la Suprema Corte de Justicia en materia de interpretación constitucional, y al mismo tiempo, sancionar las violaciones a los derechos fundamentales que se cometen en el ámbito del Poder Judicial en ocasión de un litigio.

Ante ello, el Tribunal Constitucional anula la sentencia dictada por la Tercera Sala de la Suprema Corte de Justicia, y ordena al Instituto Dominicano de Aviación Civil la entrega inmediata de los nombres de cada uno de sus empleados y funcionarios. Con esta decisión se deja zanjada la posibilidad de entrega de los nombres ante una solicitud de acceso a la información pública, no siendo el límite de la misma.

6. STC/0024/13. El *habeas data*

La actual Sentencia se refiere al Expediente núm. TC-05-2012-0036⁶⁶⁸, relativo al Recurso de Revisión de Sentencia de *habeas data* incoado por Fior

⁶⁶⁸ Sentencia núm. TC/0024/13. Expediente núm. TC-05-2012-0036, relativo al recurso de revisión de Sentencia de Habeas Data incoado por Fior D'Alisa Recio Tejada, Procuradora Fiscal Adjunta del Distrito Nacional, Coordinadora del Departamento de Investigaciones de la

D'Alisa Recio Tejada, procuradora fiscal adjunta del Distrito Nacional, coordinadora del Departamento de Investigaciones de la Procuraduría Fiscal del Distrito Nacional, en contra de Mario Pérez García, Agustín Abreu Galván, Manuel Mario Pérez.

El recurso es originado por la decisión de la Novena Sala de la Cámara Penal del Juzgado de Primera Instancia del Distrito Nacional, de entregar a Agustín Abreu Galván y compartes, los incidentes y el dictamen de convención generados durante la vista ante un representante del ministerio público, durante una querrela presentada ante ellos, para tales fines, interpusieron una demanda de *habeas data*.

No conforme con dicha decisión, la Dra. Fior D'Alisa Recio Tejada, procuradora fiscal adjunta del Distrito Nacional, interpuso el presente recurso de revisión, a fin de que sea anulada la referida sentencia.

El Tribunal Constitucional aceptó y fundamentó la revisión en función del artículo 70 de la Constitución dominicana, el cual dispone que:

“Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme a la ley. No podrá afectarse el secreto de las fuentes de información periodística”⁶⁶⁹.

En ese sentido, se establecen las garantías propias del *habeas data*, previamente comentadas.

Procuraduría Fiscal del Distrito Nacional, en contra de Mario Pérez García, Agustín Abreu Galván, Manuel Mario Pérez. Disponible en: <https://www.tribunalconstitucional.gob.do/node/1223>. (Última consulta en línea 29 de enero 2016).

⁶⁶⁹ Artículo 70, Constitución de la República Dominicana de 2016.

1) Una manifestación sustancial, que comporta el derecho de acceder a la información misma que sobre una persona se maneja; y 2) una manifestación de carácter instrumental, en tanto permite que la persona a través de su ejercicio proteja otros derechos relacionados a la información, tales como el derecho a la intimidad, a la defensa de la privacidad, a la dignidad humana, la información personal, el honor, la propia imagen, la identidad, la autodeterminación informativa, entre otros. Desde esta óptica, opera como un verdadero mecanismo de protección de los derechos fundamentales.

Desde esa perspectiva, deben ser entregados los documentos relacionados con una investigación de la cual un ciudadano es parte del proceso penal, como los que dieron lugar a la acción del *habeas data* presentada, fruto de la no entrega por parte del Ministerio Público; En este sentido, los documentos vinculan al ciudadano y, en consecuencia, deviene imprescindible su acceso y entrega.

Por tanto, el Tribunal Constitucional rechaza el recurso de revisión del *habeas data* interpuesto por la Dra. Fior D'Alisa Recio Tejada, procuradora fiscal adjunta del Distrito Nacional.

7. STC/0062/13. Nuevas reflexiones de la STC/0042/12 y el derecho de acceso a la información pública, intimidad y la protección de datos personales

Esta Sentencia hace referencia al Expediente núm. TC-04-2012-0041⁶⁷⁰, relativo al recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Allan de Jesús Tiburcio Andrickson contra la Sentencia

⁶⁷⁰ Sentencia núm. TC/0062/13. Expediente núm. TC-04-2012-0041, relativo al recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Allan de Jesús Tiburcio Andrickson contra la Sentencia núm.60, dictada por la Tercera Sala de la Suprema Corte de Justicia, en fecha quince (15) de febrero de dos mil doce (2012). Disponible en: <https://www.tribunalconstitucional.gob.do/sites/default/files/documentos/Sentencia%20TC%20062-13%20C.pdf>. (Última consulta en línea 27 de enero 2016).

núm. 60, dictada por la Tercera Sala de la Suprema Corte de Justicia, en fecha quince (15) de febrero del dos mil doce (2012).

El recurrente interpuso un recurso de revisión constitucional contra la indicada sentencia, por entender se le violan los derechos fundamentales, especialmente el derecho de acceso a la información pública. El conflicto jurídico tiene su base en que el recurrente solicitó a la Junta Central Electoral la entrega de una lista de todos sus empleados y funcionarios, así como el cargo, número de cédula y sueldo bruto mensual, fundamentándose en la Ley núm. 200-04. Ante la actitud de dicha entidad se accionó el amparo que fue rechazado. Contra él se interpuso un recurso de casación que también se rechazó.

Cabe destacar algunos fundamentos de la Suprema para rechazar el recurso:

“Que la Junta Central Electoral en cumplimiento de sus funciones constitucionales, maneja un área muy sensitiva y de importancia capital para el sostenimiento de la democracia, como lo es la celebración de las elecciones, lo que hace a sus empleados guardianes de informaciones sumamente delicadas, por lo que el pretender que se conozcan públicamente los datos personales de dichos empleados, a todas luces podría entorpecer el desarrollo de dichas funciones, y en consecuencia nuestra democracia”⁶⁷¹.

En este sentido, menciona los “datos personales” como límite al derecho de acceso a la información pública.

“ la información que pretendía obtener el accionante se refiere a un listado contentivo de datos personales de los funcionarios y empleados de la Junta Central Electoral, que son informaciones protegidas por otro derecho fundamental, como lo es el derecho a la intimidad, consagrado por el artículo 44 de la Constitución y que persigue garantizar el respeto y la no injerencia en la vida privada, familiar, el domicilio, la correspondencia y los datos personales de la persona; por lo que si bien es cierto que el derecho de acceso la

⁶⁷¹ Sentencia núm. TC/0062/13. Expediente núm. TC-04-2012-0041, relativo al recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Allan de Jesús Tiburcio Andrickson contra la Sentencia núm.60, dictada por la Tercera Sala de la Suprema Corte de Justicia, en fecha quince (15) de febrero de dos mil doce (2012). Disponible en: <https://www.tribunalconstitucional.gob.do/sites/default/files/documentos/Sentencia%20TC%20062-13%20C.pdf>. (Última consulta en línea 27 de enero 2016).

información es el principio, por ser un derecho universal que contribuye al fortalecimiento de la democracia representativa en tanto permite a los ciudadanos analizar, juzgar y evaluar en forma completa los actos de sus representantes, así como estimula la transparencia en los actos de gobierno y de la administración, no menos cierto es que cuando se trata de información relativa a la divulgación de datos personales o particulares de los empleados públicos, como ocurre en la especie, la solicitud de esta información podrá ser rechazada, ya que la publicidad de estos datos pudiera significar una invasión de la privacidad personal, protegida y resguardada por el citado artículo 44; sobre todo cuando en la petitoria el solicitante no haya demostrado que esta información es de interés público”⁶⁷².

De nuevo, se observa la importancia concedida al derecho de acceso a la información pública como derecho universal, en pro de la democracia y la transparencia. Aún con todo, encuentra límites a la hora de señalarlos, pues una vez más ese listado de datos personales es bastante confuso al referirlos bien a la intimidad, bien a la privacidad.

Por su parte, el recurrente alegaba que, aunque el número de cédula es una información confidencial, no lo son el nombre, apellido y salario de los servidores públicos, siendo mal interpretados por la Suprema, pues no se solicitan informaciones referidas en el art. 44, sino los nombres, apellidos, remuneraciones y funciones de los servidores públicos de la entidad recurrida.

Finalmente, el Tribunal Constitucional estima la especial transcendencia o relevancia constitucional, ya que ésta radica en que la solución del conflicto planteado le permitirá definir el alcance del derecho al libre acceso a la información pública, conociendo el fondo del mismo. Así, el alto Tribunal realiza una interesante jurisprudencia de este derecho y lo vincula a la Convención de las Naciones Unidas contra la Corrupción. De tal modo se señala que:

⁶⁷² Sentencia núm. TC/0062/13. Expediente núm. TC-04-2012-0041, relativo al recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Allan de Jesús Tiburcio Andrickson contra la Sentencia núm.60, dictada por la Tercera Sala de la Suprema Corte de Justicia, en fecha quince (15) de febrero de dos mil doce (2012). Disponible en: <https://www.tribunalconstitucional.gob.do/sites/default/files/documentos/Sentencia%20TC%20062-13%20C.pdf>. (Última consulta en línea 27 de enero 2016).

“la posibilidad de que las personas y grupos que no pertenecen al sector público puedan participar activamente y de manera eficiente depende, en gran medida, de la existencia de mecanismos que garanticen el derecho a la información pública”⁶⁷³

Además, el Tribunal Constitucional se ampara en el artículo 19 de la Declaración Universal de los Derechos Humanos, el artículo 13 de la Convención Americana sobre Derechos Humanos, en el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos, y en el artículo 49.1 de la Constitución Nacional, visto en las pasadas sentencias.

En igual contexto, el Tribunal se apoya en la Sentencia núm. TC/0042/2012 (segunda sentencia analizada) considerada un hito, ya que toma el lugar de jurisprudencia, sirviendo de apoyo a las nuevas sentencias, en especial cuando señala que las informaciones relativas a las nóminas de sus empleados no constituyen informaciones reservadas, ni sensibles y que, en consecuencia, deben ponerse a la disposición de todas las personas que lo requieran, criterio que se reitera en el presente caso.

Sin embargo, matiza que:

“El recurrente no sólo se ha limitado a solicitar la nómina de los empleados, sino también el número de cédula de identidad y electoral, información que es de carácter personal y que, además, no aporta nada en lo que respecta a la transparencia y al control de la corrupción en la administración pública, aspectos que constituyen los objetivos de la Ley”⁶⁷⁴.

⁶⁷³ Sentencia núm. TC/0062/13. Expediente núm. TC-04-2012-0041, (razonamiento 10.1) relativo al recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Allan de Jesús Tiburcio Andrickson contra la Sentencia núm.60, dictada por la Tercera Sala de la Suprema Corte de Justicia, en fecha quince (15) de febrero de dos mil doce (2012). Disponible en: <https://www.tribunalconstitucional.gob.do/sites/default/files/documentos/Sentencia%20TC%20062-13%20C.pdf>. (Última consulta en línea 27 de enero 2016).

⁶⁷⁴ Sentencia núm. TC/0062/13. Expediente núm. TC-04-2012-0041, (razonamiento 10.10) relativo al recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Allan de Jesús Tiburcio Andrickson contra la Sentencia núm.60, dictada por la Tercera Sala de la Suprema Corte de Justicia, en fecha quince (15) de febrero de dos mil doce (2012). Disponible en: <https://www.tribunalconstitucional.gob.do/sites/default/files/documentos/Sentencia%20TC%20062-13%20C.pdf>. (Última consulta en línea 27 de enero 2016).

Ahora bien, señala que no se puede condicionar “la entrega de la nómina de una institución pública a que el solicitante demostrare que perseguía un interés público”⁶⁷⁵.

Se reconoce como información de carácter personal el número de identificación y personal (cédula), funcionando como límite al libre acceso a la información personal, a diferencia de los nombres y salarios de los empleados.

Como consecuencia de todos estos razonamientos, se anula la sentencia de la Suprema Corte de Justicia de revocar la dictada por la Primera Sala del Tribunal Superior Administrativo, y se acoge parcialmente la acción de amparo, ordenando a la Junta Central Electoral la entrega inmediata de los nombres de cada uno de sus empleados y funcionarios, indicando el cargo y salario de cada uno de ellos.

8. STC/0084/13. Su vinculación con la STC/0042/12 y el concepto de datos personales

Esta última sentencia se corresponde con el Expediente núm. TC-04-2012-0045⁶⁷⁶, relativo al recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Alejandro Alberto Paulino Vallejo contra la Sentencia núm. 105 dictada por la Tercera Sala de lo Laboral, Tierras, Contencioso Administrativo y Contencioso Tributario de la Suprema Corte de Justicia, en fecha veintinueve (29) de febrero de dos mil doce (2012).

⁶⁷⁵ Sentencia núm. TC/0062/13. Expediente núm. TC-04-2012-0041, (razonamiento 10.11)

⁶⁷⁶ Sentencia núm. TC/0084/13. Expediente núm. TC-04-2012-0045, relativo a recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Alejandro Alberto Paulino Vallejo contra la Sentencia núm. 105 dictada por la Tercera Sala de lo Laboral, Tierras, Contencioso Administrativo y Contencioso Tributario de la Suprema Corte de Justicia, en fecha veintinueve (29) de febrero de dos mil doce (2012). Disponible en: <https://www.tribunalconstitucional.gob.do/node/1544>. (Última consulta en línea 27 de enero 2016).

Alejandro Alberto Paulino Vallejo solicita a la Cámara de Diputados de la República Dominicana la entrega de documentos contentivo de nombres, apellidos, cargos y sueldos. Ante la negativa de ésta, se recurre en amparo ante el Tribunal Superior Administrativo, quien -mediante la Sentencia núm. 089/2010-, ordenó a la Cámara, la entrega de copia certificada de la nómina de dicho órgano, así como condenándole al pago de una astreinte de cinco mil pesos dominicanos (RD\$5,000.00). Tras ello, la Cámara de Diputados, recurrió en casación esta decisión ante la Suprema Corte de Justicia, que la casó sin envío. Contra la misma decisión, se interpuso ante el Alto Tribunal recurso de revisión constitucional.

Cabe destacar algunos fundamentos de la Suprema Corte de Justicia para rechazar el recurso:

“...lo que se plantea en la especie no es que la Cámara de Diputados se haya negado a ofrecer la información solicitada por el hoy recurrido en virtud de la Ley de Libre Acceso a la Información, sino que este alega que la información suministrada por dicho órgano resulta incompleta, al solo contener la descripción de los cargos y los sueldos pagados por dicha cámara, pero no los nombres de los empleados, por entender la recurrente que esta última información corresponde a datos personales cuya publicidad podría invadir la privacidad personal”⁶⁷⁷.

Observamos que se considera que los nombres de los empleados son datos personales y de nuevo los incluye dentro de la privacidad.

Continúa este Tribunal.

“...para incluir en la información solicitada por el impetrante, los nombres y apellidos de los empleados de la Cámara de Diputados, con lo que quedarían *individualizados e identificados* frente al público con los respectivos cargos y salarios que devengan, el solicitante debió demostrar, como lo exige el artículo 18 de la Ley núm. 200-04, que la revelación de estos nombres, que realmente

⁶⁷⁷ Sentencia núm. TC/0084/13. Expediente núm. TC-04-2012-0045, relativo a recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Alejandro Alberto Paulino Vallejo contra la Sentencia núm. 105 dictada por la Tercera Sala de lo Laboral, Tierras, Contencioso Administrativo y Contencioso Tributario de la Suprema Corte de Justicia, en fecha veintinueve (29) de febrero de dos mil doce (2012). Disponible en: <https://www.tribunalconstitucional.gob.do/node/1544>. (Última consulta en línea 27 de enero 2016).

constituyen *datos personales*, se justificaba por la existencia de un interés público...”⁶⁷⁸.

Utiliza lenguaje propio de la protección de datos, “individualizados e identificados” y manifiesta en este caso, la necesidad de que exista un interés público.

“...al ordenar en su sentencia a la hoy recurrente que entregara al hoy recurrido “copia Certificada de la Nómina de la Cámara de Diputados contentiva de nombres, apellidos, cargos y sueldos”, sin explicar por qué debían incluirse en esta nomina (SIC) datos personales de estos empleados, dicho tribunal invadió, sin justificación alguna, la esfera de la privacidad e intimidad de estas personas, al autorizar revelar informaciones que no son inherentes a su actividad administrativa, sino que son datos personales protegidos por otro derecho fundamental, como lo es el derecho a la intimidad, consagrado por el artículo 44 de la Constitución, que persigue garantizar el respeto a la no injerencia en la vida privada, familiar, el domicilio, la correspondencia y los datos personales de la persona, texto que evidentemente fue violado por el Tribunal a-quo al dictar su sentencia”⁶⁷⁹.

Se observa la confusión de denominar los datos personales, como intimidad o privacidad, o considerar la vida privada o los datos personales como derecho a la intimidad. Todo ello porque la denominación “derecho de la intimidad” del art. 44 engloba derechos que debieran de tener su propia autonomía.

⁶⁷⁸ Sentencia núm. TC/0084/13. Expediente núm. TC-04-2012-0045, relativo a recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Alejandro Alberto Paulino Vallejo contra la Sentencia núm.105 dictada por la Tercera Sala de lo Laboral, Tierras, Contencioso Administrativo y Contencioso Tributario de la Suprema Corte de Justicia, en fecha veintinueve (29) de febrero de dos mil doce (2012). Disponible en: <https://www.tribunalconstitucional.gob.do/node/1544>. (Última consulta en línea 27 de enero 2016).

⁶⁷⁹ Sentencia núm. TC/0084/13. Expediente núm. TC-04-2012-0045, relativo a recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Alejandro Alberto Paulino Vallejo contra la Sentencia núm.105 dictada por la Tercera Sala de lo Laboral, Tierras, Contencioso Administrativo y Contencioso Tributario de la Suprema Corte de Justicia, en fecha veintinueve (29) de febrero de dos mil doce (2012). Disponible en: <https://www.tribunalconstitucional.gob.do/node/1544>. (Última consulta en línea 27 de enero 2016).

Tras los hechos y argumentos jurídicos del recurrente en revisión⁶⁸⁰, llegamos a que el Tribunal Constitucional considera este recurso de especial trascendencia y relevancia constitucional, porque la solución de un conflicto supone reiterar su posición respecto al alcance del derecho de acceso a la información frente al derecho a la intimidad y la protección de datos personales de los funcionarios públicos (como hemos tenido ocasión de ver en anteriores sentencias).

Interesa destacar algunos razonamientos del Alto Tribunal:

“se evidencia una colisión entre dos derechos fundamentales el derecho a la protección de datos personales y el libre acceso a la información pública, consagrados en los artículos 44.2 y 49 de la Constitución”⁶⁸¹.

Una vez más, el Tribunal Constitucional utiliza claramente la expresión el derecho a la protección de datos personales.

Además, vuelve a reiterar la jurisprudencia de la Sentencia núm. TC/0042/2012, cuando dice que los nombres y apellidos no constituyen informaciones reservadas ni sensibles, ya que los listados de funcionarios, legisladores, magistrados, empleados no pueden confeccionarse sin consignar sus nombres y apellidos. El nombre es un dato que permite identificar a las personas e individualizarlas y, en este caso, es necesario.

⁶⁸⁰ Resulta interesante la argumentación del recurrente: “El derecho consagrado en el artículo 44 de la norma constitucional, que establece límites al derecho a la intimidad, no es aplicable a los servidores públicos, ya que son asalariados del Estado, se deben al público y sería un adefesio jurídico plantear que los contribuyentes no tienen derecho a saber el nombre de los servidores públicos y de no poderse transparentar, entonces sería imposible saber si en una entidad pública (sic) hay empleador que no laboran conocidos por el argot popular como “botella”, empleados con dos sueldos, incentivos, nepotismo, clientelismo político, etc.. “

⁶⁸¹ Sentencia núm. TC/0084/13. Expediente núm. TC-04-2012-0045, relativo a recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Alejandro Alberto Paulino Vallejo contra la Sentencia núm. 105 dictada por la Tercera Sala de lo Laboral, Tierras, Contencioso Administrativo y Contencioso Tributario de la Suprema Corte de Justicia, en fecha veintinueve (29) de febrero de dos mil doce (2012). Disponible en: <https://www.tribunalconstitucional.gob.do/node/1544>. (Última consulta en línea 27 de enero 2016).

Además, el Alto Tribunal añade que el libre acceso a la información pública no sólo aplica en relación a las informaciones relativas a la nómina de sus asesores sino también a aquella información que se refiera a los nombres, apellidos, salarios y bonos percibidos por todo empleado o servidor público, funcionario público, magistrados y legisladores, en definitiva, a toda persona que de una u otra manera perciba fondos del Estado.

Asimismo, recoge para mayor abundamiento el Caso *Fontevicchia y D'Amico*, (30 de noviembre de 2011) de la Corte Interamericana de Derechos Humanos⁶⁸². También la jurisprudencia de la Sentencia núm. TC/0062/13 (antes analizada) es utilizada en relación a la información relativa al número de cédula de identidad y electoral de los empleados de la parte recurrida. Y concluye que conforme a la anterior sentencia tal información es de carácter personal y que, además, no aporta nada en lo que respecta a la transparencia y al control de la corrupción en la administración pública, por lo que las instituciones públicas no están obligadas ni tienen el derecho a divulgar dicha información.

Todos estos argumentos llevan al Tribunal Constitucional a declarar admisible el recurso de revisión constitucional incoado por el recurrente contra la primera sentencia, se anula la sentencia de la Suprema Corte de Justicia y se confirma la dictada por la Segunda Sala del Tribunal Superior Administrativo.

El Tribunal Constitucional confirma la sentencia de la Segunda Sala del Tribunal Superior Administrativo, donde se entrega la información solicitada.

Como se puede observar, con la jurisprudencia presentada el Tribunal Constitucional garantiza la supremacía de la constitución, la defensa del orden

⁶⁸² Así en esa sentencia se argumenta: “En una sociedad democrática los funcionarios públicos están más expuestos al escrutinio y a la crítica del público. Este diferente umbral de protección se explica porque se han expuesto voluntariamente a un escrutinio más exigente”.

constitucional y la protección de los derechos fundamentales. Así mismo, sus decisiones son definitivas e irrevocables, constituyendo precedentes vinculantes para los poderes públicos y todos los órganos del Estado⁶⁸³.

9. STC/0404/16. El *habeas data*

La presente sentencia se orienta al recurso de revisión constitucional en materia de *habeas data* interpuesto por comercial Boreo, S. R. L. frente a la sentencia dictada por la Segunda Cámara Penal del Juzgado de Primera Instancia del Distrito Nacional que declaró inadmisibile la acción de *habeas data* interpuesta contra la Cámara de Comercio y Producción de Santo Domingo por existir otras vías más expeditas, idóneas y efectivas para tutelar el derecho reclamado⁶⁸⁴.

Con la acción de revisión, se pretende la entrega de informaciones y posible rectificación o eliminación de datos en poder de la Cámara de Comercio y Producción de Santo Domingo, situación de las anotaciones arbitrarias e ilegítimas que pudieran afectar el registro mercantil del interesado. El Tribunal Constitucional admite el recurso del accionante sustentado en la Ley 172/13 que regula el *habeas data*; la sentencia TC/0204/13 en materia de amparo y la garantía constitucional del *habeas data* contemplada en el artículo 44.2 de la Constitución.

⁶⁸³ Artículo 184, Constitución de la República Dominicana del 2015.

⁶⁸⁴ Sentencia núm. TC/0404/16 Expediente núm. TC-05-2014-0074, relativo al recurso de revisión constitucional en materia de *habeas data* incoado por la sociedad comercial Boreo, S. R. L. contra la Sentencia núm. 052-2014, dictada por la Segunda Sala de la Cámara Penal del Juzgado de Primera Instancia del Distrito Nacional el once (11) de marzo de dos mil catorce (2014). Disponible en: <https://www.tribunalconstitucional.gob.do/consultas/secretar%C3%ADa/sentencias/tc040416>. (Última consulta en línea 16 de noviembre 2018).

En ese sentido, luego de analizar el recurso de revisión en materia de *habeas data*, y no observar violaciones a los derechos fundamentales en materia de acceso a la información y su conexión con la autodeterminación informativa. El Tribunal Constitucional admite y acoge el recurso en cuanto al fondo, declarando inadmisibile la acción constitucional de *habeas data*, no permitiendo el acceso a los registros e informaciones solicitadas por comercial Boreo, S. R. L.

10. STC/0475/16. Recalificación de la acción de Amparo *por habeas data*

Estamos ante un recurso de revisión constitucional de sentencia de amparo interpuesta por Ricardo Sosa Filoteo contra la inadmisibilidad dictada por el Tribunal Superior Administrativo (Tercera Sala) a raíz de la existencia de otras vías judiciales como la jurisdicción penal para proteger el derecho fundamental invocados⁶⁸⁵.

El Sr. Ricardo Sosa, a raíz de un proceso penal llevado en su contrato, solicita al Procurador fiscal del Distrito Nacional la entrega de la información recolectada. Ante su inacción insta a la Procuraduría fiscal del Distrito Nacional el depósito de la información y obtiene los mismos resultados, por lo que eleva la acción al TC. En ese sentido, el accionante requiere del TC la admisión del recurso y la revocación de la sentencia evacuada por el Tribunal Superior Administrativo.

⁶⁸⁵ Sentencia núm. TC/0475/18. Expediente núm. TC-05-2016. Relativo al recurso de revisión constitucional de sentencia de amparo interpuesto por Ricardo Sosa Filoteo contra la Sentencia núm.00125-2015, dictada por la Tercera Sala del Tribunal Superior Administrativo el veintiocho (28) de septiembre de dos mil quince (2015). Disponible en: <https://www.tribunalconstitucional.gob.do/consultas/secretar%C3%ADa/sentencias/tc047518/>. (Última consulta en línea 14 de noviembre 2018).

El Tribunal Constitucional recalifica la acción de amparo⁶⁸⁶ por el de *habeas data*, y así, entran al fondo del asunto del *habeas data*. En ese mismo sentido, el Tribunal vuelve a recordar vía la emisión de sus sentencias, la inaplicabilidad de la acción del *habeas data* cuando se refiera a un tercero y con ello impedir la entrega de las informaciones solicitadas. En el caso que nos compete, no pueden entregarse los exámenes psicológicos de la víctima, así como los documentos vinculados a los mismos, excepto aquellos revestidos del carácter personal del solicitante, razones por la que puede procederse con su entrega.

El Tribunal Constitucional admite la forma, acoge el fondo y la acción de *habeas data* requerida, excepto para los datos pertenecientes al tercero. El TC

⁶⁸⁶ «Mediante la Sentencia TC/0015/12, este colegiado recalificó una acción de tercería en una acción de *habeas data* en los siguientes términos: «Antes de referirnos a la inadmisibilidad del recurso, procederemos a verificar la exactitud del nombre dado al mismo. Los recurrentes identifican su recurso como una “tercería”, calificación que es totalmente errónea, ya que ellos participaron en el proceso agotado ante el tribunal que dictó la sentencia recurrida, es decir, que no son terceros, requisito que es necesario para poder interponer un recurso de tercería en cualquier materia. Por otra parte, no se trata de un recurso de tercería, porque el contenido de la instancia mediante la cual se interpone, así como los pedimentos que aparecen en la misma se corresponden con el recurso de revisión constitucional contra sentencia de amparo, previsto en el artículo 94 de la referida Ley 137-11». En tal virtud, el Tribunal Colegiado de la Cámara Penal del Juzgado de Primera Instancia del Distrito Judicial de Barahona, como tribunal de primera instancia competente también para conocer de acciones de *habeas corpus*, pudo corregir la calificación de la acción y evaluar la solicitud del accionante como un *habeas corpus*, y no como una acción de amparo, tomando en cuenta particularmente que la acción de *habeas corpus* responde a los procedimientos ordinarios establecidos en el Código Procesal Penal, que están diseñados para una mejor instrumentación de los procesos penales y, en el caso particular del *habeas corpus*, para garantizar la protección efectiva del derecho a la libertad personal». 4 Mediante la Sentencia TC/0050/14, este órgano jurisdiccional recalificó una acción de amparo ordinario en un *habeas data*, estableciendo lo dispuesto a renglón seguido: «El Tribunal Constitucional considera oportuno establecer, antes de analizar y responder los alegatos de las partes, que lo que le interesa al recurrente es conocer informaciones que le conciernen a él mismo, de manera que la cuestión planteada no está vinculada al derecho de libre acceso a la información pública, sino al derecho de acceder a datos personales. En consecuencia, aunque las partes y el tribunal a-quo hacen referencia a la acción de amparo, el Tribunal analizará el presente caso, en aplicación del principio de oficiosidad previsto en el artículo 7.11 de la Ley núm. 137-11, como una acción de *habeas data*, figura del derecho procesal constitucional, que está prevista en el artículo 70 de la Constitución y 64 de la indicada ley». 5 «Artículo 64.- *Habeas Data*. Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme la ley. No podrá afectarse el secreto de las fuentes de información periodística. La acción de *habeas data* se rige por el régimen procesal común del amparo». Disponible en: <https://www.tribunalconstitucional.gob.do/consultas/secretar%C3%ADa/sentencias/tc047518/>. (Última consulta en línea 14 de noviembre 2018).

otorga un astreinte de 10,000 pesos por cada día de retardo a favor del solicitante y en contra de la Procuraduría General de la República Dominicana

11. Conclusión

El Tribunal Constitucional de la República Dominicana desde su proceso de creación a partir de la Constitución del 2010, e instauración de la Ley núm. 137-11 Orgánica del Tribunal Constitucional y de los Procedimientos Constitucionales del 13 de julio de 2011 ha sido partícipe de importantes jurisprudencias relacionadas con los derechos fundamentales contemplados en el trabajo, tales como protección de datos personales, habeas data y aquellos derechos tutelados por ésta como intimidad, honor, privacidad, protección de datos y otros, formando parte de las normas europeas, tal es el caso de la autodeterminación informativa.

Unos derechos inculcados desde la óptica del Tribunal Constitucional, la Ley núm. 172-13 ya comentada y las jurisprudencias internacionales como la colombiana o las normas europeas caso de la autodeterminación informativa, tutelada por el *habeas data* y que a su vez no forma parte de la carta magna o la Ley núm. 172-13.

El proceso de implementación o instauración de esos derechos en las jurisprudencias constitucionales no se abordan en tiempo y espacio sino que forman parte de un proceso evolutivo en la medida que esos derechos, junto a las normativas que la integran hace su incursión en el escenario nacional e internacional. A raíz de ello, presentamos por etapas la incursión de esos derechos en las Jurisprudencias de las sentencias evacuadas por el Alto Tribunal.

La primera etapa se basa por tomar o adoptar en las consideraciones jurisprudenciales del Tribunal los artículos de la Constitución, situación del artículo 44 relacionado con la intimidad y el honor, así como el artículo 70 y su

conexión con el habeas data. A partir de la puesta en ejecución de la Ley 172-13, se inicia un proceso jurisprudencial vinculado con la normativa, impulsado por el desarrollo del artículo 44 y 70 de la Constitución de la República constituyendo la segunda parte. Además, no se obvian otros derechos, como el derecho de acceso a la información pública, libertad de expresión, y otros derechos vinculados en el trabajo.

En definitiva, podemos concluir que, de acuerdo a las sentencias emitidas por el TC, se observa un desarrollo jurisprudencial capaz de incorporar en sus decisiones, posiciones doctrinales y jurisprudenciales más allá de las normas establecidas en la República Dominicana, fortaleciendo con ello las evacuaciones jurisprudenciales del TC. En ese sentido, el Tribunal Superior Administrativo debe realizar una rápida incorporación de este accionar a sus decisiones y, así, posibilitar el alineamiento de sus decisiones en materia de derecho fundamental con las decisiones evacuadas por el Alto Tribunal.

VII. EL DESARROLLO LEGISLATIVO Y LA PERSPECTIVA DE LA PROTECCIÓN DE LOS DATOS PERSONALES EN REPÚBLICA DOMINICANA

1. Existencia de ley general de desarrollo y normativas sectoriales en materia de protección de datos. Sus antecedentes

Más allá de los preceptos constitucionales existentes en la República Dominicana en materia de protección de datos, la República Dominicana cuenta con leyes sectoriales y generales conocidas como *ómnibus*⁶⁸⁷, que abogan por una protección general del individuo contra el procesamiento automatizado de sus datos.

⁶⁸⁷ Así lo expresa ESTADELLA YUSTE, O., *La Protección de la Intimidad frente a la Transmisión Internacional de Datos Personales*, 1ª ed. TECNOS, Madrid, 1995, p. 42.

Ya desde el 2006, la doctrina dominicana sostenía que -aunque la República Dominicana se encontraba entre los países que carecían de normativa general sobre la materia de protección de datos - cabe afirmar que existían leyes especiales en determinadas áreas que trataban el tema. En cualquier caso, no cabe duda que la inexistencia de una legislación general sobre esta materia dificulta la protección de este derecho, así como los que del mismo derivan (derecho de confidencialidad, de rectificación, de corrección, de acceso y el derecho de cancelación). Por eso, se señalaba que para que este derecho sea eficaz necesita de garantías procesales y su correspondiente elenco de sanciones⁶⁸⁸.

A esto, nos gustaría añadir que todas las garantías que se establezcan son bienvenidas, pero, sobre todo, con relación al derecho a la protección de datos no sólo son importantes sus mecanismos reparadores sino todos los preventivos que eviten la vulneración del derecho que se produzca.

Como sobre este particular se volverá en páginas siguientes, pasamos simplemente a señalar algunas de las normas que han venido a constituir esa especie de “corpus” que cubría de manera parcial, sectorial y fragmentada el ámbito de la protección de datos. Cabe destacar la Ley núm. 55-93, sobre el Síndrome de Inmunodeficiencia Adquirida (SIDA), del 31 de diciembre de 1993, la Ley núm. 288-05, sobre Regulación de las Sociedades de Información Crediticia de Protección al Titular de la Información (derogada por la Ley núm. 172-13); la Ley núm. 153-98 sobre telecomunicaciones, del 27 de mayo del año 1998; la Ley núm. 126-02, del 4 de septiembre del 2002, de Comercio Electrónico, Documentos y Firmas Digitales; la Resolución núm. 7150 de 18/09/2007 de la Procuraduría General de la República para establecer las políticas para la correcta aplicación del Reglamento sobre Registro de Datos de Personas con Antecedentes Delictivos (Decreto núm. 122-07); el Reglamento de aplicación (Decreto núm. 130-05); la Resolución núm. 055-06 del Instituto Dominicano de Telecomunicaciones (INDOTEL) sobre Protección de Datos de Carácter Personal por los Sujetos Regulados; la Ley núm. 53-07, del 23 de abril

⁶⁸⁸ ACOSTA DE LOS SANTOS, H., “Protección de Datos en la República Dominicana”, op, cit., p. 84.

de 2007, contra Crímenes y Delitos de Alta Tecnología y la Ley núm. 200-04, sobre Libre Acceso a la Información Pública, del 28 de julio del 2004. Esta última, como hemos visto conforme a la jurisprudencia constitucional, ha sido estudiada e invocada ante los tribunales. Se trata además de una ley que ha de cohonestar el derecho al acceso a la información con el derecho a la protección de las personas físicas⁶⁸⁹.

2. Propuestas legislativas de protección de datos personales

La actual carta magna hace suya la protección de datos personales, siendo realidad constitucional desde el 2010. Previo a ello, y más allá del 2010 no existían leyes generales que regularan la protección de datos personales o *habeas data* en nuestro país. No es sino 3 años después de su promulgación cuando se materializa con la Ley núm. 172-13 cuyo objeto es la protección integral de los datos personales, incursionando el *habeas data* en la normativa.

Antes de la existencia de la normativa actual, se ventilaban en las cámaras legislativas dos importantes propuestas en materia de protección de datos y *habeas data*. El primero de los proyectos fue sometido por el diputado de la provincia de Santiago, Demóstenes Martínez y el segundo por el senador Félix Bautista, para ello fue apoderada una Subcomisión de Justicia representada por el diputado del Partido Revolucionario Dominicano, Carlos Gabriel García el cual funge como coordinador.

En este acápite, no nos detendremos en realizar un estudio pormenorizado de ambos proyectos por exceder las pretensiones y los límites temporales y espaciales de este trabajo. Sí nos interesa, al menos destacar como surgen, en qué momento se encuentran y cuáles son sus principales previsiones,

⁶⁸⁹ BARINAS UBINAS, B., “Los derechos fundamentales de acceso a la información pública y protección de datos personales: una aproximación a la pertinencia de su vinculación normativa en República Dominicana”, *op. cit.*, pp. 3-5.

especialmente por la concordancia con lo tratado hasta ahora, relativo a la denominación del derecho que regulan y algunos apuntes del *habeas data*. Aclaradas estas puntualizaciones pasamos a presentar los dos proyectos.

2.1. Proyecto de ley mediante el cual se crea las normas que regula y protege los datos personales o Ley de *habeas Data*

El primer proyecto corresponde a la iniciativa legislativa del dos mil diez y dos mil dieciséis (2010-2016), sometido al Congreso el 7 de abril del 2011, mediante comunicación expresa dirigida al despacho del presidente de la Cámara de Diputados con el epígrafe siguiente:

“Cortésmente le remitimos a usted la introducción del Proyecto de Ley mediante el cual se crea las normas que regula y protege los datos personales o Ley de *habeas data* en nuestro país. Para que sea colocado en la agenda de la Orden del Día que usted considere pertinente”⁶⁹⁰.

El proyecto ha sido recibido en la Cámara de Diputados el día 29 de agosto de 2012 e iniciado el día 08 de noviembre de 2012 (tres meses después), bajo el Registro núm. 03346-2010-2016 CD⁶⁹¹ de la Cámara de Diputados, bajo la digitación de Hayn Fernández y la revisión de Miguel Ángel Carvajal.

En toda ley existen dos tipos de actores, aquellos a los cuales favorece la ley -comúnmente reconocido como actores favorecidos- y otros actores a los cuales la ley obliga a cumplir sus disposiciones. En el proyecto de protección de datos personales, los actores obligados son aquellos actores responsables de los archivos, registros, base o banco de datos, cuya finalidad es la de proveer informaciones a una tercera persona. Por su parte, como actores

⁶⁹⁰ *Iniciativa N.º 03346-2010-2016-CD*. Registro de decisión. Disponible en: <https://www.camaradediputados.gov.do/masterlex/mlx/docs/2e/2/53DD/5888.pdf>. (Última consulta en línea 1 de mayo 2018).

⁶⁹¹ *Iniciativa N.º 03346-2010-2016-CD*. Registro de decisión. Disponible en: <https://www.camaradediputados.gov.do/masterlex/mlx/docs/2e/2/53DD/5888.pdf>. (Última consulta en línea 1 de mayo 2018).

favorecidos, tenemos a los titulares de los datos, conformado por las personas físicas a cuyos datos personales realizan el tratamiento en cuestión.

El proyecto de la Cámara de Diputados está conformado por 47 artículos distribuidos en 7 capítulos. A pesar de no contar con históricos constitucionales o leyes nacionales, mantiene similitud con la ley argentina, nos referimos a la *Ley núm. 25.326 de Protección de los Datos Personales*, manteniendo la misma estructura de artículos y contenido.

Los actores favorecidos en el proyecto brillan por su ausencia, al no ser consultados durante el proceso de conformación del proyecto de ley (a nuestro entender, el proyecto que reposa en esta Cámara es una fiel reproducción de la Ley de protección de datos y *habeas data* Argentina núm. 25.326).

En nuestro país, se ha producido una nueva realidad legal y procesal, marcada por tres momentos históricos que definen el ámbito constitucional dominicano, siendo considerados al momento de elaborar la nueva legislación en materia de protección de datos y *habeas data*.

- 1) Promulgación de la Constitución del 26 de enero de 2010.
- 2) Entrada en vigencia de la Ley Orgánica del Tribunal Constitucional Ley núm. 137-11 del 15 de junio de 2011, y
- 3) La conformación del Tribunal Constitucional Dominicano, a finales de diciembre de 2011.

Todo ello ha de ser tenido en cuenta a la hora de dotarse de una legislación en desarrollo.

El proyecto tiene por objeto la protección de los datos personales y el acceso a la información, registrada conforme a la Constitución de la República Dominicana en sus artículos 44.2 y 70.

Los siguientes principios, forman parte de los articulados del proyecto de protección de datos y *habeas data* del referido proyecto.

- El principio de legalidad, asegura la correcta inscripción de los datos y sus reglamentaciones.
- El principio de calidad de los datos, asegura un tratamiento adecuado, pertinente y no excesivo a los datos recogidos, así como su tratamiento pasada su utilización.
- El consentimiento como principio, el cual debe ser libre, consciente y expreso por medio escrito.
- El principio de Información, comunica a sus titulares de forma expresa y clara.
- El principio de confiabilidad, asegura el secreto profesional.
- El principio de cesión, asegura el conocimiento del cedente y del cesionario con conocimiento previo del titular.
- El principio de transferencia internacional, evita la transferencia de datos hacia Estados inseguros. En ese sentido, República Dominicana debe iniciar el proceso de ser parte del Convenio 108 del Consejo de Europa.

De igual forma, asiste a los titulares de datos los siguientes derechos:

- Derecho de información mediante solicitud al organismo de control.
- Derecho de acceso a sus datos personales.
- Derecho de rectificación, actualización o supresión de datos personales sin cargo alguno para el interesado.

El proyecto contempla los requisitos mínimos necesarios para el registro de los archivos de datos y su inscripción en bancos de datos públicos y privados.

En el Capítulo V se consagra el órgano de garantía bajo la denominación *Dirección para la Protección de los Datos Personales*, con autonomía funcional y descentralizada bajo la Procuraduría General de la República.

De la misma forma, el proyecto contempla las sanciones administrativas y penales por daños y perjuicios derivados de la inobservancia de la ley. Como el reconocimiento expreso en la ley de la figura del *habeas data*.

Por otra parte, abre la legitimación activa a las personas, tanto físicas como moral, interviniendo como coadyuvante el Defensor del Pueblo. También especifica la competencia del juez, el procedimiento aplicable, los requisitos de la demanda, los tramites de la acción, la ampliación de la demanda y la sentencia, siempre cumpliendo con su carácter de confidencialidad.

No nos detendremos más en el proyecto. Simplemente se ha de destacar, que este proyecto considera sinónimos en su denominación la protección de datos personales y el *habeas data*, como se desprende de su propio título *Proyecto de ley mediante el cual se crea las normas que regula y protege los datos personales o*⁶⁹² *Ley de habeas data*. A pesar de ello, el *habeas data* forma parte de la regulación del derecho, en especial, la contemplada en la acción judicial. Además, este proyecto entronca, conforme al último considerando, con los derechos de intimidad, honor personal, *habeas data* y tutela judicial (arts.44, 68 y 70). En nuestra opinión, hubiera sido más deseable reconocer que el ámbito de protección es el del derecho a la protección de datos con sustantividad propia y no tan vinculada a derechos de la personalidad (intimidad, honor), como queda externado en el artículo 44, numeral 2 en relación con el art.70.

Como hemos señalado, el texto analizado reproduce fielmente la ley argentina, pero lo “importa” al ámbito dominicano. El texto argentino ha recibido una valoración muy positiva⁶⁹³. Así se ha sostenido que, aunque se le denomina Ley de *habeas data*, en su regulación es más que eso, pues se

⁶⁹² La cursiva es nuestra.

⁶⁹³ RODRÍGUEZ MARCANO, E. R., *El derecho a la autodeterminación informativa en Venezuela...*op. cit., pp. 264-282.

encarga de regular toda la materia de protección de datos⁶⁹⁴. Por último, -y como indicamos en el *Capítulo II*- cabe situar a esta ley argentina (como también se ha dicho de la uruguaya) como una norma que se aproxima al modelo europeo de protección de datos personales, siendo reconocida con un nivel adecuado de protección⁶⁹⁵ en el 2003, aplicable al texto dominicano. A continuación, presentamos la segunda propuesta.

2.2. Proyecto de Ley Orgánica sobre Protección de Datos de Carácter Personal

El segundo texto, bajo la designación de Ley Orgánica sobre Protección de Datos de Carácter Personal, fue fechada el 6 de marzo del 2013, mocionada por el senador por la provincia de San Juan de la Maguana el Señor Félix Ramón Bautista Rosario⁶⁹⁶.

El proyecto de ley fue aprobado por el Senado de la República el 17 de abril del año 2013, aprobación presidida por el presidente del Senado doctor Reinaldo Pared Pérez.

Con anterioridad, el proyecto pasó por las Comisiones de Justicia y Derechos Humanos, bajo la Iniciativa núm. 01367-2013-PLO-SE⁶⁹⁷, depositada y tomada en consideración el 6 de marzo, posteriormente enviada a Comisión el 7 de marzo, siendo firmada y leída el 3 de abril. A su vez, fue puesta en

⁶⁹⁴ FERNÁNDEZ DELPECH, H., *Internet: problemática jurídica*, Abeledo -Perrot, Buenos Aires 2001, p. 213

⁶⁹⁵ TRONCOSO REIGADA, A., "El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio en los modelos de protección de datos a nivel internacional", op, cit, pp. 1-2 y pp. 30-31.

⁶⁹⁶ Iniciativa 01367-2013-PLO-SE *Ley Orgánica sobre Protección de Datos de Carácter Personal*. Disponible en: <http://www.informatica-juridica.com/ley/iniciativa-01367-2013-plo-se-ley-organica-proteccion-datos-caracter-personal/>. (Última consulta en línea 1 de mayo 2018).

⁶⁹⁷ BARIÑAS UBIÑAS, B., *Taller Impulso normativo de la Protección de Datos Personales en Centroamérica y el Caribe, Historial Ley Orgánica sobre protección de datos de carácter personal 2013*, Antigua, Guatemala, 14 de febrero de 2014. Disponible en: http://www.redipd.org/actividades/talleres/La_Antigua_02_2014/common/Ponencias_Taller_La_Antigua./REPUBLICA_DOMINICANA..pdf. (Última verificación en línea 14 de agosto 2017).

agenda y aprobado en segunda lectura el 17 de abril, siendo remitido a la Cámara de Diputados de la República Dominicana el 3 de julio del 2013. El proyecto se mueve a Comisión para su estudio y comparación con la propuesta legislativa anterior del diputado Demóstenes Castillo.

La iniciativa legislativa descansa en el artículo 42 numeral 2 de la Constitución de la República Dominicana, el cual contempla el derecho que posee el dueño del dato en acceder a la información y a los datos almacenados, así como conocer el destino, exigir actualización, rectificación, destrucción de las informaciones que lo afecten y tener acceso a los datos almacenados. Pero, con todo, y, conforme a sus considerandos y su exposición de motivos también lo entronca con el derecho a la intimidad. Ello obedece a la propia estructura del art. 44 que introduce la protección de datos dentro de la intimidad.

El proyecto de Ley Orgánica sobre Protección de Datos de Carácter Personal presentado por el senador de la provincia de San Juan, el Sr. Félix Bautista presenta de entrada los preceptos constitucionales de la República Dominicana, seguidos por los lineamientos de otras legislaciones, situándola a la altura de las constituciones latinoamericanas, caso de Chile y la Unión Europea.

Más allá de la carta magna, el proyecto contempla en su haber la Declaración Universal de Derechos Humanos del 10 de diciembre del año 1948, el Pacto Internacional de Derechos Civiles y Políticos del 23 de marzo del año 1976 y la Convención Interamericana de Derechos Humanos del 22 de noviembre del año 1969.

En ese sentido, el proyecto toma en cuenta la Ley núm. 8-92 que pone bajo la dependencia de la Junta Central Electoral, la Dirección General de la Cédula de Identificación Personal y las Oficinas y Agencias Expedidoras de Cédulas, la Oficina Central del Estado Civil y las Oficialías del Estado Civil, del 18 de marzo del año 1992; Ley núm. 19-01 que crea el Defensor del Pueblo del 1 de febrero

del año 2001; Ley núm. 76-02 que establece el Código Procesal Penal de la República Dominicana del 19 de julio del año 2002; Ley núm. 288-05 que crea las Sociedades de Intermediación Crediticia y de Protección al Titular de la Información del 18 de agosto del año 2005; Ley núm. 137-11 Orgánica del Tribunal Constitucional y los Procedimientos Constitucionales del 9 de marzo del año 2011 o la ya mencionada -y analizada por nosotros- Ley núm. 200-04 General de Libre Acceso a la Información Pública, del 28 de julio del año 2004.

El proyecto compuesto por 100 artículos distribuidos en 6 capítulos. En el primer capítulo se refiere a las disposiciones iniciales, dispuesta por dos secciones en la primera sección podemos ver el objeto, alcance, ámbito de aplicación, restricciones y principios del proyecto. Se contempla un marcado interés en la protección y tratamiento de los datos personales almacenados en sus distintas modalidades, aplicable a los datos utilizados en el territorio nacional bajo su legislación, entre los que destacan los datos generados en el Registro Civil, las videocámaras de las Fuerzas Armadas, los organismos policiales, los archivos personales con restricción a los archivos personales de personas físicas, fallecidas y jurídicas.

El proyecto se fundamenta en los principios de licitud, calidad, derecho de Información, consentimiento, seguridad, lealtad, deber de secreto, lealtad y finalidad de los datos conforme a lo previsto en la Constitución de la República Dominicana.

El capítulo II se orienta a las disposiciones generales de las personas y su ejercicio, los derechos de los afectados (acceso, rectificación, cancelación y oposición) y se exhiben las excepciones a estos derechos, especialmente en relación los ficheros de las fuerzas armadas, de seguridad, los organismos policiales y de Inteligencia. Los datos, por su parte, pueden ser presentados a un tercero (cesión) previo a la autorización del consentimiento de su titular, no siendo aplicable cuando se encuentre autorizada por ley, un proceso judicial, jueces del tribunal o urgencia del tribunal.

El proyecto de ley contempla la tutela de los derechos del interesado, protegidos por la Agencia Dominicana de Protección de Datos, otorgando un plazo de tres meses para amparar los derechos, contemplando la indemnización; con posibilidad de accionar el *habeas data*.

El capítulo III se refiere a las disposiciones orgánicas, entre las cuales destaca la creación de la Agencia Dominicana de Protección de Datos (funciones, la Dirección de Protección de Datos Personales). Se le dota de presupuesto propio, está conformada por un Consejo Consultivo y se establece un tiempo de ejercicio de 4 años para su director.

El capítulo IV contempla las disposiciones procedimentales, donde se observa la creación del Registro General de Protección de Datos, el cual funcionará como una base de datos consolidada para los datos de carácter personal y público, siendo manejado por la Agencia de Protección de Datos. A su vez, se regula la inscripción en el registro, y, se establece un procedimiento de inscripción de archivo, el cual contempla informaciones tales como el nombre del responsable, la finalidad del archivo, la forma de recolección, el destino de los datos, el tiempo de conservación de los datos, etc.

El proyecto presenta el procedimiento de administración de los ficheros de las fuerzas armadas, de seguridad, los organismos policiales o de inteligencia, así como la creación de los archivos de datos personales de titularidad privada, estableciendo el principio de creación y forma de administración, incluyendo su notificación a la Agencia Dominicana de Protección de Datos Personales. Además, el documento presenta las excepciones y el consentimiento para los datos especialmente protegidos (ideología, religión o creencias), los relativos a la salud, origen racial, vida sexual y datos de los menores de edad.

En el mismo orden, se presenta el movimiento internacional de datos, compuesto por su norma general, previendo la protección de los datos transferidos a distintos destinos, incluidos países, organismos internacionales o supranacionales, que no proporcionen o garanticen un nivel equiparable al de

la presente ley. Esto se evaluará conforme a la Agencia Dominicana de Protección de Datos, tomando en cuenta la duración del tratamiento, el país origen y el país de destino final, asegurando por medio a la publicación los países que no cuenten con un nivel adecuado de protección de datos. A tal punto, que la Agencia velará y asegurará con audiencia previa, la suspensión temporal de la transferencia, en caso de existir problemas.

El proyecto contempla excepciones entre las que se destacan los tratados internacionales, las ayudas humanitarias, consentimiento por el afectado o salvaguarda de un interés público, proceso judicial, cooperación internacional en la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

En el capítulo V observamos las disposiciones de infracciones y sanciones utilizadas en el proyecto de protección de datos, donde la Agencia Dominicana de Protección de Datos puede aplicar la sanción a los encargados de los tratamientos. Para ello se han implementado sanciones leves (20 salarios), sanciones graves (40 salarios), sanciones muy graves (60 salarios); también tipifica el tipo de sanciones y establece el procedimiento sancionador para la data pública y privada.

El capítulo VI contiene las disposiciones transitorias, modificatorias y finales del presente proyecto de ley. Entre las disposiciones transitorias se contempla la competencia de la Agencia de Protección de Datos Personales en materia de protección de datos en los tratados internacionales.

Se ha de señalar como disposiciones finales la eliminación de los registros por mora pagados antes de la presente ley, la sujeción a la presente ley de los datos y tratamientos automatizados inscritos y no inscritos dentro del plazo de 2 años de la entrada en vigor de la ley, así como la elaboración del reglamento de la ley en un tiempo no superior a 90 días de la entrada de la ley.

Como muestra de la influencia española y europea en el ordenamiento dominicano se ha de decir que la pieza legislativa es una reproducción muy similar

-por no decir literal- de la LOPD española de 1999⁶⁹⁸, -sustituta de la LORTAD de 1992- y que se articula en torno a lo establecido en la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

2.3. Estatus actual de los dos proyectos

La Cámara de Diputados de la República Dominicana conoció los dos Proyectos. El primero de los proyectos bajo las iniciativas del diputado de la provincia de Santiago, Demóstenes Martínez, y el Segundo de los proyectos por el senador Félix Bautista, ambos apoderados por una Subcomisión de Justicia representada por el diputado del Partido Revolucionario Dominicano Carlos Gabriel García, a cargo de la coordinación de la Subcomisión.

De acuerdo a comentarios realizados por el legislador, la misión de la Subcomisión era la ponderación de las dos piezas legislativas, siempre tomando en cuenta a los representantes de los organismos estatales y empresas privadas afectadas e impactadas por las piezas legislativas.

A raíz de ello, los trabajos dieron como resultado un acercamiento de la Comisión con el sector de las empresas de telecomunicaciones, formando parte de ella la empresa de telecomunicaciones VIVA. En este sentido, el coordinador de la Subcomisión Carlos Gabriel García expresó que:

“A pesar de la urgencia que tiene la sociedad dominicana de la aprobación de una ley para regular y proteger los datos personales como lo manda la Constitución de la República, no vamos a festinar el proceso de socialización de la misma para el que tenga algo que decir o aportar lo haga en beneficio de una legislación tan importante para el país”⁶⁹⁹.

⁶⁹⁸ TREVIJANO SÁNCHEZ, P. G. (Presidente consejo de redacción), *Constitución y Derechos Fundamentales*, editora La Ley, edición septiembre 2009, pp. 149-178.

⁶⁹⁹ GABRIEL GARCÍA, C., *Proyecto busca regular uso datos personales*, Periódico Hoy, 30 de julio 2013. Disponible en: <https://hoy.com.do/proyecto-busca-regular-usodatos-personales/>. (Última verificación en línea 14 de agosto 2017).

Como hemos ya comentado, el proyecto emitido por el senador Félix Bautista del Partido de la Liberación Dominicana (PLD) contó con la aprobación del Senado, a diferencia del proyecto del diputado Demóstenes Martínez.

El proyecto del diputado Demóstenes Martínez perimió en la Cámara de Diputados, por lo cual fue reintroducido el 23 de agosto con el nuevo período legislativo. Luego de ser reintroducido en la Cámara de Diputados no se observaron movimientos de información, tales como reuniones o aprobaciones. El resultado final fue la aprobación de la Ley 172-13, una ley alejada de ambos proyectos y puesta a su consideración en breve momento.

2.4. Estudio comparado de las piezas legislativas

Como hemos indicado, el primer proyecto⁷⁰⁰ es una reproducción casi fiel del texto argentino con el pro y contra manifestado, incluyendo su acercamiento a la LOPD española de 1999, aplicando las mismas consideraciones ya comentadas.

Ambos textos contemplan dentro de sus objetivos la protección y el tratamiento de los datos personales almacenados en bancos y archivos, disponen de sanciones administrativas -con excepciones y principios generales relativos a la protección de datos personales-, regulan las transferencias internacionales de datos. crean y reconocen un órgano regulador descentralizado bajo un director, con un plazo de término de 4 años, contemplan la eliminación de los registros de pagos realizados por mora previa a la entrada de la presente ley eliminando el histórico y, al mismo tiempo, acogen la acción o garantía del *habeas data* (si bien el segundo texto se remite a la legislación vigente).

⁷⁰⁰ Diputado Demóstenes Martínez

El texto del senador Félix Bautista, aunque compuesto por sus 100 artículos, no por ello resulta ser un escrito más detallado y amplio. Por su parte, el órgano de control del proyecto del diputado Demóstenes Martínez opera en el ámbito de la Procuraduría General de la República Dominicana, a diferencia del proyecto del senador Félix Bautista, formado por un órgano de control independiente, siendo instituida la Oficina Dominicana de Protección de Datos responsable de tutelar los derechos y adscrita al Ministerio de la Presidencia.

3. Actual ley de protección de datos personales de La República Dominicana

La presente ley ha sido dada a los 13 días del mes de diciembre del año 2013; año 170 de la Independencia y 151 de la Restauración. La ley fue colocada en la G.O. núm. 10737 del 15 de diciembre de 2013, dos días después de su aprobación en el congreso. Dicho texto contempla la siguiente estructura.

ESTRUCTURA LEY 172-13

1. CAPÍTULO I

DISPOSICIONES INICIALES

1.1. SECCIÓN I

DEL OBJETO, ALCANCE, ÁMBITO DE APLICACIÓN, RESTRICCIÓN Y PRINCIPIOS

1.2. SECCIÓN II

DEFINICIONES

2. CAPÍTULO II

DISPOSICIONES GENERALES

2.1. SECCIÓN 1

DE LOS DERECHOS DE LAS PERSONAS Y SU EJERCICIO

3. CAPÍTULO III

DISPOSICIONES ORGÁNICAS

3.1. SECCIÓN I

ÓRGANO DE CONTROL

4. CAPÍTULO IV

DISPOSICIONES PROCEDIMENTALES

4.1. SECCIÓN I

DE LOS FICHEROS DE TITULARIDAD PÚBLICA

4.2. SECCIÓN II

DE LOS FICHEROS DE LAS FUERZAS ARMADAS DE SEGURIDAD Y ORGANISMOS POLICIALES O DE INTELIGENCIA

4.3. SECCIÓN III

DE LOS FICHEROS DE TITULARIDAD PRIVADA

4.4. SECCIÓN IV

OTROS DATOS

4.4.1. SUBSECCIÓN I

DATOS ESPECIALMENTE PROTEGIDOS

4.4.2. SUBSECCIÓN II

DATOS RELATIVOS A LA SALUD

4.4.3. SUBSECCIÓN III

TRATAMIENTO DE DATOS DE MENORES DE EDAD

4.5. SECCIÓN V

MOVIMIENTO INTERNACIONAL DE DATOS

5. CAPÍTULO V

DISPOSICIONES DE INFRACCIONES Y SANCIONES

6. CAPÍTULO VI

DISPOSICIONES TRANSITORIAS Y FINALES

6.1. SECCIÓN I

DISPOSICIONES TRANSITORIAS

6.2. SECCIÓN II

DISPOSICIÓN FINAL

3.1. Análisis Ley de Protección de Datos Personales núm. 172-13

Como ya hemos comentando, la Ley núm. 172-13⁷⁰¹ es la actual *Ley de protección integral de datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamientos de datos destinados a dar informes, sean estos públicos o privados*. Se trata de una normativa llamada a regular la divulgación, uso y comercialización de los datos personales de los ciudadanos conforme a lo estipulado en la ley y la Constitución, haciendo necesario su fortalecimiento, especialmente en lo que tiene que ver con el tratamiento de las informaciones personales⁷⁰².

Este texto se compone de 91 artículos, distribuidos en 6 capítulos, 11 secciones, y 3 subsecciones; el capítulo I (disposiciones iniciales), capítulo II (disposiciones generales), capítulo III (disposiciones orgánicas), capítulo IV (disposiciones procedimentales), capítulo V (disposiciones de infracciones y sanciones), capítulo VI (disposiciones transitorias y finales). La normativa inicia con 7 considerandos explicativos de las razones y motivos que sustentan la presente ley, destacando el derecho a la intimidad, honor personal, el derecho de las personas a decidir, acceder a sus datos personales, amparados en la Constitución de la República Dominicana, sin dejar de lado el incremento de crímenes y delitos por robos de identidades.

⁷⁰¹ Gaceta Oficial N.º 10737 del 15 de diciembre de 2013.

⁷⁰² Cfr. Considerando 4 y 5 Ley núm. 172-13.

En ese contexto, la ley toma como insumo la carta magna, los acuerdos internacionales, las leyes y resoluciones emitidas y aprobadas por el Estado, destacando:

- La Constitución de la República proclamada el 26 de enero de 2010.
- La Declaración Universal de Derechos Humanos, del 10 de diciembre del año 1948.
- La Ley núm. 19-01, que crea el Defensor del Pueblo, del 01 de febrero del año 2001.
- La Ley núm. 136-03 que crea el Código para el Sistema de Protección y los Derechos Fundamentales de Niños, Niñas y Adolescentes, del 7 de agosto del año 2003.
- La Ley General de Libre Acceso a la Información Pública núm. 200-04, del 28 de julio del año 2004.
- La Ley núm. 288-05 que regula las Sociedades de Intermediación Crediticia y de Protección al Titular de la Información, del 18 de agosto del año 2005.
- La Ley Orgánica del Tribunal Constitucional y de los Procedimientos Constitucionales, núm. 137-11, del 13 de junio del año 2011.
- La Resolución núm. 357-05, del 9 de septiembre de 2005, que aprueba el Tratado de Libre Comercio suscrito entre la República Dominicana-Centro América y los Estados Unidos de América, en fecha 5 de agosto de 2004.

El capítulo I, titulado “disposiciones iniciales”, está formado por 2 secciones. La primera sección se refiere al objeto, alcance, ámbito de aplicación, restricciones y principios; la segunda sección aborda el tema de las definiciones, en ella podemos ver los conceptos existentes en la ley como son. los datos de carácter personal referente a cualquier información (numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo) concerniente a personas físicas identificada o identificable, los archivos, los registros; los ficheros; las Sociedades de Información Crediticia (SIC), etc.

El capítulo II contiene las “disposiciones generales” bajo el tema de los “derechos de las personas y su ejercicio”. En esta sección se observan los derechos inherentes a las personas, como son los derechos de consulta para la protección de datos, derechos de acceso, de indemnización, de rectificación y cancelación, la acción de *habeas data* y el procedimiento de reclamación aplicable a las Sociedades de Información Crediticia (SIC) para la modificación, rectificación y cancelación de la información del titular, las excepciones a los derechos de acceso, rectificación, cancelación y oposición, las excepciones al requerimiento de consentimiento donde no será necesario el consentimiento cuando la información sea obtenida de fuente de acceso público, datos entre dependencias de los órganos del Estado, datos de salud necesarios por razones de salud pública o estudios epidemiológicos, etc.

El capítulo III presenta las “disposiciones orgánicas”, compuesto por la sección I, referida al órgano de control, bajo la dirección de la Superintendencia de Bancos que en 8 artículos, plantea las funciones y atribuciones del órgano de control, así como los documentos necesarios en la formación y funcionamiento de las Sociedades de Intermediación Crediticia.

El capítulo IV, titulado “disposiciones procedimentales” contiene 5 secciones y 3 subsecciones. La primera sección bajo el título de los ficheros de titularidad pública abarca 3 artículos centrados en la creación, modificación, supresión de los ficheros de titularidad pública y el proceso de comunicación de datos entre instituciones de la administración pública, un proceso orquestado bajo el amparo de las disposiciones contenidas en la Ley núm. 41-08 de Función Pública y la Ley núm. 200-04 General de Libre Acceso a la Información Pública.

La actual Ley núm. 172-13 deposita en manos de la Ley de Función Pública y la Ley General de Libre Acceso a la Información Pública, la responsabilidad de creación, modificación o supresión de los archivos de datos correspondientes a la administración pública⁷⁰³. De entrada, nos referimos a

⁷⁰³ Artículo 37, Ley núm. 172-13.

disposiciones legislativas previas a la actual Ley núm. 172-13 que, a su vez, no incorpora las funciones o atribuciones reconocidas y otorgadas en la referida ley, en cambio, la administración pública asegura la protección de los archivos de datos públicos, por medio al uso y empleo de servidores de repartos y unidades departamentales internas, responsables de asegurar y tutelar los archivos de datos personales en manos de la administración pública⁷⁰⁴, convirtiéndose en juez y parte de la situación ante la inexistencia de un órgano de control capaz de asegurar, auditar, velar, y proteger las informaciones, garantizando la implementación de medidas preventivas y proactivas, amparando tales derechos.

En consulta realizada a la Oficina de Acceso a la Información Pública del Ministerio de Administración Pública vía la solicitud SAIP-SIP-000-24730, se observa que, a pesar de que el artículo 37 de la Ley núm. 172-13 otorga a las leyes núm. 41-08 y núm. 200-04 la responsabilidad de disponer de acciones de creación, modificación o supresión de los datos personales contenidos en los archivos del Ministerio Público, las normativas legislativas no contienen tales disposiciones.

Por su parte, el Ministerio se encuentra dotado de herramientas de gestión capaces de articular las ordenanzas contempladas en la normativa como es el caso del: a) Subsistema de Registro, Control e Información orientada al ingreso y desvinculación de los empleados públicos bajo la responsabilidad de Recursos Humanos; b) El Sistema de Administración de Servidores Públicos (SASP) a cargo de las nóminas de los empleados; c) El Sistema de Carrera Administrativa (SCA) dispuesto para los empleados que conforman el régimen de carrera administrativa del sector público, a pesar de los respaldos tecnológicos y aspectos señalados, somos partícipes de la instauración de

⁷⁰⁴ SAIP-SIP-000-24730: a) Subsistema de Registro, Control e Información, orientada al ingreso y desvinculación de los empleados públicos bajo la responsabilidad de Recursos Humanos; b) El Sistema de Administración de Servidores Públicos (SASP) a cargo de las nóminas de los empleados; c) El Sistema de Carrera Administrativa (SCA) dispuesta para los empleados que conforma el régimen de carrera administrativa del sector público.

mecanismos de aseguramiento de las informaciones contenidas en los archivos de titularidad pública, articulados por un organismo externos.

La segunda sección, con apenas un artículo, se refiere al tema de los ficheros de las fuerzas armadas, de seguridad y organismos policiales de inteligencia, quienes por sus funciones no se encuentran sujetos al régimen general de la presente ley.

La sección III dispone de 23 artículos, destinada a los ficheros de titularidad privada, dirigido a los archivos o registros de datos que no sean exclusivos del uso del personal. La sección de ficheros de titularidad privada incluye la creación y registro de los archivos de datos, el registro de las Sociedades de Información Crediticia (SIC), la limitación de los datos almacenados por los grupos profesionales (colegios) o aquellos datos utilizados para fines de publicidad o prospección comercial.

Además, también se tienen en cuenta los lineamientos generales de: a) recolección y tratamiento de información aplicables a las Sociedades de Información Crediticia (SIC); b) las medidas de seguridad y control para el manejo de la información; c) los criterios de procesamiento de información para presentación en los reportes; d) las prohibiciones a las Sociedades de Información Crediticia (recolectar, acopiar, almacenar, actualizar, grabar, organizar, sistematizar, elaborar, seleccionar, confrontar, interconectar en sus base de datos) informaciones tales como saldos y movimientos de las cuentas corrientes, ahorros, certificados de depósitos, papeles comerciales, ideologías, opiniones políticas, religiosas, salud física o psíquica, preferencia u orientación sexual. Prohibiendo a las Sociedades de Información Crediticia no difundir reportes de las informaciones presentadas previamente, así como presentar datos de insolvencia o quiebra del titular de la información.

Por su parte y, de acuerdo a lo dispuesto en la *Ley núm. 53-07 sobre Crímenes y Delitos de Alta Tecnología*, se perfila la protección de la

información o los datos almacenados o transmitidos vía las tecnologías de información y comunicaciones, considerados bienes jurídicos protegidos.

En tal sentido, en los casos de recolección y almacenamiento de datos pertenecientes a los proveedores de servicios de telecomunicaciones, la Ley⁷⁰⁵ núm. 53-07 sobre Crímenes y Delitos de Alta Tecnología dispone la creación de un reglamento orientado a la conservación de datos provenientes de los proveedores de servicios de telecomunicaciones por un período de conservación de tres meses, empleados como prueba judicial, bajo la responsabilidad del Instituto Dominicano de las Telecomunicaciones (INDOTEL)⁷⁰⁶. En ese sentido, 4 años después de promulgada la ley se emite la resolución N.º 086-11, por la que se aprueba la creación del “Reglamento *para la obtención y preservación de los datos e informaciones por parte de los proveedores de servicios de telecomunicaciones*”. A raíz de ello, fue incoada una acción directa de inconstitucionalidad ante el Tribunal Constitucional, evacuando la Sentencia núm. TC/0200/13⁷⁰⁷, por las que se derogan varias disposiciones del reglamento dispuesto por la Resolución N.º 086-11,

⁷⁰⁵ Artículo 56, Ley núm. 53-07.

“...los proveedores de servicio deberán conservar los datos de tráfico, conexión, acceso o cualquier otra información que pueda ser de utilidad a la investigación, por un período mínimo de noventa (90) días. El Instituto Dominicano de las Telecomunicaciones (INDOTEL) creará un reglamento para el procedimiento de obtención y preservación de datos e informaciones por parte de los proveedores de servicios, en un plazo de 6 meses a partir de la promulgación de la presente ley. Dicha normativa deberá tomar en cuenta la importancia de preservación de la prueba, no obstante, la cantidad de proveedores envueltos en la transmisión o comunicación”.

⁷⁰⁶ Artículo 76, Ley N.º 153-98 General de las Telecomunicaciones.

76.1. Se crea el órgano regulador de las telecomunicaciones con carácter de entidad estatal descentralizada, con autonomía funcional, jurisdiccional y financiera, patrimonio propio y personalidad jurídica. Tendrá capacidad jurídica para adquirir derechos y contraer obligaciones. Realizará los actos y ejercerá los mandatos previstos en la presente Ley y sus reglamentos y será inembargable.

76.2. El órgano regulador de las telecomunicaciones, que se denominará Instituto Dominicano de las Telecomunicaciones (INDOTEL), tendrá su domicilio en la Capital de la República y tendrá jurisdicción nacional en materia de regulación y control de las telecomunicaciones.

76.3. El órgano regulador estará sujeto a la fiscalización y control de la Contraloría General de la República.

⁷⁰⁷ Tribunal Constitucional República Dominicana., Sentencia núm. TC/0200/13 Disponible en: <https://www.tribunalconstitucional.gob.do/consultas/secretar%C3%ADa/sentencias/tc020013>. (Última verificación en línea 25 de mayo 2019).

disminuyendo su aplicabilidad, razones suficientes por la que el Consejo Directivo del INDOTEL interpuso la Resolución N.º 006-19, derogando la pasada Resolución N.º 086-11 y con ella el reglamento.

Siguiendo con lo estipulado en la sección III de la Ley núm. 172-13 se prohíbe a los medios de comunicación masivos, impresos, televisivos, radiales, electrónicos; la divulgación, publicación, reproducción, transmisión y la grabación del contenido parcial o total de un reporte de crédito.

Escapan a la presente ley los archivos de datos personales relativos a encuestas de opinión, mediciones y estadísticas, trabajos de prospección de mercados, investigaciones científicas, médicas y actividades análogas,

La ley contempla el establecimiento de códigos de conducta de práctica profesional elaborados por representantes de usuarios de bancos de datos de titularidad privada, cuya misión consiste en establecer los parámetros de tratamientos de los datos personales para asegurar y mejorar las condiciones en los sistemas de información bajo los principios de la presente ley.

La sección IV con el título de “otros datos” está compuesta de 5 artículos distribuidos en tres subsecciones. La primera subsección corresponde a “los datos especialmente protegidos” cuyo almacenamiento se encuentra prohibido, a menos que la persona física haya proporcionado su consentimiento de manera libre, consciente y voluntaria; sin embargo, las iglesias, las asociaciones religiosas, clínicas y hospitales podrán llevar un registro de sus miembros, solo con el consentimiento expreso y por escrito del afectado pueden almacenarse los datos personales que revelen opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e informaciones referente a la salud o la vida sexual.

Respecto a las infracciones penales solo serán comunicadas a los registros públicos cuando haya intervenido una apertura a juicio de conformidad por la ley.

La segunda subsección, compuesta de un solo artículo, trata sobre los “datos relativos a la salud” los cuales serán tratados por los profesionales de la salud, respetando los principios del secreto profesional.

La subsección III, bajo el título de “*tratamientos de datos de menores de edad*” normado por las disposiciones establecidas en el código bajo la protección de los derechos de los niños, niñas y adolescentes⁷⁰⁸, el código penal y otras leyes especiales.

La sección V denominada con el título “movimiento internacional de datos” establece que solo será posible con el consentimiento del titular cuando:

1. La persona física, libre y conscientemente, decidiera autorizar por voluntad propia la transferencia de datos, o cuando las leyes lo permitan.
2. Se trate de intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado o una investigación epidemiológica, o por razones de salud o higiene pública.
3. Se trate de transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable.
4. La transferencia de datos se hubiera acordado o contemplado en el marco de tratados internacionales o convenios, y en los tratados de libre comercio de los cuales sea parte la República Dominicana.
5. La transferencia de datos tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo, la trata de personas, el narcotráfico, y demás crímenes y delitos.
6. La transferencia de datos sea necesaria para la ejecución de un contrato entre el titular de los datos y el responsable del tratamiento, o para la ejecución de medidas precontractuales.

⁷⁰⁸ Ley núm. 136-03 Código para la protección de los derechos del niño, niña y adolescente.

7. La transferencia de datos legalmente exigida sea para la salvaguarda del interés público o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, o solicitada por una administración fiscal o aduanera para el cumplimiento de sus competencias.

8. La transferencia de datos se efectúe para prestar o solicitar un auxilio judicial internacional.

9. La transferencia de datos se efectúe a petición de un organismo internacional con interés legítimo desde un registro público.

El capítulo V bajo el título de “disposiciones de infracciones y sanciones”⁷⁰⁹, se encuentra compuesto de 9 artículos. Se crea la Superintendencia de Bancos como órgano competente para sancionar las infracciones administrativas de las Sociedades de Intermediación Crediticia (SIC), siendo éstas:

- a. Incluir en los reportes de crédito cualquiera de las informaciones prohibidas a las Sociedades de Información Crediticia (SIC), enumeradas en la presente ley.
- b. Negarse a facilitar el acceso a la información crediticia al titular de la misma.
- c. Denegar, sin fundamento, una solicitud de revisión o una solicitud de rectificación de la información crediticia requerida por el titular de la información.
- d. Negarse a modificar o a cancelar la información de un titular de la información, luego de que éste haya obtenido un pronunciamiento favorable en un procedimiento seguido de conformidad con lo establecido en la presente ley.

En caso de sanciones impuestas a las Sociedades de Intermediación Crediticia por la Superintendencia de Bancos, éstas pueden recurrir por ante la Junta Monetaria y, en caso de ser rechazada la impugnación o apelación, pueden recurrir ante el Tribunal Superior Administrativo o recurrir en casación.

⁷⁰⁹ El tema será desglosado más adelante, de todas formas, damos una pincelada al mismo.

Al mismo tiempo, existen sanciones excepcionales con multas que van desde diez (10) a cincuenta (50) salarios mínimos para aquellas personas físicas que:

1. Insertara o hiciera insertar, a sabiendas, datos falsos en un archivo de datos personales, de manera dolosa o de mala fe.
2. Proporcionará de manera dolosa o de mala fe, información falsa a un tercero, contenida en un archivo de datos personales.
3. Accediere a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, de cualquier forma, a un banco de datos personales.
4. Revelare a otra información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

El texto legislativo, contempla sanciones e infracciones civiles, dispuestas a continuación.

1. Denegar, sin fundamento, una solicitud de revisión o una solicitud de rectificación de la información crediticia requerida por el titular de la información.
2. Negarse a modificar o a cancelar la información de un titular de la información, luego de que éste haya obtenido un pronunciamiento favorable en un procedimiento seguido de conformidad con lo establecido en la presente ley.
3. Infringir de manera grave o reiterada las disposiciones de las sentencias de los tribunales civiles con la autoridad de la cosa irrevocablemente juzgada.

Las sanciones penales oscilan entre 10 a 50 salarios mínimos vigentes. Se conocen este tipo de sanciones cuando un usuario o suscriptor haya accedido a una base de datos para consultar de manera fraudulenta las informaciones de un titular, sin haber obtenido de este autorización previa o utilizar un reporte de la sociedad de información crediticia para cometer un crimen o un uso distinto al que se haya consignado en la autorización del cliente o consumidor con multa de diez a cien salarios, o haya accedido de manera fraudulenta la base de datos de una Sociedad de Información Crediticia para obtener y utilizar

cualquier tipo de reporte proveniente de una Sociedad de Información Crediticia, por medio del uso de claves de acceso que no le pertenecen, para ello se colocarán multas entre veinte y cien salarios mínimos vigentes.

En caso de violación de las disposiciones contenidas en la presente ley, se sancionará con prisión correccional de 6 meses a 2 años y una multa de cien (100), a ciento cincuenta (150) salarios mínimos vigentes.

Al mismo tiempo, será impuesta igual sanción para aquellos que divulguen, publiquen, reproduzcan, transmitan, o graben el contenido total o parcial de un reporte de cualquier uso proveniente de una Sociedad de Intermediación Crediticia (SIC). Debido a su importancia, al final de este capítulo del trabajo ampliaremos el tema de las penas y sanciones.

El capítulo VI bajo el título de “disposiciones transitorias y finales”, se compone de 2 secciones; la primera sección se refiere al tema de las disposiciones transitorias, puntualizando con los convenios internacionales quienes se regirán conforme a sus disposiciones. Al mismo tiempo, las Sociedades de Intermediación Crediticia (SIC) contarán con un plazo de seis meses a partir de la entrada de la presente ley para cumplir y ajustarse a lo previsto en la ley.

La sección II bajo el título de disposición final deroga en todas sus partes la Ley núm. 288-05 que regula las Sociedades de Intermediación Crediticia y de Protección al Titular de la Información, modificando toda aquella ley o parte de ley que le sea contraria.

Como conocemos, la actual ley de protección de datos y *habeas data*, surge a raíz de los dos proyectos existente en la Subcomisión. Por estas razones nos vemos obligados a realizar tales comparaciones, con la finalidad de identificar y determinar las conexiones con sus predecesoras. Por otra parte, y respondiendo al espíritu de esta investigación, también se realizará una comparación con las normas europeas que han influido en el escenario internacional, al ser consideradas modelo de referencia o marco regulativo para

las normas europeas, americanas y, -como no-, latinoamericanas envueltas en sus procesos transformacionales. Nos referimos, en este caso, a la comparación con la ley dominicana y las presentadas con anterioridad en el capítulo II: la Directiva 95/45 CE y el Reglamento 2016/679 UE.

3.2. Comparación de la Ley núm. 172-13 con sus predecesoras

Como comentamos previamente, la Ley núm. 172-13 surge a raíz de la presentación de dos iniciativas legislativas y una enmienda. La primera iniciativa fue propuesta por el actual senador de la provincia de San Juan de la Maguana perteneciente al Partido de la Liberación Dominicana (PLD) Félix Ramón Bautista Rosario; la segunda iniciativa corresponde al diputado por la provincia de Santiago, perteneciente al Partido de la Liberación Dominicana (PLD) Demóstenes William Martínez Hernández y la enmienda ha sido originada por la diputada al Congreso Nacional por la provincia Valverde, Sra. Johanny Mercedes Guzmán Rodríguez. miembro del Partido de la Liberación Dominicana . Las modificaciones fueron sometidas al conocimiento del pleno y aprobadas por las dos terceras partes de los diputados presentes. El proyecto aprobado corresponde al registro N.º 01198.

El proyecto convertido en ley contiene 91 artículos, a diferencia de la Iniciativa 4464 del senador Félix Ramón Bautista Rosario con 100 artículos y la Iniciativa 4589 del diputado Demóstenes William Martínez Hernández con 47 artículos. La Ley núm. 172-13 se apalanca en la Declaración Universal de Derechos Humanos, en la Constitución de la República, en leyes tales como la Ley núm. 200-04 de Libre Acceso a la Información Pública, la Ley núm. 288-05 que regula las Sociedades de Intermediación Crediticia y de Protección al Titular de la Información, completado con la Ley Orgánica del Tribunal Constitucional y de los Procedimientos Constitucionales núm. 137-11, la Ley núm. 19-01 que crea el Defensor del Pueblo. En sentido parecido, la iniciativa 4464 contempla aproximadamente esta mismas a las que acabamos de

referirnos pero, en cambio, la iniciativa 4589 se muestra desprovista de vistas, constituciones, leyes o reglamentos insertos durante su elaboración.

Después de abordar por separado los dos proyectos y la actual Ley de Protección Integral de los Datos Personales, pasamos a dilucidar y presentar sus principales diferencias relacionadas con los temas expuestos, ya que nuestra intención no es realizar una comparación capítulo por capítulo sino enfocarnos en los temas más trascendentes considerados en el trabajo. Pasamos a realizar tales comparaciones.

Las normas enunciadas carecen de uniformidad en cuanto a su forma y contenido pero, más allá de esas diferencias, cuentan con el desarrollo de temas comunes o coincidentes -mas no idénticos- como son sus principios, derechos, órgano de Control, transferencias internacionales, sanciones, entre otros.

Todos ellos (proyectos y normativa núm. 172-13) tienen en común la protección de los datos personales, concebidas a raíz del artículo 44 de la Constitución, referenciado a los derechos de intimidad y honor; presentando excepciones en la propuesta del proyecto del senador Félix Bautista, la cual, a pesar de no referir o hacer referencia en el proyecto, mantiene la intención en sus articulados. la Ley núm. 172-13 contempla entre sus objetivos la regulación de las Sociedades de Información Crediticia; el proyecto del senador Feliz Bautista realiza una referencia con el servicio crediticio de carácter patrimonial.

En igual contexto, en los proyectos de ley y actual normativa núm. 172-13 se contemplan los principios de calidad, derecho de información, consentimiento del afectado, seguridad de los datos, deber de secreto, confidencialidad y finalidad de los datos. A pesar de ello, no todos manifiestan de manera explícita los principios de licitud, legalidad, lealtad. Por su parte, los derechos de acceso, rectificación, supresión, actualización, incluida la acción de *habeas data* se observan en las normas planteadas.

De su lado, el órgano de control se mantiene vivo en los dos proyectos y la actual normativa núm. 172-13. Tanto en la normativa vigente como en el proyecto del diputado Demóstenes Martínez, se trata de un órgano carente de independencia funcional, administrativa y económica. No es éste el caso del proyecto del senador Feliz Bautista el cual plantea la instauración de la Agencia Dominicana de Protección de Datos, formado por un organismo independiente adscrito al Ministerio de la Presidencia, provisto de financiación, con presupuesto propio, contemplando las funciones del director del órgano de control. En este sentido, ha de ser considerado un documento muy completo en lo que a materialización o construcción del órgano de control se refiere.

En el siguiente cuadro comparativo, resaltamos los conceptos previamente enunciados y relevantes dispuestos en los proyectos y la actual Ley núm. 172-13, con la única intención de proveer otra vía de acceso a los mismos y de esa forma profundizar en su análisis.

Fig.4. Estudio Comparativo proyectos de ley y actual Ley de Protección de Datos.

Estudio Comparativo proyectos y actual Ley de Protección de Datos			
Disposiciones	Proyecto diputado Demóstenes Martínez	Proyecto diputado Félix Bautista	Actual Ley núm. 172-13
Objeto	✓	✓	✓
Protección de datos personales	✓	✓	✓
Artículo 44 Constitución	✓		✓
Derecho intimidad y honor	✓		✓
Artículo 70 de la Constitución	✓		✓
Regular las Sociedades de Información Crediticia			✓
Ámbito de aplicación	✓	✓	✓
Principios	✓	✓	✓

Licitud		✓	✓
Calidad	✓	✓	✓
Legalidad	✓		
Derecho de información	✓	✓	✓
Consentimiento del afectado	✓	✓	✓
Seguridad de los datos	✓	✓	✓
Deber de secreto / confidencialidad	✓	✓	✓
Lealtad		✓	✓
Finalidad de los datos	✓	✓	✓
Derechos	✓	✓	✓
Acceso	✓	✓	✓
Rectificación	✓	✓	✓
Cancelación-Bloqueo		✓	✓
Oposición		✓	✓
Supresión o Actualización	✓	✓	✓
Acción de <i>habeas data</i>	✓	✓	✓
Órgano de control	✓	✓	✓
Agencia Dominicana de Protección de Datos (adscrito al Ministerio de la Presidencia)		✓	
Dirección para la Protección de los Datos Personales (adscrito a la Procuraduría General de la República)	✓		
SúperIntendencia de Bancos (órgano de control)			✓
Independiente del órgano		✓	
Funciones del órgano	✓	✓	✓
Funciones del director del órgano		✓	

Financiación y presupuesto		✓	
Transferencias internacionales	✓	✓	✓
Niveles de protección	✓	✓	
Adecuado	✓		
Equivalente / Equiparable		✓	
Sanciones		✓	✓
Administrativas	✓	✓	✓
Civiles		✓	✓
Penales	✓	✓	✓

3.3. Comparación de la Ley núm. 172-13 y la Directiva 95/46/CE

De inicio, estamos en frente de dos normativas asimétricas o desiguales. A pesar de ello, contienen en sus plexos legislativos coincidencias estructurales comunes como son los considerandos, vistas, objeto, ámbito de aplicación, definiciones, principios, derecho de acceso, órgano de control, sanciones, transferencias de datos, mas no existe igualdad en los contenidos vertidos en sus disposiciones.

La Directiva 95/46 CE aplica a los datos personales sometidos al tratamiento automatizado o no automatizado, prevé los derechos de acceso, oposición; considerando las transferencias de datos a terceros Estados con adecuados niveles de protección, estableciendo excepciones en las transferencias, aceptando la implementación de códigos de conductas para la apropiada aplicación de las disposiciones nacionales a raíz del empleo de la Directiva, dispone la creación e instauración de autoridades de control independientes en los Estados, así como la creación del Grupo de Protección de Datos de naturaleza consultiva e independiente.

En tanto, la actual Ley núm. 172-13 se orienta a la protección de datos personales destinados a dar informes insertados en archivos sometidos a tratamientos de datos, regulando las Sociedades de Información Crediticia (SIC). En igual contexto, incluye los principios de licitud, calidad, derechos de información, consentimiento, seguridad, secreto, lealtad y finalidad de los datos dispuesto en la constitución y reflejado en la ley. Por otro lado, la normativa contempla la transferencia internacional de datos o movimiento internacional de datos, mas no presenta el nivel de protección requerido para el establecimiento de la transferencia. Esta norma tampoco contempla la instauración de un órgano de control independiente.

La norma núm. 172-13, a pesar de ser erigida 18 años después de la Directiva 95/46/CE, no contempla la instauración de órganos o autoridades independientes, careciendo del nivel de independencia económica y funcional que caracteriza a los órganos.

3.4. Comparación de la Ley núm. 172-13 con el Reglamento (UE) 2016/679

Al igual que las legislaciones expuestas previamente, el Reglamento (UE) 2016/679 y la normativa actual en materia de protección de datos de la República Dominicana presentan coincidencias estructurales en temas tales como vistas, objeto, ámbito de aplicación, definiciones, principios, derecho de acceso, órgano de control, sanciones, transferencias de datos.

El Reglamento implementa en sus nuevas disposiciones la ventanilla única, el consentimiento inequívoco (explícito), la supresión de datos (derecho al olvido), la portabilidad de los datos, la asunción del delegado de protección de datos, la protección de datos desde el diseño y por defecto, crea el Comité de Protección de Datos; al mismo tiempo, el Reglamento contempla la figura de un órgano de control independiente en cada uno de los Estados, con la posibilidad de contemplar más de una autoridad y en cuyo caso, asignar un órgano representativo para las demás autoridades.

Estamos delante de un Reglamento empapado y rodeado de las últimas tendencias y mejoras en materia de protección de las personas físicas en relación a la protección de datos, por lo que resulta totalmente necesario la incorporación de sus disposiciones -adecuándose a la realidad jurídica-social dominicana- en la futura reforma o adecuación de la actual normativa de *protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados*. Se muestra como vital para su acercamiento a los nuevos estándares y reformas vanguardistas en materia de protección de datos, producto a la complejidad, fortaleza y trayectorias previas de las normativas europeas materializada en su Reglamento⁷¹⁰.

El derecho a la intimidad, la privacidad y la información son derechos fundamentales y opuestos entre sí, visualizados en las normas europeas y en la actual ley de protección de datos, razones éstas que hacen necesario garantizar y amparar tales derechos fundamentales al momento de surgir conflictos entre ellos. Esto es así, pues no existen derechos absolutos. Por tanto, todos los derechos son limitados y ha de existir la posibilidad de ceder unos ante otros, orientándose a una conciliación u armonización con otros bienes, manteniendo un equilibrio entre ellos, evitando posible arbitrariedad entre los derechos (teoría de los límites inmanente)⁷¹¹.

4. Jerarquización de derechos fundamentales

El artículo 74 del capítulo III pertenece a los *principios de aplicación e interpretación de los derechos y garantías fundamentales* de la Constitución de

⁷¹⁰ El Reglamento provisto de 173 considerandos y 99 artículos, a diferencia de la normativa dominicana con 7 considerandos y 91 artículos.

⁷¹¹ MARTÍN RETORTILLO, L., DE OTTO y PARDO, I., *Derechos fundamentales y constitución*, 1ª ed. Civitas, S. A., Madrid, 1992, p. 110.

la República Dominicana del 2015. En él se establece la implementación y reglamentación de los derechos y garantías fundamentales reconocidos en la Constitución y compuesto por 4 puntos. Nos enfocaremos en dos de ellos (tercero y cuarto). El primero referenciado con el tercero apunta a los tratados, pactos y convenciones, cuyos tribunales y demás órganos del Estado asignan jerarquía constitucional y son de aplicación directa e inmediata; el segundo conectado con el cuarto se refiere a los poderes públicos, interpretando y aplicando las normas relativas a los derechos fundamentales y sus garantías, procurando armonizar los bienes e intereses protegidos por la Constitución en caso de conflicto entre derechos fundamentales⁷¹².

El numeral III asigna a los tratados, pactos y convenciones jerarquía con rango constitucional, cuando en materia de derechos y garantías fundamentales se trata, otorgando la oportunidad de reconocer con grado constitucional los tratados o acuerdos realizados con otros Estados. Es decir, que, ante la inexistencia de leyes o acuerdos internos, resulta válido aprobar las transferencias internacionales, materializadas por acuerdos realizados con otros Estados, fundamentado en la protección de los derechos fundamentales, recibiendo el apoyo y aprobación del Tribunal Constitucional.

Al mismo tiempo, el numeral cuatro asigna a los poderes públicos, incluido los jueces, la posibilidad de determinar, interpretar, ponderar la norma entre dos ocurrencias, colisiones, choques o coincidencias de derechos fundamentales para determinar cuál derecho fundamental prevalece en cada una de las situaciones analizadas. Es por ello, que somos de considerar y entrever la existencia de igualdad entre derechos fundamentales, asignando el mismo rango a cada derecho, evitando posibles peligros que pudieran orquestarse hacia ellos, producto de la intención e interés manifiesto del derecho de grupos colectivos en detrimento de los derechos individuales, exceptuando aquellos reclamos colectivos que pudieran beneficiar los derechos individuales⁷¹³. A raíz de ello, presentamos la siguiente colisión de derechos

⁷¹² Numeral 3 y 4, artículo 74 de la Constitución de la República Dominicana del 2015.

⁷¹³ FERNÁNDEZ ESTEBAN, M. L., *Nuevas tecnologías, Internet y Derechos Fundamentales*, Madrid, España, 1998, p. 124.

fundamentales contemplados en la actual ley de protección de datos personales, como son el secreto de los datos personales existentes en las Sociedades de Información Crediticia, y el derecho a la información, situación observada en la presente acción de inconstitucionalidad presentada por diversas organizaciones a la Ley núm. 172-13 de protección de datos personales.

5. Acción directa de inconstitucionalidad contra artículos de la Ley núm. 172-13

La Sentencia núm. TC/0484/16⁷¹⁴ se fundamenta en el Expediente núm. TC-01-2014-0010⁷¹⁵ sobre control concentrado de constitucionalidad, depositado el 17 de marzo de 2014 por los recurrentes Namphi A. Rodríguez⁷¹⁶, Domingo Porfirio Rojas Nina⁷¹⁷, José Gregorio Cabrera⁷¹⁸, Fundación Prensa y Derecho, Consejo Dominicano de Derechos Humanos (CODEH) y la Alianza Ciudadana para Los Derechos Fundamentales, publicado en la página del Tribunal Constitucional de la República Dominicana el 15 de julio 2014 a la 3:23 Pm, las normas atacadas son el artículo 4, párrafo segundo⁷¹⁹; artículo 5, numeral 6, literal C⁷²⁰; artículo 8, párrafo tercero⁷²¹, artículo 10, párrafo cuarto⁷²²; y

⁷¹⁴ *Tribunal Constitucional de la República Dominicana*. Disponible en: <https://www.tribunalconstitucional.gob.do/sites/default/files//documentos/TC-0484-16.pdf>. (Última consulta en línea 14 octubre de 2016).

⁷¹⁵ *Tribunal Constitucional de la República Dominicana*. Disponible en: <https://www.tribunalconstitucional.gob.do/node/2504>. (Última consulta en línea 14 de octubre 2016).

⁷¹⁶ Presidente de la Fundación Prensa y Derecho Inc.

⁷¹⁷ Presidente del Consejo Dominicano de Derechos Humanos (CODEH).

⁷¹⁸ Coordinador Alianza Ciudadana para los Derechos Fundamentales.

⁷¹⁹ Artículo 4.- Restricciones.

2. A los archivos de datos personales establecidos por los organismos de investigación y de inteligencia de la República Dominicana encargados de la prevención, persecución y castigo de los crímenes y delitos.

⁷²⁰ Artículo 5.- Principios.

artículo 25 numeral 13⁷²³, artículo 29⁷²⁴, artículo 40⁷²⁵ y artículo 48⁷²⁶ de la Ley Orgánica sobre Protección de Datos de Carácter Personal (Ley núm. 172-13),

c) Fuera de los fines establecidos en esta ley, se prohíbe la divulgación, la publicación, la reproducción, la transmisión y la grabación del contenido parcial o total de un reporte de cualquier tipo proveniente de una Sociedad de Información Crediticia (SIC), referente a un titular de los datos, en cualquiera de sus manifestaciones, en cualquier medio de comunicación masivo, sea impreso, televisivo, radial o electrónico.

⁷²¹ Artículo 8.- Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

En el supuesto de cesión o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro de cinco (5) días hábiles de efectuado el tratamiento del dato.

⁷²² Artículo 10.- Derecho de acceso.

El usuario del banco de datos debe proporcionar la información solicitada por el titular de los datos dentro de cinco (5) días hábiles posteriores a haber sido hecha de manera personal dicha solicitud, o vía acto de alguacil. Vencido el plazo sin que se satisfaga el pedido, el titular de los datos podrá incoar una acción judicial ante un juzgado de primera instancia para conocer de la existencia y acceder a los datos que de él consten en registros o bancos de datos públicos o privados, conforme al procedimiento previsto en esta ley.

⁷²³ Artículo 25.- Procedimiento de reclamación aplicable a las Sociedades de Información Crediticia (SIC) para la modificación, rectificación y cancelación de la información del titular.

13. El titular de los datos que se considere afectado por una información contenida en un reporte proveniente de una Sociedad de Información Crediticia (SIC) tiene un plazo de diez (10) días hábiles, contados a partir de haber agotado el procedimiento de reclamación estipulado en la presente ley, para iniciar su acción por ante los tribunales competentes. Después de haber agotado el procedimiento de reclamación aplicable a la Sociedad de Información Crediticia (SIC), sea este interpuesto por una persona física o jurídica, y después de que la Sociedad de Información Crediticia (SIC) haya cumplido con los requerimientos especificados en este artículo, la Sociedad de Información Crediticia (SIC) queda exenta de responsabilidad.

⁷²⁴ Artículo 29.- Naturaleza. Los archivos, registros o bancos de datos, públicos o privados, destinados a proveer informes crediticios estarán sujetos a la inspección y vigilancia de la Superintendencia de Bancos como órgano de control.

El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos, tendrá las siguientes funciones y atribuciones:

1. Asistir y asesorar a las personas físicas que lo requieran acerca de los alcances y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza.
2. Imponer las sanciones administrativas que en su caso correspondan por violación a las normas establecidas.

⁷²⁵ Artículo 40.- Ficheros de las Fuerzas Armadas, de seguridad y organismos policiales o de inteligencia. Los archivos de datos personales creados por las Fuerzas Armadas, de seguridad y organismos policiales o de inteligencia que contengan datos de carácter personal que, por

ya que, de acuerdo a los recurrentes, viola las siguientes disposiciones constitucionales exhibidas en los artículos 8, 38, 40 numeral 13 y 15, 43, 44 numeral 2, 49, 68, 69, 70 y 74 numeral 2 de la Constitución de la República Dominicana.

Los accionantes solicitan⁷²⁷ entre otras cosas, una sentencia *interpretativa*⁷²⁸ para el artículo 4 párrafo segundo, artículo 5 numeral 6 literal c, artículo 8 párrafo tercero, artículo 10 párrafo cuarto, artículo 25 numeral 13, artículo 40 y 88 de la Ley Orgánica sobre Protección de Datos de Carácter Personal (Ley núm. 172-13) para que sean considerados conformes a los artículos 8, 38, 43, 44 numeral 2, artículos 49, 68, 69, 70, 74 numeral 2 de la Constitución de la República. Esta solicitud de sentencia *exhortativa*⁷²⁹ es para que se otorgue un plazo de un (1) año al Congreso Nacional a fin de que modifique el artículo 29 de la Ley Orgánica sobre Protección de Datos de Carácter Personal (Ley núm. 172-13) con el objetivo de crear un órgano rector independiente que guarde vinculación con los derechos fundamentales tutelados en la misma. También se solicita para garantizar la conformidad de dicha norma con las disposiciones contenidas en los artículos 8 y 68 de la Constitución y para que se declare la inconstitucionalidad del artículo 88 por violar el principio legal penal, contenido en los artículos 40 (numerales 13 y 15) y 69 (numeral 7) de la Constitución de la República.

haberse recogido para fines administrativos, deban ser objeto de registro permanente, no están sujetos al régimen general de la presente ley.

⁷²⁶ Artículo 48.- Derechos de acceso, rectificación o cancelación. Cuando el interesado ejerza su derecho de acceso en relación con la inclusión de sus datos en un archivo de datos personales común de información de crédito, se registrará según lo establecido en la presente ley.

⁷²⁷ *Acción directa de inconstitucionalidad contra la ley orgánica sobre protección de datos de carácter personal (Ley núm. 172-13)*. Disponible en: <http://www.prensayderecho.org/descargas/category/2-acciones-procesales#>. (Última consulta en línea 14 de octubre 2016).

⁷²⁸ Cursiva nuestra.

⁷²⁹ *Acción directa de inconstitucionalidad contra la ley orgánica sobre protección de datos de carácter personal (Ley núm. 172-13)*. Disponible en: <http://www.prensayderecho.org/descargas/category/2-acciones-procesales#>. (Última consulta en línea 14 de octubre 2016).

El Tribunal Constitucional, luego de analizar la acción, declara que los artículos 5.6.c, 8 y 29 de la Ley núm. 172-13, sobre la Protección de Datos de Carácter Personal, del quince (15) de diciembre de dos mil trece (2013), son conformes con la constitución. El órgano de control se mantiene intacto sin modificaciones, sin dejar de lado la no independencia del órgano, punto neurálgico al momento de tomar decisiones debido a la fortaleza económica e institucional, liberándola de todo compromiso con órganos superiores, contribuyendo con ello al clima de transparencia del órgano, un órgano llamado a proteger al usuario, asegurando con ello la salvaguarda de la persona física, a raíz de la protección de los datos almacenados en archivos privados y públicos destinados a dar informes.

En ese sentido, con la decisión, el Tribunal mantiene el secreto de los datos personales existentes en las Sociedades de Información crediticia, prohibiendo su divulgación por los diferentes medios de comunicación. Asimismo, mantiene el tiempo de 5 días contemplados en la ley para notificar al cesionario del dato sobre la rectificación o supresión del dato; y como hemos comentado mantiene el rol de la Superintendencia de Bancos como órgano de control, debido a que entre sus roles se encuentra el de mantener un registro de las transacciones financieras vinculado a la aplicación del secreto bancario cuya finalidad es la de proteger la intimidad conectada como derecho fundamental a la dignidad de las personas. Esto es así entendido desde la perspectiva de que la Ley núm. 172-13 tiene como objetivo principal la protección de aquellos datos vinculados a la actividad financiera.

En el caso de los artículos 4.2 y 40 de la Ley núm. 172-13, ambos basados en restricciones para con la ley, -el primero relacionado con la aplicación de la ley a los organismos de investigación e inteligencia, y el segundo dirigido a los archivos de datos personales recogidos para fines administrativos por las fuerzas armadas, de seguridad y organismos policiales o de inteligencias-, las restricciones solo aplicarán cuando pueda constituirse en un obstáculo para el cumplimiento de las delicadas funciones que tienen dichos organismos.

“Se establece que para que el artículo 88 de la Ley núm. 172-13, sobre la Protección de Datos de Carácter Personal, del quince (15) de diciembre de dos mil trece (2013), sea conforme con la Constitución, debe tener el contenido siguiente: El suscriptor o afiliado, el cliente o consumidor, los representantes de las entidades públicas, o cualquier persona física o jurídica que viole las disposiciones contenidas en la presente ley, será sancionada con prisión correccional de seis (6) meses a dos (2) años, y una multa de cien (100) a ciento cincuenta (150) salarios mínimos del sector público. Estas sanciones serán aplicadas en los casos en que no exista otro texto en la misma ley que establezca una sanción menor. Igual sanción será impuesta a quien, fuera de los fines establecidos en esta ley, divulgue, publique, reproduzca, transmita o grave el contenido parcial o total de un reporte de cualquier tipo proveniente de una Sociedad de Información Crediticia (SIC), referente a un titular de los datos, en cualquiera de sus manifestaciones, en cualquier medio de comunicación masiva, sea impreso, televisivo, radial o electrónico⁷³⁰”.

Continúa diciendo:

“...que para que el artículo 10 de la Ley núm. 172-13, sobre la Protección de Datos de Carácter Personal, del quince (15) de diciembre de dos mil trece (2013), sea conforme con la Constitución debe tener el contenido siguiente: El usuario del banco de datos debe proporcionar la información solicitada por el titular de los datos dentro de cinco (5) días hábiles posteriores a haber sido hecha de manera personal dicha solicitud, o vía acto de alguacil. Vencido el plazo sin que se satisfaga el pedido, el titular de los datos podrá incoar una acción judicial ante un juzgado de primera instancia para conocer de la existencia y acceder a los datos que de él consten en registros o bancos de datos públicos o privados, conforme al procedimiento previsto en esta ley. No obstante, lo anterior, el procedimiento administrativo indicado no es preceptivo sino facultativo⁷³¹”.

Finalmente establece:

“...Que para que el artículo 25.13 de la Ley núm. 172-13, sobre la Protección de Datos de Carácter Personal, del quince (15) de diciembre de dos mil trece (2013), sea conforme con la Constitución debe tener el contenido siguiente: El titular de los datos que se considere afectado por una información contenida en un reporte

⁷³⁰ *Tribunal Constitucional de la República Dominicana Sentencia núm. TC/0484/16*, p. 53. Disponible en: <https://www.tribunalconstitucional.gob.do/sites/default/files//documentos/TC-0484-16.pdf>. (Última consulta en línea 14 de octubre 2016).

⁷³¹ *Tribunal Constitucional de la República Dominicana Sentencia núm. TC/0484/16*, p. 53. Disponible en: <https://www.tribunalconstitucional.gob.do/sites/default/files//documentos/TC-0484-16.pdf>. (Última consulta en línea 14 de octubre 2016).

proveniente de una Sociedad de Información Crediticia (SIC) tiene un plazo de diez (10) días hábiles, contados a partir de haber agotado el procedimiento de reclamación estipulado en la presente ley, el cual no es preceptivo sino facultativo, para iniciar su acción por ante los tribunales competentes. Después de haber agotado el procedimiento de reclamación aplicable a la Sociedad de Información Crediticia (SIC), sea este interpuesto por una persona física o jurídica, y después de que la Sociedad de Información Crediticia (SIC) haya cumplido con los requerimientos especificados en este artículo, la Sociedad de Información Crediticia (SIC) queda exenta de responsabilidad⁷³² ”.

La actual Sentencia núm. TC/048/16 del Tribunal Constitucional es originada vía la acción directa de inconstitucionalidad interpuesta, contemplando temas y sanciones considerados en la Ley núm. 172/13, el Código Penal y su Ley núm. 550-14, comentada a continuación.

6 Tutela jurídica de los principios de protección de datos

La vulneración de los derechos reconocidos en la Ley núm. 172/13 pueden ser objeto de reclamaciones a instancia del afectado o los afectados. En ese sentido, les corresponde a los órganos de jurisdicción ordinaria cuando se trate de ficheros de titularidad privada, o al Tribunal Superior Administrativo, cuando sean archivos de titularidad pública o acciones ante el órgano de control. Por su parte, la tutela de carácter penal se encuentra bajo el amparo del Código Penal y su Ley núm. 550-14.

En tanto, las personas físicas o jurídicas pueden solicitar al Defensor del Pueblo la imposición de una acción de amparo para reclamar o demandar sus derechos fundamentales tutelados en la constitución y las leyes⁷³³. Una calidad

⁷³² *Tribunal Constitucional de la República Dominicana Sentencia núm. TC/048/16*, p. 54. Disponible en: <https://www.tribunalconstitucional.gob.do/sites/default/files//documentos/TC-0484-16.pdf>. (Última consulta en línea 14 de octubre 2016).

⁷³³ Artículo 68, Ley núm. 167-11.

interpuesta en la referida ley, instituyendo o asignando desde la óptica constitucional al Defensor del Pueblo⁷³⁴, un órgano creado para proteger, defender, amparar y garantizar los mencionados derechos dispuestos en la carta sustantiva; el Defensor del Pueblo se constituye en una autoridad independiente en funciones, gozando de presupuesto propio e independencia administrativa⁷³⁵.

La Ley núm. 172-13 contempla el empleo de una autoridad judicial para interponer una acción, y con ello, solicitar o reclamar los llamados derechos de los interesados (ARCO) etc., contemplando en la propia ley la acción de *habeas data* o .como la misma ley señala, la acción de protección de datos personales, pensada, entendida, percibida de igual forma, utilizada indistintamente para el reclamo o solicitud de las acciones judiciales, correspondiente al juez del domicilio del demandado⁷³⁶ tutelando e imponiendo sanciones a las infracciones generadas y puestas a continuación.

6.1. Tutela de carácter administrativo

A raíz del artículo 29, la Superintendencia de Bancos es el órgano de control seleccionado para sancionar las infracciones administrativas cometidas por las Sociedades de Información Crediticia, siendo estas infracciones las siguientes.

- Incluir en los reportes crediticios las informaciones prohibidas a las Sociedades de Información Crediticia (SIC).
- Negar el acceso del titular a la información crediticia.
- Denegar revisión o rectificación de información crediticia del titular sin fundamento.

⁷³⁴ Título VIII del Defensor del Pueblo. *Constitución de la República Dominicana del 2015*.

⁷³⁵ Artículo 190-191 *Constitución de la República Dominicana del 2015*.

⁷³⁶ Artículo 20, Competencia, Ley núm. 172-13.

- Negar a modificar o cancelar información del titular a pesar de pronunciamiento favorable.

Al mismo tiempo, el órgano de control impondrá a las Sociedades de Información Crediticia las siguientes sanciones administrativas.

- Cuando infrinjan sentencias irrevocables imponiendo multas de diez (10) a cien (100) salarios.
- Cuando no inicien sus operaciones a partir de los 6 meses de su aprobación.

De igual forma, se contemplan sanciones excepcionales, interponiendo penas de 10 a 50 salarios mínimos por daños sufridos a las personas, por causa de violación al derecho a la privacidad, de acuerdo a las normas del derecho común, siempre que las personas físicas.

- Insertara datos falsos en archivo de datos personales.
- Proporcionará información falsa a un tercero de manera dolosa o de mala fe.
- Accediere a un banco de dato personal de forma ilegítima.
- Revelare información de bancos de datos personales destinados a mantenerse en secreto.

6.2. Tutela de carácter civil

De conformidad con el artículo 85 de la Ley núm. 172-13, se prevé un sistema de responsabilidades civiles, aplicable a las siguientes infracciones civiles:

- Se deniegue solicitud de revisión, rectificación de la información crediticia solicitada por su titular.
- Se niegue a modificar o a cancelar la información del titular de la información a partir de un pronunciamiento favorable.
- Infrinja de manera grave o de forma reiterada las sentencias irrevocables.

6.3. Tutela de carácter penal

Conforme a lo estipulado en el artículo 86 de la Ley núm. 172-13 se contemplan sanciones penales. A pesar de ello, realizaremos ciertas puntualizaciones orquestadas en el Código Penal de la República Dominicana y la Ley núm. 550-14, una ley llamada a revisar y actualizar las sanciones penales contempladas en el código penal.

La Ley contempla sanciones en los siguientes supuestos.

- Multas de 10 a 50 salarios mínimos vigentes para quienes accedan a bases de datos de forma fraudulenta, sin el consentimiento del titular.
- Prisión correccional a quien utilice o facilite sin consentimiento un reporte de crédito proveniente de una Sociedad de Información Crediticia (SIC), para los fines de cometer un delito se establecerán sanciones de prisión correccional de seis meses a 2 años y si es para cometer un crimen, se establecerán las sanciones contempladas en el Código Penal, al mismo tiempo se considerará circunstancia agravante cuando el usuario haga uso del reporte para cometer el crimen.
- Multas de 10 a 100 salarios mínimos vigentes para aquellos que den un uso diferente al presentado en la autorización del cliente o consumidor.

De acuerdo a lo contemplado en el artículo 87 de la Ley núm. 172-13, se establecen multas que van de los 20 a 100 salarios mínimos vigentes para aquellas personas que accedan de manera fraudulenta a las bases de datos de una sociedad de información crediticia por medio al uso de claves de acceso que no le pertenecen.

En caso de usar el reporte para la comisión de un delito, se establecerá sanción equivalente a prisión correccional de 6 meses a 2 años y en caso de ser usado para un crimen, se sancionará de acuerdo a lo estipulado en el Código Penal presentado a continuación.

6.3.1. Penas y sanciones

El actual Código Penal de la República Dominicana⁷³⁷, no es representativo de las necesidades de prevención, control y represión de las infracciones que se presentan en la sociedad y el mundo real, así como de la necesidad de aumentar la protección de las personas, la preservación de la convivencia social y la seguridad jurídica. Estos son algunos de los considerandos que dieron pauta a la elaboración de la Ley núm. 550-14, una ley llamada a revisar, actualizar, incorporar nuevos tipos y sanciones penales al Código. La ley establece una profunda revisión y actualización de los tipos y penas previstas en el código vigente. Para ello fueron vistas varias normas jurídicas, entre ellas, la Constitución del 26 de enero de 2010, una constitución avezada con los nuevos aires constitucionales en materia de protección, tutela y salvaguarda de los derechos fundamentales⁷³⁸ de las personas. La ley incorpora los derechos de tercera generación como intimidad, privacidad, protección de datos, estableciendo sanciones para esos derechos en la vigente ley⁷³⁹.

Las infracciones contra la vida privada se ubican en el capítulo VI bajo el título de *las Infracciones contra la personalidad*, agrupando los *atentados contra la intimidad, la vida privada* en la sección I y en la sección II, las infracciones contra las personas por medio al uso de imágenes, sonidos o montajes En ese sentido podemos ver las infracciones contra el secreto de correspondencia o documentos privados bajo la subsección II, y en la sección IV, las infracciones contra las informaciones privativas de las personas

⁷³⁷ Código Penal de la República Dominicana promulgado mediante Decreto-Ley núm. 2274 del 20 de agosto de 1884.

⁷³⁸ Artículo 1. Aplicación de derechos fundamentales. Este código reconoce y aplica los derechos fundamentales de la persona, consagrados en la Constitución de la República y en los tratados internacionales aprobados por el Congreso Nacional, así como las interpretaciones hechas a éstos por los órganos jurisdiccionales competentes, sin perjuicio de otros derechos de igual naturaleza reconocidos por el derecho penal.

⁷³⁹ Cfr. Considerando primero, segundo, sexto de la *Ley núm. 550-14 que establece el Código Penal de la República Dominicana*. Disponible en: <https://oig.cepal.org/sites/default/files/251865974-ley-no-550-14-que-establece-el-codigo-penal-de-la-republica-dominicana.pdf>. (Última consulta en línea 11 de mayo 2018).

registradas en catálogos, ficheros o sistemas automatizados de datos incluyendo la sanción por captación y uso de datos personales.

El Código Penal de la República Dominicana reformado mediante Ley núm. 550-14, establece sanciones de 1 a 2 años de prisión menor con multas de 3 a 6 salarios mínimos del sector público para las personas que recojan, recolecten, conserven, accedan o divulguen datos personales procedentes de procedimientos automatizados de datos personales de otras personas sin su consentimiento y de manera dolosa, exceptuando la obtención de aprobaciones previa ya sean estas procedentes de una autoridad legal o judicial. De igual forma las personas jurídicas son penalmente responsables, contemplando las sanciones tipificadas en el Código para las personas jurídicas, con sanciones que van desde multas, penas complementarias y disolución legal de la persona jurídica.

Al mismo tiempo, la referida ley contempla sanciones para aquellas infracciones cometidas imprudentemente, otorgando sanciones que van desde los 2 a 3 salarios mínimos fundamentado en el sector público.

Debemos contextualizar que las infracciones son de aplicabilidad tanto para los procedimientos automatizados como para los contemplados en catálogos, ficheros, a pesar de no ser referido en el capítulo más sí en el título de la sección IV de las *infracciones contra las informaciones privativas de las personas registradas en catálogos, ficheros o sistemas automatizados de datos, siendo infracciones públicas a instancias privadas.*

En la referida ley, las infracciones contra la personalidad, orientadas a la vida privada, no solo se refiere a los datos personales, sino que al unísono de la Constitución y siguiendo la estructura establecida en la Constitución del 2010, se abordan los derechos de intimidad, vida privada, imagen, sonido, al igual que la violación de los medios empleados para su distribución como sobres, llamadas telefónicas usando medios tales como las telecomunicaciones, el ciberespacio.

En ese sentido se plantean infracciones de 2 a 3 años para las personas que atenten contra la intimidad de la vida privada de otra persona, sin su consentimiento o presunción de consentimiento⁷⁴⁰, ya sea por medio a captar, conservar, registrar, confundir, difundir, transmitir palabras pronunciadas en privado o de manera confidencial o imagen tomadas de lugares privados⁷⁴¹ aplicando sanciones de 2 a 3 años de prisión y multas de 7 a 9 salarios mínimos del sector público. En ese sentido, también aplican sanciones para los fabricantes o comercializadores de aparatos que atenten contra la vida privada sin autorización oficial previa, cuya finalidad sea la de atentar contra la intimidad de la vida privada, aplicando sanciones de un día a un año con multas que van desde uno a dos salarios mínimos del sector público.

En igual contexto, se contemplan sanciones por difusión de imágenes que oscilan desde un día a un año de prisión, con multas que van de uno a dos salarios mínimos perteneciente al sector público con penas inferiores a las presentadas en los casos anteriores, siendo esta una acción penal a instancia privada. En ese sentido, las penas son de aplicabilidad para las personas jurídicas cuyas infracciones corresponden a las establecidas en la ley para estos tipos de situaciones, cabe recordar el caso de *Warren y Brandeis* comentado en el primer capítulo, representativo de la *privacy* americana, fundamentado en la publicación de imágenes fotográficas tomadas por la prensa en los eventos privados de la alta sociedad estadounidense, difundidas sin consentimiento expreso.

En el caso de las sanciones aplicadas por violación de correspondencia, ya sea por abrir, suprimir, distraer las correspondencias o documentos privados dirigidos a un tercero, las sanciones aplicadas superan a la de la imagen, siendo esta de 2 a 3 años de prisión menor y multa de 7 a 9 salarios mínimos

⁷⁴⁰ Artículo 200. Presunción de consentimiento.

Si uno de los actos incriminados en el Artículo 199 (visto en el mismo párrafo) se comete a la vista y a sabiendas del interesado, y éste no expresa oposición estando en capacidad de hacerlo, se presumirá su consentimiento.

⁷⁴¹ Encontrada en algún lugar privado.

del sector público, de igual forma aplica cuando se empleen medios telemáticos, telecomunicaciones o el ciberespacio para captar correspondencia o documentos privados⁷⁴².

Vemos que, a pesar de contemplar temas tales como intimidad, vida privada, datos personales. En la presente ley se realiza una separación de los términos empleados, así como queda establecido en el capítulo VI orientado a la personalidad.

En otro orden, el desarrollo, auge y evolución de las telecomunicaciones de información y comunicaciones crea el escenario propicio para la incursión de nuevos delitos sustentados en la base tecnológica existente y en continuo crecimiento. Un escenario apropiado para la incursión de la Ley núm. 53-07 en el escenario dominicano debido a la ausencia de normativas capaces de contrarrestar esos delitos tecnológicos de ámbito nacional e internacional⁷⁴³. Lo que a su vez permite un acercamiento con las estrategias globales de seguridad cibernética⁷⁴⁴; teniendo como objeto la protección de los sistemas en riesgos, para ello, cuenta con la capacidad de disponer e implementar sanciones y medidas de prevención⁷⁴⁵.

⁷⁴² Artículo 209 y párrafo I, Ley núm. 550-14.

⁷⁴³ Considerando cuarto, Ley núm. 53-07 sobre Crímenes y Delitos de Alta Tecnología. Disponible en: https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf (Última consulta en línea 22 de mayo 2019).

⁷⁴⁴ Considerando quinto, Ley núm. 53-07.

⁷⁴⁵ Artículo 8, 9, 10, Ley núm. 53-07.

Artículo 8.- Dispositivos Fraudulentos. El hecho de producir, usar, poseer, traficar o distribuir, sin autoridad o causa legítima, programas informáticos, equipos, materiales o dispositivos cuyo único uso o uso fundamental sea el de emplearse como herramienta para cometer crímenes y delitos de alta tecnología, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo.

Artículo 9.- Interceptación e Intervención de Datos o Señales. El hecho de interceptar, intervenir, injerir, detener, espiar, escuchar, desviar, grabar u observar, en cualquier forma, un dato, una señal o una transmisión de datos o señales, perteneciente a otra persona por propia cuenta o por encargo de otro, sin autorización previa de un juez competente, desde, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones, o de las emisiones originadas por éstos, materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas físicas o morales, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo, sin

6.3.2. Código Penal

El propio Código Penal de la República Dominicana establece entre sus articulados penas para las personas que descubran y divulguen secretos de otros, ubicados en papeles y cartas, obtenidos por medio a su apropiación, siendo reducidas las penas cuando no sean divulgados su contenido. En ese sentido, los documentos mencionados contienen datos personales, siendo aplicables las sanciones previstas en la Ley núm. 550-14 ya presentadas⁷⁴⁶ disponiendo de un año de prisión menor y multa de uno a dos salarios del sector público a los infractores. A pesar de ello, la ley contempla excepciones por medio a la cual pueden realizarse tales revelaciones⁷⁴⁷.

perjuicio de las sanciones administrativas que puedan resultar de leyes y reglamentos especiales.

Artículo 10.- Daño o Alteración de Datos. El hecho de borrar, afectar, introducir, copiar, mutilar, editar, alterar o eliminar datos y componentes presentes en sistemas electrónicos, informáticos, telemáticos, o de telecomunicaciones, o transmitidos a través de uno de éstos, con fines fraudulentos, se sancionará con penas de tres meses a un año de prisión y multa desde tres hasta quinientas veces el salario mínimo

⁷⁴⁶ Art. 378, Código penal de la República Dominicana. Disponible en: https://www.oas.org/juridico/mla/sp/dom/sp_dom-int-text-cp.pdf. (Última consulta en línea 11 de mayo 2018).

⁷⁴⁷ Artículo 208, Ley núm. 550-14.

1) Si la ley impone o autoriza la divulgación del secreto.

2) Si el secreto es divulgado al Ministerio Público u otra autoridad judicial o administrativa competente por una persona con el deber de guardar secretos en razón de su profesión u oficio, siempre que se cuente con el consentimiento de la víctima, y que se trate de sevicias comprobadas en el ejercicio de la profesión u oficio, que hacen presumir la comisión de violencias sexuales o físicas contra la víctima, o cualquier otra infracción grave.

3) Cuando una persona, en razón de su profesión u oficio y en el deber de guardar secretos, informa al Ministerio Público u otra autoridad judicial o administrativa competente acerca de la ocurrencia de atentados sexuales u otras sevicias, así como de cualquier otra infracción grave infligidas a un niño, niña o adolescente o contra una persona que no esté en condiciones de protegerse en razón de su edad o estado físico o síquico.

CAPÍTULO IV

REFLEXIONES EN TORNO AL ÓRGANO DE CONTROL COMO VIGILANTE OMNIPRESENTE EN LAS TRANSFERENCIAS INTERNACIONALES EN EUROPA Y LATINOAMERICA, CON ESPECIAL ATENCIÓN EN LA REPÚBLICA DOMINICANA

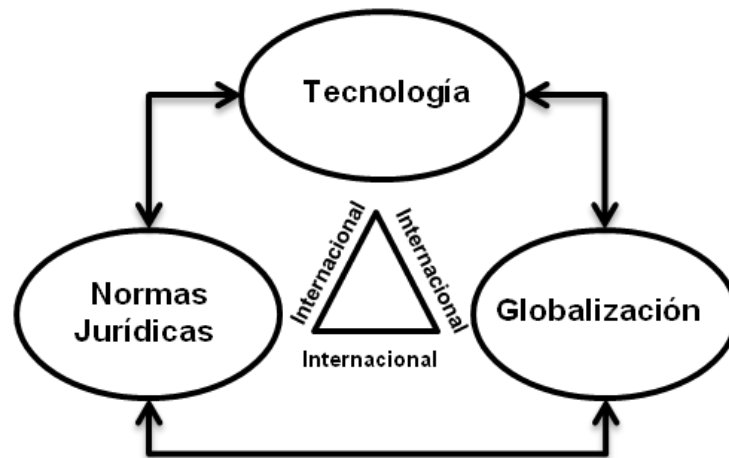
1. EL ÓRGANO DE CONTROL Y LAS TRANSFERENCIAS INTERNACIONALES EN LAS NORMAS JURÍDICAS EUROPEAS Y LATINOAMERICANAS. REFLEXIONES OMNIPRESENTE.

1. Consideraciones iniciales

Durante el desarrollo del trabajo, hemos sido partícipes de la concatenación y el carácter vinculante entre tecnología–globalización–normas jurídicas; reconociendo su estrecha vinculación de manera casi simultánea y en ambos sentidos, adquiriendo el carácter internacional a raíz del crecimiento de las mismas, sobrepasando su connotación nacional, entrando en terreno internacional⁷⁴⁸ y global, fruto de su expansión, tal como queda reflejado a continuación.

⁷⁴⁸ Cfr. "...como consecuencia de la internacionalización, la nación ya no tiene límites en el territorio del Estado y eso implica que el conocimiento no se restringe al medio, sino que se extiende a todo el planeta, porque el mundo del conocimiento no tiene fronteras. Este panorama también está impregnado por la tecnología...", TRAVIESO, J. A (Director), *Derecho Internacional 2-0*, visto en *Régimen Jurídico de los Datos Personales*, tomo I, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014, p. 31.

Figura 5. Vinculación entre tecnología, normas jurídicas, globalización.



En capítulos anteriores abordamos los temas de protección de datos personales y el *habeas data* en los escenarios de la Unión Europea, Convenio de Europa, OCDE etc. En este lugar, nos detendremos en aquellas legislaciones nacionales e internacionales⁷⁴⁹ conectadas con el órgano de control y las transferencias internacionales (entre ellas, directivas, reglamentos, convenios y leyes nacionales, incluidas las correspondientes a los Estados Iberoamericanos). Estos Estados se encuentran, además, en distintas situaciones. Nos encontramos, así, con países que aún no han desarrollado sus legislaciones internas o con Estados que, a pesar de poseer legislaciones nacionales relacionadas con el órgano de control y con las transferencias internacionales, no cuentan con los últimos avances legislativos en materia de órgano de control y transferencias internacionales de datos, siendo instituidas, reconocidas y aceptadas por organismos internacionales, entornos europeos y latinoamericanos.

⁷⁴⁹ “Varios países cuentan con regulaciones generales y sectoriales, así como jurisprudencia sobre tratamiento de datos personales. Aunque se ha procurado armonizar internacionalmente los principales aspectos sobre el tratamiento de datos personales, en la práctica cada estado cuenta con normas que parcialmente siguen documentos Internacionales pero que al mismo tiempo están impregnadas de las particularidades sociales, políticas, culturales, y jurídicas de cada uno...”, REMOLINA ANGARITA, N., *Recolección Internacional de datos personales: un reto del mundo post-internet*, 1ª ed. Agencia Española de Protección de datos, Madrid, 2015, p. 43.

Una situación que nos obliga a permanecer en el modelo europeo⁷⁵⁰. Este modelo está dotado de normas generales y específicas en materia de protección de las personas físicas en relación con el tratamiento de los datos personales y su libre circulación; con organismos capaces de tutelar tanto desde la órbita de los Estados, como desde las organizaciones llamadas a proteger a las personas físicas con relación a sus datos personales en el ámbito europeo (Consejo de Europa, las autoridades de control de los Estados pertenecientes a la Unión Europea⁷⁵¹, el Comité, la Comisión, etc.).

Por su parte, Latinoamérica se encuentra inmersa en la construcción de su Estándar⁷⁵² en materia de protección de datos, un Estándar vinculado con la tecnología y su tendencia transnacional o global.

En cambio, la tecnología se desplaza a todos los Estados del globo terráqueo, tornándose global y única. En ese sentido, el Estándar o normativa jurídica debe adquirir el carácter global, convirtiéndose en uno solo⁷⁵³, transitando en los Estados desde sus plexos constitucionales a sus normas internas y viceversa, adquiriendo en algunos casos el carácter general o específico. Estamos frente a tecnologías de alcance global, como las utilizadas

⁷⁵⁰ “...Los países europeos miembros de la Unión Europea poseen el más alto, complejo y avanzado sistema de tutela de datos personales, al contar con leyes nacionales generales y sectoriales de protección de datos...”; Visto en BEL MALLÉN, I., CORREDORA y ALFONSO, L. (Coordinadores), *Derecho de la Información*, 1ª ed. ARIEL, S. A., Barcelona, 2003, p. 135.

⁷⁵¹ “Los rasgos principales de las leyes europeas son:1) existencia de reglas sustantivas generales aplicables al tratamiento automatizado de datos relativos a personas identificadas o identificables; 2) atribución de derechos a las personas titulares de los datos y de obligaciones a las personas responsables del fichero; 3) disposiciones especiales en el almacenamiento, colección, procesamiento y transmisión en los FID; 4) creación de una autoridad competente encargada de vigilar la aplicación de la ley; Así lo expresa ESTADELLA YUSTE, O., *La Protección de la Intimidad frente a la Transmisión Internacional de Datos Personales*, 1ª ed. TECNOS, Madrid, 1995, p. 42.

⁷⁵² Diversos estándares se han realizado. El último fue el presentado este mismo año por la Red Iberoamericana de Protección de Datos, conteniendo 45 artículos incluido los Principios de su conformación.

⁷⁵³ Entrevista a REMOLINA ANGARITA N., *Protección de datos personales y proactiva empresarial, derecho y empresa*, escuela de Postgrado PUCI, publicado 12 de octubre 2015. Disponible en: <http://m.youtube.com>. (Última consulta en línea 16 de junio 2017).

en los motores de búsquedas y las aplicaciones globales, desarrolladas para los smartphones, cámaras de videovigilancias, drones, etc.

En tal sentido y -como previamente hemos comentado- en este Capítulo nos orientaremos al órgano de control y las transferencias internacionales del espacio europeo y latinoamericano, no sin antes compartir a manera de reflexión, la metáfora del Vigilante Omnipresente. Y explicamos el por qué ya que -a pesar de ser solo una metáfora- nos mueve a pensar en un mundo desprovistos de normativas vinculadas con la protección de las personas físicas. ante el desarrollo y evolución de las TIC, capaz de extraer, manejar y transferir grandes volúmenes de datos personales a enormes distancias, disminuyendo el tiempo y el espacio, colocando en riesgo la integridad y el honor de las personas. Ante ello, se muestra totalmente necesario, la implementación de organismos dispuestos a contribuir y garantizar estos procesos. Nos referimos al establecimiento de órganos o autoridades de control en los Estados, dotadas de independencia⁷⁵⁴ funcional y económica.

Reflexiones en torno al vigilante omnipresente

Como si fueran los ojitos de WhatsApp⁷⁵⁵, intentamos ver a nuestro alrededor quien nos mira, sumergidos en un mundo bajo la sombra de un gran ojo⁷⁵⁶, capaz de ver lo que hacemos, un Panóptico⁷⁵⁷, un Gran Hermano⁷⁵⁸ que

⁷⁵⁴ Cfr. "...most data protection laws establish a regulatory authority with responsibility for the implementation and enforcement of legislation. where such an agency exists, it is appropriate to consider the authority as a key focus of evaluation because of the central part it plays in the wide range of processes that comprise data protection. traducción en castellano "...la mayoría de las leyes de protección de datos establecen una autoridad reguladora con responsabilidad en la implementación y aplicación de la legislación. donde existe tal agencia, es apropiado considerar la autoridad como un foco clave de evaluación debido a la parte central que desempeña en la amplia gama de procesos que comprenden la protección de datos..."; tomado de BENNETT, C. & D. RAAB, C., *The governance of privacy, policy instruments in global perspective*, 2ª ed. London, England, 2006, p. 255.

⁷⁵⁵ *Emoji de los ojos*. Disponible en: <https://emojiterria.com/es/ojos/>. (Última consulta en línea 11 de agosto 2017).

⁷⁵⁶ "El ojo que todo lo ve, eso es el Gran Hermano", extracto del video 1984 *George Orwell en español*. Disponible en: <https://www.youtube.com/watch?v=sxnMQ97YLvU>. (última verificación

nos vigila⁷⁵⁹, nos cuida, nos controla⁷⁶⁰ a cada instante, a cada momento, sumergidos en un mundo desprovisto de suficientes herramientas para evitar detenerlo o protegernos de él⁷⁶¹, sin normas jurídicas o medios globales para protegernos de su mirada, más allá de la necesidad de estar con él, de evitar su mirada, estamos adictos a él, a tal punto de no querer estar sin él, pero en muchas ocasiones nos sentimos como niños sin protección, delante de un

en línea 11 de agosto 2017); Gran Hermano (Big Brother): el brazo omnipotente del gobierno; término extraído de la novela 1984. De Georges Orwell (N. Del T). *Disponible en:* <http://www.formarse.com.ar/libros/Libros-recomendados-pdf/1984%20de%20G.Orwell.pdf>. (Última consulta en línea 02 de agosto 2017).

⁷⁵⁷ “Una casa compuesta por un edificio circular para las habitaciones de los presos y una torre en el centro ocupada por los inspectores cuerpos de vigilancia, todo el edificio es como una colmena, cuyas celdillas todas pueden verse desde un punto central; invisible el inspector reina como un espíritu; pero en caso de necesidad puede este espíritu dar inmediatamente la prueba de su presencia real, esta casa de penitencia propuesta por Jeremías Bentham es el llamado Panóptico utilizado para expresar con una sola palabra su utilidad esencial, que es la facultad de ver con una mirada todo cuanto se hace en ella, la obra editada a finales del siglo XVII” I. BENTHAM, J., *el Panóptico*, las ediciones de la piqueta, Madrid, 1979, pp. 36-37. *Disponible en:* <https://iedimagen.files.wordpress.com/2012/02/bentham-jeremy-el-panoptico-1791.pdf>. (Última consulta en línea 02 de agosto 2017); en ese sentido WHITAKER, R., *el fin de la privacidad...* op. cit., p. 46.

⁷⁵⁸ “... en el vértice de la pirámide está el Gran Hermano. Éste es infalible y todopoderoso. Todo triunfo, todo descubrimiento científico, toda sabiduría, toda felicidad, toda virtud, se considera que procede directamente de su inspirador y poder. Nadie ha visto nunca al Gran Hermano. Es una cara en los carteles, una voz en la tele pantalla. Podemos decir que nunca morirá y no hay manera de saber cuándo nació. El Gran Hermano es la concreción con que el partido se presenta al mundo. Su función es actuar como punto de mira para para todo...”; ORWELL, G., *George Orwell 1984*. *Disponible en:* <http://www.formarse.com.ar/libros/Libros-recomendados-pdf/1984%20de%20G.Orwell.pdf>. (Última consulta en línea 02 de agosto 2017).

⁷⁵⁹ “En un futuro, no se podrá pensar, si piensas diferente a ello, lo sabrán, te buscarán y te encontrarán, no podrás escapar”; extracto del video 1984 George Orwell en español. *Disponible en:* <https://www.youtube.com/watch?v=sxnMQ97YLvU>. (Última consulta en línea 11 de agosto 2017).

⁷⁶⁰ “Te pondrán en contra de todo lo que amas y serás uno de ellos y una vez logrado dirán lo que ellos quieren, serás el que ellos quieren”, extracto del video 1984 *George Orwell en español*. *Disponible en:* <https://www.youtube.com/watch?v=sxnMQ97YLvU>. (Última consulta en línea 11 de agosto 2017).

⁷⁶¹ “Si se hallara un medio de hacerse dueño de todo lo que puede suceder a un cierto número de hombres, de disponer todo lo que les rodea, de modo que hiciese en ellos la impresión que se quiere producir, de asegurarse de sus acciones, conexiones, y de todas las circunstancias de su vida, de manera que nada pudiera ignorarse, ni contrariar el efecto deseado, no se puede dudar que un instrumento de esa especie, será un instrumento muy enérgico y muy útil que los gobiernos podrían aplicar a diferentes objetos de la mayor importancia”; BENTHAM, J., *Genealogía del poder el Panóptico*, las ediciones de la piqueta, Madrid, 1979, p. 34. *Disponible en:* <https://iedimagen.files.wordpress.com/2012/02/bentham-jeremy-el-panoptico-1791.pdf>. (Última consulta en línea 02 de agosto 2017).

juguete⁷⁶² que debe ser controlado, porque a pesar de ofrecernos confort, risas y placer, necesita ser vigilado⁷⁶³. Estamos tan inmerso en él, que no nos percatamos de su daño⁷⁶⁴. ¡Es tan alto el placer que no nos permite ver el riesgo de ese ojo de poder!⁷⁶⁵.

Ante tal situación, necesitamos otro ojo protector que vigile el anterior, formado por normas, acciones proactivas, preventivas, capaz de detectar lo que no vemos, de evitar las creaciones del primer ojo, que no cuenta con

⁷⁶² Smartphone, redes sociales, Internet.

⁷⁶³ “incluso cuando duermes, el gran hermano te vigila...solo podemos pensar en nosotros mismos...te guiamos poco a poco, hasta un punto sin retorno, no sentirás amor, pasión, dolor, estarás hueco, te llenaremos nosotros mismos, de amor con el gran hermano...el partido controla todos los registros, la memoria humana...esta es una historia sobre el futuro, podría ser la historia de nuestros hijos, sino conservamos la herencia de su libertad”; extracto del video 1984 *George Orwell en español*. Disponible en: <https://www.youtube.com/watch?v=sxnMQ97YLvU>. (Última consulta en línea 11 de agosto 2017).

⁷⁶⁴ “...El Gran Hermano representa la imagen anti-utópica de todos los peligros contra la democracia y las libertades, que subyacen a una utilización perversa de la tecnología en el ámbito político; aunque con la salvedad, de que su disentimiento no pretende tanto atacar el desarrollo tecnológico como advertir de las amenazas de su utilización por gobiernos totalitarios (Orwell, 1980; cfr. Sobre la anti-utopía de Orwell, Pérez Luño, 1987, 132 y ss); Así lo expresa PÉREZ-LUÑO, A.E., *Internet y la garantía de los derechos fundamentales en* MURILLO VILLAR, A. y BELLO PAREDES, S. (Coordinadores), *Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías*, 1ª ed. Servicios de Publicaciones Universidad de Burgos, Burgos España, 2005, pp. 33-34.

⁷⁶⁵ “...Benthan no ha pues simplemente imaginado una figura arquitectónica destinada a resolver un problema concreto, como el de la prisión, la escuela o el hospital. Proclama una verdadera invención que él mismo denomina “huevo de Colón”. Y, en efecto, lo que buscaban los médicos, los industriales, los educadores y los penalistas, Bentham se lo facilita: ha encontrado una tecnología de poder específica para resolver los problemas de vigilancia.....Benthan ha pensado y dicho que su procedimiento óptico era la gran innovación para ejercer bien y fácilmente el poder. De hecho, dicha innovación ha sido ampliamente utilizada desde finales del siglo XVIII. Sin embargo, los procedimientos de poder puestos en práctica en las sociedades modernas son mucho más numerosos, diversos y ricos. Sería falso decir que el principio de visibilidad dirige toda la tecnología de poder desde el siglo XIX”; Entrevista realizada a Michel Foucault por Jean Pierre Barou titulada el ojo del poder, traducción de Julia Varela y Fernando Álvarez-Uría BENTHAM, J., *Genealogía del poder el Panóptico*, las ediciones de la piqueta, Madrid, 1979. Disponible en: <https://iedimagen.files.wordpress.com/2012/02/bentham-jeremy-el-panoptico-1791.pdf>. p. 12. (Última consulta en línea 02 de agosto 2017).

“...El Centro de Mando y Control o el Ojo Único ya no son necesarios, puesto que puede conseguirse el mismo efecto mediante una multitud dispersa, incluso competitiva, de ojos que, en su totalidad, forman un sistema de vigilancia más dominante y penetrante que el de Orwell. La fuerza de este nuevo panóptico reside en la participación voluntaria de la gente gracias a los beneficios y ventajas que puede apreciar, con lo cual es menos propensa a percibir los inconvenientes y las amenazas...” WHITAKER, R., *El fin de la privacidad...* op. cit., p. 173.

mecanismos eficaces de protección de datos por origen, por diseño. Es por ello que una real protección de sus datos conectados con la privacidad e intimidad, contribuirá con la real y efectiva protección de las personas físicas.

La intención es realizar un símil, una metáfora de nuestra realidad en un mundo global, conectado con los grandes desarrollos tecnológicos y capacidades de almacenamiento e interacción existente en el mundo actual, y de una manera u otra, reflejarnos en el Leviatán⁷⁶⁶, el Panóptico⁷⁶⁷ o el Gran Hermano⁷⁶⁸, en ese gran ojo que nos ve y nos vigila. En los actuales momentos Europa goza de normas jurídicas⁷⁶⁹ capaces de agrupar a los Estados de la Unión, realizando días tras días una protección de las personas físicas en relación a sus datos personales, al punto que en los actuales momentos se encuentra sumergida en la implementación del Reglamento de protección de datos, transitando de una Directiva a un Reglamento, evidenciando sus avances en la tutela real y efectiva de los datos personales en post de la

⁷⁶⁶ “Hace tres siglos Thomas Hobbes explicaba el Estado moderno con una grandiosa metáfora biológica, el Leviatán, el monstruo colectivo dotado de conocimiento y de poder superior a los de cualquier ciudadano particular. Pues bien, el Estado que la sociedad industrial avanzada genera en sus relaciones de poder económico y social, se configura fácilmente en la imaginación del hombre común, con una metáfora tecnológica: es el Estado gobernado por medio de computadoras, o incluso mediante máquina antropomórfica: los robots. De ahí, que sea comprensible por qué los ordenadores han asumido en la sociedad tecnológica el papel simbólico de una nueva condición de la vida colectiva y se presentan como el nuevo Leviatán de la segunda mitad del siglo XX”; PÉREZ LUÑO, A. E., “Informática y Libertad. Comentario al artículo 18.4 de la Constitución Española”, *Revista de Estudios Políticos (Nueva Época)*, núm. 24, Noviembre-Diciembre 1981, p. 38.

⁷⁶⁷ “El primer principio que caracteriza al Panóptico es la presencia universal”; BENTHAM, J., *El Panóptico*, las ediciones de la piqueta, Madrid, 1979, p. 75.
Disponible en: <https://iedimagen.files.wordpress.com/2012/02/bentham-jeremy-el-panoptico-1791.pdf>. (Última consulta en línea 02 de agosto 2017).

⁷⁶⁸ “Las predicciones que Orwell fijó para 1984 no se han cumplido y es un deber de todos el impedir que algún día se cumplan. Como técnica instrumental, la informática es neutra, por lo que el uso que se haga de ella determinará si realmente coadyuva al progreso humano y a las libertades públicas, o nos lleva a la regresión social”; así lo prologa DE CARRERAS, L., abogado, profesor de Derecho de la Información de la Universidad Ramón Llull en el texto de: FREIXAS GUTIÉRREZ, G., *la protección de los datos de carácter personal en el derecho español*, 1ra. Ed. Bosch, Barcelona, 2001, p. 8.

⁷⁶⁹ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

protección de las personas físicas⁷⁷⁰, incorporando la figura del órgano de control independiente⁷⁷¹ y el Comité Europeo de Protección de Datos.

Al unísono de la propuesta de estándares de principios de protección de datos y ante la imposibilidad de creación de una ley general de protección de datos⁷⁷², Latinoamérica debe aumentar los esfuerzos de creación de un órgano de control latinoamericano⁷⁷³, enclavado en el centro de una organización supranacional conectada con cada uno de los Estados que formen parte de la organización, con una estructura capaz de velar por el espacio latinoamericano en materia de protección de las personas relacionadas con el tratamiento de datos personales. De esa forma, vigilará a ese Gran Hermano matizado por su rápido crecimiento, avance, conexión y distribución de contenido, vigilado por órganos de control independientes, con normas jurídicas y mecanismos de protección, capaces de asegurar la vigilancia de ese Gran Hermano que avanza en Europa y Latinoamérica, por ser de escala y naturaleza global.

El órgano de control latinoamericano tendrá bajo su sombrilla a los órganos de control de los Estados adscritos a la organización, siendo capaz de crear los mecanismos de administración, organización, control y regulación de la

⁷⁷⁰ “primera vez que un derecho fundamental está regulado por un reglamento comunitario que no requiera transposición sino de adaptación, no se puede repetir en una norma nacional lo que se dice en un reglamento...el derecho comunitario no deroga, desplaza las leyes nacionales y la convierte inaplicable”; Piñar Mañas, J. L., *Adecuación de la legislación española al nuevo escenario de la protección de datos.*, exponente cursos de Verano UPV/EHU Nuevo escenario tras la aprobación del Reglamento General de Protección de Datos, Palacio Miramar, Donostia, San Sebastián, España, 22 de Junio, 2017.

⁷⁷¹ El artículo 29 sobre protección de datos., Nota de prensa, *Independencia de las autoridades de protección de datos*, 06/18/2015. Disponible en: http://ec.europa.eu/justice/data-protection/article-29/press-aterial/press-release/art29_press_material/2015/20150618_wp29_press_release_on_the_independence_of_data_protection_authorities.pdf. (Última consulta en línea 28 de febrero 2017).

⁷⁷² “(...) no existe un texto sobre tratamiento de datos personales que jurídicamente vincule y obligue a todos los países, ni tampoco uno o varios mecanismos internacionales para garantizar la efectividad del Derecho al debido tratamiento de datos personales”; REMOLINA ANGARITA, N., *Recolección Internacional de datos personales: un reto del mundo post-Internet*, 1ª ed. Agencia Española de Protección de datos, Madrid, España, 2015, p. 43.

⁷⁷³ La Unión Europea considera la creación del Supervisor Europeo de Protección de Datos y una o varias autoridades de control en los Estados miembros; España contempla varias autoridades de control entre las que se destaca, la Agencia Vasca de Protección de datos, la Agencia Española de Protección de Datos, la Agencia Catalana de Protección de Datos.

organización, preparando las leyes que regularán la interacción de los organismos de control de los Estados y el órgano de control latinoamericano de escala supranacional.

En capítulos previos, ha quedado en evidencia la intención manifiesta de trabajar en post de la protección de los datos personales en la región, intención fallida con el anteproyecto de Ley Iberoamericana de Protección de Datos, materializado con los *Estándares de Protección de Datos para los Estados Iberoamericanos*, en vía de ser asumido por los Estados Iberoamericanos al momento de elaborar sus leyes nacionales en materia de protección de datos. Se tratan de unas propuestas encaminadas y soportadas por los Jefes de Estados Iberoamericanos y algunas organizaciones como la Red Iberoamericana de Protección de Datos (RIPD), el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) conocido anteriormente como el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) y otros organismos, incluida la Organización de Estados Americanos (OEA).

A pesar del recorrido realizado en materia de protección de datos, *habeas data*, transferencias internacionales y órganos de control, falta camino por recorrer, en especial para Latinoamérica como veremos a continuación.

2. Normas jurídicas previas, punto de partida

En anteriores apartados, presentamos los primeros pasos y la conformación de la evolución de la protección de datos y el *habeas data*. En estos momentos nos detendremos en dar una pincelada de esos derechos orquestados por normas legislativas procedentes de diversos entornos geográficos como el americano (Norte América, Latinoamérica, etc.), europeo (Alemania, Suecia, España, etc.), especialmente de las normas conectadas y que en cierto modo han servido de base para la conformación del órgano de control y las transferencias internacionales.

A raíz de la consolidación de la línea maestra de la tecnología durante la década de los 70 -período en el cual la tecnología de la informática pasa por un período de momentánea estabilidad- los profesionales de la informática impulsados por sus preocupaciones dirigen su atención a los problemas económicos, sociales, jurídicos, políticos de la época. Más allá del ámbito tecnológico, ante tal situación, se observa la necesidad de proteger, controlar la información almacenada ante su posible y eventual vulneración, colocando en riesgos los diversos bienes jurídicos necesarios de ser protegidos, no solo la intimidad ⁷⁷⁴.

A su vez, la tecnología bajo el amparo de la informática y las telecomunicaciones, influye y ha influido en el desarrollo de las normas en materia de protección de datos, privacidad e intimidad, situación que estaremos percibiendo a lo largo del desarrollo y análisis de las informaciones presentadas.

Es así como durante el proceso de evolución, se observarán normas cuyo espíritu será el de frenar el avance de las nuevas tecnologías informáticas y con él impedir su rápido crecimiento ante la imposibilidad de controlar su gran velocidad de desarrollo e impacto, en detrimento de los derechos fundamentales ya establecidos. Es importante puntualizar que, a partir de los años 70,⁷⁷⁵ se incrementa la actividad de investigación en materia de protección a la intimidad y sus posibles peligros ante la recolección de los datos de carácter personal, pero no es sino, a partir del 1973, cuando ocurre la verdadera explosión del proceso normativo, matizado por dos corrientes, la de Europa Continental orientada a las “leyes de datos” o de “leyes de protección

⁷⁷⁴ Central de Informática., *Informática Leyes de Protección de Datos, Documentación Informática núm. 2, serie Verde /Legislación*, 1ª ed. Presidencia del gobierno, Madrid, España, 1977, p. 7.

⁷⁷⁵ BENNETT, C. y D. RAAB, C., *The governance of privacy, policy instruments in global perspective*, 2ª ed. London, , 2006, p. 8 y ss.

de datos”, y el modelo o corriente de habla inglesa sustentada en leyes de protección a la intimidad (*privacy*)⁷⁷⁶.

En 1970⁷⁷⁷ se promulga en Alemania⁷⁷⁸, la célebre “Ley de Protección de Datos”⁷⁷⁹ de Hesse⁷⁸⁰, convirtiéndose en la primera norma jurídica positiva en Europa⁷⁸¹ y podemos incluir del mundo, que tuvo como objeto la regulación de la protección de datos⁷⁸², en temas tales como almacenamiento, transmisión, modificación o cancelación de datos, tutelando los datos que son objeto de

⁷⁷⁶ Documentación Informática., *Flujo Internacional de Datos, recomendación de la OCDE de 23 de septiembre de 1980*, tratados Internacionales núm. 2, 1ª ed. Presidencia del Gobierno, serie amarilla, servicio central de publicaciones, Madrid, 1982, pp. 25-27.

⁷⁷⁷ “La llegada de la década de los setenta aportó...el advenimiento de una legislación específica sobre los bancos de datos y sobre la protección de la “*privacy*”, o sea, sobre la protección de los datos informáticos personales: una legislación que, en base al ejemplo proveniente de los Estados Unidos, se extendió a todos los países de civilización industrial avanzada durante aquella década.....dicha legislación tuvo su consagración, como instrumento de protección de un nuevo derecho fundamental, en las constituciones de Portugal (1976) y de España (1978) y en una nueva ley constitucional en Austria (1978) así como en el Convenio Europeo del 28 de enero de 1981...”; FROSSINI, V., *Hacia un derecho de la información*, visto en CARRASCOSA LÓPEZ, V. (Director), *Informática y Derecho, II Congreso internacional de Informática y Derecho*, 1ª ed. Universidad Nacional de Educación a Distancia, Mérida, Sevilla, España, 1996, p. 811.

⁷⁷⁸ Promulgada el 7 de octubre de 1970 por el ministro presidente del Estado de Hesse. El transcurso de cerca de siete años y la promulgación, dentro del año 1977, de una ley federal de Protección de Datos (v., infra), ha movido a un planteamiento de la regulación de los problemas básicos de esta ley (funciones del Comisario Parlamento de Protección de Datos, mantenimiento del equilibrio constitucional, etc.). A este respecto, ofrece gran interés del sexto informe de Actividades del Comisario, de fecha 10 de marzo de 1977 (Hessischer Landtag, 8. Wahlperiode, Drucksache 8/3962), en el cual se esboza un nuevo proyecto que, por una parte, perfila los principios de la ley de 1970 y, por otra, trata de adaptar ésta a la Ley Federal; Así se expresa en Central de Informática., *Informática Leyes de Protección de Datos, Documentación Informática núm. 2, serie Verde /Legislación*, 1ª ed. Presidencia del gobierno, Madrid, España, 1977. nota p. 16.

⁷⁷⁹ CARRASCOSA LÓPEZ, V., *Informática y Derecho 1*, 1ª ed. Universidad Nacional de Educación a Distancia, Mérida, Sevilla, España, 1992, p. 17.

⁷⁸⁰ Corresponde a uno de los 16 Estados Federados de Alemania, su capital es Wiesbaden.

⁷⁸¹ Así lo expresa PÉREZ LUÑO, A. E., *Internet y la garantía de los derechos fundamentales en MURILLO VILLAR. A. y BELLO PAREDES, S. (Coordinadores), Estudios Jurídicos sobre la sociedad de la información y nuevas tecnologías*, 1ª ed. Servicios de publicaciones Universidad de Burgos, Burgos, España, 2005, p. 26.

⁷⁸² HERRERO HIGUERAS, M., *Panorama General de la Legislación Mundial sobre protección de datos*, CITEMA, España, p. 35, tomado de *IX encuentro implicaciones socio-jurídicas de las tecnologías de la información*, CITEMA, España, 1991.

tratamiento en organismos público⁷⁸³, ya para el 27 de enero de 1977 se aprueba la Ley Federal de Protección de Datos de la República Federal Alemana, y el 14 de julio del mismo año se promulga la Ley de Derechos Humanos del Canadá, donde su parte IV se titula “Protección de la Información Personal”.

En 1973, Suecia se convierte en el primer país pionero en dotarse de una ley de protección de datos de carácter personal de ámbito nacional con la aprobación de la *Dátala Act.*⁷⁸⁴, entre cuyos fines se encuentra la creación de un registro público, permitiendo el registro de ficheros electrónicos de datos, tanto en el orden público como en el privado, nombrando un ente regulador y con características de inspección de sus datos personales.

En 1974 el Congreso de Estados Unidos promulga la *Privacy Act* originada a raíz de los escándalos de Watergate. De este modo pasó a ser considerado el país que siguió a Suecia en el tema de la regulación de datos y es EEUU quien coloca límites al gobierno para proteger la libertad de las personas en aras a evitar posibles abusos del gobierno al momento de investigar y almacenar información.

En el 1976 se dota a la Constitución de Brasil del artículo 35 relacionado con la protección de datos, y el 6 de enero de 1978 Francia establece la Comisión Nacional de la Informática y las Libertades, cuyo fin es el de asegurar el buen desempeño de la tecnología de la información al servicio de los ciudadanos, sin afectar derechos tales como identidad, privacidad o libertades públicas, prohibiendo las interconexiones nuevas entre sistemas informáticos dependientes de ministerios distintos, tratando de recortar la preeminencia del

⁷⁸³ ALMAZARA ALMAIDA, C. (Coordinador), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. LEX NOVA, S.L, Valladolid, España, 2007, p. 34.

⁷⁸⁴ CASTAÑEDA GONZÁLEZ, A. (Coordinador), *Derecho Tecnológico respuesta legales a nuevos retos*, 1ª ed. Experiencias, S. L., Barcelona, 2004, p. 29.

ordenador, recordando el autoritarismo del Big Brother, siendo el objetivo dominar, no paralizar la informática⁷⁸⁵.

En 1978, España y Portugal incorporan a su Constitución la limitación de la informática como garantía de protección de la intimidad, y el honor. En 1981, el Consejo de Europa aprueba el *Convenio n.º 108, del 28 de enero de 1981*, siendo ratificado por España en noviembre de 1985, el Convenio presentó a posteriori su Protocolo Adicional al Convenio n.º 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencia de datos. El Convenio compromete a los países signatarios a incluir en sus ordenamientos jurídicos internos aquellas normas que tienen como objetivo garantizar los principios y garantías contemplados en el Convenio, sirviendo de fuente de inspiración para las legislaciones europeas posteriores en temas de protección de datos de carácter personal⁷⁸⁶, sin dejar de lado el escenario iberoamericano, ya que sus normas han sido reflejo y han formado parte de las normas europeas.

En 1984 la Constitución brasileña incorpora el *habeas data* a su Constitución y ya para el 1995, la Unión Europea aprueba la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. En el año 2000 se incluye el derecho a la protección de datos de carácter personal a la Carta de los Derechos Fundamentales de la Unión Europea⁷⁸⁷, dejando ver la necesidad de

⁷⁸⁵ CARRASCOSA LÓPEZ, V. (Coordinador), *Informática y Derecho 1*, 1ª ed. Universidad Nacional de Educación a Distancia, Mérida, Sevilla, España, 1992, p. 19.

⁷⁸⁶ CASTAÑEDA GONZÁLEZ, A., (Coordinador), *Derecho Tecnológico respuesta legales a nuevos retos*, 1ª ed. Experiencias, S. L, Barcelona, 2004, p. 30.

⁷⁸⁷ CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA

Artículo 8 Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.
3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

tutela del derecho bajo una autoridad independiente como se refleja en su numeral tercero del artículo 8. La disposición, supone una interesante garantía para la tutela de la intimidad de los ciudadanos europeos frente a cualquier tipo de injerencia indebida en esa esfera perpetrada a través de la red⁷⁸⁸.

Desde el punto de vista constitucional, las cartas magnas latinoamericanas y las normas legislativas de los Estados Latinoamericanos no reflejan una estandarización en temas de intimidad, protección de datos, *habeas data*, órganos de control, transferencias internacionales⁷⁸⁹. Muestras de ello, puede ser observado en las constituciones latinoamericanas como son los casos de las constituciones de Perú que prohíbe a los servicios informáticos suministrar informaciones ligadas a la intimidad⁷⁹⁰ contemplando a su vez la figura del *habeas data* como norma procedimental⁷⁹¹; del Estado Federado de Argentina en su artículo 43 de la Constitución Federal de 1994 conteniendo los derechos ARCOS (acceso, rectificación, cancelación, oposición, supresión) no así, la figura del *habeas data*; de Honduras en su artículo 182, contempla los derechos al honor e intimidad y la figura del *habeas data*⁷⁹². Al mismo tiempo,

⁷⁸⁸ Así lo expresa PÉREZ LUÑO, A. E., *Internet y la garantía de los derechos fundamentales en MURILLO VILLAR, A. y BELLO PAREDES, S.* (Coordinadores), Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías, 1ra.ed. editora Servicios de publicaciones Universidad de Burgos, Burgos España, 2005, p. 26.

⁷⁸⁹ “Como otros tantos aspectos, las transferencias internacionales de datos (TID) son reguladas de forma distinta en aquellos países Iberoamericanos que ya cuentan con una legislación destinada a la protección de los datos personales y/o la privacidad de los individuos”, LÓPEZ CARBALLO, D. (Coordinador), *Protección de datos y habeas data: una visión desde Iberoamérica*, imprenta nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2015, p. 166.

⁷⁹⁰ “A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar”; *Constitución Peruana 1993*, artículo 2, numeral 6. Disponible en: http://www.oas.org/juridico/spanish/per_res17.pdf. (Última consulta en línea 20 de abril 2018).

⁷⁹¹ “La acción de *habeas data*, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2º, incisos 5 y 6 (modificados por la ley 26,470 publicada el 12/06/1995) de la Constitución Peruana 1993, artículo 200, numeral 3”. Disponible en: http://www.oas.org/juridico/spanish/per_res17.pdf. (Última consulta en línea 20 de abril 2018).

⁷⁹² Cfr. Numeral 2 del artículo 182 de la Constitución de Honduras 1982. Disponible en: https://www.oas.org/dil/esp/Constitucion_de_Honduras.pdf. (Última consulta en línea 20 de abril 2018).

la República del Ecuador contempla en su carta magna del 2008 el acceso, rectificación, cancelación de sus datos personales, contemplado en el artículo 15 de su Constitución.

Ante ausencia o debilidad de autoridades u órganos de control independientes en los Estados, Latinoamérica implementa con rango constitucional y leyes generales la figura del *habeas data*⁷⁹³, disponiendo en algunos Estados de normativas en materia de protección de datos conectadas con el *habeas data*, y en otras, considerada como términos u expresiones iguales.

3. Aproximación europea

En el capítulo segundo, hemos observado la inexistencia de normas homogéneas, tanto legislativas como constitucionales en materia de protección de datos, *habeas data*, órgano de control y transferencias internacionales entre los Estados Iberoamericanos, Estados con normas mínimas e inexistentes en materia de protección de datos, y Estados con normas existentes o en procesos de formación⁷⁹⁴. Ahora bien, los Estados Iberoamericanos apoyados en sus costumbres, idiomas, familias jurídicas, etc. ven como modelo a seguir las normas jurídicas de los Estados europeos, con el agravante, de que en

⁷⁹³ “Por ello es un deber y una constante, el que subyacente a la protección del derecho fundamental de *habeas data* y tratamiento de datos personales, garantizar la defensa y buen uso del grueso de derechos fundamentales que pueden verse inmerso en esta clase de relación, tales como los derechos la privacidad, la intimidad, el buen nombre, la imagen, la autonomía universitaria, y en general toda clase de derecho fundamental, y los derechos humanos”; LÓPEZ CARBALLO, D. (Coordinador), *Protección de datos y habeas data: una visión desde Iberoamérica*, imprenta nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2015, p. 39.

⁷⁹⁴ “.....existen claramente dos bloques de países Iberoamericanos, aquellos que no cuentan con legislación sobre protección de datos y como mucho en sus textos constitucionales regulan la figura del *Habeas Data*, y aquellos que, o bien tienen proyectos de Ley en tramitación Parlamentaria, o ya cuentan con legislación en materia de protección de datos personales”; LÓPEZ CARBALLO, D. (Coordinador), *Protección de datos y habeas data: una visión desde Iberoamérica*, imprenta nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2015, p. 182.

estos momentos la Unión Europea se aboca en la construcción de su nueva normativa jurídica en materia de protección de datos. Nos referimos a su Reglamento⁷⁹⁵, convirtiendo en obsoletas e inadecuadas aquellas regulaciones iberoamericanas, fundamentadas o referenciadas con la Directiva 95/46/CE y el Convenio 108, por estar ajenas a las mejoras implementadas en el Reglamento⁷⁹⁶, sin descartar los articulados existentes en el Reglamento, basado o fundamentado en las anteriores legislaciones y convenios internacionales.

Tales decisiones convierten en sombrío el panorama de la protección de datos en Iberoamérica, especialmente en aquellos Estados Latinoamericanos que no abocan sus normas legislativas de protección de datos con los nuevos tiempos, dejando de lado en sus legislaciones el impacto de los desarrollos tecnológicos⁷⁹⁷ conectados con el crecimiento del comercio⁷⁹⁸, el aumento de

⁷⁹⁵ " La Comisión Europea presentó su reforma de la UE sobre protección de datos en enero de 2012 para que Europa sea apto para la era digital. Más del 90% de los europeos que quieren los mismos derechos de protección de datos en toda la UE-y con independencia de donde se procesa sus datos. el Reglamento es un paso esencial para fortalecer los derechos fundamentales de los ciudadanos en la era digital y facilitar los negocios mediante la simplificación de las normas para las empresas en el mercado único digital. Una sola ley también acaba con la fragmentación actual y las cargas administrativas costosas, lo que lleva a un ahorro para las empresas de alrededor de 2.3 millones de euro al año....."; Comisión Europea., *reforma de las normas de protección de datos de la U.* Disponible en: http://ec.europa.eu/justice/data-protection/reform/index_en.htm. (Última consulta en línea 28 de enero 2017).

⁷⁹⁶ " El Reglamento de protección de datos establece un régimen europeo homogéneo, ofreciendo a los ciudadanos derecho y seguridad jurídica...el reglamento se preocupa por establecer bases eficaces para que la protección sea efectiva y los operadores puedan trabajar dentro del derecho...trata de mantener una protección de datos respetuosa de los individuos...refuerza las Autoridades de protección de datos, la cooperación, flujos verticales"; LUCAS MURILLO DE LA CUEVA, P., *Marco Jurídico Europeo en la Protección de Datos*, exponente cursos de Verano UPV/EHU Nuevo escenario tras la aprobación del Reglamento General de Protección de Datos, Palacio Miramar, Donostia, San Sebastián, 22 de Junio, 2017.

⁷⁹⁷ "...retos en privacidad surgidos de los avances tecnológicos como Internet of thing, Big Data, smartphones u otros dispositivos wearables, redes sociales, cloud computing, etc"; LÓPEZ CARBALLO, D. (Coordinador), *Protección de datos y habeas data: una visión desde Iberoamérica*, imprenta nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2015, p,182.

⁷⁹⁸ "...el Reglamento de protección de datos, va a globalizar la protección de datos, las compañías que generen comercios con personas de la Unión Europea, estarán sujetas al Reglamento"; PIÑAR MAÑAS, J, L., *Adecuación de la legislación española al nuevo escenario de la protección de datos.*, exponente cursos de Verano UPV/EHU Nuevo escenario tras la aprobación del Reglamento General de Protección de Datos, Palacio Miramar, Donostia, San Sebastián, 22 de junio, 2017.

las transferencias internacionales y el fenómeno de la globalización⁷⁹⁹.

Preocupaciones similares son expuestas por Pérez Luño cuando expresa:

“La necesidad de tutelar la vida privada de los individuos ha rebasado, en los últimos años, la esfera estricta del derecho interno para plantearse como una exigencia del orden jurídico internacional. (...) Uno de los aspectos de mayor interés en la reglamentación jurídica de la informática a escala internacional es el que se refiere a la transmisión de datos personales entre diversos países. El problema del flujo transnacional o internacional de datos ha suscitado un abierto conflicto de interés entre los países productores y los países consumidores de datos informáticos. Los países tecnológicamente avanzados se hallan en condiciones de recoger informaciones, almacenarlas y distribuirlas con la utilización de la informática. Por el contrario, los países subdesarrollados sólo pueden recibir y consumir informaciones; es más, en determinados casos ni tan siquiera pueden servirse de ellas por carecer de los medios técnicos necesarios para aprovecharlos. Esta circunstancia ha determinado que los países desarrollados mantengan una posición decidida a favor de una libertad ilimitada de intercambios de informaciones entre todos los países subdesarrollados, que carecen de una tecnología informática propia, exigen que se reconozca la facultad de ejercer un control sobre los datos que pueden recogerse en su territorio”⁸⁰⁰.

El modelo de protección de datos entre países iberoamericanos, provistos, desprovisto y en proceso de conformación de sus legislaciones nacionales, debe estar a la vanguardia de las nuevas legislaciones internacionales⁸⁰¹,

⁷⁹⁹ “la velocidad a la que se suceden las innovaciones tecnológicas y el fenómeno de la globalización han transformado profundamente la magnitud y los métodos de recogida, acceso, utilización y transferencia de los datos personales. Hay varias razones poderosas para revisar y mejorar la normativa vigente, aprobada en 1995; la creciente globalización de los flujos de datos, el hecho de que se recojan, transfieran e intercambien ingentes volúmenes de información personal en milésimas de segundo, entre continentes y por todo el mundo, y la aparición de la computación en nube”; Comisión Europea; *¿ De qué modo adaptará la reforma de la protección de datos en la UE la normativa vigente a la evolución tecnológica?*, ficha informativa Enero 2016, PDF ISBN 978-92-79-60187-3, Disponible en: ec.europa.eu/newsroom/document.cfm?doc_id=41597. (Última consulta en línea 28 de febrero 2017).

⁸⁰⁰ PÉREZ LUÑO, A., *Derechos humanos, Estado de derecho y Constitución*, Tecnos, Madrid, p. 354; visto en BEATRIZ CALLE, S., *Apuntes sobre la protección de datos personales a la luz de la actual norma de habeas data en Colombia*, Colombia, 2009, p. 133.

⁸⁰¹ “...la Unión Europea ya hace tiempo que se dio cuenta que la Directiva 95/46/CE no contaba con mecanismos útiles y eficaces para los nuevos retos y desafíos en privacidad ante los avances tecnológicos reseñados. Ello llevó a la Comisión Europea a presentar el 25 de enero de 2012 su propuesta de Reglamento del Parlamento europeo y del Consejo.” LÓPEZ CARBALLO, D. (Coordinador), *Protección de datos y habeas data: una visión desde*

evitando una desconexión con las últimas normas jurídicas desarrolladas y pensadas, teniendo en cuenta la evolución y actualización de los cambios tecnológicos y globales⁸⁰² que impactan el comercio, las empresas⁸⁰³, asegurando una real protección de las personas físicas mediante la salvaguarda de sus intereses.

4. Concepto y características del órgano de control en normas jurídicas europeas

4.1. Autoridad de control Vs. órgano de control

A lo largo y ancho del trabajo de investigación, hemos empleado y estaremos usando indistintamente el término de autoridad de control u órgano de control, razones estas, que nos obligan a hurgar el término empleado en las normas existentes y contempladas en la investigación, tal es el caso de las legislaciones europeas e iberoamericanas, incluyendo la normativa dominicana en materia de protección de datos personales.

Para ello, emplearemos el escenario de las legislaciones del Consejo de Europa en materia de protección de las personas; la normativa de la Unión Europea; la legislación española; y las normativas de países pertenecientes al entorno latinoamericano, incluido los proyectos de ley de la República

Iberoamérica, imprenta nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2015, p. 184.

⁸⁰² “La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales....la tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones Internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales”; Considerando 06 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de Abril de 2016.

⁸⁰³ DAVARA RODRÍGUEZ, M. A., *Las Telecomunicaciones y las Tecnologías de la información en la Empresa: Implicaciones Socio-Jurídica*, en CARRASCOSA LÓPEZ, V. (Coordinador), *Informática y Derecho 1*, 1ª ed. Universidad Nacional de Educación a Distancia, Mérida, Sevilla, España, 1992, pp. 27-28.

Dominicana y su actual normativa en materia de protección integral de los datos personales.

El Convenio 108 del Consejo del 28 de enero de 1981 utiliza el término de autoridad de control⁸⁰⁴, un término alusivo a una autoridad con independencia de funciones y poderes de investigación e intervención. La Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 reconoce el término de autoridad de control⁸⁰⁵ ejerciendo sus funciones con independencia, contemplando poderes de investigación, intervención, con capacidad procesal y cooperación entre autoridades. Por último, el Reglamento (UE) 2016/679 implementa la figura de la autoridad de control⁸⁰⁶ con poderes de independencia en sus funciones, poder de investigación, de sanción. Ante esa situación, en el entorno del Consejo de Europa, la Comunidad Europea y la actual Unión Europea, el término empleado es el de autoridad de control.

En el escenario español se denota una situación distinta, matizado por sus normativas más representativas en materia de protección de datos como son la normativa 5/1992 (LORTAD), una ley que contempla desde sus considerandos⁸⁰⁷ las atribuciones del órgano de control, siendo este, un órgano independiente, instituido para lograr una mayor eficacia en sus disposiciones como se refiere en los articulados de la propia ley, estipulando como órgano de control a la Agencia de Protección de Datos⁸⁰⁸. La próxima norma española a señalar es la 15/1999 (LOPD) una normativa carente de considerandos. A

⁸⁰⁴ “Artículo 1, Autoridades de Control”; *Protocolo Adicional del Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos*, traducción no oficial realizada internamente por la Agencia de Protección de Datos.

⁸⁰⁵ “Artículo 28, Autoridad de control”, Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995.

⁸⁰⁶ “Artículo 51, Autoridad de Control”, Reglamento (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016 implementa la figura de la autoridad de control.

⁸⁰⁷ Cfr. “Considerando 5”, Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. BOE-A-1992-24189.

⁸⁰⁸ “Título VI, Agencia de Protección de Datos”, Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. BOE-A-1992-24189.

pesar de ello, contempla en sus disposiciones a la Agencia de Protección de Datos, dotada de personalidad jurídica propia y plena independencia⁸⁰⁹. No obstante, la normativa sustituye el término Agencia Española de la normativa 5/1992 (LORTAD) por el de autoridades de control en la Ley 15/1999 (LOPD)⁸¹⁰ englobando a las comunidades autónomas. Así, cuando se refiere a las comunidades autónomas se emplea el término órgano⁸¹¹. De todo ello cabe concluir que las normativas españolas en materia de protección de datos usan o emplean indistintamente el término autoridades de control u órganos de control.

Por su parte, la propuesta de *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*, contempla desde sus considerandos la instauración de una autoridad de control independiente con poderes de investigación, situación observada en las disposiciones de la norma legislativa⁸¹². Por su parte, y siguiendo con los modelos iberoamericanos, la Ley núm. 172-13 de la República Dominicana utiliza en sus disposiciones el término órgano de control, constituyendo una muestra del manejo y uso del término utilizado en los distintos escenarios que conforman el entorno iberoamericano.

⁸⁰⁹ “La Agencia Española de Protección de Datos (AEPD) es una autoridad administrativa independiente. Esta expresión fue acuñada por la doctrina a finales del siglo XX para designar a un nuevo tipo de instituciones que fueron surgiendo en aquel momento y que no encajaban en el esquema tradicional de la organización del Estado y de la Administración. Eran organismos públicos que disponían de una considerable autonomía y que actuaban en ámbitos de especial trascendencia económica, política o social, desempeñando funciones reguladoras o de prestación de servicios, como por ejemplo, Banco de España, la Comisión Nacional del Mercado de Valores, el Consejo de Seguridad Nuclear y la AEPD.” ARENAS RAMIRO, M. y ORTEGA GIMÉNEZ, A. (Directores), *Protección de Datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)*, 1ª ed. Sepín, S. L. Madrid, 2019, p. 219.

⁸¹⁰ Artículo 40, potestad de inspección, Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. BOE-A-1999-23750.

⁸¹¹ Artículo 41. Órganos correspondientes de las Comunidades Autónomas,

⁸¹² Capítulo VII, autoridades de control, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*, 20 de junio de 2017, Red Iberoamericana de protección de datos.

Visto lo anterior y, a manera de cierre, nos vemos en la obligación de utilizar o emplear indistintamente el término autoridad de control u órgano de control en el trabajo, situación muy similar a lo externado en la normativa española 15/1999 (LOPD), ya que de acuerdo a los conceptos emitidos y términos empleados, estos no gozan de una diferenciación conceptual en las normativas, colocándonos en la posición de asumirlos como términos sinónimos e indistintos a la hora de ser abordados en el trabajo.

4.2. Incidencia del órgano de control en las normas legislativas

En esta ocasión, nuestra intención es hurgar en las definiciones contenidas en las normas legislativas, dejando en evidencia, que a pesar de no estar o no ser consideradas parte de sus definiciones, el término es empleado en las normas legislativas de protección de las personas físicas en relación a su tratamiento de dato o normas en materia de protección de datos o *habeas datas*. De todo el universo posible de normativa nos centraremos sólo en aquella más relevante para nuestro estudio. Examinaremos esta cuestión en la Directiva 95/46/CE, en el Reglamento (UE) 2016/679 y en la normativa española y dominicana.

La Directiva 95/46/CE no contempla entre sus definiciones el órgano de control, a pesar de contener en su legislación un acápite reservado para ello. A su vez, el Reglamento (UE) 2016/679 considera un acápite para la autoridad de control, visualizando desde el inicio la figura, contemplando su propia definición, entendiendo como autoridad de control a la autoridad pública independiente establecida por un Estado miembro en base a las disposiciones del artículo 51 del Reglamento, siendo necesario apuntar, que nos referimos a una autoridad que goza de total independencia con características públicas.

Ni la LORTAD de 1992 ni la LOPD de 1999, contemplan en sus definiciones el término de autoridad u órgano de control, a pesar de ser considerado internamente en la ley. En idéntico sentido nos encontramos en el caso de la

normativa dominicana o Ley núm. 172/13 encaminada a la protección de datos personales⁸¹³.

4.3. Tipos de autoridad de control

Durante el desarrollo del capítulo, presentamos diversos modelos y propuestas de conformación de autoridades u órganos de control. Sin embargo a modo de presentación, solo refrescaremos los modelos ya planteados, siendo puntualizados más adelante a raíz del desarrollo del capítulo.

Un primer modelo es el conformado por un órgano que goza de total independencia en funciones, con presupuesto asignado, sin dependencia jerárquica de un organismo público o de instituciones gubernamentales. Se trata de una autoridad *ad hoc* focalizada en la protección de datos personales. Es el modelo representativo de los Estados que conforman la Unión Europea y dispuestos en sus normativas como es el previsto en el caso del Reglamento (UE) 2016/679.

Un segundo modelo se refiere al compuesto por autoridades bajo el amparo de otras instituciones nacionales, preferiblemente el poder judicial. Estamos ante un modelo desplegado por aquellos Estados alejados de los modelos vanguardistas como el europeo y matizado por la poca inversión en temas de protección de las personas físicas en relación al tratamiento de datos personales.

4.4 Funciones de la autoridad de control

Las normas legislativas en materia de protección de datos contemplan en sus articulados las funciones de las autoridades de control, unas funciones contenida en sus legislaciones nacionales y supranacionales, haciendo

⁸¹³ Capítulo III, Sección I, Ley núm.172-13.

imperiosa su incursión en estas líneas. A raíz de ello, incluiremos en esta sección las funciones contempladas y existentes en las siguientes normativas u órganos de control como las leyes españolas de protección de datos, la Directiva 95/46/CE, el Reglamento (UE) 2016/679, la Agencia Española de Protección de Datos, la Agencia Vasca de Protección de datos y -como no- la normativa del Consejo de Europa, en especial, el Convenio 108 y la Ley de protección de datos de la República Dominicana (Ley núm. 172/13). Iniciaremos con la normativa de la Republica Dominicana que a diferencia del Reglamento solo tiene un órgano de control.

La Ley núm.172-13 asigna al órgano de control funciones de asistencia y asesoramiento de las personas físicas, imponiendo sanciones administrativas⁸¹⁴ por violación a las normas establecidas, siendo la Superintendencia de Bancos el órgano de control instituido para estos fines, de acuerdo a la ley⁸¹⁵.

Mediante la *LORTAD* de 1992 se crea el Registro General de Protección de Datos y la Agencia de Protección de Datos⁸¹⁶, así como la asignación del director de la Agencia y las funciones del órgano de control, siendo éstas las de: velar por el cumplimiento de la ley, emitir autorizaciones, dictar instrucciones de adecuación, ordenar la cesación de los tratamientos automatizados, atender peticiones, reclamaciones, proporcionar información a los afectados, ejercer potestad sancionadora, informar de los proyectos desarrollados en la ley, recabar ayuda de los responsables de los ficheros, velar por la publicidad de los ficheros, redactar memoria anual, velar por el cumplimiento estadístico, ejercer el control y adoptar las autorizaciones de los movimientos Internacionales de datos⁸¹⁷.

⁸¹⁴ Capítulo II, Ley núm.172-13.

⁸¹⁵ Artículo 29, Ley núm.172-13.

⁸¹⁶ Artículo 34, apartado 1, Ley Orgánica 5/1992, de 29 de octubre.

⁸¹⁷ Artículo 35, funciones de la Agencia de Protección de datos, Ley Orgánica 5/1992, de 29 de octubre.

Con la *LOPD* de 1999 se contemplan las funciones del órgano de control asignado a la Agencia de Protección de Datos las cuales se refieren a :velar por el cumplimiento y aplicación de la legislación, asegurar y garantizar la emisión de autorizaciones, dictar instrucciones de adecuación de los tratamientos a la ley, atender peticiones, reclamaciones, informar a las personas, requerir medidas de adecuación, ordenar la cesación, cancelación de tratamientos a los responsables y encargados cuando no se cumplan las disposiciones de la normativa, sancionar e informar acerca de los proyectos, redactar memoria anual, controlar y adoptar autorizaciones fruto de los movimientos internacionales de datos, velar y cumplir la ley de la función estadística pública u otras posibles atribuciones conferidas en la ley, dejando la posibilidad de que sean incluidas otras funciones al órgano de control en la medida que se despliega la normativa⁸¹⁸.

4.5. Autoridad supranacional de control

Con la Directiva 95/46/CE del Parlamento Europeo y el Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, podemos decir que se tejen las bases de conformación de una autoridad supranacional de control mediante la creación del Grupo de Protección de las Personas en lo que respecta al tratamiento de datos personales, reconocido como Grupo 29⁸¹⁹. Un grupo de carácter consultivo e independiente, formado por representantes de las autoridades de control de los Estados partes y un representante de la Comisión⁸²⁰ encargado de efectuar medidas de ejecución comunitarias, estableciendo autoridades independientes en los Estados con funciones de investigación, intervención, capacidad procesal en caso de

⁸¹⁸ Artículo 37, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

⁸¹⁹ A raíz del artículo 29 de la Directiva 95/46/CE.

⁸²⁰ Cfr. Artículo 30-31, Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995.

infracciones. De igual forma, sus decisiones pueden ser objeto de recurso jurisdiccional, atenderán solicitudes, presentarán informes periódicos, asumirán competencia territorial, manteniendo el secreto profesional⁸²¹, como vemos, parte de sus disposiciones se encuentran redactadas en la Ley Orgánica 5/1992, de 29 de octubre, una normativa publicada 3 años antes.

Por su parte, el Consejo de Europa, mediante su *Protocolo Adicional al Convenio n.º 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos del 8 de noviembre de 2001*, asigna al órgano de control funciones y poderes de investigación e intervención, comenzar procedimientos legales o dirigirse a las autoridades judiciales en caso de violaciones de derecho interno, sus decisiones pueden ser recurridas judicialmente⁸²².

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, de aplicación en toda la Unión Europea, contempla mecanismos de coherencias, garantizando la aplicación coherente del Reglamento, estableciendo autoridades de control en los Estados, las cuales deben gozar de igualdad de funciones y poderes efectivos, creando el Comité, un organismo independiente dentro de la Unión, con personalidad jurídica propia, sustituto del Grupo de Protección de Datos creado por la Directiva 95/46/CE⁸²³. Al mismo tiempo, el Reglamento contempla las competencias, funciones y poderes de las autoridades de control⁸²⁴, no siendo competente en aquellos procesos de tratamientos en manos de los tribunales, pero si en

⁸²¹ Artículo 28, Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995.

⁸²² Artículo 1, Protocolo Adicional n.º 108, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos del 8 de noviembre de 2001, Estrasburgo.

⁸²³ Cfr. Considerandos 129, 135, 139 Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

⁸²⁴ Sección 2, Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

aquellos casos donde: a) los tratamientos transfronterizos sean realizados por el responsable o encargado; b) ocurran reclamaciones por infracción del Reglamento; c) se informe a la autoridad de control principal en un plazo de tres semanas después de haber sido informada.

El artículo 57 del Reglamento, contempla un pliego de funciones del órgano de control entre ellas, controlar la aplicación del Reglamento, sensibilizar al público, asesorar, facilitar información al interesado, tratar, investigar e informar acerca de las reclamaciones, cooperar y asistir a otras autoridades de control u autoridad pública, seguimiento a los cambios proporcionados por las TIC, adoptar cláusulas contractuales tipo, elaborar y mantener lista de impacto, alentar, dictaminar y aprobar códigos de conducta, fomentar la creación de mecanismos de certificación, aprobar los criterios de certificación y llevar revisiones de certificación, autorizar las cláusulas contractuales, contribuir con las actividades del comité, llevar registros de infracciones y presentación de reclamaciones por las autoridades; el desempeño de la autoridad es gratuito para el interesado⁸²⁵; no queremos dejar a un lado los poderes asignados a las autoridades de control en el Reglamento, iniciaremos con los poderes de investigación en el Reglamento como son ordenar y facilitar información para el responsable, el encargado o el representante de estos, realizar investigaciones de auditorías, notificar infracciones cometidas al reglamento, obtener acceso a los datos personales necesarios para ejercer sus funciones, obtener acceso a los locales del encargado y el responsable, en el caso de los poderes correctivos tenemos el del carácter sancionador cuando las operaciones puedan e infrinjan lo dispuesto en el Reglamento, ordenar la atención a las solicitudes del interesado, imponer límites al tratamiento, suspender los flujos de datos hacia terceros países u organización; la autoridad tendrá poderes de autorización y consulta, entre ellos asesorar al responsable, emitir dictámenes, aprobar proyectos de códigos de conducta, acreditar organismos de certificación, expedir certificaciones, adoptar clausulas tipos, autorizar clausula

⁸²⁵ Cfr. Artículo 57, Funciones, Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

contractuales, acuerdos administrativos, aprobar normas corporativas vinculantes, entre otras⁸²⁶.

4.6. Autoridad de control en las primeras normativas jurídicas europeas

En materia de protección de datos, se inicia un proceso de convergencia y coincidencia de leyes, a tal punto que en un periodo menor a 10 años entran en vigor leyes procedentes de Austria, Dinamarca, Noruega y Francia; en ese sentido, durante el período mencionado, la informática juega un rol importante, suscitando nuevos escenarios legislativos con la aparición de las telecomunicaciones, las nuevas tecnologías, la economía etc.⁸²⁷, sin dejar de lado los acontecimientos ocurridos en ese período como fueron el escándalo de Watergate, el proyecto SAFARI, el informe L`informatisation de la société , el caso G.klass⁸²⁸, motivando y dando paso a la creación de las primeras legislaciones en materia de protección de datos, órgano de control y transferencias internacionales.

Ante esa situación, el sistema de ombudsman⁸²⁹ surge como una institución llamada a la protección de los derechos de tercera generación⁸³⁰, los cuales

⁸²⁶ Cfr. Artículo 58. Poderes, Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

⁸²⁷ Central de Informática., *Informática Leyes de Protección de Datos, Documentación Informática núm. 2, serie Verde /Legislación*, 1ª ed. Presidencia del gobierno, Madrid, 1977, pp. 9-10.

⁸²⁸ Cfr. "la Data Surveillance Bill, la Data Lag sueca de 1973, la Privacy Act norteamericana de 1974". PÉREZ LUÑO, A. E., *Informática y Libertad. Comentario al artículo 18.4 de la Constitución Española...*op. cit., pp. 38-39.

⁸²⁹ El Ombudsman o Defensor del Pueblo de la República Dominicana se instituye a partir de la Ley núm.19-01, elevando o tomando el rango constitucional por medio a la Constitución del 2010, materializándose tres años más tarde en el 2013.

⁸³⁰ MARTÍNEZ DE PISÓN, J., *Las generaciones de Derechos Humanos*, Visto en BETEGÓN, J., LAPORTA, F. J., RAMÓN DE PÁRAMO, J. y PRIETO SANCHÍS, L. (Coordinadores), *Constitución y derechos fundamentales*, Ministerio de la Presidencia, Secretaría General Técnica, Centro de Estudios Políticos y Constitucionales, Madrid, 2004, P. 423-433..

junto a los tribunales tutelan y garantizan tales derechos, protegiendo a los ciudadanos de los tratamientos informatizados de datos personales, instaurando sistemas unipersonales o colegiados entre los que se destaca el Privacy Commissioner canadiense o escandinavo, el Datainspektionen para Suecia, en el caso Danés tenemos el Registertilsynet, para Noruega el Datatilsynet, en el caso de Alemania se encuentran los Comisarios para la protección de datos (Datenschutzbeauftragten) aplicable a escala federal y los länder quienes cuentan con sus propias leyes de protección de datos, en Francia se estableció la Commission Nationale de l'Informatique et des Libertés a raíz del establecimiento de la Ley del 1978 relativa a la informática, archivos y libertades; en Gran Bretaña se estableció el Registrar y el Data Protection Tribunal; Con el sistema de ombudsman se logra y se adquieren funciones dinamizadoras, orientadoras, clarificadoras para agilizar, evitar agresiones y daños a los derechos humanos, derechos fundamentales y los procedimientos de tutela de las libertades⁸³¹, Todo ello expuesto y presentado en las primeras normativas relacionadas con el órgano de control o las instituciones ombudsman creadas como ya hemos comentado para tutelar y garantizar aquellos derechos de tercera generación y expuesto a continuación en las próximas normas.

4.6.1. El Comisario de Protección de Datos de la Ley de Hesse

El Parlamento de la región de Hesse (*Hessischer Landtag*), de la República Federal Alemana aprueba el 17 de octubre de 1970 una Ley de Protección de Datos de Hesse, instituyendo la figura del Comisario de Protección de Datos o Comisario para la Protección de la Información (*Datenschutzbeauftragter*)⁸³² responsable de la entrega de informes periódicos al Parlamento de Hesse⁸³³ a

⁸³¹ PÉREZ LUÑO, A. E., *Las generaciones de derechos Humanos...*op. cit., pp. 213-214,

⁸³² FROSINI, V., *Cibernética, derecho y sociedad...*op. cit., p. 180.

⁸³³ PÉREZ LUÑO, A. E., "Informática y Libertad. Comentario al artículo 18.4 de la Constitución Española..."op. cit., p. 40.

propuesta del Estado, ligado a la administración pública, centrado en la protección de las informaciones recogidas en bancos de datos, siendo ejercido por un funcionario a título accesorio en situación de licencia o funcionario excedente, siendo elegido por el período de la legislación, admitiendo reelección al final de los períodos legislativos pudiendo renunciar o ser cesado del puesto, al mismo tiempo goza de total independencia, no estando sujeto a órdenes o instrucciones de órgano alguno, manteniendo el secreto durante y después de sus funciones, el ministro presidente es competente en conceder autorización para formular declaración alguna, entre cuyas funciones se encuentra la de velar la observación de los preceptos de la ley u otros que aseguren la confidencialidad de los datos de los ciudadanos y de los documentos concernientes a los ciudadanos individualmente considerados, dando cuenta a las autoridades que tutelan la información de las violaciones observadas, proponiendo medidas precautorias para el mejoramiento de la protección de datos ⁸³⁴. Después de varios años es cuando el Comisario ocupa su cargo, presentando su primer informe parlamentario el 10 de febrero de 1976, ya para el 15 de noviembre del mismo año, se aprueba la Ley Federal sobre la Protección de las Informaciones estableciendo el Comisario Federal.

4.6.2. Comisario Federal de Protección de Datos

La Ley Alemana Federal de Protección de Datos⁸³⁵, planteaba entre sus cometidos el de evitar el detrimento de los intereses dignos de protección de los

⁸³⁴ Artículos 7 al 10 Ley de protección de datos de Hesse, CENTRAL DE INFORMÁTICA., *Informática Leyes de Protección de Datos, Documentación Informática núm. 2, serie Verde / Legislación*, 1ª ed. Presidencia del gobierno, Madrid, 1977, nota p. 19-21.

⁸³⁵ Promulgada el 27 de enero de 1977 (Bundesgesetzblatt, I, Z 1997 A, páginas 201 y ss.). En la traducción se ha procurado adaptar la numeración y nomenclatura de los preceptos al sistema usual de nuestro Derecho positivo. Así, se ha sustituido la palabra y signo de párrafo (que en el uso de nuestro Derecho se confunde con artículo o apartado) por la de <<artículo>>. Como primera subdivisión del artículo se usa el <<párrafo>> (Absatz), aunque sin numeral, entendiéndose por tal el texto comprendido entre dos puntos y aparte; le sigue la <<proposición>> (Satz), más generalizada que la voz <<inciso>>, y en su caso la <<semiproposición>> (Halbsatz). Finalmente, la única subdivisión numerada de la proposición es el <<apartado>> Así se expresa en CENTRAL DE INFORMÁTICA., *Informática Leyes de Protección de Datos, Documentación Informática, núm. 2, serie Verde / Legislación*, 1ª ed. Presidencia del gobierno, Madrid, 1977. nota p. 15.

afectados, mediante la protección de los datos personales contra el abuso producido en ocasión del almacenamiento, comunicación, modificación y cancelación (proceso) de tales datos, protegiendo los datos personales almacenados en registros, informatizados, modificados, cancelados o comunicados a partir de registros informatizados por autoridades o entes públicos, personas naturales o jurídicas, sociedades, personas naturales o jurídicas; la Ley Federal al igual que la Ley de Hesse contempla la figura del Comisario de Protección, pero en este caso hablamos de un Comisario Federal de Protección de Datos designado por 5 años por el presidente federal, permitiendo una sola y nueva designación, manteniendo total independencia en el ejercicio de su cargo sujeto a la ley, bajo la tutela del Gobierno Federal, dependiente del Ministerio Federal del Interior y sujeto al control jerárquico y presupuestario del Ministerio Federal del Interior, estando obligado a guardar secreto durante y después de su gestión, solo con la anuencia del Ministerio Federal podrá emitir declaraciones, al mismo tiempo, el Comisionado Federal de protección de datos goza de unas series de funciones y disposiciones entre los que se encuentra la observación de los preceptos de la presente ley. La misma ley contempla la creación de un Comisario de Protección de Datos dirigido a las personas, sociedades y agrupaciones de personas que elaboren automáticamente datos personales y ocuparen de manera permanente a cinco trabajadores, el Comisario no estará sujeto a instrucciones superiores velando por la observancia de la presente ley, recibiendo apoyo de la autoridad de tutela que fuere competente en virtud del derecho estatal, velando a su vez por otras disposiciones sobre protección de datos del ámbito de la presente ley⁸³⁶.

⁸³⁶ Ley Alemana Federal de Protección de Datos, Artículos 1-47, Visto en: CENTRAL DE INFORMÁTICA., *Informática Leyes de Protección de Datos, Documentación Informática, núm. 2, serie Verde / Legislación*, 1ª ed. Presidencia del gobierno, Madrid, 1977, pp. 35-74.

4.6.3. *La Inspección de Datos de Data Lag Sueca*

La Ley Sueca de Información Crediticia de 1973, contempla la figura de la Inspección de Datos, responsable de ejercer la autorización de la actividad de información sobre la solvencia crediticia, concedida por un espacio de 10 años, con restricciones para aquellas personas sujetas a restricciones de adquirir bienes inmuebles, evitando recoger o almacenar informaciones sobre ideas políticas, religiosas, razas o color de una persona, al mismo tiempo, la inspección de datos será responsable de la observancia de la presente ley evitando ocasionar gastos o molestias innecesarias por el proceso de vigilancia, entre ellas, inspeccionar a las personas que ejercieren la actividad de información sobre la solvencia crediticia y la recogida de los documentos relacionados con la actividad existiendo sanciones penales e indemnización de daños y perjuicios a los responsables de ejercer la actividad sin autorización, difundir noticias falsas e infringir los artículos 6-9, 13, 14; las acciones de impugnación se ejercerán ante su Real Majestad por recurso de alzada siendo ejercida su defensa por el Canciller de la Justicia.⁸³⁷

4.6.4. *La Comisión de Protección de Datos / El Consejo de Protección de Datos en Austria*

La Ley Austriaca de 18 de octubre de 1978 de Protección de Datos Personalizados, contempla el derecho de toda persona a exigir y hacer valer en juicio el secreto de los datos personales que le conciernen, la ley contempla la figura del órgano de control⁸³⁸ creando una Comisión de Protección de Datos y un Consejo de Protección de Datos para salvaguardar la protección de datos establecido en la presente Ley Federal, sin perjuicio de la competencia de los

⁸³⁷ Ley Sueca de Información Crediticia, Artículos 1-23, Visto en: CENTRAL DE INFORMÁTICA., *Informática Leyes de Protección de Datos, Documentación Informática, núm. 2, serie Verde /Legislación*, 1ª ed. Presidencia del gobierno, Madrid, 1977, pp. 126-133.

⁸³⁸ Artículo 35.

Tribunales Ordinarios, siendo competencia de la Cancillería Federal la gestión de los órganos mencionados.

4.6.5. Comisión Nacional de Informática y Libertades

La Ley Francesa relativa a la Informática, los Ficheros y las Libertades, es una ley que data del 6 de enero de 1978 conocida como Ley núm. 78-17⁸³⁹, es una ley que a nuestro entender coloca límites a la libertad informática cuya actuación no deberá atentar a la identidad humana, ni a los derechos del hombre, ni a la vida privada, ni a las libertades individuales o públicas tal como lo expresa su artículo 1, creando una Comisión Nacional de Informática y Libertades encargadas de velar por la presente ley, especialmente informar a las personas acerca de sus derechos y obligaciones mediante la consulta y vigilancia de la aplicación de la informática a los tratamientos de informaciones nominativas, gozando de potestad reglamentaria en los supuestos previstos en la presente ley, bajo el presupuesto del Ministerio de justicia, siendo una autoridad administrativa independiente, sus dieciséis miembros serán nombrados por un espacio de 5 años.

4.6.6. La inspección de Datos Noruega

La Ley Noruega de 9 de Junio de 1978, núm. 47, de registros personales, es una ley como su nombre lo indica aplicable a los registros personales y otros usos de los datos personales que pudieran emplearse, entendiendo por datos personales aquellas informaciones y apreciaciones que, directa o indirectamente, pudieran ser puestas en relación con personas individuales,

⁸³⁹ Ley núm. 78-17 de 6 de enero de 1978., Visto en: CENTRAL DE INFORMÁTICA., *Informática Leyes de Protección de Datos, Documentación Informática, núm. 3, serie Verde /Legislación*, 1ª ed. Presidencia del gobierno, Madrid, 1983, pp. 87 y ss.

asociaciones o fundaciones, susceptibles de ser identificadas⁸⁴⁰, el Rey tiene la potestad de disponer sobre su no aplicación a determinados artículos debido a las atribuciones que le atribuye el artículo 3 de la Constitución Noruega de 1814, creando una Inspección de Datos como órgano especial dependiente del Rey y del departamento que el Rey determine, delegando según la Real Orden de 21 de diciembre de 1979 en el Ministerio de Justicia.

Los mecanismos de control y las transferencias internacionales orientadas a la protección de los datos personales, no solo forman parte de las primeras legislaciones en materia de protección de datos, más allá de ellas se observa su franco crecimiento, evolución y madurez, en la medida que se insertan en la evolución de las normativas, situación puesta en contexto en los siguientes epígrafes.

4.7. Autoridades de control en el Convenio 108 del Consejo de Europa

El Convenio n.º 108 contempla *el Protocolo Adicional al Convenio n.º 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencia de datos dado en Estrasburgo el 8 de noviembre de 2001*, asegura en su preámbulo que el ejercicio con completa independencia de las autoridades de control constituye un elemento de protección efectiva de las personas respecto al tratamiento de sus datos personales, a tal punto, que las autoridades de control acuerdan la asignación de poderes de investigación, iniciar procedimientos legales o de dirigirse a las autoridades judiciales respecto a su derecho Interno, ejerciendo sus funciones con completa independencia incentivando la cooperación entre las autoridades de control⁸⁴¹.

⁸⁴⁰ La Ley Noruega de 9 de junio de 1978, Visto en: Central de Informática., *Informática Leyes de Protección de Datos*, Documentación Informática, núm. 3, *serie Verde* /Legislación, 1ª ed. Presidencia del gobierno, Madrid, 1983, pp. 87 y ss.

⁸⁴¹ Artículo 1, autoridad de control, Protocolo Adicional al Convenio N.º 108, Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-2010-14380>. (Última consulta en línea 7 de marzo 2018).

4.8. Autoridades de control en la Directiva 95/46/CE

La Directiva 95/46 de la entonces Comunidad Europea⁸⁴² contempla en sus preceptos⁸⁴³ el tema de la autoridad de control y la creación del Grupo de Protección de las personas en lo que respecta al tratamiento de datos personales asentado en sus articulados⁸⁴⁴, el Grupo gozará de independencia con capacidades de consulta.

La Directiva, contempla la posibilidad de crear en los Estados miembros una o varias autoridades públicas con poderes de investigación, intervención, capacidad procesal, ejerciendo funciones con total independencia y sentido de cooperación entre ellas.

Las autoridades de control, informarán de las solicitudes realizadas por las personas en relación con los derechos y libertades relacionadas con el tratamiento de sus datos personales.

4.9. Autoridades de control en la Ley Orgánica 15/1999 (LOPD)

La Ley Orgánica de protección de datos de carácter personal 15/1999, de 13 de diciembre, presenta en su título VI la Agencia de Protección de Datos como órgano de control, el documento contempla la naturaleza, el régimen jurídico, la asignación del director, la composición del Consejo Consultivo y las funciones.

⁸⁴² Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible en: www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678. (Última consulta en línea 8 de marzo 2018).

⁸⁴³ Capítulo VI, autoridad de control y grupo de protección de las personas en lo que respecta al tratamiento de datos personales. Disponible en: www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678. (Última consulta en línea 8 de marzo 2018).

⁸⁴⁴ Artículo 29 al 30. Disponible en: www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678. (Última consulta en línea 8 de marzo 2018).

Hablamos de un órgano independiente de las administraciones públicas, con personalidad jurídica propia, entre sus funciones se encuentra asegurar el cumplimiento de la ley, recibir peticiones y reclamaciones de los afectados, redactar memoria anual y enviarla al Ministerio de Justicia, ejercer control y adoptar autorizaciones relacionadas con el movimiento internacional de datos, ejerciendo funciones de cooperación internacional, con capacidad de inspección de ficheros y revestido de capacidad sancionadora.

4.10. Autoridades de control en el Reglamento (UE) 2016/679

La nueva normativa de protección de datos de la Unión Europea (UE) consumada en el Reglamento (UE) 2016/679, introduce mejoras y adecuaciones en materia de órgano de control y transferencias internacionales a diferencia de su predecesora la Directiva 95/46/CE; comenzaremos desde las iniciativas relacionadas con el órgano de control dispuestas en las consideraciones del Reglamento destinadas al órgano de control, seguido por sus disposiciones internas.

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016⁸⁴⁵, contempla el tema de una o varias autoridades de control independientes en los Estados miembros, contribuyendo con la aplicación coherente del presente Reglamento en toda la Unión, el Reglamento contempla: a) las normas relativas al establecimiento de la autoridad de control, su competencia, funciones, poderes e informe de actividades de las autoridades de control; b) la cooperación entre las autoridades de control; c) la Comisión, facilitando asistencia mutua y operaciones conjuntas entre los órganos de control, creando a su vez el Comité Europeo de Protección de Datos, sustituto del Grupo de Protección de Datos, los órganos de control

⁸⁴⁵ Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

pueden solucionar conflictos por medio al Comité o los procedimientos de urgencia.

Con el objetivo de evitar cargas administrativas y financieras generadas por las notificaciones indiscriminadas establecidas en la Directiva 95/46/CE, a raíz de la obligación de notificar el tratamiento de datos personales a las autoridades de control, el Reglamento considera la eliminación de notificaciones indiscriminada generales, siendo sustituida por procedimientos y mecanismos eficaces, en particular, para aquellas operaciones de tratamientos que impliquen el uso de nuevas tecnologías⁸⁴⁶.

De la misma forma, debe consultarse a la autoridad de control antes de iniciar actividades de tratamiento si su responsable considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación⁸⁴⁷. Al mismo tiempo, la autoridad de control debe ser consultada durante la tramitación de las medidas legislativas o reglamentarias que establecen el tratamiento de datos personales⁸⁴⁸.

El Reglamento, contempla la necesidad de fomentar la cooperación entre autoridades de control, incentivando el intercambio de información con sus homólogas, sin dejar de lado a las autoridades de datos de terceros países⁸⁴⁹.

La norma, aboga por el establecimiento de autoridades de control entre los Estados, considerando la posibilidad de establecer más de una autoridad de control de la mano con la estructura constitucional y administrativas del Estado, garantizando a su vez el mecanismo de coherencia y su estrecha colaboración entre ellas; la independencia de las autoridades no la exime de los controles financieros o judiciales, disponiendo de recursos financieros, humanos e

⁸⁴⁶ Cfr. Considerando número 89 del Reglamento (UE) 2016/679.

⁸⁴⁷ Cfr. Considerando número 94 del Reglamento (UE) 2016/679.

⁸⁴⁸ Cfr. Considerando número 96 del Reglamento (UE) 2016/679.

⁸⁴⁹ Cfr. Considerando número 116 del Reglamento (UE) 2016/679.

infraestructura propia; supervisando las disposiciones del Reglamento y contribuyendo con la aplicación del mismo en toda la Unión⁸⁵⁰.

Formando parte de los considerandos que dieron pautas a los cimientos de los nuevos cambios reflejados en el Reglamento y su vinculación con la autoridad de control, descansando a lo largo y ancho del capítulo VI.

Con el Reglamento, se crea el Comité Europeo de Protección de datos, gozando de total independencia, garantizando la aplicación coherente del Reglamento, sustentado en el mecanismo de coherencia⁸⁵¹; el Reglamento dispone la creación de la ventanilla única, permitiendo a las empresas la posibilidad de disponer de un solo punto de contacto al momento de necesitar realizar operaciones con los 28 Estados en situaciones que involucren o impacten a toda la Unión Europea, fortaleciendo la cooperación y la coherencia entre los Estados, proporcionando seguridad jurídica a las empresas, ante normas homogéneas⁸⁵², coherentes, con aplicaciones uniformes entre los Estados.

La libre circulación de datos entre los Estados, representa un riesgo para los datos involucrados en la transferencia, en desmedro de lograr una efectiva protección de las personas físicas más allá de la instauración de autoridades independientes en los Estados, situación por las que se hace necesario el

⁸⁵⁰ Cfr. Considerando 117, 119, 120, 129, 133, 135 del Reglamento (UE) 2016/679.

⁸⁵¹ “Cualquier medida de ejecución dictada por una autoridad de control será ejecutable en toda la Unión Europea. Carecerán de validez jurídica y por ello, no serán ejecutables las medidas dictadas por la autoridad de control, cuando siendo preceptivo, no se sometan al mecanismo de coherencia o se dicten existiendo “Objetivos graves”, LÓPEZ CARBALLO, D. (Coordinador), *Protección de datos y habeas data: una visión desde Iberoamérica*, imprenta nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2015, p. 195.

⁸⁵² “Una normativa única en toda la UE tendrá importantes consecuencias para las empresas y aumentará el atractivo de Europa como lugar para hacer negocios, al tiempo que ayudará a la UE en su afán por impulsar normas estrictas de protección de datos en todo el mundo”; Comisión Europea *¿Como simplificará la reforma de la protección de datos en la UE la normativa vigente?*, ficha informativa enero 2016, PDF ISBN 978-92-79-60374-7. Disponible en: ec.europa.eu/newsroom/document.cfm?doc_id=41593. (Última consulta en línea 28 de febrero 2017), p, 2.

conocimiento y empleo de las principales normas legislativas conectadas con las transferencias internacionales expuestas a continuación.

5. Transferencias internacionales de datos

5.1. Conceptos claves

Las transferencias⁸⁵³ internacionales de datos forman parte de las normativas en materia de protección de datos, su impacto está directamente conectado con el crecimiento económico de los Estados producto del aumento de mercancía, situación planteada en los preámbulos de las normativas en materia de protección de datos, reuniones de Jefes de Estado y de Gobierno, u organizaciones internacionales presentadas en el primer capítulo y tratadas a continuación.

El intercambio de información entre dos o más Estados, se encuentra rodeado y al asecho de grandes peligros para la protección de los datos personales, presentando dificultades debido a su característica internacional e ilimitada, obstaculizando con ello su descubrimiento, prevención y castigo.

Provistos de informaciones fraccionadas, a raíz de las diferencias jurídicas existente entre los Estados donde se mueve la información, producto al desplazamiento, transferencia o flujo de información, siendo importante la reglamentación del flujo internacional de datos, soportado en las legislaciones internas de los Estados y como no, en las normas internacionales en materia de protección de datos, focalizadas en las transferencias internacionales, evitando comprometer los derechos y las libertades del individuo fruto al

⁸⁵³ “Transferencia del lat. *Transferens*, -entis, part. Act. de *transferre*, transferir. F. Acción y efecto de transferir. Transferir del lat. *Transferre*. Tr. Pasar o llevar algo desde un lugar a otro”, ACADEMIA ESPAÑOLA, R., *diccionario de la lengua español*, tomo II, vigésima segunda edición, editora Espasa Calpe, S. A., Madrid, 2001, p. 635. También puede verse en ACADEMIA ESPAÑOLA, R., *diccionario de la lengua español*, tomo II, vigésima primera edición, editora Espasa Calpe, S. A., Madrid, 1992, p. 1424.

movimiento de los datos personales orquestados entre las fronteras de los Estados⁸⁵⁴.

Es así, como el movimiento de los datos empleados durante el proceso de la transferencia internacional de datos no puede bajo ningún concepto afectar los datos personales involucrados en la transferencia, asegurando su asiduidad y él reconocido principio de continuidad de la protección de datos ante una transferencia internacional de datos, siendo necesario el esclarecimiento del concepto antes de proseguir o continuar con su exposición⁸⁵⁵.

5.2. Terminología y proceso

Existen varias acepciones relacionadas con los términos empleados en el movimiento de información entre los Estados, en la legislación extranjera se les conoce como transborder data flows y flux internacional de données⁸⁵⁶, en el caso Español la expresión que más se aproxima al caso anglosajón y francófono es la de “flujos internacionales de datos”, el término flujo se relaciona con movimientos de cosas fluidas o líquidas⁸⁵⁷, a diferencia del término transmisión referenciado con el envío de información utilizando las ondas hertzianas; por su parte, existen varias definiciones relacionadas con el flujo Internacional de datos, muestra de ello se observa en las definiciones

⁸⁵⁴ PÉREZ LUÑO, A. E., *Internet y los Derechos Humanos, Derecho y...op. cit.*, pp. 101 y ss.

⁸⁵⁵ DE FRUTOS, J. M., *Globalización de la privacidad: hacía unos estándares comunes*, conferencia presentada en el VI Encuentro Iberoamericano de Protección de Datos, realizado en Cartagena de Indias, Colombia, mayo de 2008, pp. 27-30, tomado de REMOLINA ANGARITA, N., *Insuficiencia de la regulación Latinoamericana frente a la recolección Internacional...op. cit.*, pp.181,182,194.

⁸⁵⁶ “La reciente tendencia doctrinal propone cambiar el término inglés *transborder data flows* por el de *international data services*. Se afirma que hoy día se da más énfasis al sector de los servicios en general que al de intercambio o flujo. ROBINSON, P., “*Legal Issues Raises by TDF*”, *CUSLJ*, vol.11,1986, p.295. Citado por ESTADELLA YUSTE, O, *ibid.*, p. 79, nota 1.

⁸⁵⁷ G. GARZÓN, *El marco jurídico del flujo de datos transfronterizas*, *IBI, Doc. TDF 102, Roma*, 1981, pp.6-7. Citado por ESTADELLA YUSTE, O, *ibid.*, p. 79, nota 3.

presentadas por la ONU⁸⁵⁸, el Convenio n.º 108⁸⁵⁹, la Instrucción 1/200⁸⁶⁰ etc., independientemente de la expresión flujo internacional de datos o transferencia internacional⁸⁶¹ de datos⁸⁶² estas deben incluir: a) la comunicación o transferencia de información entre diferentes Estados llevado a cabo entre un individuo emisor y un receptor, denominado transmisión de información *point-to-point*; b) el objeto empleado en la comunicación o transferencia de información de datos o información a que son sometidas las operaciones que, en su totalidad o en parte, necesitan la ayuda de procedimientos automatizados⁸⁶³, teniendo en cuenta que los flujos son más que simplemente un intercambio de datos.

⁸⁵⁸ Movimiento a través de las fronteras nacionales para procesar, almacenar y recuperar datos, otra definición es Los flujos transfronterizos de datos son definidos por el centro de las Naciones Unidas sobre corporaciones transnacionales como *el movimiento a través de límites nacionales de datos computarizados, capaces de ser leídos por una máquina para su procesamiento, almacenamiento o recuperación* (Centro de las Naciones Unidas sobre Corporaciones Transnacionales, 1982, p. 8) tomado de QUESADA RODRÍGUEZ, A., *protección de datos y telecomunicaciones convergentes*, 1ª ed. Agencia Española de Protección de Datos, Madrid, 2015, p. 233.

⁸⁵⁹ “Transmisión a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento”; CONSEJO DE EUROPA, *Convenio sobre la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal*, Europ. T.S.núm.108, 1981. Publicado, inter alia, ILM, vol.19, 1981, p. 371. Citado por ESTADELLA YUSTE, O., *ibid.*, p. 80, nota 5.

⁸⁶⁰ “(...) La Instrucción 1/2000 define las transferencias internacionales de datos como toda transmisión de datos fuera del territorio español, independientemente de su consideración como cesión o tratamiento por encargo (acceso a los datos por cuenta de terceros). El elemento esencial utilizado para la calificación reside en el hecho de la salida de los datos fuera del territorio español”, así lo expresa ALMUZARA ALMAIDA, C. (Coordinador).; *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. LEX NOVA, S. L., Valladolid, 2007, p. 427.

⁸⁶¹ PIÑAR MAÑAS, J. L. y RECIO GAYO, M., *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, 1ª ed. Wolters Kluwer España, S. A., Madrid, 2018, pp. 156-160.

⁸⁶² La OECD lo define como: “flujo transfronterizo de datos personales” es el movimiento de datos personales a través de fronteras nacionales. Disponible en: <http://www.oecd.org/sti/ieconomy/15590267.pdf>. (Última consulta en línea 2 de diciembre 2017).

⁸⁶³ J. L. PIÑOL RULL, “Los flujos internacionales de datos: aproximación a su regulación jurídica”, UNED, t.IV, Barbastro, 1987, p. 137. Citado por ESTADELLA YUSTE, O, *ibid.*, p. 80, nota 6.

El *medio* empleado en el proceso de las transmisiones internacionales de datos juega un rol estelar y protagónico en el proceso de las transmisiones internacionales de datos, de acuerdo al Convenio 108 y su numeral primero, las transmisiones internacionales a través de las fronteras nacionales pueden ser ejecutadas empleando cualquier medio que fuere, constituyendo los datos su objeto protegido sin dejar de lado los archivos repositorios de los datos, surtiendo efecto en la protección de su contenido, alineando *los datos personales* a la intimidad, privacidad y con ello la protección de las personas físicas.

Una transmisión internacional tiene además del medio un <<transmitente>> que corresponde a toda persona física o jurídica ya sea esta pública o privada sobre la cual recae la responsabilidad del fichero o de los tratamientos de los datos de carácter personal que son objeto de la transferencia internacional y <<destinatario>> al que recibe los datos transferidos ubicados más allá de las fronteras, ya sea una persona física o jurídica, pública o privada⁸⁶⁴. El destinatario puede ser el afectado o interesado o una persona distinta al interesado llamado en ocasiones tercero. De acuerdo al Real Decreto 1720 de 2007 del 21 de diciembre, designa una cesión o comunicación de datos al tratamiento de datos que supone la revelación a una persona distinta al interesado según lo expresado en su artículo 5⁸⁶⁵, presentando afinidad e igualdad en los términos sección o comunicación de datos, términos indistinto para referirse a la revelación de datos dirigidas a terceros o no afectados en el proceso de una sección o comunicación de datos realizados en una transferencia internacional, formando parte de las definiciones contenidas en la LOPD⁸⁶⁶. A raíz del proceso ejecutado en la transferencia, el destinatario se

⁸⁶⁴ ALMUZARA ALMAIDA, C. (Coordinador.), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. LEX NOVA, S. L., Valladolid, 2007, pp. 428-429.

⁸⁶⁵ VERITAS FORMACIÓN, B., *Ley de protección de datos personales*, 1ª ed. FUNDACIÓN CONFEMENTAL, Madrid, 2009, p. 147.

⁸⁶⁶ Artículo 3, literal i, LOPD, BOE» núm. 298, de 14/12/1999.
Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750>. (Última consulta en línea 16 de noviembre 2017).

convierte en compromisario, obteniendo la capacidad de decisión sobre el contenido, uso y finalidad del tratamiento.

El proceso de exportación e importación⁸⁶⁷ no es ajeno a las transmisiones internacionales de datos, asignando mayor énfasis al proceso de exportación⁸⁶⁸ sin dejar a un lado el proceso de importación, contemplando como modelo o ejemplo el Estado español. Una vez que los datos son transmitidos fuera del territorio, el tratamiento de tales datos queda bajo la sombra o amparo de la legislación correspondiente al Estado destinatario de las informaciones, escapando de los mecanismos de control del Estado exportador, dígase las autoridades de control o en el caso mencionado a la Agencia Española de Protección de datos (AEPD), razones valederas para mostrarnos la necesidad de mantener estrictas vigilancias y garantías al proceso de transferencias internacionales de datos⁸⁶⁹.

Otros consideran, que la importación y exportación de datos personales ubicados en un país y enviados a otros países, son reconocidos bajo la expresión de “*transferencia internacional de datos personales*”, “*circulación*

⁸⁶⁷ Artículo 3, literal d), e); Decisión 2001/497/CE de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE, notificada con el número c (2001) 1539.

d) Se entenderá por <<exportador de datos>> el responsable del tratamiento que transfiere los datos personales.

e) Se entenderá por <<importador de datos>> el responsable del tratamiento que convenga en recibir del exportador de datos personales para su posterior tratamiento de conformidad con los términos de la presente Decisión; la Decisión 2004/915/CE de 27 de diciembre de 2004 que modifica la 2001/497/CE presenta la siguiente definición de importador de datos donde se entenderá el responsable del tratamiento que acepte recibir datos personales procedentes del exportador de datos para su posterior tratamiento de conformidad con los términos de las presentes cláusulas y que no esté sujeto al sistema de un tercer país por el que se garantice una protección adecuada.

⁸⁶⁸ Para un análisis sobre el tema, ver A.M.C. NUGTER, *Transborder Flow of Personal Data within the European Community*, Kluwer, Deventer, 1990, p. 235. Citado por ESTADELLA YUSTE, O., *ibid.*, p. 109, nota 6.

⁸⁶⁹ ALMUZARA ALMAIDA, C. (Coordinador), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. LEX NOVA, S. L., Valladolid, 2007, p. 428.

*transfronteriza de datos personales”, “flujos transfronterizos de datos de carácter personal” o “transmisión internacional de datos”*⁸⁷⁰.

Las transferencias internacionales de datos involucran normas jurídicas que van más allá de las fronteras de los Estados, sobrepasando su ámbito territorial y nacional en aras de la protección de los datos personales, evitando obstáculos al comercio⁸⁷¹ en detrimento de la economía sin afectar las relaciones internacionales entre los Estados⁸⁷².

Como vemos, la transferencia internacional se refleja en las normas internas de los Estados o comunidades, siendo una actividad muy regulada en el ámbito de las legislaciones europeas⁸⁷³, como son los casos de la Directiva 95/46/CE, la Ley española (LOPD), el Reglamento de la Unión Europea, entre otras.

La LOPD concentra en sus artículos 33 y 34, las reglas que rigen la materia de transferencia internacional, supeditada o reflejada en los artículos 25 y 26 de la Directiva y la Instrucción 1/2000 de la Agencia Española de Protección de

⁸⁷⁰ REMOLINA ANGARITA, N., *Insuficiencia de la regulación Latinoamericana frente a la recolección Internacional...op. cit.*, p.193.

⁸⁷¹ “(...) La necesidad económica y cultural de participar en el flujo internacional de informaciones obligará a nuestros legisladores a sacudir su pereza, pues de no hacerlo nuestras empresas o nuestros centros de cultura e investigación no podrán beneficiarse de los datos de los países más avanzados de nuestro entorno. Esos países condicionan la transmisión de sus datos e informaciones al exterior a la existencia en el país receptor – en este caso España – de normas de protección de datos. De no contar con un sistema adecuado de garantías podríamos vernos ante la penosa situación de convertirnos en meros suministradores de datos al exterior, quedándonos marginados del aprovechamiento del flujo internacional de informaciones”; PÉREZ LUÑO, E., *Panorama general de la legislación española sobre protección...op. cit.*, p. 33.

⁸⁷² “(...) Una exageración en la limitación del flujo Internacional de datos se refleja en la pérdida de negocios para sectores productivos probablemente ajenos a toda actividad lucrativa relacionada con el manejo de información”; MILLÉ, A., *informaciones de carácter personal Derecho Comparado y prospectiva*, visto en CARRASCOSA LÓPEZ, V. (Coordinador), *Informática y Derecho, II Congreso internacional de Informática y Derecho*, 1ra. ed., Universidad Nacional de Educación a Distancia, Mérida, Sevilla, 1996, p. 1390.

⁸⁷³ VERITAS FORMACIÓN, B., *Ley de protección de datos personales*, 1ª ed. FUNDACIÓN CONFEMENTAL, Madrid, 2009, p. 167.

Datos⁸⁷⁴, prohibiendo la Agencia de Protección de Datos transferencias a aquellos países que no contemplen un nivel equiparable de protección como se menciona en el artículo 33.1 de la LOPD, o cuenten con la aprobación de la Agencia, como continúa diciendo su artículo 34, estableciendo igual o similar protección en el país destino, protegiendo y salvaguardando las normas del país exportador en materia de derechos fundamentales como intimidad, privacidad etc.

5.3. Tránsito de datos a terceros países u organismos internacionales

El aumento de los flujos internacionales en y hacia Latinoamérica, incrementará la expansión del comercio entre los Estados Iberoamericanos, fortaleciendo su cooperación, sin dejar de lado los Estados pertenecientes a la Unión Europea, las organizaciones internacionales, u otros Estados más allá del ámbito latinoamericano.

Una situación que invita a instaurar niveles de protección de datos en sus normativas de protección, contemplando el establecimiento de métodos alternativos como códigos tipos, cláusulas contractuales, etc. Ante la ausencia de niveles de seguridad requeridos, permitiendo o posibilitando la transferencia o flujo de datos hacia terceros países desprovistos de normas equivalentes o adecuadas en materia de protección de datos.

5.3.1. Niveles de protección de datos

El proceso de los flujos transfronterizos envueltos en las legislaciones establecidas en los convenios, normas nacionales e internacionales al momento de ejecutar los flujos de datos hacia otros Estados, contempla diferentes concepciones; iniciamos con el Convenio 108, el cual establece

⁸⁷⁴ ALMUZARA ALMAIDA, C. (Coordinador), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. LEX NOVA, S. L., Valladolid, 2007, p. 428.

excepciones a los flujos transfronterizos de datos de carácter personal, entre ellos, la posibilidad de establecer flujos transfronterizos de datos de carácter personal con destino al territorio de otra parte cuando esta se encuentra en la capacidad de establecer una protección equivalente⁸⁷⁵, el termino equivalente prevalece en el proceso de la transferencia internacional impulsada por el Convenio 108, ahora bien, el Protocolo Adicional al Convenio n.º 108 contempla transferencias de datos personales a destinatarios que no formen parte del Convenio cuando el Estado u organización asegure un nivel adecuado de protección⁸⁷⁶, es así como, luego de transcurrido más de 15 años de la entrada del Convenio, el nivel de protección se mueve de niveles de protección equivalentes a niveles de protección adecuados, alineado con el escenario de las nuevas legislaciones, y con ello, flexibilizar la transferencia de datos entre los Estados, sin debilitar o colocar en riesgo la protección de los datos envueltos en la transferencias.

La Comunidad Europea contempla en su Directiva 95/46/CE un nivel de protección de datos adecuado al momento de ejecutar transferencias de datos personales a terceros países que sean objeto de tratamiento, o Estados destinados a ser objeto de tratamiento con posterioridad a su transferencia, posibilitando únicamente la ejecución de transferencia, cuando sin perjuicio del cumplimiento de las disposiciones del derecho nacional adoptado y con arreglo a las demás disposiciones de la presente Directiva, el país tercero garantice ese nivel de protección⁸⁷⁷, respetando las estructuras y características locales del país destinatario⁸⁷⁸; en el Reglamento (UE) 2016/679 aplicable a partir del

⁸⁷⁵ Artículo 12, numeral 3, Convenio n.º 108 del Consejo de Europa, 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

⁸⁷⁶ Artículo 2, literal 1, Protocolo Adicional del Convenio N.º 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencia de datos del 8 de noviembre de 2001.

⁸⁷⁷ Artículo 25, numeral 1, Directiva 95/46 CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en los que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

⁸⁷⁸ ALMUZARA ALMAIDA, C. (Coordinador), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. LEX NOVA, S. L., Valladolid, 2007, p. 430.

25 de mayo de 2018 se establece un nivel de protección adecuado para aquellas transferencias de datos personales realizadas a un tercer país u organización internacional a la par o al unísono con la Directiva 95/46/CE⁸⁷⁹; por su lado y producto al principio de supremacía del derecho comunitario sobre el derecho nacional, las decisiones de la Comisión respecto al valor adecuado reconocido en su Directiva y en su Reglamento de aplicación nacional, los Estados asumirán en sus normativas nacionales las decisiones otorgadas por la Comisión.

En el caso de España, la LORTAD consideraba un nivel de protección equiparable al momento de contemplar transferencias temporales o definitivas de datos de carácter personal a países que no proporcionen un nivel de protección equiparable al que presta la presente ley⁸⁸⁰, la actual Ley Orgánica de Protección de Datos Personales de España (LOPD) otorga el mismo nivel de protección de su antecesora (LORTAD), reconociendo en su artículo 33 el carácter equiparable⁸⁸¹ cuando se refiere al nivel de protección de los datos personales, la misma ley contempla que en caso de que el Estado no cumpla con la existencia de una ley equiparable, la Agencia Española de Protección de Datos otorgará autorización cuando el país de destino cumpla con un nivel adecuado de garantías, observando las circunstancias necesarias que ocurren durante el proceso de las transferencias, considerando: a) la naturaleza de los datos; b) la finalidad y la duración del tratamiento o de los tratamientos previstos, c) el país de origen y el país de destino final; d) las normas de derechos generales o sectoriales vigentes en el país tercero de que se trate; e)

⁸⁷⁹ Artículo 45, literal 1, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

⁸⁸⁰ Artículo 32, *Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter persona*. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189>. (Última consulta en línea 23 de junio 2018).

⁸⁸¹ Artículo 33, numeral 1, *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750>. (Última verificación en línea 21 de septiembre 2017).

el contenido de los informes de la Comisión de la Unión Europea, así como f) las normas profesionales y las medidas de seguridad en vigor en dichos países⁸⁸², es decir, la norma no cierra el proceso a las transferencias de datos a terceros países u organizaciones que no gocen de normativas equiparables a la Unión Europea y los Estados partes, incluido España con su ley actual, si no que por medio a la Agencia de Protección de Datos se otorga un salvoconducto hacia las garantías necesarias en materia de protección de datos cuando se trate de transferencias o movimientos internacionales de datos hacia terceros países.

Ante tales situaciones, se crean mecanismos que garantizan y hacen posible el proceso de transferencias internacionales de datos de países que cuentan con normas en materia de protección de datos como la Unión Europea, a países que no cuentan con niveles equiparables en materia de protección de datos incluido los Estados Iberoamericanos y americanos, incluyendo los Estados Unidos, siendo considerado el principal destinatario de las transferencias internacionales hacia los considerados países terceros⁸⁸³; entre los denominados terceros países se encuentran: a) aquellos que cumplen con lo establecido en la Comisión para la realización de transferencias internacionales; b) los beneficiarios de aprobación de la Comisión Europea (nivel adecuado) u otros, a los cuales se les reconoce el nivel adecuado en algunos sectores o determinado tipo de transferencia, para el primer caso se encuentran los 28 Estados miembros de la Unión Europea y tres países miembros del Espacio Económico Europeo (EEE) (Noruega, Liechtenstein e Islandia), para el segundo, los aprobados por la Comisión con rango de nivel adecuado, estos son⁸⁸⁴ Andorra⁸⁸⁵, Argentina⁸⁸⁶, Canadá (organizaciones

⁸⁸² Artículo 33, numeral 1, *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750>. Y artículo 25 numeral 2 directiva 95/46 CE. (Última verificación en línea 21 de septiembre 2017).

⁸⁸³ ALMUZARA ALMAIDA, C. (Coordinador), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. LEX NOVA, S. L., Valladolid, 2007, p. 435.

⁸⁸⁴ *Protección de Datos, Normas para la protección de datos personales dentro y fuera de la UE*. Disponible en:

comerciales)⁸⁸⁷, Islas Feroe⁸⁸⁸, Guernesey⁸⁸⁹, Israel⁸⁹⁰, Isla de Man⁸⁹¹, Jersey⁸⁹², Nueva Zelanda⁸⁹³, Suiza⁸⁹⁴, Uruguay⁸⁹⁵ y Estados Unidos (EE.UU)⁸⁹⁶.

http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

(Última consulta en línea 20 de noviembre 2017).

⁸⁸⁵ 2010/625 / UE : *Decisión de la Comisión de 19 de octubre de 2010 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales en Andorra* (notificada con el número C (2010) 7084) Texto con EEE pertinencia.

⁸⁸⁶ 2003/490 / CE : *Decisión de la Comisión de 30 de junio de 2003 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales en Argentina*.

⁸⁸⁷ 2002/2 / CE : *Decisión de la Comisión de 20 de diciembre de 2001 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales prevista en la Ley Canadiense de Protección de Datos Personales y Documentos Electrónicos* (notificada en el documento número C (2001) 4539)

⁸⁸⁸ 2010/146 / UE : *Decisión de la Comisión de 5 de marzo de 2010 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada proporcionada por la Ley de Feroe sobre tratamiento de datos personales* (notificada con el número C (2010) 1130).

⁸⁸⁹ 2003/821 / CE : *Decisión de la Comisión de 21 de noviembre de 2003 sobre la protección adecuada de los datos personales en Guernesey* (Texto pertinente a efectos del EEE) [notificada con el número C (2003) 4309].

⁸⁹⁰ 2011/61 / UE : *Decisión de la Comisión de 31 de enero de 2011 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales por parte del Estado de Israel con respecto al tratamiento automatizado de datos personales* (notificada en el documento C (2011) 332).

⁸⁹¹ 2004/411 / CE : *Decisión de la Comisión de 28 de abril de 2004 sobre la protección adecuada de los datos personales en la Isla de Man*.

⁸⁹² 2008/393 / CE : *Decisión de la Comisión de 8 de mayo de 2008 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales en Jersey* (notificada con el número C (2008) 1746).

⁸⁹³ 2013/65 / UE : *Decisión de Ejecución de la Comisión de 19 de diciembre de 2012 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales por Nueva Zelanda* (notificada con el número C (2012) 9557).

⁸⁹⁴ 2000/518 / CE : *Decisión de la Comisión de 26 de julio de 2000 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales facilitada en Suiza* [notificada con el número C (2000) 2304].

⁸⁹⁵ 2012/484 / UE: *Decisión de Ejecución de la Comisión de 21 de agosto de 2012 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales por parte de la República Oriental del Uruguay*

5.3.2. Excepciones a las transferencias internacionales

Desde su creación, la Directiva 95/46 zanjeo diferencias insalvables con las normas estadounidenses, debido a su política legislativa de mínimos, haciendo que los niveles de protección de los Estados Unidos (EE. UU) no estuvieran a la par con las normas exigidas por la Unión Europea en materia de protección de datos (nivel adecuado), ante tal situación, impulsado por las empresas estadounidenses ante una disminución de sus negocios, se originaron propuestas y acuerdos para el establecimiento de flujos transnacionales entre la Unión Europea y Estados Unidos, específicamente en temas como la libre circulación de los datos con las empresas europeas y las estadounidenses, creando acuerdos bilaterales entre EE.UU y la Unión Europea, surgiendo acuerdos como el de Puerto Seguro o *Safe Harbour*⁸⁹⁷, un escenario muy diferente al planteado por aquellos Estados considerados con un nivel adecuado de protección otorgados por las decisiones ejecutadas por la

con respecto al tratamiento automatizado de datos personales (notificado con arreglo al documento C (2012) 5704).

⁸⁹⁶ Estados Unidos por medio a la Decisión de Puerto Seguro de la Comisión 2000/520/CE de 26 de Julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos (*DO L* 215, de 25 de agosto de 2000), esta decisión fue declarada invalida el 6 de Octubre de 2015 por el tribunal de justicia de la Unión Europea; el 6 de noviembre de 2015 la Comisión Europea adoptó una comunicación sobre la transferencia de datos personales de la UE a los Estados Unidos tras la sentencia del Tribunal de justicia en el asunto C-362/14 (Schrems), cuyo objetivo se convirtió en proporcionar una visión general de las herramientas alternativas utilizadas en el proceso de las Transferencias Transatlántica de datos en ausencia de decisiones de adecuación, siendo publicado un proyecto de decisión de adecuación y compromisos de las autoridades estadounidenses el 29 de febrero de 2016, ya para el 13 de abril de 2016, el Grupo de Trabajo del artículo 29 emite un dictamen sobre el proyecto de decisión de adecuación del proyecto de protección de la UE y los Estados Unidos; el 8 de Julio de 2016, el Comité del artículo 31 (comitología) aprueba el proyecto de decisión revisado; el 12 de Julio de 2016, la Comisión adoptó la Decisión 2016/1250 sobre la adecuación de la protección del Escudo de privacidad UE-EE.UU, de conformidad con la Directiva 95/46/ CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección proporcionada por el escudo de privacidad UE-EE.UU, bajo la notificación con el número C (2016) 4176. “*Decisiones de la Comisión sobre la adecuación de la protección de datos personales en terceros países* “. Disponible en: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm. (Última consulta en línea 20 de noviembre 2017).

⁸⁹⁷ Los principios de puerto seguro se fundamentan en las directrices de protección de datos de la Organización para la Cooperación y el Desarrollo Económico (OCDE), adoptadas el 23 de septiembre de 1980 y las preguntas más frecuentes o FAQ.

Comisión, siendo aplicable a todas las transferencias internacionales de datos sin restricción alguna, gozando del privilegio manifiesto de aquellos Estados que cumplen con el nivel adecuado de protección de datos de la UE, un privilegio de doble vía, aplicado a transferencias internacionales de datos procedentes de países terceros con niveles adecuados hacia la Unión Europea y los procedentes de la Unión Europea hacia los terceros países.

Debemos puntualizar, que tanto Canadá como Estados Unidos, no cuentan con amplios niveles adecuados de protección de datos para el ejercicio o ejecución de transferencias internacionales hacia terceros países que cuentan con normas adecuadas o equivalentes como los reconocidos por las decisiones de la Comisión, a pesar de ello, las normas europeas, dígase el Convenio n.º 108⁸⁹⁸, su Directiva 95/46 CE⁸⁹⁹, el Reglamento (UE) 2016/679⁹⁰⁰, y las leyes nacionales de los Estados, tales son los casos de la Ley Orgánica 15/99⁹⁰¹

⁸⁹⁸ Artículo 2, numeral 2, Protocolo Adicional del Convenio n.º 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y relativo a Transferencias de Datos.

⁸⁹⁹ Artículo 26, Excepciones, Directiva 95/46 CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

⁹⁰⁰ Artículo 46 Transferencias mediante garantías adecuadas, artículo 47 Normas Corporativas Vinculantes, Artículo 48 Transferencias o Comunicación no autorizadas por el Derecho de la Unión, Artículo 49 Excepciones para situaciones específicas, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

⁹⁰¹ Artículo 34 Excepciones, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público.

(LOPD) y su antecesora, la Ley Orgánica 5/92⁹⁰² LORTAD etc. Establecen excepciones al proceso de transferencias internacionales de datos personales a países terceros que no gozan de normas adecuadas, permitiendo el establecimiento de flujos transfronterizos de datos desde y hacia países terceros, no considerados con niveles adecuados; con la medida, contribuyen a la ejecución de contratos o acuerdos entre las partes, protegiendo la vida, fomentando la economía de los países terceros que no cuentan con niveles adecuados, evitando el menor obstáculo posible en el establecimiento de flujos transfronterizos entre los Estados, cuyas normas nacionales se encuentran en desarrollo, o por el contrario, no cuentan con la fortaleza económica, institucional, legislativa etc. para ser seleccionados por la Comisión y formar parte de los terceros países con normas adecuadas en el establecimiento de transferencias internacionales.

El apartado 2 y 4 del artículo 26 de la Directiva 95/46/CE correspondiente a las excepciones, contempla la capacidad de los Estados miembros de la Unión Europea de autorizar transferencias internacionales a los Estados que no garanticen un nivel adecuado cuando el responsable del tratamiento pueda ofrecer garantías suficientes relacionadas con la protección de la vida privada, sus derechos y libertades fundamentales, cuyas garantías podrán derivarse de cláusulas contractuales; cuando las cláusulas contractuales tipos ofrezcan las garantías *suficientes*⁹⁰³, los Estados miembros adoptarán las medidas

Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

⁹⁰² Artículo 33 Excepciones, *Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD)*. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189>. (Última consulta en línea 23 de junio 2018).

⁹⁰³ Cursiva nuestra.

necesarias para ajustarse a la decisión de la Comisión, el apartado 2 ofrece flexibilidad en el proceso de transferencia de datos a terceros países y el apartado 4 establece cláusulas contractuales tipos⁹⁰⁴.

5.3.3. Cláusulas contractuales tipo

La flexibilidad en el proceso de las transferencias internacionales, permite facilitar el movimiento o flujos de datos procedentes de las comunidades, para ello, los responsables del tratamiento deben estar en capacidad de realizar transferencias internacionales a escala mundial utilizando un único conjunto de normas de protección de datos ante su inexistencia, las cláusulas contractuales son de amplia utilidad para llevar a cabo transferencias de datos personales desde todos los Estados miembros⁹⁰⁵ a terceros países.

Con la Decisión 2001/497/CE del 15 de junio⁹⁰⁶ relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE, se ofrece garantías suficientes en el establecimiento de transferencias de datos personales a terceros países que no ofrecen niveles adecuados, con la Decisión, se ofrecen niveles de mínimos

⁹⁰⁴ Considerando 4, Decisión 2001/497/CE de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE, notificada con el número c (2001) 1539. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32001D0497>. (Última consulta en línea 14 de septiembre 2017).

⁹⁰⁵ “A fin de facilitar los flujos de datos procedentes de la Comunidad, es conveniente que los responsables del tratamiento estén en condiciones de realizar transferencias de datos a escala mundial ateniéndose a un único conjunto de normas de protección de datos. En ausencia de una normativa internacional en esta materia, las cláusulas contractuales tipo constituyen una herramienta de gran utilidad que permite transferir datos personales desde todos los Estados miembros con arreglo a un conjunto de normas comunes. En este sentido, la Decisión 2001/407/CE...establece un conjunto de cláusulas contractuales tipo que prevé garantías adecuadas para la transferencia de datos a terceros países”. Considerando 1 Decisión 2001/497/CE.

⁹⁰⁶ Con la Decisión 2004/915 de 27 de diciembre de 2004 se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países, notificado con el número c (2004) 5271. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32004D0915>. (Última consulta en línea 14 de septiembre 2017).

en el establecimiento de transferencias internacionales hacia terceros países, siendo aplicable únicamente a la protección de datos, no aplicable a las transferencias de datos personales por el responsables del tratamiento, aplicando para ello la Decisión 202/16/CE del 27 de diciembre de 2001 sustituida por la Decisión 2010/87/UE de 5 de febrero de 2010 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecido en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, en donde el encargado del tratamiento actúa en nombre del responsable no exigiendo las mismas garantías entre el responsable y el encargado del tratamiento quien actúa en nombre del responsable⁹⁰⁷.

La utilización de cláusulas contractuales tipos, no tiene un carácter obligatorio, ya que representan una de las distintas posibilidades contempladas en la Directiva 95/46/CE para el establecimiento de transferencias internacionales hacia terceros países de forma lícita, posibilitando al exportador e importador la selección de cualquier método jurídico, alternativas de cláusulas contractuales⁹⁰⁸, que ofrezca las garantías suficientes contemplada en la Directiva, evitando posibles modificaciones, mezclas, ya sean de forma total o parcial; con la Decisión 2004/915⁹⁰⁹, se implementa el sistema de responsabilidades para el exportador e importador de datos ante los

⁹⁰⁷ Considerando 8, Decisión 2001/497/CE de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE, notificada con el número c 2001/1539. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32001D0497>. (Última consulta en línea 14 de septiembre 2017).

⁹⁰⁸ Considerando Segundo de la Decisión 2004/915/CE

⁹⁰⁹ Condicionantes básicos para la adopción de nuevas cláusulas contractuales tipos.

- a) que las cláusulas contractuales tipo propuestas aporten un nivel de protección comparable al de las adoptadas en virtud de la Decisión 2001/497/CE de la Comisión;
- b) que las cláusulas propuestas ofrezcan un valor añadido que supere el mero hecho de ser más favorables para las empresas, y sean también más favorables para los ciudadanos.

Dictamen 8/2003 sobre el proyecto de cláusulas contractuales tipo presentado por un grupo de asociaciones empresariales («The alternative model contract»), grupo del artículo 29 sobre protección de datos, adoptado el 17 de diciembre de 2003. 11754/03/ES WP 84.

Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp84_es.pdf (Última consulta en línea 27 de noviembre).

interesados, estableciendo las cláusulas (culpa in eligendo) mediante la cual el exportador es responsable de no realizar esfuerzos razonables para determinar que el importador sea capaz de cumplir con sus obligaciones⁹¹⁰.

5.3.4. Sistema de responsabilidades

Al analizar el Dictamen 8/2003 sobre el proyecto de cláusulas contractuales tipo, fruto de la presentación realizada por el grupo de asociaciones empresariales (<<The alternative model contract>>⁹¹¹ a raíz de la propuesta de modificación de la Decisión 2001/497/CE y creación de la Decisión 2004/915/CE⁹¹² de 27 de diciembre de 2004, el grupo de protección se enfoca en el aseguramiento de indemnizaciones para las personas, más que en la búsqueda de responsabilidades para el exportador e importador de datos, disponiendo de los medios necesarios que les permitan ejercer derechos de terceros beneficiarios, para ello se recomienda aclarar el sistema de responsabilidades subsidiarias y complementarlo con unas series de recomendaciones, algunas de ellas implementadas en la Decisión 2004/915/CE de 27 de diciembre de 2004⁹¹³.

⁹¹⁰ Considerando 3 y 5, Decisión 2004/915/CE de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países, notificada con el número C 2004/5271. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32004D0915>. (Última consulta en línea 14 de septiembre 2017).

⁹¹¹ Grupo de Asociaciones empresariales conformado por: Cámara Internacional de Comercio (ICC), Japan Business Council in Europe (JBCE), European Information and Communications Technology Association (EICTA), EU Committee of the American Chamber of Commerce in Belgium (Amcham), Confederation of British Industry (CBI), International Communication Round Table (ICRT) y Federation of European Direct Marketin Associations (FEDMA). Considerando Segundo de la Decisión 2004/915/CE.

⁹¹² "...un nivel de protección de datos equivalente al proporcionado por el conjunto de cláusulas adoptado por la Decisión 2001/497, aunque utilizando mecanismos diferentes". Considerando Segundo de la Decisión 2004/915/CE.

⁹¹³ Extracto de modificaciones implementadas en la decisión 2004/915/CE, a raíz del dictamen 8/2003 sobre el proyecto de cláusulas contractuales tipo presentado por un grupo de asociaciones empresariales («The alternative model contract»), adoptado el 17 de diciembre de 2003: <<Los responsables del tratamiento podrán optar por uno de los conjuntos - I o II - recogidos en el anexo. Sin embargo, no podrán modificar las cláusulas ni combinar elementos de distintas cláusulas ni los conjuntos>>, << A efectos del apartado 1, cuando el responsable

El Grupo de Protección de las Personas en lo que respecta al tratamiento de Datos Personales, en lo sucesivo denominado <<Grupo>> tiene su origen a raíz de la creación del artículo 29 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995⁹¹⁴, reemplazado por el Comité Europeo de Protección de Datos⁹¹⁵, otorga el visto bueno al proyecto de cláusulas contractuales tipo presentado por la cámara de Comercio Internacional y asociaciones empresariales, coincidiendo con la Comisión ante la posibilidad de adoptar otras cláusulas contractuales tipo, permitiendo mayor variedad y flexibilidad al momento de ser escogida por los operadores económicos, contribuyendo con las transferencias de datos personales a terceros países realizado por las empresas, garantizando la protección de los derechos y libertades fundamentales de las personas, siendo beneficiados por la Directiva Comunitaria.

Las autoridades de control de los Estados miembros sustentada en sus funciones y capacidades, serán competentes para evaluar si el exportador cumple o cumplió con la legislación nacional durante el proceso de las transferencias internacionales con terceros países, garantizando una adecuada protección durante la transferencia, con la facultad de mediar, prohibir o

del tratamiento ofrezca garantías suficientes derivadas de las cláusulas contractuales tipo contenidas en el conjunto II del anexo, las autoridades competentes responsables de la protección de datos podrán ejercer sus facultades para prohibir o suspender los flujos de datos en cualquiera de los siguientes casos: a) si el importador de datos se niega a cooperar de buena fe con las autoridades responsables de la protección de datos o a cumplir las obligaciones que le incumben claramente en virtud del contrato; b) si el exportador de datos se niega a adoptar las medidas necesarias para hacer cumplir el contrato al importador de datos en el plazo normal de un mes a partir del momento en que la autoridad competente responsable de la protección de datos se lo notifique.>>

Decisión 2001/497/CE de 15 de junio de 2001, *relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE*, notificada con el número c (2001) 1539. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32004D0915>. (Última consulta en línea 14 de septiembre 2017).

⁹¹⁴ Artículo 1, *Directiva 95/46 CE*. Disponible en: www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678. (Última consulta en línea 8 de marzo 2018).

⁹¹⁵ Artículo 2, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* (Reglamento general de protección de datos). Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807>. (Última consulta en línea 8 de marzo 2018).

suspender la transferencia bajo el amparo de la Directiva 95/46/CE⁹¹⁶ y el Reglamento (UE) 2016/679⁹¹⁷.

En las próximas líneas abordaremos las transferencias internacionales en las normas legislativas.

5.4. Transferencia internacional en las primeras constituciones y legislaciones

5.4.1 Ley Austriaca de Protección de Datos Personales de 18 de octubre de 1978

La Ley Austriaca de 18 de octubre de 1978 de Protección de Datos Personalizados, presenta en su cuarta sección las condiciones necesarias para la transmisión ejecutada por medios automáticos desde Australia al extranjero, siendo ejecutadas siempre y cuando cumplan las siguientes condiciones y cuenten con la autorización de la Comisión de Protección de Datos: 1) existencia de habilitación legal; 2) consentimiento por escrito del interesado; 3) garantía de las medidas idóneas para la indeterminabilidad del interesado; 4) la facilitación de datos correspondientes al pago de prestaciones en dinero a una empresa de crédito; las siguientes condiciones no contemplan autorización de la Comisión de Protección de Datos: 1) transmisiones de datos realizadas por el comitente en calidad del interesado, 2) la existencia en otros Estados de leyes comparables a la ley federal, 3) la existencia de convenio internacional.

⁹¹⁶ Considerando 7, 15 y 21, artículo 4, numeral 1, *Decisión 2001/497/CE de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE*, notificada con el número c 2001/1539.

⁹¹⁷ Numeral 3, artículo 46; literal r, numeral 1 del artículo 57, *Reglamento (UE) 2016/679*. Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807>. (Última consulta en línea 8 de marzo 2018).

5.4.2. Ley Noruega núm. 47 de Registros Personales de 9 de junio de 1978

La Ley Noruega de 9 de junio de 1978, número 47, de Registros Personales contempla la transferencia de datos al extranjero, no pudiendo ser enviado al extranjero los datos relacionados con raza, ideas políticas o religiosas, delito, personas procesada o condenadas en causa criminal, datos de la salud, abuso de estupefacientes, comportamiento sexual, situación familiar más allá de parentesco, estado civil etc. sin la autorización del Rey o la creación de registros de persona que hubiere de hacer uso de medios electrónicos, pudiendo dictar disposiciones de colaboración entre la inspección de datos y las autoridades inspectoras de otros países⁹¹⁸.

5.5. Transferencia internacional en la ONU

El 14 de diciembre de 1990 en la 68ª sesión plenaria, mediante resolución 45/95, la Asamblea General, recordando: a) la Resolución 44/132 de la 82ª Sesión Plenaria del 15 de diciembre de 1989; b) las Resoluciones 1990/42 de la Comisión de Derechos Humanos de 6 de marzo de 1990; y c) la Resolución 38 del mismo año perteneciente al Consejo Económico y Social del 25 de mayo de 1990 titulado “Principios rectores sobre la utilización de ficheros computarizados de datos personales” aprobados durante la sesión plenaria, exhorta a los Estados miembros tomarlo en consideración en sus leyes y reglamentos⁹¹⁹; el documento, presenta las orientaciones a las cuales deben sujetarse los Estados para llevar a la práctica las normas relativas a los archivos de datos personales informatizados, es bueno aclarar que como expresa el documento, los procedimientos se dejan a la iniciativa de cada Estado, sujetos a las orientaciones del documento compuesto por dos

⁹¹⁸ Artículo 9, 36, Ley núm. 78-17 de 6 de enero de 1978, Central de Informática., *Informática Leyes de Protección de Datos*, Documentación Informática, núm. 3, serie Verde /Legislación, 1ª ed. Presidencia del gobierno, Madrid, 1983, pp. 9 y 36.

⁹¹⁹ Cuadragésimo Quinto Período de Sesiones, Asamblea General.
Cfr. Disponible en: <http://www.un.org/es/comun/docs/?symbol=A/RES/45/95>. (Última consulta en línea 1 de dic.2017).

acápites, el primero contiene diez principios relativos a las garantías mínimas que deben prever las legislaciones nacionales y el segundo corresponde a la aplicación de las directrices a los archivos de datos personales mantenidos por organizaciones gubernamentales.

El primer acápite relacionado con los principios, se observa en el noveno principio los flujos transfronterizos de datos establecidos entre dos o más Estados, siendo viable cuando las legislaciones de los Estados ofrezcan salvaguardias comparables, capaces de proteger la privacidad⁹²⁰, haciendo posible la libre circulación de información en cada uno de los Estados, si por alguna razón, el nivel de protección de uno o ambos Estados es incapaz de garantizar u ofrecer las salvaguardas necesarias a la protección de la privacidad⁹²¹ no deberán imponerse limitaciones indebidas a tal circulación, siendo posible en las medidas exigibles para la protección de la privacidad, evitando con ello el empleo de prácticas de protección desproporcionadas con mira a proteger la privacidad⁹²².

⁹²⁰. “Cuando la legislación de dos o más países afectados por un flujo transfronterizo de datos ofrezca salvaguardas similares para la protección de la intimidad, la información debe poder circular tan libremente como dentro de cada uno de los territorios afectados. En caso de que no existan salvaguardas recíprocas, no deberán imponerse limitaciones indebidas a tal circulación, sino solamente en la medida en que lo exija la protección de la intimidad”. Agencia de Protección de Datos., *Principio 9, Flujo transfronterizo de datos, Directrices de protección de datos de la ONU* Disponible en: https://www.agpd.es/portaleswebAGPD/canaldocumentacion/legislacion/organismos_internacionales/naciones_unidas/common/pdfs/D.3BIS-cp--Directrices-de-Proteccion-oo-n-de-Datos-de-la-ONU.pdf. (Última consulta en línea 30 de octubre).

⁹²¹ En las traducciones observadas, son manejados indistintamente los términos privacidad e intimidad, así como los términos similares, comparables, cuando se refiere a las salvaguarda o garantías, a continuación, presentamos el texto original en inglés “Transborder data flow. When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands”, visto en REMOLINA ANGARITA, N., *Recolección Internacional de datos personales: un reto del mundo...op. cit.*, p. 191, nota 155.

⁹²² Principio 9, Flujo transfronterizo de datos.

“Cuando la legislación de dos o más países afectados por un flujo transfronterizo de datos ofrezca salvaguardas similares para la protección de la intimidad, la información debe poder circular tan libremente como dentro de cada uno de los territorios afectados. En caso de que no existan salvaguardas recíprocas, no deberán imponerse limitaciones indebidas a tal circulación, sino solamente en la medida en que lo exija la protección de la intimidad”. Disponible en:

Es bueno traer a colación, que la Carta como hemos definido en el capítulo dos, aboga y fomenta la amistad y la solución de problemas entre los Estados y sus nacionales, fomentando la cooperación y solución de problemas internacionales de corte económico, razones por las que entendemos, que su principio evita la generación de medidas extremas o contrarias entre uno de los Estados o ambos, fundamentado en la protección de la intimidad.

5.6. Transferencia internacional en el Convenio 108 del Consejo de Europa

El Convenio 108, plantea en sus considerandos la necesidad de incrementar la protección de los derechos y de las libertades fundamentales, sin dejar de lado la intensificación de la circulación de datos de carácter personal fruto de los tratamientos automatizados de datos por medio a las fronteras, obedeciendo a esos considerando, el Convenio 108 del Consejo de Europa abraza en el capítulo III del Convenio, lo referente a los flujos transfronterizos de datos de carácter personal, evitando prohibir u obstaculizar los flujos transfronterizos a expensa de protección de la vida privada, no obstante, contempla posible excepciones a considerar, entre ellas la protección equivalente o burlar legislaciones por medio al empleo de territorios equivalentes.

Más allá del Convenio de 1981, el 8 de noviembre de 2001, se acuerda el Protocolo Adicional, un Protocolo capaz de conectar las transferencias de datos con el órgano de control⁹²³, siendo responsable del cumplimiento de los principios básicos de la protección de datos y los flujos transfronterizos de datos.

https://www.agpd.es/portaIwebAGPD/canaIdocumentacion/legislacion/organismos_internacionales/naciones_unidas/common/pdfs/D.3BIS-cp--Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf. (Última consulta en línea 30 de octubre 2017).

⁹²³ Artículo 1- Autoridades de Control

Cada parte preverá que una o más Autoridades sea responsables de asegurar la conformidad de las medidas oportunas que dé cumplimiento en el Derecho interno a los principios contenidos en los Capítulos II y III del Convenio y en el presente Protocolo.

Con el objetivo de proteger los derechos humanos, las libertades, y la privacidad, fruto de la importancia de los flujos de información e incremento del intercambio de datos a través de las fronteras, los Estados adscritos al Protocolo acuerdan realizar transferencias de datos personales a destinatarios no sometidos a la competencia del Convenio cuando estos aseguren niveles adecuados de protección o cumplan con las excepciones dispuestas en el Protocolo⁹²⁴.

5.7. Transferencia internacional en la Directiva 95/46/CE

La Directiva 95/46/CE del Parlamento Europeo y el Consejo, contempla en sus considerandos la libre circulación de datos entre los Estados internos de la Unión Europea, requiriendo niveles de protección equivalentes al momento de realizar transferencias internacionales entre sus miembros, apoyado en la necesidad de coordinar sus legislaciones internas sustentado en la regulación coherente de los flujos transfronterizos de datos personales, posibilitando la libre circulación entre ellos, al mismo tiempo, la Directiva considera necesario el establecimiento de flujos transfronterizos para el desarrollo del comercio internacional, permitiendo flujos transfronterizos de datos a terceros países⁹²⁵ que garanticen niveles adecuados⁹²⁶ rodeado de sus excepciones o circunstancias relacionadas⁹²⁷.

⁹²⁴ Artículo 2 numeral 2.

- a) Si el derecho interno así lo establece a causa de:
- Intereses concretos del afectado, o
 - Intereses legítimos, especialmente los de carácter público.

⁹²⁵ Artículo 25, numeral 3.

Los Estados miembros y la comisión se informarán recíprocamente de los casos en que se consideren que un tercer país no garantiza un nivel de protección adecuado.

⁹²⁶ “Considerando, por otra parte, que cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia”, Considerando 57, Directiva 95/46 del Parlamento Europeo y del Consejo.

⁹²⁷ Directiva 95/46 del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, considerando 3, 8, 9, 56.

Las excepciones contempladas en la Directiva, permiten el establecimiento de transferencias internacionales a terceros países, a pesar de no contar con los niveles adecuados exigidos en la Directiva que prohíben tales transferencias cuando estos niveles de protección no son los adecuados; entre las excepciones contempladas en los considerandos de la Directiva tenemos consentimiento del interesado, contrato, acción judicial, interés público; atribuyendo a la Comisión competencia de ejecución amparados en procedimientos entre la Comunidad y terceros Estados⁹²⁸.

Como hemos comentado, la Directiva plantea y contempla en el capítulo IV, bajo la descripción del título *transferencia de datos personales a países terceros*, los principios y excepciones de las transferencias internacionales de datos a países terceros tal como se refleja en los artículos 25 y 26 de su Directiva.

5.8. Transferencia internacional en la Ley Orgánica 15/1999 (LOPD)

La *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*, contempla al igual que su antecesora la *Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal*, el movimiento internacional de datos a países que guarden niveles equiparables al que ofrece la ley, similares a los principios formadores del Convenio 108 del Consejo de Europa y al de Schengen⁹²⁹, incluyendo autorización del Director de la Agencia de Protección de Datos, siempre y cuando existan garantías adecuadas a ser evaluadas por la Agencia, manteniendo como hemos visto la hegemonía de la Agencia en el proceso de ejecución de las transferencias internacionales, evaluando las circunstancias que ameritan la ejecución de la transferencia internacional sin dejar de lado las garantías adecuadas del país destino.

⁹²⁸ Cfr. Considerando 57, 58, 66 de la Directiva 95/46/CE.

⁹²⁹ ULL PONT, E., *Derecho público de la informática, protección de datos...* op. cit., p. 153.

El documento contempla excepciones al movimiento internacional de datos, permitiendo la ejecución de transferencias internacionales soportado en las excepciones previstas en la ley.

5.9. Transferencia internacional en el Reglamento (UE) 2016/679

Las transferencias internacionales no escapa al *Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* y por el que se deroga la Directiva 95/46 CE de protección de datos personales, a diferencia de la pasada Directiva, con el Reglamento se busca armonizar y eliminar posibles obstáculos a la circulación de los datos personales en la Unión Europea, logrando una equivalencia coherente y homogénea de protección de las personas físicas en toda la Unión, evitando obstáculos que pudieran dificultar la libre circulación de datos personales en el mercado interior, proporcionando seguridad jurídica y transparencia a los operadores económicos, garantizando una supervisión coherente, sanciones equivalentes y cooperación efectiva entre las autoridades de control de los diferentes Estados miembros⁹³⁰.

El Reglamento contempla la necesidad de establecer flujos transfronterizos de datos personales entre los Estados miembros y terceros Estados, garantizando la expansión del comercio y cooperación internacional, siendo la Comisión el órgano encargado por la Unión Europea para decidir acerca del nivel de protección adecuado que debe tener un tercer país u organización, aportando la seguridad y uniformidad jurídica necesaria para el establecimiento de la transferencia internacional, con la posibilidad de realizar acuerdos entre los Estados y terceros países sin afectar las disposiciones del Reglamento.

⁹³⁰ Cfr. Considerando 10,13 del Reglamento (UE) 2016/679. Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807>. (Última consulta en línea 8 de marzo 2018).

El Reglamento (UE) 2016/679 contempla en su capítulo V bajo el epígrafe *transferencias de datos personales a terceros países u organizaciones internacionales*: a) el principio general de las transferencias; b) las transferencias basadas en una decisión de adecuación; c) las transferencias mediante garantías adecuadas; d) las normas corporativas vinculantes; e) transferencias o comunicaciones no autorizadas por el Derecho de la Unión; f) las excepciones para situaciones específicas; y g) la cooperación internacional en el ámbito de la protección de datos personales comprendido desde el artículo 44 al 50 del referido Reglamento.

6. Órgano de Control y transferencias internacionales en Latinoamérica

6.1. Autoridades de control latinoamericanas

Durante nuestra exposición, hemos presenciado y abordado el órgano de control desde el punto de vista del espacio europeo, en esta ocasión, le toca el turno al espacio iberoamericano aunado en el crecimiento⁹³¹, actualización, homologación de las normas iberoamericanas en materia de protección de datos, agilizando la incorporación de autoridades de control en el espacio iberoamericano, con características y niveles de protección no homogéneos, a pesar del esfuerzo de los Estado en aproximarse a las normativas europeas reguladas por legislaciones comunes para los Estados.

⁹³¹ “La intensa actividad legislativa que vive Iberoamérica en materia de protección de datos se une a la acción y nacimiento de organismos de control nacionales como la Autoridad Nacional de Protección de Datos de Perú, la Agencia de Protección de Datos de los Habitantes en Costa Rica, o el fortalecimiento de otras ya existentes y de reconocida trayectoria como el Instituto Federal de Acceso a la Información y Protección de Datos en México o la Dirección Nacional de Protección de Datos y su homóloga en Buenos Aires de Argentina”, visto en LÓPEZ CARBALLO, D.(Coordinador), *Protección de datos y habeas data: una visión desde Iberoamérica*, imprenta nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2015, p. 16.

La estructura organizacional imperante en los Estados Iberoamericanos, vinculado a su aspecto cultural, presupuestal y niveles democráticos⁹³², contribuyen con la creación de órganos de control disímiles o asimétricos entre ellos. A pesar de procurar su acercamiento a la protección de datos y a los órganos de control de las normas europeas, algunos Estados alcanzan y se aproximan al modelo europeo, tales son los casos de Argentina y Uruguay que reciben el reconocimiento de la Comisión Europea, más otros, a pesar del desarrollo de sus normas, no alcanzan el reconocimiento de la Comisión Europea, situación de México y otros Estados como el peruano que emplean la autoridad de control en el ámbito administrativo, destinado a proteger posibles violaciones a los derechos de acceso a la información pública, dicho lo anterior, pasamos a conocer de manera sucinta las principales autoridades de protección de datos latinoamericanas.

Los Estados Unidos Mexicanos, forman parte de los Estados Latinoamericanos cuya autoridad de control mantiene un alto nivel de independencia, nos referimos al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), conocido como Instituto Federal de Acceso a la Información Pública y Protección de Datos (IFAI) perteneciente a la Administración Pública Federal, gozando de autonomía operativa, presupuestaria, protegiendo los datos personales en manos de las dependencias y entidades. Por medio a la Ley de Protección de Datos Personales peruana se crea a partir del 2011⁹³³ la Autoridad Nacional de Protección de Datos Personales de Perú, ejercida por la Dirección General de Protección de Datos bajo la responsabilidad del Viceministerio de Justicia y Derechos Humanos, responsable de supervisar la referida Autoridad, careciendo de independencia, no siendo reconocida su autonomía, al punto de

⁹³² ZAMUDIO SALINAS, D. L., *La Ley de Protección de Datos Personales Peruana. Reflexiones Comparativas.*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014, p. 1172.

⁹³³ ZAMUDIO SALINAS, D. L., *La Ley de Protección de Datos Personales Peruana. Reflexiones Comparativas.*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A. Buenos Aires, 2014, p. 1172.

ser considerado por algunos una institución de tercer nivel⁹³⁴. Uruguay contempla como órgano de control la Unidad Reguladora y de Control de Datos Personales (URCDP) bajo la dirección de un Consejo Ejecutivo⁹³⁵, dispuesto por tres miembros, dos de ellos designados por el Gobierno, y un tercero ocupado por el director de la Agencia, siendo reconocida por el Grupo del Art. 29 gozando de una autoridad supervisora independiente con facultades, normas y reglamentaciones⁹³⁶. En el caso de Costa Rica, vía la promulgación de la Ley núm. 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales presentado por la Asamblea Legislativa de la República de Costa Rica, se crea en el 2001⁹³⁷ la Agencia de Protección de Datos de los Habitantes (PRODHAB), un órgano desconcentrado, adscrito al Ministerio de Justicia y Paz, responsable de administrar sus propios recursos y presupuestos, así como la de mantener independencia de criterio y plena libertad para la firma de contratos y convenios conectados a sus funciones⁹³⁸. Por otro lado, la República de Argentina asigna mediante el Reglamento 1558/2001⁹³⁹ y el artículo 29 de la Ley núm. 25.326, la Dirección Nacional de Protección de Datos Personales como órgano de control con facultades

⁹³⁴ ZAMUDIO SALINAS, DL., *La Ley de Protección de Datos Personales Peruana. Reflexiones Comparativas.*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014, pp. 1176-178.

⁹³⁵ ROTONDO, F., *Protección de Datos Personales en la República de Uruguay*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014, p. 1147.

⁹³⁶ DE AZEVEDO CUNHA, M. V., *Protección de Datos en el Mercosur: Hacia un Marco...* op. cit., p. 1118.

⁹³⁷ QUESADA RODRÍGUEZ, A., *Protección de datos y telecomunicaciones convergentes*, 1ª ed. Agencia Española de protección de datos, Madrid, 2014, p. 340.

⁹³⁸ ZAMUDIO SALINAS, D. L., *La Ley de Protección de Datos Personales Peruana. Reflexiones Comparativas.*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014, p. 1175.

⁹³⁹ Cfr. Decreto 1558/2001 de 29 de noviembre de 2001. Reglamentación de la ley de protección de datos personales. Disponible en: [http://www2.congreso.gob.pe/sicr/cendocbib/con2_uibd.nsf/983EC5385CB1658E052577B9006C2DB7/\\$FILE/Decreto_1558_Reglamenta_Ley_25.326.pdf](http://www2.congreso.gob.pe/sicr/cendocbib/con2_uibd.nsf/983EC5385CB1658E052577B9006C2DB7/$FILE/Decreto_1558_Reglamenta_Ley_25.326.pdf). (Última consulta en línea 20 de abril 2018).

sancionadoras, fiscalizadoras, asesoramiento, registraci3n y reglamentaci3n⁹⁴⁰, 3rgano encargado de recibir las inscripciones de las bases de datos reguladas en la propia Ley n3m. 25.326, actuando como 3rgano descentralizado, con autonom3a funcional, adscrito al Ministerio de Justicia y Derechos Humanos del Estado, bajo la direcci3n de un director designado por el Poder Ejecutivo, recibiendo la anuencia del Senado de la Naci3n. Nicaragua contempla la Direcci3n de Protecci3n de Datos Personales (DIPRODAP) adscrita al Ministerio de Hacienda y Cr3dito P3blico, dirigida por un director nombrado por el Ministerio representativo de su m3xima autoridad.

A pesar de la intensa actividad legislativa de Iberoam3rica, no todos los Estados Iberoamericanos cuentan con organismos de control, es el caso de la Rep3blica Federativa de Brasil que adem3s de no contar con una ley espec3fica en materia de protecci3n de datos tampoco posee un ente regulador especializado en el tema⁹⁴¹. La Rep3blica de Chile no cuenta con el establecimiento de un 3rgano de control capaz de velar por la protecci3n de los datos personales y al mismo tiempo, supervisar los datos almacenados en registros o bancos de datos, situaci3n de la que no es ajena el sistema normativo estadounidense, razones por las cuales presentamos la siguiente acotaci3n.

“El sistema normativo en materia de protecci3n de la privacidad de los Estados Unidos, no contempla la necesidad de incorporar mecanismos de vigilancia y control en sus normas, conformadas por leyes 3mnibus, careciendo de magistraturas o instituciones especializadas responsables de los mecanismos de control y vigilancia, situaci3n muy diferente a los sistemas europeos, quienes a pesar de contar con leyes 3mnibus, integran en sus legislaciones, mecanismos de control, capaces de proveer las garant3as necesarias para una real protecci3n de las personas respecto al

⁹⁴⁰ P3REZ PONTE, M., *Facultades y atribuciones del 3rgano de control de la ley nacional de protecci3n de datos personales 25,326*, visto en TRAVIESO, J. A. (Director), *R3gimen Jur3dico de los Datos Personales*, tomo I, 1^a ed. ABELEDOPERROT S. A., Buenos Aires, 2014, p. 151.

⁹⁴¹ QUESADA, A., *Protecci3n de datos y telecomunicaciones convergentes*, 1^a ed. Agencia Espa3ola de protecci3n de datos, Madrid, 2014, p. 317.

tratamiento de sus datos personales y a la libre circulación de estos datos⁹⁴².

6.2. Transferencias internacionales latinoamericanas

En capítulos recientes, hemos sido partícipe de la inexistencia de homologación en las normas jurídicas en materia de protección de datos entre los Estados Iberoamericanos ya sea desde: a) su concepción Léxico-Jurídica; b) costumbres; c) historia; d) procesos políticos y jurídicos; tal situación no es ajena al escenario cubierto por las transferencias internacionales de los Estados Iberoamericanos, cuyas legislaciones internas son reguladas de formas distintas, al igual que las ya conocidas normas de protección de datos, intimidad, privacidad y otros derechos fundamentales; tales diferencias permean las áreas involucradas en los procesos ocurridos en las transferencias internacionales como son los requisitos necesarios en la puesta en ejecución de las transferencias internacionales, los tipos de niveles empleados al momento de ejecutar una transferencia internacional y las funciones del órgano de control ante solicitudes de aprobación, reflejado en las normas internas de los Estados.

Al mismo tiempo, la denominación conceptual del término transferencia internacional incluyendo definiciones, características específicas envueltas en el proceso y los contenidos contemplados en las transferencias, varían, a pesar de ello, algunos Estados contemplan sus homogeneidades por proceder de fuentes comunes como las normas europeas, americanas, y las provenientes de los Estados Latinoamericanos, quienes por medio a la aplicación de técnicas del derecho comparado tropicalizan sus normas.

Desde sus inicios, el acercamiento, interacción, apoyo, conexión de Europa con Latinoamérica, es una realidad, y más si nos abocamos a los tiempos de la

⁹⁴² MIGUEL A., EKMEKDJIAN y CALOGERO, P., “*Habeas data*” *El derecho a la intimidad frente a la revolución informática*, Buenos Aires, Ediciones Depalma, 1996, pp. 33 y 34, visto en PUCCINELLI, O., *El Habeas data en Indoiberoamérica*, Temis, Bogotá, 1999, p. 191.

Comunidad Económica Europea (CEE) y como no, la actual Unión Europea (UE), mostrando un especial interés en contribuir con la democratización de la región vía sus instituciones, como es el caso del Consejo, la Comisión y el Parlamento⁹⁴³, agenciando la defensa de los derechos humanos y contribuyendo con la pacificación de la zona, ejemplo de ello fueron los conflictos ocurridos en Centro América durante el periodo de la CEE, estableciendo lazos de unión en el continente, es ahí la necesidad por las que mantienen una estrecha colaboración con los países democrático, ya que sin ello, no será posible concretizar el desarrollo y recuperación democrática y económica en la zona, es decir, al igual que los Estados europeos durante su proceso de conformación, los Estados Latinoamericanos deben hacer ingentes esfuerzos en mantener lazos de cooperación entre ellos⁹⁴⁴, situación que desde nuestro punto de análisis no escapa a la protección y defensa de los derechos humanos, incluida la protección de datos personales como derecho fundamental, y con ello, la protección de las personas físicas a raíz del incremento del flujo o movimiento internacional de datos personales entre los Estados, tal es el caso de los flujos o movimientos de datos ejecutados entre las naciones latinoamericanas y otros Estados.

Es por ello, que el contacto o aproximación de las normas legislativas en los Estados Latinoamericanos, genera que a expensa de las legislaciones europeas, estos no escatiman esfuerzos en legislar e incluir en sus normas de protección de datos el tema de las transferencias internacionales, a tal grado de considerarla en sus leyes de protección de datos, fungiendo como mecanismo asegurador y protector de los derechos fundamentales en materia de privacidad, honor, intimidad, protección de datos, que trasgreden a los titulares al momento de la ejecución de transferencias internacionales a terceros países, planteando la necesidad de conocer la situación legislativa de

⁹⁴³ ALDECOA, F., *por un mayor compromiso de la Comunidad Europea con América Latina*, seminario sobre las relaciones económicas entre América Latina y la Comunidad Económica Europea (CEE), fundación Friedrich Ebert, Madrid, 1988, p. 117.

⁹⁴⁴ ALDECOA, F., *por un mayor compromiso de la Comunidad Europea con América Latina*, seminario sobre las relaciones económicas entre América Latina y la Comunidad Económica Europea (CEE), fundación Friedrich Ebert, Madrid, 1988, p. 108-109

los Estados a los cuales se realizará la transferencia como mecanismo de asegurar una real protección de los datos personales y con ello, garantizar los otros derechos envueltos al momento de realizar el proceso de movimiento o flujo de datos hacia otros Estados.

A raíz de las dudas y preocupaciones respecto al envío o flujo de datos hacia otros Estados incluyendo los pertenecientes a terceros países, los Estados Latinoamericanos hacen suyo el tema de las transferencias internacionales, implementando en sus legislaciones y normas internas, los principios que soportan el proceso de las transferencias, amparadas o bajo la influencia de normativas internacionales, en especial las normativas europeas en materia de transferencias internacionales.

Las transferencias internacionales, al igual que las legislaciones internas de los Estados Latinoamericanos en materia de protección de datos y derechos fundamentales, no gozan de una homologación entre los mismos, a pesar de proceder, coincidir o partir muchas veces de las mismas fuentes como pueden ser las legislaciones europeas, americanas o latinoamericanas en proceso de formación y actualización, al compás de las transformaciones generadas y en proceso que ocurren y están ocurriendo en los Estados Latinoamericanos. De la misma manera, el concepto de transferencia internacional cambia o más bien no es igual en los Estados, generando con ello, diferentes acepciones o definiciones respecto al concepto de transferencia internacional de datos nombrada en algunos casos como transmisión de datos, transferencia internacional de datos, transferencia o flujos transfronterizos de datos⁹⁴⁵.

⁹⁴⁵ “En la Constitución Chilena, la transmisión de datos se define como el tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del responsable. En la normativa española se define la transferencia Internacional de Datos como el tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español. La normativa mexicana considera la transferencia como toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento, especificando en su reglamento que la transferencia implica la comunicación de datos personales dentro o fuera del territorio nacional, realizada a persona distinta del titular, del responsable o del encargado. La normativa de Perú define los flujos transfronterizos de datos como transferencia internacional de datos personales a un

Planteadas las cuestiones, nos referimos a los Estados Latinoamericanos cuyas normas internas contemplan los flujos transfronterizos de datos, caracterizado por no ser un proceso estático, aislado, sino, un proceso en constante movimiento producto a los cambios tecnológicos, sociales, legislativos que permean las normativas internacionales en materia de protección de datos.

Producto de la disparidad existente en los niveles de protección de las transferencias internacionales en las normas de protección de datos y *habeas data* en los Estados Latinoamericano, nos vemos en la obligación de presentar una relación de los niveles de protección considerados en las normas.

6.3. Niveles de protección latinoamericana

De entrada, pasamos a identificar el nivel de protección contemplado en las legislaciones latinoamericanas, comenzaremos con la legislación Argentina, la cual prevé niveles adecuados de protección en el país de destino. Chile no exige niveles equiparables. Colombia requiere niveles adecuados de protección⁹⁴⁶. Costa Rica no contempla niveles de protección. España requiere niveles equiparables. México no contempla niveles equivalentes. Nicaragua requiere niveles de protección adecuados contemplando sus excepciones. Perú contempla niveles adecuados. Portugal exige de niveles de protección

destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban. La República Dominicana dispone que un Transferencia Internacional de Datos es un tratamiento de datos que supone una transmisión de los mismos fuera del territorio de la República Dominicana, sin importar el soporte, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del archivo de datos personales establecido en territorio dominicano". LÓPEZ CARBALLO, D. (Coordinador), *Protección de datos y habeas data: una visión desde Iberoamérica*, imprenta nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2015, pp.166-175.

⁹⁴⁶ Ley estatutaria núm. 1581 del 17 de octubre del 2012 por la cual se dictan disposiciones generales para la protección de datos personales, art. 26. Disponible en: <https://www.sisben.gov.co/Documents/Informaci%C3%B3n/Leyes/LEY%20TRATAMIENTO%20DE%20DATOS%20-%20LEY%201581%20DE%202012.pdf>. (Última consulta en línea 18 de abril 2018).

adecuado. República Dominicana no plantea niveles equivalentes. Uruguay requiere niveles de protección adecuados⁹⁴⁷.

De acuerdo a los niveles de protección empleados en los procesos de transferencias internacionales de datos, el movimiento o flujo internacional de datos a terceros países requiere de ciertos niveles de aprobación, siendo la autoridad de control de los Estados, el órgano encargado de aprobar tales requerimientos previa solicitud de los mismos al momento de considerar la ejecución de una transferencia internacional de datos a terceros países.

6.4. Niveles de autorización latinoamericana

A continuación, presentamos los Estados que requieren y aquellos que no requieren de autorizaciones previas de las autoridades de control al momento de contemplar una transferencia o flujo transfronterizo de datos a terceros Estados, iniciamos con Argentina, que no requiere autorización previa de la Dirección Nacional de Protección de Datos Personales (DNPDP)⁹⁴⁸. Chile no exige autorización previa⁹⁴⁹. Colombia no requiere en forma expresa el requisito de la autorización previa por parte de la Superintendencia de Industria y Comercio (SIC). Costa Rica no exige autorización previa de la Agencia de Protección de Datos de los Habitantes (PRODHAB)⁹⁵⁰. España requiere

⁹⁴⁷ LÓPEZ CARBALLO, D. (Coordinador), *Protección de datos y habeas data: una visión desde Iberoamérica*, imprenta nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2015, pp.166-175.

⁹⁴⁸ Art. 12, Ley núm. 25.326. Protección de los Datos Personales. Disponible en: https://www.agpd.es/porta/webAGPD/canaldocumentacion/legislacion/iberoamerica/leyes_nacionales/common/pdfs/LEY-25.326-Proteccion-de-los-datos-personales.pdf. (Última consulta en línea 18 de abril 2018).

⁹⁴⁹ Ley núm. 19.628 de Protección de Datos de Carácter Personal Chilena, publicada el 28 de agosto del 1999
Disponible en: <https://www.leychile.cl/Navegar?idNorma=141599&idVersion=2011-07-23>. (Última consulta en línea 18 de abril 2018).

⁹⁵⁰ Art. 14, Ley núm. 8968 de protección de la persona frente al tratamiento de sus datos personales, publicada en la gaceta n.º 170 de 05 de septiembre de 2011. Disponible en: <http://www.tse.go.cr/pdf/normativa/leydeprotecciondelapersona.pdf>. (Última consulta en línea 18 de abril 2018).

autorización previa de la Agencia Española de Protección de Datos cuando no se garantice un nivel equivalente. México no requiere de autorización previa del INAI, pero sí informar de su ejecución. Nicaragua no exige autorización previa de la Dirección de Protección de Datos Personales (DIPRODAP) contemplando requisitos para los mismos al momento de la ejecución⁹⁵¹. Perú requiere comunicación previa de la Dirección General de Protección de Datos Personales (DGPDP) aunque la prevé en su Reglamento. Portugal precisa de comunicación previa de la Comisión Nacional de protección de Datos (CNPD) si el país no asegura un nivel adecuado. República Dominicana no exige autorizaciones previas⁹⁵². Uruguay requiere autorización vía registral por medio a garantías derivadas de un contrato siendo autorizado por la Unidad Reguladora y Control de Datos Personales (URCPD)⁹⁵³.

Es importante recordar y puntualizar, que las normas implementadas en los Estados a nivel internacional en materia de protección de datos personales, contemplan ciertas excepciones durante los procesos de transferencias internacionales en los Estados, entre ellas citamos, el consentimiento previo del interesado, las cláusulas contractuales tipos y otras más.

⁹⁵¹ Ley núm. 787 de Protección de Datos Personales, art.-publicada en la gaceta N.º 61 del 29 de marzo del 2012. Disponible en: <http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d>. (Última consulta en línea 18 de abril 2018).

⁹⁵² Ley núm. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados, art. G.O. N.º 10737 del 15 de diciembre de 2013. Disponible en: <http://www.gob.do/index.php/recursos/2014-12-16-21-02-56/category/3-constitucion-y-leyes-rd?download=58:ley-no-172-13&start=20>. (Última consulta en línea 22 de marzo 2018).

⁹⁵³ Art. 23, Ley núm. 18.331, de protección de datos personales y acción de habeas data de 11 de agosto de 2008. Disponible en: <https://www.agesic.gub.uy/innovaportal/v/302/1/agesic/ley-n%C2%B0-18331-de-11-de-agosto-de-2008.html>. (Última consulta en línea 18 de abril 2018).

6.5. Ámbito público, ámbito privado

Hemos visto, como al observar las normas latinoamericanas en materia de protección de datos, se examina una tendencia muy marcada con las normativas europeas, situación del caso argentino y su Ley núm. 25.326, o el uruguayo, reconocido y aceptado por la Comisión como un Estado con normativas adecuadas en materia de protección de datos, a nuestro entender, con la entrada del *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, se vislumbra un acercamiento e incorporación al escenario Iberoamericano, un Reglamento aplicable al tratamiento parcial o automático de los datos personales⁹⁵⁴, permitiendo la revisión de otros actos jurídicos de la Unión en materia de protección de datos como el Reglamento núm. 45/2001⁹⁵⁵ de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión, es decir, estamos delante de dos ámbitos de protección de los derechos de las personas físicas, uno generado por la manipulación de sus datos personales existentes en instituciones públicas (ámbito público) y otro generado en el sector privado (ámbito privado).

⁹⁵⁴ Artículo 98, *Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016*. “La Comisión presentará, si procede, propuestas legislativas para modificar otros actos jurídicos de la Unión en materia de protección de datos personales, a fin de garantizar la protección uniforme y coherente de las personas físicas en relación con el tratamiento. Se tratará en particular de las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento por parte de las instituciones, órganos, y organismos de la Unión y a la libre circulación de tales datos”.

⁹⁵⁵ Artículo 3, numeral 1, *Reglamento núm. 45/2001 del Parlamento Europeo y del Consejo de 1 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos*.

1. Las disposiciones del presente Reglamento se aplicarán al tratamiento de datos personales por parte de todas las instituciones y organismos comunitarios, en la medida en que dicho tratamiento se lleve a cabo para el ejercicio de actividades que pertenecen al ámbito de aplicación del Derecho comunitario. Disponible en: <https://www.boe.es/doue/2001/008/L00001-00022.pdf>. (Última consulta en línea 25 de mayo 2018).

6.6. Mecanismos de aseguramiento

A raíz de tales observaciones, contemplamos acciones orientadas y encaminadas al mismo fin y objetivo, como la protección de las personas físicas orientada al tratamiento de sus datos personales, a pesar de ello, cada norma contempla su propio mecanismo de aseguramiento por medio de autoridades independientes responsable de la protección de datos establecidos en normas europeas como la Directiva 95/46/CE, el Reglamento (UE) 2016/679, el Reglamento 45/2001 (CE) donde se observan irrefutables mecanismos de control y supervisión como el Supervisor Europeo de Protección de Datos⁹⁵⁶, el Grupo de Protección de las Personas⁹⁵⁷, el Comité Europeo de Protección de Datos.⁹⁵⁸

El Supervisor Europeo de Protección de Datos Personales instituido a partir del Reglamento 45/2001 del Parlamento Europeo y el Consejo, es un órgano independiente, con atribuciones de supervisor del Reglamento u otras disposiciones relacionadas con el tratamiento de datos personales, con funciones, atribuciones y competencias; al mismo tiempo, con la Directiva 95/46/CE se crea la autoridad de control y el Grupo de Protección de Datos.

La autoridad de control goza de total independencia con poderes de investigación, intervención, capacidad procesal, cooperación; en el caso del grupo de protección de las personas en lo que respecta al tratamiento de datos personales creado bajo el artículo 29 de la Directiva 95/46 CE, reconocido

⁹⁵⁶ Cfr. Capítulo V, autoridad de control independiente: el Supervisor Europeo de Protección de Datos. *Reglamento núm. 45/2001 del Parlamento Europeo y del consejo de 1 de diciembre de 2000*. Disponible en: <https://www.boe.es/doue/2001/008/L00001-00022.pdf>. (Última consulta en línea 25 de mayo 2018).

⁹⁵⁷ Cfr. Capítulo VI, autoridad de control y grupo de protección de las personas en lo que respecta al tratamiento de datos personales, artículo 28 y 29, Directiva 95/46 del Parlamento Europeo y del Consejo de 24 de octubre de 1995, Capítulo VI autoridad de control independiente. *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016*.

⁹⁵⁸ Cfr. Sección 3, *Comité Europeo de Protección de Datos. Reglamento (UE) del Parlamento Europeo y del Consejo de 27 de abril de 2016*.

como Grupo 29, es un grupo de carácter consultivo e independiente, entre sus cometidos se encuentra la contribución de la aplicación homogénea de la Directiva en los Estados y el asesoramiento de la Comisión, en ese sentido, con el Reglamento de Protección de Datos, se crea el Comité Europeo de Protección de Datos derogando el Grupo de Trabajo 29. El Comité es un organismo independiente perteneciente a la Unión Europea con personalidad jurídica y funciones, al mismo tiempo y con el interés de asegurar la cooperación entre autoridades de control, se crea el mecanismo de coherencia, una figura establecida en el Reglamento para cuando exista la posibilidad de que una decisión tomada por un órgano de control pudiera general o producir consecuencias, secuelas jurídicas que pudieran impactar a otros órganos de control⁹⁵⁹.

A raíz del caso Cambridge Analytica⁹⁶⁰ observamos la imperiosa necesidad de contar con mecanismos y normativas capaces de asumir el compromiso de protección de los datos personales en los Estados miembros y más allá de sus fronteras, sustentados en la capacidad de asegurar y proteger el movimiento de los datos personales fuera de las fronteras de los Estados.

⁹⁵⁹ Cfr. Considerando 135, 136, 139, *Reglamento (UE) 2016/679*. Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807>. (Última consulta en línea 8 de marzo 2018).

⁹⁶⁰ “Estamos en pañales, porque cómo se va a multar a una empresa que no tiene un establecimiento en México, lo que hace muy difícil hacer efectiva la multa. Quedamos en un Estado de indefensión. Por ello, es fundamental promover mecanismos de colaboración internacional en este sentido. Porque muchas de las vulneraciones ya se están dando desde afuera” María Solange Maqueo, profesora investigadora del centro de investigación y Docencia Económica (CIDE) especialista en protección de datos personales. SANTILLÁN O., *Falla Inai en protección de datos personales, 26 de mayo de 2018*. Disponible en: <http://www.ejecentral.com.mx/falla-inai-en-proteccion-de-datos-personales/>. (Última consulta en línea 26 de mayo 2018).

II. EL ÓRGANO DE CONTROL y LAS TRANSFERENCIAS INTERNACIONALES EN LA REPÚBLICA DOMINICANA

1. Consideraciones iniciales

República Dominicana forma parte de los países con leyes generales en materia de protección de datos, una situación no existente antes del 2013, que es cuando sale a la luz su actual *Ley núm.172-13, que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamientos de datos destinados a dar informes, sean estos públicos o privados.*

Previo a la ley, se mantuvieron gravitando en el Congreso de la República dos importantes piezas legislativas, nos referimos al proyecto originario del senador Félix Bautista y al proyecto del diputado Demóstenes Martínez, los cuales analizaremos desde la óptica del órgano de control y las transferencias internacionales.

Por su parte y debido al nivel de relevancia y visibilidad de la transparencia y el acceso a la información pública en la República Dominicana, nos hemos visto en la necesidad de incluirlo en este punto, y conectarlo con la normativa latinoamericana y europea, en especial, con los Estados Unidos Mexicanos y España conectada con las Comunidades Autónomas.

Es de nuestro interés traer a colación un extracto de la Sentencia del Tribunal Constitucional relacionada con la interposición de una acción de inconstitucionalidad dirigida contra la Ley 172-13, ya vista y analizada previamente, pero en esta ocasión nos concentraremos en la decisión relacionada con el órgano de control, y que a su vez, forma parte fundamental de la decisión.

2. Órgano de control en los proyectos de ley

El primero “*Proyecto de ley mediante el cual se crean las normas que regulan y protegen los datos personales o Ley de Habeas Data*” bajo la auditoría del diputado Demóstenes Martínez, el proyecto considera la creación de la Dirección para la Protección de los Datos Personales como órgano de control bajo la sombrilla de la Procuraduría General de la República Dominicana, responsable de la designación de los funcionarios y el fiel cumplimiento de sus responsabilidades.

Entre las funciones y atribuciones del órgano de control desplegadas en el anteproyecto de ley, se señala la imposición de sanciones administrativas, la constitución en querellantes de las acciones penales por violaciones a la presente ley y la dedicación exclusiva del director a sus funciones.

El segundo proyecto conocido bajo el epígrafe “*proyecto de ley Orgánica sobre Protección de Datos de Carácter Personal*” presentado por el senador Félix Ramón Bautista Rosario, contempla la creación de la Agencia Dominicana de Protección de Datos como órgano de control, en esta ocasión, nos referimos a una institución descentralizada, autónoma en el orden administrativo, financiero y técnico, pero ante todo, con la capacidad de actuar con total independencia de la administración pública al momento de ejercer sus funciones.

La Agencia formará parte y estará sometida a la vigilancia del Ministerio de la Presidencia bajo la dirección de un director designado por el presidente de la República, establecido por un período de 4 años, gozando de plena independencia y objetividad, asistido por un Consejo Consultivo⁹⁶¹, la Agencia

⁹⁶¹ Artículo 44. Consejo Consultivo.

- 1) Un representante de la Administración del Estado, designado por el Gobierno.
- 2) Dos expertos en la materia, propuestos por las Universidades del modo que se prevea reglamentariamente.
- 3) Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.

actuará en función y conformidad con: a) la Ley núm. 41-08 de Función Pública⁹⁶²; b) la Ley núm. 340-06 de Compras y Contrataciones de Bienes y Servicios⁹⁶³, como las de c) Obras y Concesiones del 18 de agosto de 2006.

La Agencia contempla los siguientes preceptos funcionales: a) cumplir con lo estipulado en la presente ley; b) adecuar los tratamientos a los principios emanados en la ley; c) atender las reclamaciones de los afectados proporcionando información de sus derechos; d) ordenar el cese o cancelación de los tratamientos cuando no cumplan las disposiciones de la ley con capacidad sancionadora; y e) manejar el Registro general de Protección de Datos.

3. Órgano de control en la Ley de Protección de Datos Personales núm. 172-13

3.1. Origen del órgano de control

El órgano de control dominicano surge a raíz de la Ley núm. 172-13⁹⁶⁴; la Superintendencia de Bancos es el organismo designado⁹⁶⁵ en la propia ley

4) Un representante del sector de archivos de datos personales privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.

⁹⁶² Ley núm. 41-08 de Función Pública y crea la Secretaría de Estado de Administración Pública, del dieciséis (16) de enero del año dos mil ocho (2008).

Disponible en: <http://unpan1.un.org/intradoc/groups/public/documents/icap/unpan029758.pdf>. (Última consulta en línea 24 de abril 2018).

⁹⁶³ Ley núm. 340-06 sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones. Disponible en:

http://www.oas.org/juridico/PDFs/Mesicic5_RepDo_RespuestaC_Ane6.pdf. (Última consulta en línea 24 de abril 2018).

⁹⁶⁴ Cfr. Ley núm. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. G.O. N.º. 10737 del 15 de diciembre de 2013. Disponible en: <http://www.gob.do/index.php/recursos/2014-12-16-21-02-56/category/3-constitucion-y-leyes-rd?download=58:ley-no-172-13&start=20>. (Última consulta en línea 22 de marzo 2018).

para salvaguardar los datos personales asentados en archivos, creada y regulada por la Ley Monetaria y Financiera⁹⁶⁶ de la Junta Monetaria; en ese orden, la Junta Monetaria, el Banco Central y la Superintendencia de Bancos de la República Dominicana componen la Administración Monetaria y Financiera, siendo la Junta Monetaria el órgano superior de ambas entidades⁹⁶⁷.

En las atribuciones conferidas a la Junta Monetaria y reflejadas en la ley⁹⁶⁸ se observa: a) la aprobación de los presupuestos del Banco Central y de la Superintendencia de Bancos (signataria del órgano de control)⁹⁶⁹; b) la conformación de la estructura orgánica de las entidades⁹⁷⁰; c) la designación, suspensión o remoción de los funcionarios del Banco Central y de la Superintendencia de Bancos a propuesta del gobernador y el superintendente de bancos según corresponda⁹⁷¹; d) la designación del contralor del Banco Central y la Superintendencia de Bancos⁹⁷².

⁹⁶⁵ Cfr. Artículo 29,- Naturaleza. Los archivos, registros o bancos de datos, públicos o privados, destinados a proveer informes crediticios estarán sujetos a la inspección y vigilancia de la Superintendencia de Bancos como órgano de control.

⁹⁶⁶ Cfr. Ley núm. 183-02 que aprueba la Ley Monetaria y Financiera, regula junto a la Constitución el Sistema Monetario y Financiero de la República Dominicana. Disponible en: <http://www.omg.com.do/files/Uploads/Documents/Ley%20No.%20183-02,%20Que%20Aprueba%20la%20Ley%20Monetaria%20y%20Financiera.pdf>. (Última consulta en línea 17 de abril 2018).

⁹⁶⁷ Cfr. Artículo 5, Ley núm. 183-02.

⁹⁶⁸ Ley núm. 183-02 que aprueba la Ley Monetaria y Financiera, regula junto a la Constitución el Sistema Monetario y Financiero de la República Dominicana.

⁹⁶⁹ Artículo 9, literal e de la Ley núm. 183-02.

⁹⁷⁰ Cfr. artículo 9, literal d de la Ley núm. 183-02.

⁹⁷¹ Cfr. artículo 9, literal j de la Ley núm. 183-02

⁹⁷² Cfr. artículo 9, literal k de la Ley núm. 183-02.

La Junta Monetaria la preside el gobernador del Banco Central con representación oficial y exclusiva de la Junta Monetaria, sin la posibilidad de delegar en ningún miembro de la misma⁹⁷³.

El patrimonio de la Superintendencia es propio e inembargable, elabora sus propios presupuestos anuales incluidos el ejercicio de supervisión aprobado por la Junta Monetaria⁹⁷⁴, la designación del superintendente estará a cargo del presidente de la República por un período de 2 años, pudiendo ser renovable⁹⁷⁵.

3.2. Funciones del órgano de control

El artículo 29 de la Ley núm. 172-13 contempla en sus numerales 1 y 2 las funciones y atribuciones del órgano de control otorgado en la ley, a pesar de ello, solicitamos un requerimiento al órgano regulador para conocer prima facie lo estipulado en la ley; a raíz de ello y por medio a la solicitud SAIP-000-10217 de fecha 22-02-2018 se presenta un requerimiento en la Oficina de Acceso a la Información (OAI)⁹⁷⁶ de la Superintendencia de Bancos⁹⁷⁷, con el requerimiento

⁹⁷³ Ley núm. 183-02 artículo 10 Composición de la Junta Monetaria. La Junta Monetaria está integrada por tres (3) miembros ex officio y seis (6) miembros designados por tiempo determinado. Son miembros ex officio: el gobernador del Banco Central, quién la presidirá, el secretario de estados de finanzas y el superintendente de bancos. Al presidente de la Junta Monetaria le corresponderá la representación oficial y exclusiva de la Junta Monetaria, sin que pueda delegarla en ningún miembro de la misma.

⁹⁷⁴ Ley núm. 183-02 artículo 57. Obligación de sometimiento y alcance. Las entidades de intermediación financieras estarán.....bajo la supervisión de la Superintendencia de Bancos...la supervisión podrá consistir en análisis de gabinete e inspección de campo. La Superintendencia de Bancos establecerá a principios de cada año calendario un plan general estimativo de las supervisiones que deban llevarse en el sistema. En el literal a) del mismo capítulo correspondiente al análisis de gabinete donde las entidades sometidas a supervisión remitirán a la Superintendencia de Bancos....nombre de los depositantes....., los requerimientos de información podrán ser generales para todas las entidades de intermediación financiera o particulares.....tal como lo expresa el literal b) de inspección de campo.....las entidades de intermediación financieras ...están obligados a permitir y facilitar las labores de inspección en sus propias dependencias por parte de los supervisores bancarios...

⁹⁷⁵ Artículo 21, literal b, Ley núm. 183-02.

⁹⁷⁶ Documento recibido por la responsable de acceso a la información de la Superintendencia de Bancos Sra. Rosanna Vásquez.

se pretende conocer la estructura del órgano de control y el sistema de reportes (ticketings) de casos manejados por el órgano de control adscrito a la Superintendencia de Bancos.

La respuesta⁹⁷⁸ al requerimiento fue enviada vía email⁹⁷⁹ por la Oficina de Acceso a la Información Pública el día 01 de marzo de 2018, con ella⁹⁸⁰, se hace partícipe la inexistencia de creación de un órgano de control, es decir, las atribuciones conferidas en la ley son asumidas por la Superintendencia de Bancos, sin la necesidad de crear estructuralmente el órgano de control contemplado en la Ley núm. 172-13 y estipulado en el artículo 29 de la referida ley, adoptando la Superintendencia de Bancos las funciones de inspección y vigilancia de los archivos, registros o bancos de datos utilizados para fines crediticios, ya sean estos archivos públicos o privados.

Respecto a las estadísticas o sistemas de reportes (ticketing), la Superintendencia no registra informaciones de datos estadísticos relacionados con la nombrada ley, al mismo tiempo, se informa de la inexistencia de reclamos o estadísticas relacionadas con posibles asistencias y asesorías a personas físicas en temas de los derechos que la ley garantiza, a pesar, de ser parte integral de la mencionada ley como queda expreso en el numeral 1 del artículo 29 de la Ley núm. 172-13⁹⁸¹.

⁹⁷⁷ Avenida México N.º 52 esq. Leopoldo Navarro, Santo Domingo, República Dominicana.

⁹⁷⁸ La respuesta superó la fecha de compromiso establecida para el 15 de marzo del 2018.

⁹⁷⁹ Vía el email: alertas@digeig.gob.do con copia a oai@sib.gob.do y un servidor

⁹⁸⁰ Respuesta a su solicitud de información:

Buenas tardes señor Durán; Damos respuesta a su solicitud de información, al respecto se le informa que la ley número 172-13, no crea en sí misma un órgano de control, más bien designa a la Superintendencia de Bancos, con las funciones de inspección y vigilancia sobre los archivos, registros o bancos de datos, públicos o privados, destinados a proveer informes crediticios, de acuerdo al artículo 29 de dicha ley. Asimismo, se le informa que la Superintendencia de Bancos no registra ninguna estadística sobre la aplicación de dicha ley, ya que no ejerce ninguna otra función que no se encuentre expresamente contenida en la ley número 172/13. Nos reiteramos a sus órdenes, agradecemos acusar recibo de este mensaje, saludos

⁹⁸¹ Artículo 29. Ley núm. 172-13.
Párrafo 2 numeral 1

Un año después de la solicitud previa, realizamos en mayo del 2019 una segunda solicitud a la Superintendencia de Bancos (SIB) instituida como órgano de control, responsable de asistir y asesorar a las personas físicas así como la interposición de sanciones administrativas producto de las violaciones cometidas a la presente ley, la solicitud incluye: a) las estadísticas de reclamaciones y/o quejas recibidas por la Superintendencia de Bancos (SIB) de parte de los ciudadanos, por casos de mala utilización de informaciones crediticias / personales; b) datos incorrectos pertenecientes a los titulares; c) demandas de actualización de información en manos de las sociedades de información crediticia; d) así como las jornadas de capacitación, difusión o entrenamientos dispuestos por la institución para el conocimiento de los derechos del ciudadanos en materia de protección de datos y *habeas data* otorgados en la Ley núm. 172-13.

De acuerdo a las respuestas cursadas y recibidas por la Superintendencia de Bancos (SIB) signataria del órgano de control de la Ley núm. 172-13, durante el período del 2017 y el 2018 se han recibido 9 reclamaciones vinculadas al órgano, de las cuales 8 pertenecen al 2017 y 1 corresponde al 2018 bajo el concepto de “Reporte de información errónea a los buros de créditos”, en ese sentido y de acuerdo a los datos recibidos, durante el 2017 no se han realizado supervisiones a las Sociedades de Información Crediticias (SIC), una situación que al margen de llamarnos la atención certifica la conexión de la ley con los datos provenientes de los buros de créditos destinados a dar informes y al mismo tiempo, sustentado en la respuesta obtenida de la Superintendencia de Bancos (SIB), no existen planes de verificación o programas de supervisión para las Sociedades de Información Crediticias (SIC), en igual sentido, desde la Oficina de Servicio y Protección al Usuario (PROUSUARIO), no se han realizado campañas de verificación más allá de una ligera promoción de los derechos y deberes considerados en la ley

El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos, tendrá las siguientes funciones y atribuciones:

1. Asistir y asesorar a las personas físicas que lo requieran acerca de los alcances y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza.

por medio a la estrategia de educación contemplada por la Superintendencia de Bancos (SIB) vía la exposición en redes sociales, charlas, etc.

De su parte, de las doce mil novecientas cuarenta y cinco (12,945) solicitudes completadas, producto de las diecinueve mil trescientas dieciocho (19,318) solicitudes realizadas y recibidas vía las Oficinas de Acceso a la Información Pública (OAI), instauradas en las oficinas gubernamentales o dependencias públicas del Estado, cincuenta y siete (57) representan el 0,44 %, una cifra inferior al 0,5 % de las ordenes completadas y seleccionadas como protección de datos personales por el usuario⁹⁸², una situación que a nuestro entender afecta la data e información involucrada en la recolección de datos proveniente de la plataforma⁹⁸³, ya que lo señalado como datos personales por el usuario, no es más que el conocido *habeas data* propio e impropio conectado con el acceso a la información pública.

⁹⁸² Portal Único de Solicitudes de Acceso a la Información Pública (SAIP), *Estadísticas Generales*. Disponible en: <https://saip.gob.do/estadisticas-generales>. (Última consulta en línea 25 de mayo 2019).

⁹⁸³ Las 57 solicitudes acuñadas como protección de datos personales, se encuentran distribuidas en las siguientes instituciones: Procuraduría General de la República (PGR), Consejo Nacional para la Niñez y la Adolescencia (CONANI), Instituto Nacional de Atención e Integridad a la Primera Infancia (INAPI), Dirección General de Impuestos Internos (DGII), Ministerio de Educación de la República Dominicana (MINERD), Dirección General de Aduana (DGA), Oficina Nacional de la Propiedad Industrial (ONAPI), Seguro Nacional de Salud (SENASA), Ministerio de Salud Pública y Asistencia Social (MISPAS), Ministerio de Interior y Policía (MIP), Instituto Dominicano de las Telecomunicaciones (INDOTEL), Superintendencia de Bancos (SIB), Ministerio de Administración Pública (MAP), Procurador General de la República (PGR), Procuraduría General de la República (PGR), Tribunal Constitucional (TC), Ministerio de Medio Ambiente y Recursos Naturales (MMARENA), Instituto del Tabaco de la República Dominicana (INTABACO), Hospital Docente Semma Santo Domingo, Instituto Nacional de Bienestar Estudiantil (INABIE), Instituto Dominicano de Investigación Agropecuaria y Forestal (IDIAF), Ministerio de Relaciones Exteriores (MIREX), Cámara de Cuenta de la República (CC), Ayuntamiento de Sabana de la Mar, Ministerio de Industrias, Comercio y MiPymes (MICM), Dirección General de Ética e Integridad Gubernamental (DIGEIG), Dirección Nacional de Control de Drogas (DNCD), Instituto Nacional de Recursos Hidráulicos (INDRHI), Ministerio de Trabajo (MT), Suprema Corte de Justicia (SCJ), Empresa Distribuidora de Electricidad del Sur (EDESUR), Empresa Distribuidora de Electricidad del Sur (EDESUR), Empresa Distribuidora de Electricidad del Este (EDEESTE), Sistema Nacional de Atención a Emergencia y Seguridad (911), Oficina Presidencial de Tecnología de la Información y Comunicaciones (OPTIC), Tesorería de la Seguridad Social (TSS).

3.3. Oficina de Servicio y Protección al Usuario (PROUSUARIO)

En el organigrama oficial de la Superintendencia de Bancos⁹⁸⁴ correspondiente al mes de Julio del 2013⁹⁸⁵, podemos observar⁹⁸⁶ la existencia de la Oficina de Servicios y Protección al Usuario (PROUSUARIO)⁹⁸⁷ responsable de la defensa de los usuarios del sistema financiero, garantizando la protección de sus derechos; entre los servicios ofrecidos por la Oficina de Servicios y Protección al Usuario se destaca el de proveer asesoría y

⁹⁸⁴ *Organigrama Superintendencia de Bancos 2013.*

Disponible en: https://www.sib.gob.do/oai/Organigrama_Oficial_Aprobado_CI_06_13.pdf. (Última consulta en línea 3 de marzo del 2018).

⁹⁸⁵ La ley núm. 172-13 fue presentada el 13 de diciembre del 2013 y publicada en la gaceta Oficial el 15 de diciembre del 2018 cinco meses posteriores a la fecha de organigrama.

⁹⁸⁶ Servicio al público

La Oficina de Servicios y Protección al Usuario (PROUSUARIO) es, dentro de la Superintendencia de Bancos, la instancia cuyo propósito es desarrollar e implementar los mecanismos de defensa de los usuarios del sistema financiero, así como atender de forma efectiva sus requerimientos para garantizar la protección de sus derechos.

Los servicios al público que ofrece la Oficina de Servicios y Protección al Usuario son los siguientes:

- Realizar análisis e investigación de las reclamaciones presentadas por los usuarios del Sistema Financiero Nacional, sirviendo como ente mediador entre los usuarios y las Entidades de Intermediación Financiera (EIF), amparados en el cumplimiento de las disposiciones establecidas en la Ley Monetaria y Financiera N.º 183-02 y el Reglamento de Servicios y Protección al usuario
- Garantizar que los contratos de productos y servicios, presentados por las Entidades de Intermediación Financieras, estén libres de cláusulas abusivas.
- Dar respuesta a las consultas de información financiera presentadas a solicitud de usuarios o representantes legales.
- Proporcionar asesoría y asistencia a todos los interesados y a los usuarios del sistema financiero en asuntos que requieran de una opinión legal o financiera.

Disponible en: <https://www.sib.gob.do/transparencia/servicio-al-publico>. (Última consulta en línea 3 de marzo del 2018).

⁹⁸⁷ "...la Superintendencia de Bancos creó la Oficina de Protección al Usuario de los Servicios Financieros, PROUSUARIO. El objetivo principal que dio razón de ser a esta Oficina fue asistir a los usuarios de las Entidades de Intermediación Financiera y Cambiarias (EIF y Cs) en el manejo de los productos y servicios contratados, bajo el criterio de mejorar y cooperar con la optimización del sistema financiero, con garantía de la calidad y la correcta orientación al usuario respecto al ejercicio de sus derechos. Asimismo, proveer a los usuarios de informaciones útiles para la prevención de ilícitos relacionados a sus productos y servicios, así como de mecanismos efectivos para la adecuada protección de sus derechos, una vez agotados los recursos en las instituciones del sistema. Todo esto explica por qué la Protección de los Derechos de los Usuarios es el segundo eje estratégico del Plan Estratégico 2016-2020. *Memoria institucional 2016, Superintendencia de bancos de la República Dominicana.*

Disponible en: <https://www.sib.gob.do/pdf/Memoria-Institucional-SIB-2016.pdf>, p. 36, (Última consulta en línea 12 de marzo 2018).

asistencia, empleando mecanismos efectivos a los usuarios e interesados que requieran de una opinión legal o financiera, específicamente a los usuarios del sistema financiero, previo agotar sus solicitudes en las instituciones del sistema.

En un segundo requerimiento, hemos solicitado⁹⁸⁸ a la Oficina de Acceso a la Información Pública (OAI) adscrita a la Superintendencia de Bancos, el organigrama actualizado de la institución, con el objetivo de verificar si más allá de la publicación de la Ley núm. 172-13, se han realizado cambios organizacionales significativos que permitan insertar la figura del órgano de control en el organigrama de la institución.

La respuesta⁹⁸⁹ no se hizo esperar y a dos días de la solicitud recibimos⁹⁹⁰ informaciones de nuestro requerimiento, el documento entregado corresponde al organigrama del 2013, descartando posibles cambios organizacionales o asignación de nuevas responsabilidades luego de la promulgación de la ley.

Con la promulgación de la Ley núm. 172-13 no se crea un órgano de control con estructura organizacional y funciones, sino, que los requerimientos contemplados en el artículo 29 de la Ley núm.172-13 perteneciente a los usuarios del sistema financiero, se trasladan o pasan a formar parte de las atribuciones de la Superintendencia de Bancos conferido en la actual *Ley núm. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados.*

⁹⁸⁸ Solicitado el 3 de marzo del 2018.

⁹⁸⁹ Respuesta el 5 de marzo del 2018.

⁹⁹⁰ Respuesta a su solicitud de información: “Buenos días señor Durán; En respuesta a su solicitud, le informamos que el organigrama oficial de la SIB, es el que se encuentra publicado en el siguiente link de nuestro portal institucional. https://www.sib.gob.do/oai/Organigrama_Oficial_Aprobado_CI_06_13.pdf Nos reiteramos a sus órdenes agradecemos validar respuesta, saludos”. Disponible en: <https://outlook.live.com/owa/?path=/mail/inbox/rp>. (Última consulta en línea 5 de marzo 2018).

Por otro lado y a manera de comparación, la figura del Defensor del Pueblo u ombudsman nace a partir de la Ley núm. 19-01 del primero de febrero del año 2001⁹⁹¹, transitando a su vez por una posterior modificación consumada 9 años después, nos referimos a la Ley núm. 367-09 del 23 de diciembre de 2009⁹⁹², con la Constitución del 2010 el Defensor del Pueblo (DP) adquiere rango constitucional, una figura llamada a la protección de los derechos de sus nacionales respecto a las malas actuaciones de la administración pública del Estado o posibles prestadoras⁹⁹³ de servicio público, fortaleciendo la democracia⁹⁹⁴, gozando de independencia, apegada solo a la ley, siendo neutra, con autonomía funcional, administrativa y presupuestaria⁹⁹⁵, tutelando y protegiendo aquellos derechos fundamentales individuales y colectivos, consagrados en la Constitución y vulnerados por la administración pública,

⁹⁹¹ Gaceta Oficial núm. 10072.

⁹⁹² Gaceta Oficial núm. 10556.

⁹⁹³ Considerando primero, *Defensor del Pueblo, Ley núm. 19-01 que instituye el defensor del pueblo*, participación ciudadana, república dominicana, p. 5. Disponible en: http://www.oas.org/juridico/spanish/mesicic2_repdom_sc_anexo_12_sp.pdf. (Última consulta en línea 6 de mayo 2018).

⁹⁹⁴ “El proceso de fortalecimiento de la democracia dominicana requiere del desarrollo sostenido de las instituciones del Estado, de la preservación de la gobernabilidad, la creación de nuevas instituciones y de la participación activa de la ciudadanía. La figura del Defensor del Pueblo se inscribe en esa dirección e instituido en nuestro país por la ley 19-01 del 1ro. de febrero del 2001. Se propone proteger los derechos ciudadanos, fortalecer la administración pública, preservar el Estado de Derecho e impulsar la cultura democrática...” *Defensor del Pueblo, Ley 19-01 que instituye el defensor del pueblo*, participación ciudadana, república dominicana, p. 3. Disponible en: http://www.oas.org/juridico/spanish/mesicic2_repdom_sc_anexo_12_sp.pdf. (Última consulta en línea 6 de mayo 2018).

⁹⁹⁵ Artículo 1, Ley núm. 19-01.

Por otro lado, “En materia presupuestaria, la institución recibió durante el período comprendido entre el 1 de mayo de 2017 al 30 de abril de 2018 la asignación total de RD\$150,000,000.00; ejecutándose RD\$82,491,359.37, para un 55%. En adición a su asignación presupuestaria, el Defensor del Pueblo amplió su patrimonio o disponibilidad financiera en RD\$23,110,707.47 por concepto de intereses financieros, obtenidos de las inversiones en certificados financieros durante el año. Dichas inversiones, fueron realizadas con el objetivo de hacerle frente a los planes y proyectos pendientes de ejecutar, establecidas en el Plan Estratégico Institucional (PEI) y los Planes Operativos Anuales (POA) de los períodos 2014, 2015, 2016 y 2017 como la construcción de la Sede Central”. Defensor del Pueblo, Informe anual de gestión 2017-2018, del 1 de mayo de 2017 al 30 de abril de 2018, pp. 21-22. República Dominicana. Disponible en: http://defensordelpueblo.gob.do/transparencia/phocadownload/PlanEstrategico/informe_de_gestion/Informe%20de%20gestion%202017-2018.pdf (Última verificación en línea 20 de mayo 2019).

velando por su correcto funcionamiento⁹⁹⁶. Una estructura creada, pero no orquestada bajo el amparo de la actual Ley núm. 172-13 para la protección integral de los datos personales, siendo instituida para estos fines la Superintendencia de Bancos como órgano responsable de la inspección y vigilancia de los bancos de datos creados para proveer informes crediticios.

En las estadísticas analizadas del Defensor del Pueblo en materia de protección de los derechos fundamentales, no se observan registros o planes relacionados con la protección de datos personales, considerados derechos fundamentales desde el orden constitucional, dejando desprotegida la protección de las personas físicas en relación al tratamiento de datos personales y su libre circulación, no formando parte de los planes estratégicos del Defensor del Pueblo, no formando parte de sus atribuciones, tal como lo establece la ley.

En ese contexto, el Defensor del Pueblo de la República Dominicana realiza campañas publicitarias⁹⁹⁷, encuestas, planes estratégicos conectados con la protección de los derechos fundamentales, no evidenciando casos ligados con la protección de las personas físicas en relación al tratamiento automático o no de los datos personales⁹⁹⁸, presentando diferencias y similitudes con la

⁹⁹⁶ Artículo 2, Ley núm. 19-01.

⁹⁹⁷ Defensor del Pueblo, Informe anual de gestión 2017-2018, del 1 de mayo de 2017 al 30 de abril de 2018. República Dominicana. Disponible en: http://defensordelpueblo.gob.do/transparencia/phocadownload/PlanEstrategico/informe_de_gestion/Informe%20de%20gestion%202017-2018.pdf (Última verificación en línea 20 de mayo 2019).

⁹⁹⁸ “Durante el período comprendido entre el 1 de mayo de 2017 y el 30 de abril de 2018, el Defensor del Pueblo emitió de oficio 1,040 requerimientos,...., a distintas entidades de la Administración Pública (33%), Administración Pública Local (14%), Poder Legislativo (43%), Poder Judicial (2%), Órganos Constitucionales (1%),...entidades privadas (7%), en defensa de los derechos humanos, fundamentales e intereses colectivos y difusos, particularmente el medio ambiente, la seguridad ciudadana, fortalecimiento del servicio 911 y el patrimonio histórico, cultural y arquitectónico...., registró 1,197 expedientes, 529 reclamaciones dentro de las competencias constitucionales y legales del organismo y 668....fuera de las competencias de la institución,...., la institución produjo 524 cierres de reclamaciones y 629 orientaciones....En cuanto a la educación, promoción e investigación en materia de Derechos Humanos, fundamentales y medioambientales, el Defensor del Pueblo trabajó con ahínco en su programa de talleres y charlas de sensibilización que impactaron a 10,479 personas en 124 charlas, en su mayor parte jóvenes tanto del Distrito Nacional como de provincias de las 3 regiones del país, en distintas instituciones públicas y privadas....También fueron entregados a

Superintendencia de Bancos (SIB), la primera (diferencias) se produce a raíz de la gran cantidad de actuaciones del Defensor del Pueblo en favor de los derechos humanos y fundamentales, la segunda (similitudes), se sustenta en la inexistencia de procesos concretos en favor de la protección de las personas físicas en relación a la protección de datos personales.

3.4 Instructivo de las Sociedades de Información Crediticia (SIC)

Las Sociedades de Información Crediticia (SIC) se rigen por el procedimiento establecido en su instructivo⁹⁹⁹, el cual contempla la capacidad de establecer las previsiones y lineamientos observados por las SIC en la actual Constitución de la República Dominicana del 13 de junio de 2015 y la actual Ley núm. 172-13 del 13 de diciembre de 2013 entre otros.

El documento contiene el historial crediticio de la persona física, así como el modelo de supervisión empleado y las documentaciones provistas por las Sociedades de Información Crediticia (SIC) a la Superintendencia de Bancos (SIB) como órgano de control encargado de supervisar a las Sociedades de Información Crediticia (SIC), ejerciendo labores de inspección y vigilancia, a tal punto, que los recursos recaudados por multas impuestas a las Sociedades de Información Crediticia (SIC) por violaciones al artículo 81 de la Ley núm. 172-

la población 66,990 materiales educativos producidos y editados por el organismo. Estos materiales informan y educan sobre Derechos Humanos, Derechos Fundamentales y Derechos Medioambientales. Asimismo, enseñan sobre las funciones, misión y visión del Defensor del Pueblo...contratación de estudios científicos de campo relativos a las "conocimientos, actitudes y prácticas de la población en materia de derechos humanos" y sobre "la seguridad social". Defensor del Pueblo, Informe anual de gestión 2017-2018, del 1 de mayo de 2017 al 30 de abril de 2018, pp. 21-22. República Dominicana. Disponible en:

http://defensordelpueblo.gob.do/transparencia/phocadownload/PlanEstrategico/informe_de_gestion/Informe%20de%20gestion%202017-2018.pdf (Última verificación en línea 20 de mayo 2019).

⁹⁹⁹ Instructivo para las Sociedades de Información Crediticia (SIC) 29/07/2016, Pág. 1. Disponible en:<https://www.sib.gob.do/pdf/vistaspublicas/2016-07-29-Instructivo-para-las-sociedades-de-informacion-crediticiaversi3n-final.pdf>. (Última consulta en línea 12 de marzo 2018).

13, sean destinados a cubrir parcialmente los gastos de Supervisión que se realizan a las Sociedades de Información Crediticia (SIC)¹⁰⁰⁰.

4. El principio de Transparencia

La transparencia, forma parte del eje transversal que dirige el Gobierno dominicano y la administración pública, siendo reconocida en los artículos 138¹⁰⁰¹, 139¹⁰⁰² y 146¹⁰⁰³ de la Constitución de la República Dominicana. Incorporada a su vez, en los considerandos¹⁰⁰⁴ que dieron luz a la Ley núm. 200-04 General de Acceso a la Información Pública, una ley llamada a estimular la transparencia en el Gobierno dominicano y su administración por medio a la ejecución y empleo del derecho de acceso a la información gubernamental, siendo eje fundamental del desarrollo y fortalecimiento de la democracia representativa, permitiendo a los ciudadanos analizar, juzgar y evaluar en toda su amplitud las actuaciones de sus representantes. Vemos dos aspectos de la transparencia, uno identificado como la transparencia

¹⁰⁰⁰ Instructivo para las Sociedades de Información Crediticia (SIC) 29/07/2016, pág. 29. Disponible en: <https://www.sib.gob.do/pdf/vistaspublicas/2016-07-29-Instructivo-para-las-sociedades-de-informacion-crediticiaversi3n-final.pdf>. (Última consulta en línea 12 de marzo 2018).

¹⁰⁰¹ Constitución 2015, artículo 138, 3 Principios de la Administración Pública. La Administración Pública está sujeta en su actuación a los principios de eficacia, jerarquía, objetividad, igualdad, transparencia, economía, publicidad y coordinación, con sometimiento pleno al ordenamiento jurídico del Estado. La ley regulará: 1) El estatuto de los funcionarios públicos, el acceso a la función pública con arreglo al mérito y capacidad de los candidatos, la formación y capacitación especializada, el régimen de incompatibilidades de los funcionarios que aseguren su imparcialidad en el ejercicio de las funciones legalmente conferidas;

¹⁰⁰² Constitución 2015, artículo 139, el procedimiento a través del cual deben producirse las resoluciones y actos administrativos, garantizando la audiencia de las personas interesadas, con las excepciones que establezca la ley.

¹⁰⁰³ Constitución 2015, artículo 146 Control de legalidad de la Administración Pública. Los tribunales controlarán la legalidad de la actuación de la Administración Pública. La ciudadanía puede requerir ese control a través de los procedimientos establecidos por la ley. 5 proscripción de la corrupción. Se condena toda forma de corrupción en los órganos del Estado. En consecuencia: 1) Será sancionada con las penas que la ley determine, toda persona que sustraiga fondos públicos o que, prevaliéndose de sus posiciones dentro de los órganos y organismos del Estado, sus dependencias o instituciones autónomas, obtenga para sí o para terceros provechos económicos; [...]

¹⁰⁰⁴ Cfr. Considerando décimo, Ley núm. 200-04.

<<activa>>¹⁰⁰⁵, enfocada en la actividad pública, articulada mediante el principio de publicidad o legitimidad activa, el otro, referido al derecho de acceso a la información pública, una situación que nos permite analizar y colocar en contexto las dos variantes o divergencias relacionadas con el acceso a la información pública presentada previamente.

El acceso a la información pública se encuentra matizado por contemplar y a su vez, no considerar un interés personal de los datos solicitados, siempre y cuando estos no muestren restricciones dispuestas en la ley; empezaremos diciendo, que al referirnos al acceso de la información pública consideramos un interés legítimo del solicitante (legitimidad activa) hacia los datos existente en los registros públicos, por entender que vulneran o afectan nuestros derechos protegidos por la ley como pueden ser el derecho de intimidad, privacidad, honor, etc. de la persona asentada en el registro público, con la posibilidad de realizar correcciones, rectificaciones, cancelaciones etc. nos referimos a la figura del *habeas data*, con posibilidad de tener acceso a los archivos públicos o privados. En cambio, cuando nos referimos a la segunda variante conocida como acceso a la información pública, el solicitante puede acceder a los datos de la administración o instituciones públicas, permitiendo conocer, controlar, y participar de las actividades de la administración pública¹⁰⁰⁶.

Ante esa situación, la Ley de Acceso a la Información Pública¹⁰⁰⁷ forma parte de los aires de transparencias dispuestos por los Estados a la hora de

¹⁰⁰⁵ MARCOS DEL RINCÓN, J., "La Administración electrónica en las leyes 39 y 40/2015 de 1 de octubre. Una visión en conjunto", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 45, Septiembre-Diciembre 2017, p. 226.

¹⁰⁰⁶ DURÁN RIBERA, W, R., *Contenido y alcances del habeas data en Bolivia*, Anuario de Derecho Constitucional Latinoamericano, 2006, pp. 928-929.

¹⁰⁰⁷ "Derechos de los Ciudadanos al Libre Acceso a la Información Pública SOLICITAR información de cualquier órgano del Estado Dominicano y de todas las sociedades anónimas, compañías anónimas o compañías por acciones con participación estatal. RECIBIR información completa, veraz, adecuada y oportuna de cualquier órgano del Estado Dominicano y de todas las sociedades anónimas, compañías anónimas o compañías por acciones con participación estatal. ACCESO gratuito a la información en tanto que no requiera reproducción de la misma. SOLICITAR, RECIBIR y DIFUNDIR informaciones pertenecientes a la administración del Estado. CONOCER los proyectos de reglamentos y otras disposiciones de carácter general que rigen las relaciones entre los particulares y la administración. OPINAR sobre los proyectos de reglamentos y otras disposiciones de carácter general que rigen las relaciones entre los particulares y la administración. OBTENER información sobre los servicios

contribuir con el acercamiento de la administración pública y la sociedad civil, a raíz de las solicitudes manifiestas de la ciudadanía y la presentación de los datos solicitados por parte de las administraciones públicas.

Un derecho de acceso a la información pública contemplado en los modelos del *habeas data*, nos referimos al *habeas data* impropio dirigido a la obtención de información de carácter público, es decir, un *habeas data* de acceso a la información pública conocido como “*habeas data* público”¹⁰⁰⁸.

Reconociendo que el *habeas data* de acceso a la información pública (*habeas data* público), tiene por objeto el acceso a la información pública, estableciendo acciones procesales constitucionales específicas, formando parte a su vez del *habeas data* impropio no dirigido a la protección de datos de carácter personal asentados en bases o bancos de datos, sino, en obtener información pública negada indebidamente al legitimado activo o a replicar información de carácter personal, divulgada por medios tradicionales de difusión.

La tecnología de información y comunicaciones permite el aumento de la participación del ciudadano en el gobierno, vía el acceso a la información pública, transparentando su accionar, fortaleciendo la democracia e instaurando un gobierno abierto. La transparencia y el acceso a la información

que ofrece el Estado y sus tarifas. SABER la estructura, integrantes, normativas de funcionamiento, proyectos, informes de gestión, y bases de datos de la administración pública. CONOCER sobre los presupuestos y cálculos de recursos y gastos aprobados, su evolución y estado de ejecución. TENER información sobre los programas y proyectos, sus presupuestos, plazos, ejecución y supervisión. ESTAR AL TANTO sobre las licitaciones, concursos, compras, gastos y resultados. ACCEDER a la nómina del Estado y sus remuneraciones. CONOCER la declaración jurada patrimonial de los funcionarios del Estado cuando su presentación corresponda por ley. RECIBIR información sobre el listado de beneficiarios de programas asistenciales, subsidios, becas, jubilaciones, pensiones y retiros. SABER sobre el estado de cuentas de la deuda pública, sus vencimientos y pagos. BUSCAR las leyes, decretos, resoluciones, disposiciones, marcos regulatorios y cualquier tipo de normativa. SOLICITAR Y RECIBIR oportunamente cualquier tipo de documentación financiera relativa al presupuesto público. Disponible en: <http://transparencia.dicom.gob.do>. (Última consulta en línea 30 de mayo 2018).

¹⁰⁰⁸ PUCCINELLI, O., *Tipos y subtipos de habeas data en América latina*, editorial ASTREA, 2004. Disponible en: <https://www.astrea.com.ar/resources/doctrina/doctrina0158.pdf>. (Última consulta en línea 1 de julio 2018).

contribuyen con una real democracia evitando convertirse en un sistema elitista¹⁰⁰⁹.

Con el Memorándum del presidente Barack Obama del 21 de junio del 2009, titulado Transparencia y Gobierno Abierto¹⁰¹⁰ emitido desde la casa blanca y dirigido a los jefes departamentales y agencias ejecutivas del Gobierno de Estados Unidos, visibiliza y coloca en el tapete la transparencia y el Gobierno Abierto. Con el memorando se apela por un gobierno transparente, participativo, colaborativo¹⁰¹¹. Ya para el 2011 se crea la plataforma internacional Alianza para el Gobierno Abierto¹⁰¹².

La República Dominicana forma parte de los Estados que encaminan sus esfuerzos en favor de la transparencia, de ahí su intención de unirse a la Alianza para el Gobierno Abierto con sus siglas en inglés (OGP) a partir de octubre del 2011¹⁰¹³, una iniciativa llevada a cabo por 70 países¹⁰¹⁴, ONG y representantes de la sociedad civil, promoviendo sus tres pilares bautizados como principios, siendo estos transparencia, participación ciudadana y Gobierno Abierto¹⁰¹⁵.

¹⁰⁰⁹ TRONCOSO REIGADA, A. (Director), *Comentario de la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno*, 1ª ed. Aranzadi, S.A.U, Pamplona, 2017, pp. 70-76.

¹⁰¹⁰ Traducción en español.

¹⁰¹¹ OBAMA, B., Transparency and Open Government. Memorándum for the heads of executive departments and agencies, The White House, 21 junio 2009. Disponible en: <https://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government>. (Última consulta en línea 24 de octubre 2019).

¹⁰¹² Cfr. *Alianza para el Gobierno Abierto (OGP)*, 2011. Disponible en: http://www.opengovpartnership.org/sites/default/files/OGP_Booklet_Spanish_Digital.pdf. (Última consulta en línea 30 de mayo 2018).

¹⁰¹³ *Open Government Partnership*. Disponible en: <https://www.opengovpartnership.org/countries/dominican-republic>. (Última consulta en línea 31 de mayo 2018).

¹⁰¹⁴ México al igual que la República Dominicana, desde el 2011, es parte de los estados cofundadores de la Alianza para el Gobierno Abierto (AGA) por sus siglas en español, ocupando la presidencia desde el 2014 al 2015.

¹⁰¹⁵ Cumbre Internacional de la Alianza para el Gobierno Abierto 2016. Disponible en: <http://datos.gob.es/es/eventos/cumbre-internacional-de-la-alianza-para-el-gobierno-abierto-2016>. (Última consulta en línea 30 de mayo 2018).

De su lado, denotamos la existencia de Oficinas de Acceso a la Información Pública (OAI) en las instituciones comprometidas con la transparencia y el libre acceso a la información pública de la República Dominicana, representadas por Responsables de Acceso a la Información Pública (RAI)¹⁰¹⁶ conectados con la Dirección General de Ética e Integridad Gubernamental (DIGEIG), capaz de orquestar Comisiones¹⁰¹⁷ de Ética Pública (CEP) a nivel nacional¹⁰¹⁸; de su parte, la DIGEIG la conforma un director general y un director ejecutivo bajo la dependencia del Ministerio de la Presidencia¹⁰¹⁹, signatario de una independencia comprometida, producto de la conexión existente entre el director general y el partido de gobierno¹⁰²⁰, y más, cuando nos referimos a la Dirección General de Ética e Integridad Gubernamental (DIGEIG), una institución responsable del aseguramiento de la transparencia e integridad en la administración pública.

No solo la Alianza para el Gobierno Abierto (AGA)¹⁰²¹ inserta el tema de la transparencia como parte de los pilares que soportan su declaración, sino, que

¹⁰¹⁶ A junio del 2018 existían 237 instituciones públicas con Responsables de Acceso a la información pública, entre el período del 2006 al 2012 fueron designadas 178 Responsables de Acceso a la Información Pública (RAI). Dirección General de Ética e Integridad Gubernamental., *Instituciones públicas con Responsables de Acceso a la Información (RAI)*, junio 2018. Disponible en: <https://digeig.gob.do/transparencia/images/docs/estadisticas/2018/%20JUNIO%202018/RAI%20Designados-Junio2018.pdf>. (Última verificación en línea, 22 de mayo 2019).

¹⁰¹⁷ Decreto 143-17 crea las Comisiones de Éticas.

¹⁰¹⁸ Durante el período de Julio 2017 a junio 2018, fueron conformadas 215 Comisiones de Ética Pública (CEP) a nivel nacional. Dirección General de Ética e Integridad Gubernamental., Comisiones de Ética Pública (CEP) conformadas a nivel nacional, de Julio 2017 a junio 2018. Disponible en: <https://digeig.gob.do/transparencia/images/docs/estadisticas/2018/%20JUNIO%202018/CEP%20Conformadas-Junio2018.pdf>. Última verificación en línea, 22 de mayo 2019).

¹⁰¹⁹ Organigrama Dirección General de Ética e Integridad Gubernamental (DIGEIG), organigrama directivo. Disponible en: <https://digeig.gob.do/index.php/sobre-nosotros/organigrama>. (Última verificación en línea, 22 de mayo 2019).

¹⁰²⁰ El director general, es miembro del Comité Político del Partido de la Liberación Dominicana (PLD).

¹⁰²¹ Cfr. "...Plataforma internacional para países reformadores comprometidos con los principios de transparencia y acceso a la información, rendición de cuentas, participación y colaboración ciudadanas e innovación y tecnología...surge como respuesta a la crisis de confianza en el sistema democrático y en los gobiernos contemporáneos y busca renovar la confianza de los ciudadanos en sus autoridades fomentando los principios de transparencia,

la transparencia está inmersa en las normas legislativas de los gobiernos, tal es el caso de la normativa española 19/2013 conectada con la Alianza por el Gobierno Abierto (Open Government) y la Alianza por el Gobierno Abierto de los Documentos Oficiales del Consejo de Europa¹⁰²², una ley que tiene por objeto ampliar y reforzar la transparencia de la actividad pública, así como regular y garantizar el derecho de acceso a la información contemplado en la Constitución¹⁰²³ y al mismo tiempo, establecer las líneas a seguir (obligaciones) para un buen gobierno, todo ello anclado en un sistema de obligaciones y consecuencias ante un incumplimiento¹⁰²⁴. Estamos delante de dos derechos, el primero, de carácter fundamental perteneciente a la protección de datos, y el segundo, de acceso a la información pública reflejado y reconocido en la Carta¹⁰²⁵, considerando y haciendo imperativo la armonización de la transparencia y el derecho de acceso a la información de los ciudadanos con la protección de datos¹⁰²⁶; en ese sentido, en el informe elaborado en el 2017 por

acceso a la información, participación ciudadana, rendición de cuentas y uso estratégico de tecnologías de la información para orientar las acciones de las instituciones públicas hacia el máximo beneficio social...". *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)*. Disponible en: <http://inicio.inai.org.mx/SitePages/Transparencia/GobiernoAbierto.aspx>. (Última consulta en línea 16 de julio 2018).

¹⁰²² COTINO, L., *Derechos humanos, Internet y TICs*. En Rey (dir). Los derechos humanos en España, un balance crítico. Tirant Lo Blanch, Valencia, 2015. También en SÁNCHEZ DE DIEGO, M. (2014). "El «día después» de la ley de transparencia", *Revista Jurídica de Castilla y León*, núm. 33, 2014, pp. 1-27.

¹⁰²³ Artículo 105 literal b. "La ley regulará: El acceso de los ciudadanos a los archivos y registros administrativos". *Constitución Española de 1978*. Disponible en: <https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf> (Última consulta en línea 10 de agosto 2018).

¹⁰²⁴ Cfr. "Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno". Disponible en: <https://www.boe.es/boe/dias/2013/12/10/pdfs/BOE-A-2013-12887.pdf>. (Última consulta en línea 3 de septiembre 2018).

¹⁰²⁵ Artículo 42 Derecho de acceso a los documentos
Todo ciudadano de la Unión o toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro tiene derecho a acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión. Disponible en: http://www.europarl.europa.eu/charter/pdf/text_es.pdf. (Última consulta en línea 14 de agosto 2018).

¹⁰²⁶ MARCOS DEL RINCÓN, J., "La Administración electrónica en las leyes 39 y 40/2015 de 1 de octubre. Una visión en conjunto", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 45, Septiembre-Diciembre 2017, p. 227.

la Comisión para la reforma de las administraciones públicas, se prevé un triple alcance que tendría efecto en el proyecto de Ley núm.19/2013 antes de ser convertido en ley, entre ellas *incrementar y reforzar la transparencia en la actividad pública, reconocer y garantizar el acceso a la información y establecer las obligaciones de buen gobierno que deben cumplir los responsables públicos*¹⁰²⁷, con la obligación de la publicidad activa se garantiza la transparencia en la actividad pública, es decir, la transparencia en la actividad pública se articula por medio a obligaciones de publicidad activa como lo manifiesta el informe.

La transparencia, el acceso a la información pública y las normas de buen gobierno, son los ejes fundamentales de la referida ley, con la misma y previamente presentado, se fortalece la transparencia en la actividad pública, garantizando el acceso a la información y el establecimiento de obligaciones que conforman un buen gobierno, vinculando las administraciones públicas, los órganos legislativos y el poder judicial sujeto al Derecho Administrativo; la propia ley contempla la creación del portal de transparencia, y el establecimiento de un único punto de acceso, soportado en el desarrollo tecnológico y los medios tecnológico existente, facilitando con ello, la participación de la sociedad, la transparencia del Estado y el acceso a la información acorde a los tiempos y los intereses de los ciudadanos, la disposición crea el Consejo de Transparencia y Buen Gobierno, actuando con autonomía y plena independencia¹⁰²⁸.

La misma ley considera en sus artículos¹⁰²⁹ los criterios de ponderación a tomar en cuenta al momento de solicitar informaciones públicas

¹⁰²⁷ Resumen Ejecutivo 2017, Reforma de las Administraciones Públicas, Comisión para la reforma de Administraciones Públicas (CORA), Ministerio de Hacienda y Administraciones públicas, Ministerio de la presidencia. Disponible en: <http://transparencia.gob.es/transparencia/dam/jcr:b1c69477-9882-41a5-9f6d-5cbb46fa12b4/reforma-AAPP.PDF>. (Última consulta en línea 24 de agosto 2017).

¹⁰²⁸ Cfr. Preámbulo Ley núm. 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno". Disponible en: <https://www.boe.es/boe/dias/2013/12/10/pdfs/BOE-A-2013-12887.pdf>. (Última consulta en línea 3 de septiembre 2018).

¹⁰²⁹ Cfr. Artículo 15, protección de datos personales, Ley núm. 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno". Disponible en:

correspondientes a datos privados, ameritando el uso de los criterios de ponderación¹⁰³⁰ o aplicación suscritos en el mismo, bajo la estrecha colaboración del Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos; en el caso de las ciudades con estatutos de autonomía como las autónomas, la propia ley contempla la posibilidad de seleccionar el órgano independiente que recibirá los reclamos *frente a toda resolución expresa o presunta en materia de acceso*¹⁰³¹, o hacer uso del Consejo de Transparencia y Buen Gobierno, abriendo la posibilidad de designar sus propios órganos independientes de protección de datos¹⁰³², en este caso, la Agencia Vasca de Protección de Datos.

Con la entrada en vigor del Reglamento de protección de datos, se abre la oportunidad en los Estados de *incorporar a su derecho nacional elementos del presente Reglamento*¹⁰³³, a raíz de ello, el Parlamento Vasco contempla la aprobación del proyecto de ley de protección de datos personales Vasco, un proyecto que integra bajo un mismo órgano regulador el tema de la transparencia y la protección de datos personales, así como lo expresa la disposición adicional primera, en proceso de aprobación por el Grupo Nacionalista Vasco y el Grupo Socialista Vasco¹⁰³⁴, otorgando a la Agencia de Protección de Datos Vasca plena competencia en materia de transparencia y

<https://www.boe.es/boe/dias/2013/12/10/pdfs/BOE-A-2013-12887.pdf>. (Última consulta en línea 3 de septiembre 2018).

¹⁰³⁰ Disposición adicional quinta. Colaboración con la Agencia Española de Protección de Datos. “El Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos adoptarán conjuntamente los criterios de aplicación...en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados...”. Ley núm. 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Disponible en: <https://www.boe.es/boe/dias/2013/12/10/pdfs/BOE-A-2013-12887.pdf>. (Última consulta en línea 3 de septiembre 2018).

¹⁰³¹ Art. 24, numeral 1, Ley núm. 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

¹⁰³² Disposición 4ta. Numeral 3, Reclamación, Ley núm. 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

¹⁰³³ Cfr. Considerando 8, Reglamento (UE) 2016/679.

¹⁰³⁴ En el mes de junio 2018 se contempló la tercera vista.

protección de datos, contemplando una gerencia para estos fines y una total competencia para la Agencia. Un modelo adoptado internacionalmente por los Estados, incluidos México en Latinoamérica y España en la Unión Europea, específicamente la comunidad de Andalucía y en proceso la Vasca, con la salvedad de no contar por el momento con un desarrollo normativo, dando la posibilidad a la Comunidad Vasca de ser la primera comunidad en contar con un desarrollo legislativo en función del modelo planteado¹⁰³⁵. La conformación de las acciones en favor de la transparencia en la Comunidad Vasca no es nueva, sino que ha estado precedida de eventos y acciones, entre ellos, los esfuerzos realizados en el 2008 en búsqueda de un determinado equilibrio y ponderación entre la transparencia y la protección de datos, ya para el año 2014, la Agencia Vasca realiza una monografía especial cuyo enfoque se orienta a la necesidad de equilibrio entre la protección de datos y la transparencia.

Por su parte, el tema de la transparencia, acceso a la información pública y como no, la protección de datos personales han formado parte de las normativas españolas, incluso, momentos antes del establecimiento de la Ley núm.19/2013 del 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno¹⁰³⁶, y la entrada del nuevo Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

En ese sentido, el desarrollo de las TIC impacta la comunión entre el ciudadano y las administraciones pública, con la Ley núm.30/1992 de 26 de noviembre de *régimen jurídico de las administraciones públicas y del procedimiento administrativo común*, se entreteje una comunión entre la telemática y el gobierno o administración pública, unificando *las reglas*

¹⁰³⁵ URÍA ETXEBARRIA, M., *Protección de datos y transparencia: Compañeros de viaje.*, Discurso inaugural curso de verano, Agencia Vasca de Protección de Datos, Donostia, San Sebastián, 21 de junio, 2018. Disponible en: <http://www.avpd.euskadi.eus/webcast/s04-5273/es/> (Última consulta en línea 10 de agosto 2018).

¹⁰³⁶ LÓPEZ GUERRA, L., Prólogo en la obra: TRONCOSO REIGADA, A. (Director), *Comentario de la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno*, 1ª ed. Aranzadi, S.A.U, Pamplona, 2017, p. 81.

*reguladoras de los aspectos orgánicos del poder ejecutivo con las que disciplinaban los procedimientos*¹⁰³⁷, con el paso del tiempo, la normativa demandó otra regulación¹⁰³⁸, materializada en la Ley núm.11/2007 del 22 de Junio de *acceso electrónico de los ciudadanos a los servicios públicos*, formando parte de aquellos Estados que ponen al servicio de la administración pública, el desarrollo de las nuevas tecnologías y comunicaciones¹⁰³⁹ haciendo que las administraciones públicas se vean en la obligación de reforzar sus administraciones para cumplir con este derecho de acceso, mejorando sus estructuras tecnológicas, aportando la eficiencia y eficacia necesaria que requiere la administración, reduciendo el uso de materiales físicos como el papel y sus procesos conectados, aumentando la garantía y la transparencia en la administración, orquestada por una administración electrónica en constante conexión con el ciudadano mediante el uso de la tecnología y sus grandes volúmenes de datos ofrecidos por la administración electrónica a expensa de la reducción de cargas físicas como el uso de papel; por su parte, existen normas asociadas, dispuestas a contribuir con la mejora de las posibles dispersiones existente entre las norma y contribuir con la coherencia entre los regímenes jurídicos creados, incluidas las leyes sectoriales de acceso a la información pública en materia de medio ambiente y reutilización de la información pública, tales como la Ley núm. 27/2006 del 18 de julio, *por la que se regulan los derechos de acceso a la información, de participación pública y*

¹⁰³⁷ BOE-A-2015-10566, Ley núm. 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Disponible en: <https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10566-consolidado.pdf>. (Última consulta en línea 24 de agosto 2018).

¹⁰³⁸ (...) La Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno presenta lagunas y deficiencias y es un texto mejorable, como lo son todas las normas jurídicas que tratan de realizar avances, conciliando valores y actores contrapuestos pero su aprobación ha abierto ya definitivamente la puerta al acceso a la información pública en España....Se ha dicho.....que es una ley cicatera.....se aprobó en un contexto de crisis económica....preocupado por la consolidación fiscal y por la sostenibilidad económica y social ...donde era difícil la aprobación de leyes que supusieran reconocimiento de derechos sociales con impacto en el gasto público....se enmarca en el fortalecimiento del Estado democrático. TRONCOSO REIGADA, A. (Director), *Comentario de la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno*, 1ª ed. Aranzadi, S.A.U, Pamplona, 2017, pp. 76-77.

¹⁰³⁹ GALINDO, F. y J. ROVER (EDS), A., *Derecho, gobernanza y tecnologías de la información en la sociedad del conocimiento*, 1ra. ed. prensa universitaria de Zaragoza, AECID, Zaragoza, España, 2009, pp. 167-169.

de acceso a la justicia en materia de medio ambiente¹⁰⁴⁰, la Ley núm. 37/2007 de 16 de noviembre, sobre reutilización de la información del sector público¹⁰⁴¹, la Ley núm.17/2009, de 23 de noviembre, sobre libre acceso a las actividades de servicios y su ejercicio¹⁰⁴²; la Ley núm.2/2011, de 4 de marzo, de economía sostenible¹⁰⁴³, la ya vista Ley núm.19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, la Ley núm.20/2013, de 9 de diciembre, de garantía de la unidad de mercado¹⁰⁴⁴ con la normativa 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas¹⁰⁴⁵ se clarifica la Ley núm.30/1992 y la Ley núm.11/2007, haciendo hincapié en la agilización de aquellos procedimientos sustentado en funcionamiento electrónico y de esta manera lograr la anhelada seguridad jurídica en manos de las administraciones públicas¹⁰⁴⁶, y con la Ley núm.40 de 1 de octubre de 2015 se recoge lo relacionado al funcionamiento electrónico del sector público contemplado en la Ley núm. 11/2007 y las previstas en el Decreto núm. 1671/2009, un decreto

¹⁰⁴⁰ BOE-A-2006-13010, Ley núm. 27/2006 del 18 de Julio.

Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2006-13010>. (Última consulta en línea 10 de agosto 2017).

¹⁰⁴¹ BOE-A-2007-19814, Ley núm.37/2007 de 16 de noviembre. Disponible en:

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-19814. (Última consulta en línea 10 de agosto 2017).

¹⁰⁴² BOE-A-2009-18731, Ley núm. 17/2009, de 23 de noviembre. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2009-18731&p=20131210&tn=2>. (Última consulta en línea 24 de agosto 2018).

¹⁰⁴³ BOE-A-2011-4117, Ley núm. 2/2011, de 4 de marzo, de Economía Sostenible. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2011-4117>. (Última consulta en línea 24 de agosto 2018).

¹⁰⁴⁴ Ley núm. 20/2013, de 9 de diciembre, de garantía de la unidad de mercado, BOE-A-2013-12888. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-2013-12888>. (Última consulta en línea 24 de agosto 2018).

¹⁰⁴⁵ Ley núm. 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. BOE-A-2015-10565. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565>. (Última consulta en línea 24 de agosto 2018).

¹⁰⁴⁶ Preámbulo Ley núm. 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones públicas. BOE-A-2015-10565. Disponible en: <http://www.boe.gob.es/buscar/act.php?id=BOE-A-2015-10565&p=20151002&tn=1#preambulo>. (Última consulta en línea 23 de agosto 2018).

que desarrolla la Ley núm. 11/2007 en aquellas disposiciones no derogadas por la Ley núm. 39/2015 de 1 de octubre¹⁰⁴⁷.

La transparencia, no solo forma parte integral de las normativas europeas, como es el caso de la norma española¹⁰⁴⁸, sino, que contamos con Estados Latinoamericanos donde la transparencia es parte integral de sus normas, y Estados partícipes y cofundadores de la Alianza para el Gobierno Abierto, en esta ocasión, nos referimos al caso Mexicano, un Estado Federal con normativas en materia de transparencia y uno de los Estados fundadores de la Alianza para el Gobierno Abierto, siendo reconocido como uno de los Estados más completo¹⁰⁴⁹ en normativas de protección de datos, a tal punto de asegurar su consolidación en la materia y convertirse en un Estado modelo con capacidad de influenciar en materia de protección de datos, transparencia y acceso a la información pública en los Estados, incluida Latinoamérica,

¹⁰⁴⁷ MARCO DEL RINCÓN, J., “La Administración Electrónica en las leyes 39 y 40/2015 de 1 de octubre. Una visión en conjunto”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 45, Septiembre-Diciembre 2007, p. 189. Ley núm. 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Disponible en: <https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10566-consolidado.pdf>. (Última consulta en línea 24 de agosto 2018).

¹⁰⁴⁸ En España, más allá de la Ley 19/2013 coexisten otras leyes de transparencia en casi todas las comunidades autónomas como: la Ley 4/2011, de 31 de marzo, de la Buena Administración y del Buen Gobierno de las Illes Balears; la Ley 4/2013, de 21 de mayo, de Gobierno Abierto de Extremadura; Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía; la Ley 3/2014, de 11 de septiembre, de Transparencia y Buen Gobierno de La Rioja; Ley 12/2014, de 16 de diciembre, de Transparencia y Participación Ciudadana de la Comunidad Autónoma de la Región de Murcia; la Ley 12/2014, de 26 de diciembre, de transparencia y de acceso a la información pública (Canarias); la Ley 19/2014, de 29 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno (Cataluña); Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía.; la Ley 3/2015, de 4 de marzo, de Transparencia y Participación Ciudadana de Castilla y León; la Ley 8/2015, de 25 de marzo, de Transparencia de la Actividad Pública y Participación Ciudadana de Aragón, y la Ley 2/2015, de 2 de abril, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunitat Valenciana....no así en Asturias, Cantabria, Castilla, la Mancha, Madrid y País Vasco SERRANO MAÍLLO, I., MARTÍNEZ PASTOR, E. y BELTRÁN ORENES, P., “Una revisión crítica de la Ley española 19/2013”, *Revista Transparencia & Sociedad*, Núm. 5-Diciembre 2017, p. 56.

¹⁰⁴⁹ “En la actualidad es posible afirmar que México cuenta con un cuerpo normativo sólido en materia de protección de datos personales, dentro del cual se destacan por su relevancia...: Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y la Ley Federal de Protección de Datos en posesión de los Particulares...”. QUESADA RODRÍGUEZ, A., *Protección de datos y telecomunicaciones convergentes*, 1ª ed. Agencia Española de Protección de Datos, Madrid, 2015, p. 338.

fundamentada en sus rasgos particulares como cultura, entornos geopolíticos y procedencia de sistema jurídico.

El proceso de transformación constitucional mexicano se ampara en sus más de 300 reformas constitucionales, incluidos los temas de protección de datos y acceso a la información, formando parte del marco integral normativo de su mecanismo de control, ahora bien, el desarrollo normativo constitucional en temas de acceso a la información pública y protección de datos se ampara y ubica en los numerales 6 y 16 del pliego constitucional, como hemos mencionado, el proceso constitucional actual en materia de protección de datos y acceso a la información forma parte de las transformaciones a que ha sido sometida la Constitución actual mexicana en los últimos años, en muchos aspectos una reforma constitucional a la altura de las normas europeas a pesar de la inexistencias de certificaciones como las previamente analizadas (Argentina, Uruguay); unas reformas que datan desde la primera reforma constitucional del 5 de febrero de 1917, reformando la Constitución del 5 de febrero de 1857¹⁰⁵⁰, contemplando en los numerales 6 y 16 el germen constitucional que da paso al acceso a la información y la protección de datos¹⁰⁵¹ presente en la actual Constitución mexicana conectada con sus reformas constitucionales¹⁰⁵².

En materia de protección de datos, su marco normativo está compuesto por la *Ley Federal de Protección de Datos Personales en Posesión de Particulares* y la *Ley General de Protección de Datos Personales en Posesión de Sujetos*

¹⁰⁵⁰ *Constitución política de los Estados Unidos Mexicanos del 5 de febrero de 1917*, que reforma la constitución del 5 de febrero de 1857. Disponible en: <http://www.ordenjuridico.gob.mx/Constitucion/1917.pdf>. (Última consulta en línea 23 de julio 2018).

¹⁰⁵¹ QUESADA RODRÍGUEZ, A., *Protección de datos y telecomunicaciones convergentes*, 1ª ed. Agencia Española de Protección de Datos, Madrid, 2015, p. 337.

¹⁰⁵² A partir de la reforma constitucional del 05-02-1917, los artículos 6 y 16 han sido objeto de adecuaciones o reformas constitucionales, el artículo 6 presenta al menos 6 reformas siendo estas: DOF: 06-12-1977, DOF:13-11-207, DOF:20-07-2007, DOF: 11-06-2013, DOF: 07-02-2014, DOF: 29-01-2016, seguido del artículo 16 con 8 reformas constitucionales siendo estas: DOF: 03-02-1983, DOF: 03-09-1993, DOF: 03-07-1996, DOF: 08-03-1999, DOF: 18-06-2008, DOF: 01-06-2009, DOF: 25-06-2009, DOF: 15-09-2017. *Portal Cámara de Diputado Mexicano*. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_150917.pdf. (Última consulta en línea 23 de julio 2018).

*Obligados*¹⁰⁵³; la normativa actual en temas de acceso a la información pública contempla la *Ley General de Transparencia y Acceso a la Información Pública*¹⁰⁵⁴, fundamentada en sus antecesoras la *Ley Federal de Transparencia y Acceso a la Información Pública* y la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*¹⁰⁵⁵, la regulación de la protección de datos en México inicia a partir de la Ley Federal de Transparencia y Acceso a la Información Pública del 2002¹⁰⁵⁶.

El mecanismo de control a cargo del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), se caracteriza por ser un organismo que goza de total autonomía, tutelando los derechos de protección de datos y acceso a la información pública establecidos en su pliego constitucional, garantizando la entrega de información de los entes conectados con recursos públicos; garantizando a su vez la protección de los datos personales pertenecientes a los sujetos obligados y particulares, es decir, nos referimos a un órgano de control que tiene a su cargo el acceso a la información pública transparentando la función pública y por ende, protegiendo y asegurando los datos personales, concentrando en su marco normativo las leyes de transparencia y acceso a la información pública como la protección de datos personales, formando parte del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, una instancia encargada de realizar esfuerzos de cooperación, difusión,

¹⁰⁵³ DOF: 26/01/2017. Decreto por el que se expide la Ley General de protección de Datos Personales en posesión de Sujetos Obligados. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017. (Última consulta en línea 28 de julio 2018).

¹⁰⁵⁴ DOF 04 mayo 2015. Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública. Disponible en: <http://www.dof.gob.mx/index.php?year=2015&month=05&day=04>. (Última consulta en línea 28 de julio 2018).

¹⁰⁵⁵ Marco Normativo, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2018. Disponible en: <http://inicio.inai.org.mx/SitePages/marcoNormativo.aspx>. (Última consulta en línea 23 de junio 2018).

¹⁰⁵⁶ MUÑOZ FRANCO, G., *La Protección de Datos Personales en México*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014, p. 1037.

coordinación¹⁰⁵⁷ en materia de transparencia, acceso a la información y protección de datos amparado en la Ley General de Transparencia y Acceso a la Información Pública y aquellas normas relacionadas y de posible aplicación¹⁰⁵⁸.

En igual sentido y a raíz de los estudios realizados y presentado por la OCDE sobre la gobernanza pública mexicana, denominado “*hacia una gestión pública más efectiva y dinámica en México*”, se plantea la necesidad de hacer más eficiente y eficaz¹⁰⁵⁹ la gestión del Gobierno mexicano a raíz de los sucesos acaecidos en la década de los 80, como son: a) un aumento de las exportaciones; b) disminución de las importaciones; c) privatización de las empresas públicas; d) crisis económica; f) dependencia del petróleo; y, g) reducción del tamaño del sector público, siendo necesario proveer y apoyar la reforma del gobierno, una reforma crucial en la ansiada recuperación económica del sector público, convirtiéndose en eje prioritario del Estado; ante tal situación, se exhorta el empleo y uso de las tecnologías de información y comunicación, creando *sociedades de comunicación e información abiertas y transparentes*; implementando medidas entre las que se destaca la eliminación de un 67% de las regulaciones internas, publicación de manuales administrativo de actividades del gobierno, etc.¹⁰⁶⁰, a su vez, el gobierno realiza ingentes esfuerzos en mejorar la gestión interna de la administración pública manteniendo una visión conectada con las bondades proporcionadas por las TIC¹⁰⁶¹.

¹⁰⁵⁷ Consejo Nacional, 2018. Disponible en: <http://snt.org.mx/index.php/consejo-nacional>. (Última consulta en línea 23 de julio 2018).

¹⁰⁵⁸ Sistema Nacional de Transparencia, 2018. Disponible en: <http://snt.org.mx/>. (Última consulta en línea 23 de julio 2018).

¹⁰⁵⁹ Eficiencia y eficacia: el gobierno se esfuerza por generar productos públicos de calidad, incluyendo los servicios que presta a los ciudadanos, al mejor costo, y garantiza que lo ofrecido cumpla con las intenciones originales de los formuladores de políticas públicas.

¹⁰⁶⁰ Adquisiciones, Obras Públicas, Recursos Humanos, Recursos Financieros y Recursos Materiales, Tecnologías de la Información y Comunicaciones, Transparencia, Auditoría y Control.

¹⁰⁶¹ La visión del gobierno mexicano se centra en aprovechar plenamente las TIC para garantizar el desarrollo de una sociedad de la información competitiva, incluyente e innovadora.

La República Dominicana, en específico el Gobierno dominicano, ha aunado esfuerzos en garantizar la transparencia en los distintos organismos que componen el tren gubernamental, motivado por las consecuencias que genera la corrupción administrativa, socavando la integridad moral del pueblo dominicano e impactando su desarrollo económico y social¹⁰⁶², a raíz de ello, se crean mecanismos de prevención capaces de integrar los diferentes sectores que constituyen la administración pública, una de las primeras iniciativas se concretizó mediante la creación del Departamento de Prevención de la Corrupción (DPCA)¹⁰⁶³ bajo la dependencia de la Procuraduría General de la República, siendo su jefe máximo el procurador, responsable de la organización y coordinación del plan nacional de lucha contra la corrupción por vía expresa del poder ejecutivo, en ese mismo orden, se ordena a los secretarios de Estados, directores y administradores generales, la formación de una Comisión de Ética Pública encargada de la transparencia de la gestión administrativa sirviendo de enlace del departamento de prevención de la corrupción¹⁰⁶⁴, creando planes destinados al fortalecimiento de la ética y la

La estrategia del gobierno mexicano (su Agenda de Gobierno Digital) cuenta con dos elementos principales: 1) la adopción y el uso de TIC por parte de la sociedad y un mercado en el que los factores impulsores principales son los precios, la calidad y la cobertura, y 2) la adopción y el uso de TIC por parte del gobierno, para el que las motivaciones centrales se enfocan en mejorar la eficiencia operativa de las instituciones públicas, reducir los costos de transacción entre ciudadanos y el gobierno, y producir bienes públicos. Adicionalmente, el gobierno amplió su enfoque visionario y conceptual de desarrollo del gobierno electrónico que está impulsando los proyectos e iniciativas nacionales relacionados con las TIC y el gobierno electrónico. La Agenda de Gobierno Digital se basa de hecho en la siguiente definición: “El uso de TIC para fomentar la construcción, protección y distribución de bienes públicos y comunes”, así como en la definición de varios conjuntos de información como bienes públicos, como los registros civiles y de la propiedad, las estadísticas nacionales y los registros criminales, de justicia y de educación. OCDE (2011), *Hacia una gestión pública más efectiva y dinámica en México*, OECD.

Disponible en: <https://www.oecd.org/gov/regulatory-policy/48808023.pdf>. (Última consulta en línea 6 de agosto 2018).

¹⁰⁶² Cfr. *Decreto 149-98 que crea las Comisiones de Ética Pública*.

Disponible en: http://www.sisalril.gob.do/pdf/transparencia/decreto_149_98.pdf. (Última consulta en línea 3 de septiembre 2018).

¹⁰⁶³ *Decreto N.º 322-97 del 24 de julio de 1997 que crea el Departamento de Prevención de la Corrupción Administrativa*.

Disponible en: http://www.oas.org/juridico/pdfs/mesicic4_reptom_dec322.pdf. (Última consulta en línea 5 de julio 20018).

¹⁰⁶⁴ Artículo 1 *Decreto 149-98 que crea las Comisiones de Ética Pública*. Disponible en: http://www.sisalril.gob.do/pdf/transparencia/decreto_149_98.pdf. (Última consulta en línea 3 de septiembre 2018).

transparencia en la gestión pública, en ese sentido, con la creación del Código de Ética del Servidor Público¹⁰⁶⁵ se busca la normalización de la conducta de los servidores públicos en función de los principios éticos que moldearán su desempeño, por su parte, y siguiendo los planes pautados por el Gobierno vía la Dirección general de Ética e Integridad Gubernamental (DIGEIG), se establecen mejoras a la estructura y funcionamiento de la Comisión de Ética Pública (CEP)¹⁰⁶⁶ siguiendo los lineamientos instituidos por el Gobierno en materia de transparencia, ética de la función pública y combate a la corrupción, conformado por diversas posiciones de las dependencias del Estado, siete (7) en total, incluida la dependencia del responsable de acceso a la información pública, con la medida, se busca involucrar a los servidores públicos al momento de evaluar y tomar decisiones ante la Comisión, de esta manera, se encuentran comprometidos por ser parte del proceso, siendo aptos de recibir sanciones del ejecutivo ante posibles faltas frente a la Comisión, evitando la desvinculación de sus departamentos mientras sean miembros de la Comisión, asegurando el compromiso de sus decisiones.

En tal sentido, se crea el Consejo Asesor en Materia de Lucha Anticorrupción de la Presidencia¹⁰⁶⁷ de la República, encargado de elaborar y someter a la presidencia proyectos legislativos tendentes a combatir la corrupción, siendo conformado por miembros titulares de instituciones gubernamentales, no gubernamentales, representantes de la sociedad civil,

¹⁰⁶⁵ Cfr. *Ley N.º 120-01 del 20 de Julio del 2001 que instituye el Código de Ética del Servidor Público*. Disponible en: <http://www.contraloria.gob.do/Sitecontraloria/images/docs/ley-no-120-01.pdf>. (Última consulta en línea 7 de julio 20018).

¹⁰⁶⁶ *Decreto 143-17 proceso de actualización Comisión de Ética Pública (CEP)*. Disponible en: <https://es.scribd.com/document/346596887/Decreto-143-17>. (Última consulta en línea 9 de julio 2018).

¹⁰⁶⁷ Decreto. N.º 783-01 que crea e integra el Consejo Asesor en Materia de Lucha Anticorrupción de la Presidencia de la República. *Legislación básica de la Administración Pública de República Dominicana, departamento de Prevención de la Corrupción*, Procuraduría General de la República, Agencia de los Estados Unidos para el Desarrollo Internacional (USAID), p. 206. Disponible en: http://www.oas.org/juridico/spanish/dna_res2.pdf. (Última consulta en línea 5 de julio 2018).

sector eclesiástico¹⁰⁶⁸; por su parte, República Dominicana es signataria vía ratificación de la Convención Interamericana contra la Corrupción de la Organización de Estados Americanos (OEA) asumiendo el compromiso al frente del organismo internacional¹⁰⁶⁹, de ahí la necesidad de fortalecer la ética en las instituciones del Gobierno mediante la conformación de la Comisión de Ética y Combate a la Corrupción, un organismo multisectorial integrado por el Gobierno, la sociedad civil y el sector empresarial, asesorando al Poder Ejecutivo en materia de promoción de la ética, la transparencia y el combate a la corrupción, con la decisión se deroga el decreto anterior¹⁰⁷⁰; los recursos económicos serán provisto por el Poder Ejecutivo recibiendo el apoyo técnico de los organismos multilaterales y nacionales¹⁰⁷¹, es importante notar el esfuerzo del Gobierno con la Comisión, un impulso que, más allá del aspecto económico, pone a disposición de la Comisión los distintos estamentos del Gobierno como el representante del Gobierno, la Procuraduría, la Contraloría General de la República, la Secretaría de Estado de Finanzas y otras instituciones incluidas las iglesias, el sector privado, foros ciudadanos etc.

Siguiendo con el apoyo gubernamental y tras la contienda electoral del 2012, la sociedad dominicana exigió a los candidatos realizar acuerdos que fomenten la ética, la transparencia, y el combate a la corrupción, como ya hemos externado la República Dominicana forma parte de los Estados signatarios de

¹⁰⁶⁸ El Secretario de la Presidencia, El Consultor Jurídico del Poder Ejecutivo, El Procurador General de la República, El Contralor General de la república, El Director del Departamento de Prevención de la Corrupción, El Procurador Fiscal del Distrito Nacional, El Procurador Fiscal de Santiago de los Caballeros, Un representante de la Iglesia Católica Dominicana, Un representante de la Iglesia Evangélica Dominicana, Participación Ciudadana (representante de la Sociedad Civil), Alianzas ONG'S (Representante de la Sociedad Civil), Asociación de jóvenes de la Paz (Representante de la Sociedad Civil).

¹⁰⁶⁹ Cfr. "...mecanismos necesarios para prevenir, detectar, sancionar y erradicar los actos de corrupción.". Considerando segundo, *decreto N.º 101-05 que crea la Comisión de Ética y Combate a la Corrupción*.

Disponible en: http://www.hacienda.gov.do/images/docs/marco_legal/decretos/decreto_101-05.pdf. (Última consulta en línea 5 de julio 2018).

¹⁰⁷⁰ Artículo 6.- Queda derogado el Decreto N.º 783-01 del 24 de julio del año 2001. Disponible en: http://www.hacienda.gov.do/images/docs/marco_legal/decretos/decreto_101-05.pdf. (Última consulta en línea 5 de julio 2018).

¹⁰⁷¹ Cfr. *Decreto N.º 101-05 que crea la Comisión de Ética Pública y Combate a la Corrupción*. Disponible en: http://www.hacienda.gov.do/images/docs/marco_legal/decretos/decreto_101-05.pdf. (Última consulta en línea 5 de julio 2018).

la Convención Interamericana contra la Corrupción de la OEA y la Convención de la Organización de las Naciones Unidas Contra la Corrupción (CNUCC), situaciones que ameritan por parte del Gobierno dominicano aunar esfuerzos en el fortalecimiento del régimen ético conectado con un sistema de consecuencias, asegurando el cumplimiento de la ley y con ello, penalizar las conductas inadecuadas que ocurran en el seno de la administración pública, amparado en la necesidad de racionalizar la estructura organizativa del poder ejecutivo unificando funciones, cuyos resultados retribuirían positivamente con lo esperado y reclamado por la sociedad ante las experiencias generadas por medio a la puesta en funcionamiento de diversos modelos¹⁰⁷² implementados en el ámbito del Poder Ejecutivo.

Repercutiendo con la creación de la Dirección de Ética e Integridad Gubernamental (DIGEIG)¹⁰⁷³ sustituta de la Comisión Nacional de Ética y Combate a la Corrupción (CNECC)¹⁰⁷⁴ asumiendo su continuidad, sustentada en una base legal con mayor autonomía, cuyos resultados se amparan en *la ética, la transparencia, gobierno abierto, lucha contra la corrupción, conflicto de interés, y libre acceso a la información, en el ámbito administrativo gubernamental*¹⁰⁷⁵, con recursos procedentes del presupuesto nacional y

¹⁰⁷² Cfr. “Que existen experiencias en la región, de distintos modelos institucionales con responsabilidad de trabajar los temas de educación, prevención de la corrupción, conflicto de intereses, acceso a la información, gobierno abierto e investigaciones administrativas, en el ámbito del poder ejecutivo”. *Decreto N.º 486-12 que crea la Dirección General de Ética e Integridad Gubernamental (DIGEIG)*. G. O. N.º 10693 del 31 de agosto de 2012. Disponible en: http://www.poderjudicial.gob.do/documentos/PDF/decretos/Dec_486-12.pdf. (Última consulta en línea en línea 6 de julio 2018).

¹⁰⁷³ “El gobierno abierto y la e-Transparencia conforman una doctrina política que sostiene que los temas de gobierno y administración pública deben ser abiertos a todos los niveles posibles en cuanto a transparencia...La institución del gobierno Dominicano encargada del Gobierno abierto, la e-Transparencia y los datos abiertos es la Dirección de Ética e Integridad Gubernamental (DIGEIG)..”. *e-Transparencia, Gobierno y Datos Abiertos (Open Government)*. Disponible en: <http://www.gob.do/index.php/e-sociedad/2014-12-17-20-08-19/2014-12-17-20-09-52>. (Última consulta en línea 4 de julio 2018).

¹⁰⁷⁴ Cfr. *Decreto N.º 101-05 de 16 de febrero que crea la Comisión de Ética Pública y Combate a la Corrupción*. Disponible en: http://www.hacienda.gov.do/images/docs/marco_legal/decretos/decreto_101-05.pdf. (Última consulta en línea 5 de julio 2018).

¹⁰⁷⁵ Artículo 1. *Decreto. N.º 486-12 que crea la Dirección General de Ética e Integridad Gubernamental (DIGEIG)*. G. O. N.º 10693 del 31 de agosto de 2012.

asignaciones especiales; por otra parte, la Dirección estará adscrita al Ministerio de la Presidencia a cargo de un director general nombrado por el presidente de la República¹⁰⁷⁶ y contará con un director ejecutivo¹⁰⁷⁷ responsable de los aspectos técnicos y operativos de la dirección, de este modo, la dirección se convierte en el órgano rector de la ética e integridad en la administración pública, incluyendo lo relacionado con la Ley de Acceso a la Información Pública núm. 200-04, al igual de responder a las asignaciones otorgadas en sus funciones como: a) velar por la difusión e implementación de la Ley núm.41-08 de función pública; b) fortalecer la ética y la transparencia, c) asesorar las diversas comisiones de ética; d) diseñar e implementar programas de capacitación junto al Ministerio de Administración Pública (MAP) y el Instituto Nacional de Administración Pública (INAP); e) mantener un registro de las Oficinas de Acceso a la Información (OAI); f) evaluar sus niveles de cumplimiento; y g) analizar los mecanismos de transparencias, entre otros, incluidos en sus cuarenta y dos puntos¹⁰⁷⁸.

5. Órganos adscritos a la presidencia gubernamental

Con la actual Ley núm. 172-13 promulgada el 13 de diciembre de 2013, diversas instituciones gubernamentales procedieron a inhabilitar las consultas

Disponible en: http://www.poderjudicial.gob.do/documentos/PDF/decretos/Dec_486-12.pdf. (Última consulta en línea 6 de julio 2018)

¹⁰⁷⁶ Cfr. Decreto 246-16 que designa al Lic. Lidio Cadet Jiménez, Director General de la Dirección General de Ética e Integridad Gubernamental (DIGEIG).

Disponible en: <https://digeig.gob.do/index.php/despacho-del-director>. (Última consulta en línea 9 de julio 2018).

¹⁰⁷⁷ Cfr. Decreto 234-17 que designa al Director Ejecutivo DIGEIG. Disponible en:

<https://digeig.gob.do/images/docs/DECRETO%20234-17.%20Designaci%C3%B3n%20Director%20Ejecutivo%20DIGEIG.pdf> (Última consulta en línea 8 de julio 2018).

¹⁰⁷⁸ Cfr. Decreto. N.º 486-12 que crea la Dirección General de Ética e Integridad Gubernamental (DIGEIG). G. O. N.º 10693 del 31 de agosto de 2012. Derogando el decreto N.º 101-05 que crea la Comisión de Ética Pública y Combate a la Corrupción y su reglamento N.º 310-05. Disponible en:

http://www.poderjudicial.gob.do/documentos/PDF/decretos/Dec_486-12.pdf. (Última consulta en línea 6 de julio 2018).

de sus datos personales, como es el caso de la Tesorería de la Seguridad Social (TSS), en vista de ello, todo lo relacionado con los datos personales procedentes del Sistema Dominicano de Seguridad Social deberá ser utilizado por los mecanismos de la Dirección de Información y Defensa de los Afiliados (DIDA)¹⁰⁷⁹; estamos delante de los esfuerzos encaminados por el Gobierno dominicano a raíz de sus iniciativas en materia de transparencia de la administración y sus leyes representadas por su marco legal¹⁰⁸⁰ encabezado por la Ley de Acceso a la Información Pública núm. 2000-04 y sus iniciativas como la creación del Portal de Transparencia de la Dirección General de Comunicación (DICOM)¹⁰⁸¹, órgano portavoz y encargado de coordinar las políticas de comunicación del Gobierno¹⁰⁸², el portal electrónico del Gobierno¹⁰⁸³ concebido para tener acceso, realizar transacciones e interactuar con los servicios en líneas del Gobierno dominicano agrupados en información/conocimiento (e-Sociedad), ciudadanos/empresas (e-Servicios), gobiernos locales (e-Municipios), marco regulatorio (e-Políticas), recursos/documentos (Herramientas), Rep. Dom., (País), asistencia/apoyo (Ayuda), al mismo tiempo la Oficina Presidencial de Tecnologías de la Información y Comunicación de la República Dominicana (OPTIC)¹⁰⁸⁴, órgano

¹⁰⁷⁹ *Portal Oficial del Estado dominicano, Seguridad y Delito Electrónico (Cyber Security and Crimen)*, 2018. Disponible en: <http://www.gob.do/index.php/seguridad-y-delito-electronico>. (Última consulta en línea 29 de mayo 2018).

¹⁰⁸⁰ Un marco legal compuesto por la Constitución de la República Dominicana, 16 Leyes, 15 decretos, 1 resolución, 1 reglamento.

¹⁰⁸¹ *Decreto 490-12, mediante el cual se crea la Dirección General de Comunicaciones (DICOM)*. Disponible en: https://presidencia.gob.do/themes/custom/presidency/docs/microsite-dicom/decreto_490_12.pdf. (Última consulta en línea 29 de mayo 2018).

¹⁰⁸² *Decreto 490-12, mediante el cual se crea la Dirección General de Comunicaciones (DICOM)*. Disponible en: https://presidencia.gob.do/themes/custom/presidency/docs/microsite-dicom/decreto_490_12.pdf. (Última consulta en línea 29 de mayo 2018).

¹⁰⁸³ *Portal electrónico del gobierno dominicano*. Disponible en: www.dominicana.gob.do. (Última consulta en línea 28 de mayo 2018).

¹⁰⁸⁴ “La Oficina Presidencial de Tecnologías de la Información y Comunicaciones de la República Dominicana, institución con dependencia del Poder Ejecutivo, creada con la responsabilidad de planificar, dirigir y ejecutar las acciones necesarias para implementar el Gobierno Electrónico en el país mediante la difusión y uso de las Tecnologías de la Información y Comunicación (TIC)”, *Oficina Presidencial de Tecnologías de la Información y Comunicación*

encargado de la estrategia de Gobierno Electrónico, responsable de *planificar, dirigir y ejecutar las acciones necesarias para implementar el gobierno electrónico en el país apoyado en la difusión y uso de las Tecnologías de la información y comunicación (TIC)*.¹⁰⁸⁵

6. La Oficina Presidencial de Tecnología de Información (OPTIC)

En ese mismo sentido y ante la imperiosa necesidad manifiesta de las tecnologías de información y comunicaciones (TIC), la modernización del Estado, la democratización del uso, acceso, aplicación de las tecnologías de Información y comunicaciones (TIC) en el país; amparado en los considerandos del Decreto 1090-04 se crea la Oficina Presidencial de Tecnología de Información y Comunicaciones (OPTIC), bajo la presidencia del Poder Ejecutivo con independencia económica¹⁰⁸⁶, fruto de los compromisos asumidos por el Estado dominicano con otros Estados y organismos internacionales por medio a sus reuniones y cumbres internacionales como la declaración de Bávaro, la Cumbre Mundial para la Sociedad de la Información en Ginebra entre otras¹⁰⁸⁷.

2018. Disponible en: <http://www.optic.gob.do/index.php/sobre-nosotros/quienes-somos>. (Última consulta en línea 29 de mayo 2018)

¹⁰⁸⁵ *Oficina Presidencial de Tecnologías de la Información y Comunicación*. Disponible en: <http://optic.gob.do/index.php/sobre-nosotros/quienes-somos>. (Última consulta en línea 29 de mayo 2018).

¹⁰⁸⁶ Artículo 1. *Decreto 1090-04*

Se crea la Oficina Presidencial de Tecnología de Información y Comunicación (OPTIC), como dependencia directa del Poder Ejecutivo, con autonomía financiera, estructural y funcional, con el fin de lograr la incorporación de los estamentos que integran nuestra nación a la Sociedad de la Información, mediante la difusión y uso de las Tecnologías de Información y Comunicación (TICs).

Artículo 10. *Decreto 229-07*

Ratificar el Decreto 1090-04, del 3 de septiembre de 2004, que crea la Oficina Presidencia de las Tecnologías de la Información y Comunicación (OPTIC), como dependencia directa del Poder Ejecutivo, con autonomía financiera, estructural y funcional para la coordinación y el desarrollo de la estrategia del gobierno electrónico.

¹⁰⁸⁷ *Decreto 1090-04 presidencia de la República Dominicana*.

Disponible en: <http://www.optic.gob.do/phocadownload/Marco-Legal/DECRETO%201090-04.pdf>.

(Última consulta en línea 31 de mayo 2018).

La Oficina Presidencial de Tecnología de Información Y Comunicaciones (OPTIC) y su director ejecutivo¹⁰⁸⁸ asumen las funciones y atribuciones del instituto audiovisual de Informática (IADI) y la Comisión Nacional de Informática (CNI), en ese contexto y a raíz del Decreto número 229-07¹⁰⁸⁹ que establece las políticas gubernamentales sobre tecnologías de punta de la OPTIC sustentado en los avances del Internet, la revolución de las comunicaciones, el cambio de las TIC, el surgimiento de la disciplina de Gobierno electrónico¹⁰⁹⁰, el cambio de las relaciones entre personas, empresa y gobiernos, el aislamiento tecnológico de las dependencias del gobierno, los preparativos de creación del Gobierno electrónico, la ausencia de ley y su reglamento, son parte de los considerandos establecidos en el decreto; un decreto que al mismo tiempo contempla funciones, principios rectores y pautas a seguir por la Oficina Presidencial de Tecnologías de la Información y Comunicaciones (OPTIC)¹⁰⁹¹.

Así mismo, el Decreto 229-07 contiene las normativas de las TIC en la administración pública, a raíz de ello, el portal oficial del Estado dominicano contempla el marco regulatorio de los servicios en líneas ofrecidos como son la agenda digital dominicana, las políticas nacionales de las TIC, las políticas para

¹⁰⁸⁸ Cfr. *Decreto 469-12 que designa al Ing. Armando García como Director General de la Oficina Presidencial de Tecnología de la Información y Comunicación*. Disponible en: <https://www.optic.gob.do/index.php/marco-legal-m>. (Última consulta en línea 9 de julio 2018).

¹⁰⁸⁹ Cfr. *Decreto 229-07 ratifica el Decreto N.º 1090-04 que creó la Oficina Presidencial de las Tecnologías de la Información y Comunicaciones (OPTIC)*. Disponible en: <https://optic.gob.do/index.php/marco-legal-m?download=12:decreto-229-07-instructivo-de-aplicacion-gobierno-electronico>. (Última consulta en línea 9 de julio 2018).

¹⁰⁹⁰ (...) E-government is about transforming government to be more citizen-centered. Technology is a tool in this effort, su traducción en Castellano "El gobierno electrónico trata de transformar el gobierno para que esté más centrado en los ciudadanos. La tecnología es una herramienta en este esfuerzo". The Working Group, *Roadmap for E-Government in the developing World*, April 2002, p. 3. Disponible en: <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan005030.pdf>. (Última consulta en línea 29 de julio 2018).

¹⁰⁹¹ *Decreto N.º 297-07 ratifica el Decreto N.º 1090-04*. Disponible en: <https://www.google.com/search?q=Decreto+No.+229-07&og=Decreto+No.+229-07&aqs=chrome..69i57j69i59.2033j0j7&sourceid=chrome&ie=UTF-8>. (Última consulta en línea 31 de mayo 2018).

el buen gobierno¹⁰⁹², políticas para tecnologías emergentes¹⁰⁹³, marco legal TIC's, e- Gob. y normativas TIC¹⁰⁹⁴, siendo parte integral de las funciones de la OPTIC.

Es así, como por medio a las normativas (NORTIC) se plantean las directrices y recomendaciones a seguir por los organismos del Estado en los procesos de implementación, uso y manejo seguro de los medios sociales (NORTIC A1), tecnologías de la información y comunicación (TIC) (NORTIC A2), publicación de los datos producidos (NORTIC A3), interoperabilidad entre los organismos del gobierno dominicano (NORTIC A4), elaboración, prestación y gestión de sus servicios como la implementación de servicios transaccionales (NORTIC A5), desarrollo y gestión del software (NORTIC A6), la seguridad de las tecnologías de la información (NORTIC A7), gestión de las redes sociales (NORTIC E1)¹⁰⁹⁵, e implementación y gestión de la conectividad en el Estado dominicano (NORTIC B1).

Existe una estrecha relación entre la tecnología y la eficacia en la gestión de la administración pública, al grado de reconocer el uso de la tecnología en la

¹⁰⁹² Las políticas para el buen Gobierno la componen las siguientes partes: Gobierno Consolidado, Delito Electrónico y Ciber-Seguridad, Unificación de Proyectos TIC del Estado Dominicano, Centro de Datos del Estado, Gestión de Contingencias y Desastres, Software Público/ Libre, Identificación Inteligente, privacidad e Información Personal, Integración de Sistemas.

¹⁰⁹³ Las políticas establecidas para las tecnologías emergentes se encuentran compuesta por las siguientes partes de: Tecnologías Disruptivas y Bleeding, Datos Masivos (Big Data). Computación en la Nube (Cloud Computing), Derechos Electrónicos (E-Waste), El Internet de las Cosas (Internet of things) y otros conceptos como: e-salud / e-health, e-Educación, Open Data.

¹⁰⁹⁴ Normas sobre Tecnologías de Información y Comunicaciones. NORTIC, 2018. Disponible en: <http://optic.gob.do/nortic/index.php/documentos/category/normativas>. (Última consulta en línea 16 de julio 2018).

¹⁰⁹⁵ “Las NORTIC son normas de tecnologías de la información y comunicación, creadas por el Departamento de Estandarización, Normativa y Auditoría Técnica (ENAT), en el 2013, las cuales tienen como objetivo principal el establecimiento de estándares generales, relacionados con aspectos tecnológicos”. *Normas sobre tecnologías de la información y comunicación (NORTIC) 2018*. Disponible en: <http://optic.gob.do/nortic/index.php/nortic>. (Última consulta en línea 30 de mayo 2018).

administración pública, redundando en la eficacia de la misma¹⁰⁹⁶, razones por las que los Estados acercan las tecnologías de la información y comunicaciones a la administración pública, situación que no escapa la República dominicana.

7. Administración electrónica, transparencia, buen gobierno, órgano de control, protección de datos

Existen diversas concepciones relacionadas con los términos empleados a la hora de designar la conexión, interacción, uso y aplicación de las tecnologías de información y comunicaciones (TIC) a las administraciones públicas o el gobierno, a raíz de ello, se acuñan en los Estados los términos de Administración electrónica, e-Administración, Gobierno electrónico, e-Gobierno, e-Government, formando parte de sus normas internas¹⁰⁹⁷; en la doctrina anglosajona se utiliza el e-Governance para denotar el uso de las tecnologías de la información y comunicaciones con el gobierno a nivel general y en toda su expresión.

Es así, como a raíz de la presentación de la Comunicación de la Comisión de las comunidades europeas el 26 de septiembre del 2003 al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones, se presenta el papel de la administración electrónica en el futuro de Europa¹⁰⁹⁸, donde se establece la administración electrónica (e-Government)

¹⁰⁹⁶ PÉREZ LUÑO, A. E., "Informática y libertad. Comentario al artículo 18.4 de la Constitución española...op. cit., p. 52. También puede verse en. PÉREZ LUÑO, A. E., *Internet y los Derechos Humanos*, Derecho y...op. cit., p. 117.

¹⁰⁹⁷ (...) Habitualmente se utilizan como conceptos equivalentes las expresiones Administración electrónica (e-Government) y Gobierno electrónico....la primera se refiere al estudio del uso de las tecnologías de la información y de la comunicación (TIC)..por las Administraciones públicas cuando desarrollan sus actividades burocráticas...el e-Gobierno...implica la utilización de las TIC en las tareas del gobierno en toda su extensión... puede verse en GALINDO, F. y J. ROVER (EDS) A., *Derecho, gobernanza y tecnologías de la información en la sociedad del conocimiento*, 1ra. ed. prensa universitaria de Zaragoza, AECID, Zaragoza, 2009, pp. 193-197.

¹⁰⁹⁸ COM (2003), Bruselas, 26/9/2003. Disponible en:

como una combinación de cambios organizativos y nuevas actitudes enfocadas a hacer mejor los servicios públicos, los procesos democráticos y las políticas democráticas, con el apoyo de las tecnologías de la información y comunicaciones (TIC); la comunicación, ha sido presentada luego de transcurrido 3 años de los acuerdos de Lisboa tendentes a impulsar las TIC en la Unión Europea reconocidos como <<Estrategia de Lisboa>>¹⁰⁹⁹.

Fundamentado en acuerdos internacionales, política de transparencia y apoyo gubernamental¹¹⁰⁰, el Gobierno dominicano asume el compromiso de crear instituciones independientes con autonomía económica y funcional, soportado en normas legislativas incluidas las leyes y reglamentos, sin dejar de lado las disposiciones presidenciales que emanan de los decretos.

En ese sentido, amparado en el desarrollo tecnológico y las tecnologías existentes, el Gobierno dominicano abre las puertas al Gobierno Abierto y la e-transparencia¹¹⁰¹, creando el gobierno electrónico, portal que permite el acceso de la ciudadanía a los distintos estamentos del Estado bajo la garantía de la Ley de Acceso a la Información Pública¹¹⁰² y sus Oficinas de Acceso a la

<https://eur-lex.europa.eu/legalcontent/ES/TXT/PDF/?uri=CELEX:52003DC0567&from=ES>.
(Última consulta en línea 26 de junio 2018).

¹⁰⁹⁹ MARCOS DEL RINCÓN, J., “La Administración electrónica en las leyes 39 y 40/2015 de 1 de octubre. Una visión en conjunto”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 45, Septiembre-Diciembre 2017, p. 188.

¹¹⁰⁰ Decretos presidenciales: 783-01, 149-98, 1090-04, 101-05, 229-07, 297-07, 469-12, 486-12, 490-12, 486-12, 246-16, 143-17, 234-17.

¹¹⁰¹ *Portal de Transparencia de la Oficina Presidencial de Tecnologías de la Información y Comunicación, (OPTIC.)* Disponible en: <http://optic.gob.do/transparencia/>. (Última consulta en línea 16 de julio 2018).

¹¹⁰² Artículo 5 Ley núm. 200-04. “Se dispone la información y la incorporación al sistema de comunicación por Internet o a cualquier otro sistema similar que en el futuro se establezca, de todos los organismos públicos centralizados y descentralizados del Estado. Incluyendo el Distrito Nacional y los municipios, con la finalidad de garantizar a través de éste un acceso directo del público a la información del Estado.

Todos los poderes y organismos del Estado deberán instrumentar la publicación de sus respectivas “páginas Web” a los siguientes fines:

- a) Difusión de información: Estructura, integrantes, normativas de funcionamiento, proyectos, informes de gestión, base de datos;
- b) Centro de intercambio y atención al cliente o usuario: Consultas, quejas y sugerencias;
- c) Trámites o transacciones bilaterales.

Información (OAI) ubicadas en las instituciones gubernamentales y la Web. Amparado en estructuras tecnológicas robustas, fortaleciendo las instituciones gubernamentales.

La Dirección de Ética e Integridad Gubernamental (DIGEIG) responsable de velar por la integridad y la e-transparencia Gubernamental, así como la Oficina Presidencial de Tecnologías de la información y Comunicación (OPTIC) encargada del aparato tecnológico del gobierno, son instituciones adscritas a la presidencia, bajo la sombrilla del Ministerio de la Presidencia.

En cambio, mediante el artículo 29 de la Ley núm.172-13, se contempla la asunción de la Superintendencia de Bancos como órgano de control, cuyo presupuesto es aprobado por la junta monetaria, formando parte de la administración monetaria y financiera, dejando entrever la inexistencia del establecimiento de un órgano de control que goce de independencia económica y funcional, no estando adscrito al poder ejecutivo.

Por su parte y basado en los hechos precedentes, el Gobierno dominicano hace ingentes esfuerzos en transparentar las ejecutorias de la administración pública, una transparencia conectada con la Ley de Acceso a la Información Pública y sus oficinas como puerta de entrada de requerimientos, ubicadas en instituciones gubernamentales esparcidas a lo largo y ancho del territorio nacional, sin dejar de lado el acceso online vía web, puntos neurálgicos de acceso al ciudadano, incluyendo el ciudadano común o ciudadano de a pie como también se le reconoce, que solo tiene interés en conocer las ejecutorias gubernamentales a diferencia del investigador, incluido el periodístico, medios de comunicación colectivos o miembro de una organización no gubernamental con intenciones de mostrar a una gran audiencia o colectivo, las ejecutorias gubernamentales invocando la transparencia estatal.

A raíz de ello, y en función de las instituciones creadas y adscritas al Gobierno dominicano en temas de transparencia, acceso a la información

La información a que hace referencia el párrafo anterior, será de libre acceso al público sin necesidad de petición previa.

pública, tecnología de Información, como la Dirección de Ética y Transparencias (DIGEIG) y la Oficina Presidencial de Tecnología y Comunicaciones (OPTIC) bajo dependencia directa de la Presidencia¹¹⁰³, vemos viable la vinculación directa del órgano de control de la Ley núm.172-13 con la presidencia, estableciendo un órgano de control independiente desde el punto de vista económico, y funcional, a raíz de la conexión y vinculación de la protección de datos personales con la protección de las personas físicas.

Con la iniciativa, se reúne bajo una misma estructura económica, funcional, organizativa y normativa, los temas de transparencia, acceso a la información pública y protección de datos personales; tales son los casos de los proyectos de la Comunidad Vasca, la Andaluza o la puesta en funcionamiento de la normativa mexicana, contemplando bajo un mismo órgano de control la *Ley de Transparencia, Acceso a la Información Pública y la Protección de Datos Personales*.

Por su parte, la protección de datos es el límite de la transparencia, no la excusa para evitar la entrega de posibles solicitudes de información del gobierno y convertirse en obstáculo de la transparencia en la administración gubernamental, con ello, y ante esa situación, como hemos comentado, no podemos mirar en la protección de datos, la excusa o retranca para evitar obtener las informaciones gubernamentales necesarias que nos conducirán a la transparencia, siendo la protección de datos un límite a la transparencia, y no, una cuartada¹¹⁰⁴ para la entrega de la información gubernamental en detrimento de la transparencia; son dos instituciones no contrapuestas, sino complementarias, de ahí la necesidad de agrupar las dos sensibilidades bajo

¹¹⁰³ Portal de transparencia, *estructura orgánica ministerio de la presidencia*, 2018. Disponible en: <https://minpre.gob.do/transparencia/estructura-organica-ministerio-de-la-presidencia/>. (Última consulta en línea 16 de julio 2018).

¹¹⁰⁴ PUENTE ESCOBAR, A., *Protección de datos y transparencia: compañeros de viajes*, cursos de Verano UPV/EHU, San Sebastián, 2018.

un mismo órgano de control¹¹⁰⁵, teniendo a su cargo la ponderación de los dos derechos al momento de existir una colisión de derecho.

Por tanto, un buen gobierno amparado en la democracia¹¹⁰⁶ debe transparentar sus ejecuciones gubernamentales mediante el acceso de sus nacionales a las informaciones públicas, evitando que la información tipificada como personal por el Gobierno, se convierta en obstáculo o barrera para su entrega, materializando el equilibrio entre buen gobierno, transparencia, acceso a la información pública, protección de datos personales; en ese sentido y a raíz de la capacidad de almacenamiento de información ubicada en dispositivos electrónicos tales como computación en las nubes¹¹⁰⁷, discos, USB, tarjetas

¹¹⁰⁵ Es factible colocar la transparencia y la protección de datos, bajo un mismo órgano de control” respuesta externada por la directora de la Agencia Vasca de Protección de Datos (A.V.P.D) Margarita Uría Etxebaría, ante la idoneidad de mantener bajo un mismo mecanismo de control los dos derechos, URÍA ETXEBARÍA, M., *protección de datos y transparencia: compañeros de viajes*, cursos de Verano UPV/EHU, San Sebastián, 2018. de la misma forma lo expresa el director del Consejo de Transparencia y Protección de Datos de Andalucía Manuel Medina Guerrero luego de su exponencia de la Mesa redonda: Autoridades de control e implementación de la normativa en materia de protección de datos: MEDINA GUERRERO, M., *La posición de las autoridades de control en el nuevo marco regulador de la protección de datos*, Congreso Internacional sobre el Impacto del Reglamento Europeo de Protección de Datos: Análisis Nacional y Comparado, Universitat Jaume I, Castellón de la Plana, 18 de Mayo 2018.

¹¹⁰⁶ Cfr. “ En la democracia es donde únicamente se advierte la íntima relación entre protección de datos personales, derecho a la información y confidencialidad.....el objeto de la sociedad democrática no consiste solamente en que sus regulaciones de protección de datos personales aseguren la confidencialidad....la libertad de información es un complemento indispensable de la protección de datos personales”...” la relación entre democracia, libertad de información, derecho de acceso a los archivos, protección de datos personales y confidencialidad es tan íntima que la falta de uno solo de los componentes configura un sistema autoritario” TRAVIESO, J. A. (Director), *Los Derechos Humanos y la Informática visto en Régimen Jurídico de los Datos Personales*, tomo I, 1ª Ed. ediciones ABELEDOPERROT S. A., Buenos Aires, 2014, p. 9.

¹¹⁰⁷ Cfr. “...una de las tendencias actuales más importantes en el mundo de la tecnología está relacionada con el avance de la computación en la nube (en inglés, cloud computing), a través del cual mucha de las funcionalidades, aplicaciones, y herramientas tecnológicas de una empresa – entre ellas, las bases de datos—se encuentran en el ciberespacio.....La noción de *cloud computing* importa la migración o externalización de los recursos y actividades informáticas de una entidad, entre ellas, hardware, software, etc., aun proveedor que brinda los servicios en el ciberespacio a través de servidores diseminados sin una ubicación geográfica determinada. De esta forma, hardware y software ya no son procurados y operados por los mismos usuarios, sino que son obtenidos como servicios brindados por terceros alojados en Internet. Por ende, las herramientas informáticas pasan a estar fuera del alcance del usuario, siendo que son accedidas en forma remota y cuando son requeridas”. PERUZZOTTI, M., *El impacto de la ley de protección de los datos personales en el sector público*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014, p. 865.

electrónicas u otros medios técnicos sometidos a grandes velocidades de búsquedas de información de los datos almacenados. Se hace necesario la construcción y empleo de sistemas¹¹⁰⁸, técnicas de encriptación¹¹⁰⁹ y mecanismos capaces de asegurar, proteger la intimidad y la privacidad de las personas, fruto del acceso de terceros sin consentimiento a los datos personales almacenados en los Estados y más allá de sus fronteras. Una situación que nos permite ampliar los mecanismos de protección de las personas físicas fuera de las fronteras de los Estados, siendo necesaria la creación de normativas internacionales capaces de proteger los datos de las personas fuera de los límites de los Estados.

A su vez, el desarrollo del Internet y el aumento de las TIC revisten una gran conexión con la protección de datos personales durante el proceso de ejecución de transferencias internacionales de datos entre los Estados, siendo considerado motivos suficientes y necesarios al momento de concebir los proyectos normativos en materia de protección de datos en el Estado dominicano previo a la promulgación de la Ley núm.172-13, razones por las que nos vemos impelido en traer a colación los proyectos de ley depositados en la Cámara de Diputados y el Senado de la República Dominicana, en especial, lo referente a las disposiciones relacionadas con la transferencia internacional de datos.

¹¹⁰⁸ Cfr. “Internacionalmente se ha identificado al menos cinco modelos de sistema de regulación para proteger los datos personales y otros derechos conexos, a saber: Disposiciones constitucionales; leyes generales; leyes sectoriales; la contratación y la autorregulación. Cada país define el camino a tomar para abordar este tema...”. REMOLINA ANGARITA, N., *realidades y reflexiones sobre el tratamiento de datos personales en Latinoamérica*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ediciones ABELEDOPERROT S. A., Buenos Aires, 2014, p. 1072.

¹¹⁰⁹ Cfr. “Privacy-Enhancing Technologies (PETs) Las PETs incluyen técnicas como la encriptación utilizada no sólo para almacenar información de forma segura, sino también para asegurar su integridad, transportarla, ya sea mediante soportes físicos como a través de una red, o para generar accesos seguros a datos personales, las PET pueden ser clasificadas en: a) Herramientas de gestión de privacidad. b) Metadatos de privacidad. c) Herramientas de protección de privacidad. d) herramientas de anonimización, de pago anónimo, de seguridad. SEGURA, P., *Internet de las cosas*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo I, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014, pp. 534-535.

8. Transferencia internacional en los proyectos de Ley de Protección de Datos Personales

El primero de los proyectos¹¹¹⁰ contempla en el artículo 12 el tema de la transferencia internacional, en ella, se manifiesta la ejecución de transferencias a los Estados que contemplen niveles de protección adecuados, exceptuando temas de colaboración judicial, intercambios de carácter médico, transferencias bancarias sustentadas en tratados internacionales y aquellas transferencias fundamentadas en cooperación internacional con organismos de inteligencia en post de la lucha contra el terrorismo, crimen organizado, trata de personas y narcotráfico¹¹¹¹.

El segundo proyecto¹¹¹², bajo el título de *Movimiento Internacional de Datos*¹¹¹³ ubicado en la sección VI del proyecto, compuesto por 5 artículos, conecta el movimiento internacional de datos con la Agencia Dominicana de Protección de Datos, con la capacidad de suspender temporalmente las transferencias hacia un importador que pudiera colocar en riesgo aquellas transferencias de datos con posibilidad de generar riesgo a los afectados mediante la vulneración de las normas de protección de datos establecidas en el Derecho interno; al mismo tiempo, presenta un listado de excepciones a la norma, como aquellas transferencias necesarias para solicitar auxilio judicial internacional, tratamiento, prevención, prestación de asistencia sanitaria, consentimiento del afectado, ejecución de contrato entre afectado y el responsable del archivo, necesidad de ejecución de un contrato, salvaguardar interés público, el reconocimiento de un interés público, ejercicio o defensa de un derecho de proceso judicial, y las transferencias fundamentadas en

¹¹¹⁰ Autoría del diputado Demóstenes W. Martínez Hernández.

¹¹¹¹ Cfr. artículo 12, numeral 1 y 2 del proyecto de ley.

¹¹¹² Autoría del senador Félix Bautista.

¹¹¹³ El tema del movimiento Internacional de datos reflejado en el proyecto proviene de la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal, al igual que los temas de la Agencia de Protección de datos.

protección del terrorismo, crimen organizado, trata de personas y narcotráfico sustentadas en acuerdos internacionales¹¹¹⁴.

Toda transferencia de datos, debe ser ejecutada manteniendo niveles equiparables de protección de datos o en su defecto, contar con la aprobación de la Agencia Dominicana de Protección de Datos, manteniendo garantías adecuadas, el proceso no exime la inscripción en el registro General de Protección de Datos.

9. Transferencia internacional en la Ley de Protección de Datos Personales núm. 172-13

En la Ley núm. 172-13, se emplean indistintamente los términos transferencia o movimiento internacional de datos para referirse al desplazamiento de datos hacia un Estado u organización internacional, dejando relucir el empleo de diferentes términos para referirse al mismo concepto o acepción; Es así como la sección V de la ley contempla el movimiento internacional de datos, seguida del concepto de transferencia internacional de datos previamente definido en la legislación.

La normativa contempla las excepciones a tomar en cuenta en el proceso de las transferencias internacionales que requieran aprobación del titular de los datos tales como la autorización del titular o la ley, carácter médico, transferencias bancarias, tratados internacionales, cooperación internacional (crimen organizado, terrorismo, narcotráfico, etc.), ejecución de un contrato, protección del interés público, auxilio judicial internacional, solicitud internacional.

La Ley núm.172-13, incorpora en el artículo 80 de su legislación el tema de las transferencias internacionales; la iniciativa legislativa proviene del proyecto de ley del diputado Demóstenes Martínez; la actual pieza legislativa de

¹¹¹⁴ Cfr. artículos 81 y 82 del proyecto

protección de datos Ley núm.172-13, no contempla entre sus disposiciones las atribuciones del órgano de control tales como funciones, responsabilidades y los permisos necesarios para el establecimiento, solicitud y aprobación de las transferencias internacionales contempladas en las legislaciones comentadas; por su parte y como ya hemos comentado, en la actual normativa de protección de datos se designa a la Superintendencia de Bancos como órgano encargado de velar por la “*inspección y vigilancia de los archivos, registros o bancos de datos, públicos o privados destinados a proveer informes crediticios*” despojándola de la facultad de velar por el proceso de las transferencias internacionales, una situación muy distinta a las atribuciones contempladas en el proyecto del senador Félix Bautista fundamentado en la Ley 15/1999¹¹¹⁵ (LOPD) ya comentada.

Tal como lo hemos acordado al principio de la sección, pasamos a ver las informaciones vertidas por el Tribunal Constitucional, en torno al órgano de control.

10. Opinión del Tribunal Constitucional dominicano respecto al órgano de control de la Ley núm.172-13

En el capítulo III analizamos y traemos a colación la acción directa de inconstitucionalidad interpuesta contra los artículos de la Ley núm. 172-13, por los recurrentes Namphi A. Rodríguez, Domingo Porfirio Rojas Nina, José Gregorio Cabrera, Fundación Prensa y Derecho, Consejo Dominicano de Derechos Humanos (CODEH) y la Alianza Ciudadana para Los Derechos Fundamentales, en esta ocasión, nos dirigimos a la solicitud de modificación del artículo 29 planteada en la acción, la cual estima la creación de un órgano rector independiente, vinculado a la protección de los derechos fundamentales tutelados en la misma. El Tribunal declara mediante sentencia la

¹¹¹⁵ Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750>. (Última consulta en línea 6 de marzo 2018).

constitucionalidad del artículo 29 de la Ley núm.172-13 del 15 de diciembre de 2013.sobre *protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados.*

Con el dictamen, se mantiene vivo el artículo 29 de la Ley núm.172-13 referente al órgano de control, asumiendo la Superintendencia de Bancos las atribuciones del órgano de control, manteniendo el registro de las transacciones financieras vinculadas con la aplicación del secreto bancario, cuya finalidad es la protección de la intimidad conectada con la dignidad de las personas como derecho fundamental y la protección de aquellos datos vinculados a la actividad financiera.

La evacuación de la sentencia emitida por el Tribunal Constitucional en relación al órgano de control, tiene como fundamento el artículo 1 de la Ley núm.172-13 donde refrenda el objeto de la ley cuando expresa “...*tratamiento de datos destinados a dar informes...*” no así contempla la información del párrafo del referido artículo amparado en el artículo 44 de la Constitución de la República Dominicana referido en “...*garantizar que no se lesione el derecho al honor y la intimidad de las personas, y a facilitar el acceso a la información...*” situación por la que puntualizamos que el artículo 44 relacionado con la intimidad y el honor, no solo se refiere a los derechos asignados a la protección de datos destinados a dar informes¹¹¹⁶, tal como se estipula en las consideraciones emitidas por el Tribunal respecto a la acción directa de inconstitucionalidad, sino, en aquellos casos que afecten a las personas, independientemente sean utilizados para dar informes crediticios o no, aunque como se evidencia en la legislación actual, esta absorbe, derogando en toda su parte la Ley núm. 288 destinada a regular las

¹¹¹⁶ “...De hecho, el objeto principal de la referida Ley núm. 172-13 lo constituye la protección de aquellos datos vinculados a la actividad financiera.”. *Tribunal Constitucional de la República Dominicana, Sentencia* núm. TC/0484/16, p. 51. Disponible en: <https://www.tribunalconstitucional.gob.do/sites/default/files//documentos/TC-0484-16.pdf>. (Última consulta en línea 14 de octubre 2016).

Sociedades de Información Crediticia¹¹¹⁷, una situación que pone a flote el objeto de la normativa.

La Ley núm.172-13, es una normativa creada y empleada para los datos de carácter personal ubicados en archivos o bancos de datos, destinados, utilizados y susceptibles al tratamiento¹¹¹⁸, aplicable para todo el territorio nacional; a raíz de ello, consideramos estar delante de una normativa de alcance general para todos los datos, no solo para los destinados a dar informes, razones necesarias para abocarnos en crear un órgano de control orientado en la protección y tutela de los datos personales, una situación contraria a lo expresado en la Sentencia núm.TC/0484/16 de acción directa de inconstitucionalidad interpuesta.

Al mismo tiempo, estamos en presencia de la acción de *habeas data* contemplada en la Ley núm.172-13, una acción compelida desde la óptica del constitucional y reflejado en la ley para los datos cuya procedencia se originen de una relación comercial, laboral o contractual, independientemente se establezca con un ente público o privado dejando entrever que la acción de *habeas data* contemplada en la ley, no solo aplica a los datos destinados a dar informes, en ese orden, la Sentencia núm. TC/0157/13¹¹¹⁹ se apuntala en la Sentencia núm. TC/0024/13¹¹²⁰ refrescando el concepto del *habeas data* instituida en el artículo 70 de la Constitución, expresando que:

¹¹¹⁷ Ley núm. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados, art. G.O. N.º 10737 del 15 de diciembre de 2013. Disponible en: <http://www.gob.do/index.php/recursos/2014-12-16-21-02-56/category/3-constitucion-y-leyes-rd?download=58:ley-no-172-13&start=20>. (Última consulta en línea 22 de marzo 2018).

¹¹¹⁸ Artículo 2 Ley núm. 172-13. Disponible en: <http://www.gob.do/index.php/recursos/2014-12-16-21-02-56/category/3-constitucion-y-leyes-rd?download=58:ley-no-172-13&start=20>. (Última consulta en línea 22 de marzo 2018).

¹¹¹⁹ Sentencia núm. TC/0157/13, p. 14, Disponible en: <https://tribunalsitestorage.blob.core.windows.net/media/7581/sentencia-tc-0157-13-c.pdf>. (Última consulta en línea 20 de diciembre 2018).

¹¹²⁰ Comentada en el capítulo III, p.48-49.

“10.2.4. Este Tribunal ha establecido que el *habeas data* es una garantía constitucional a disposición de todo individuo, que le permite acceder a cualquier banco de información, registro de datos y referencias sobre sí mismo, sin necesidad de explicar las razones de su interés; y le permite, además, solicitar la corrección de las informaciones que contengan alguna imprecisión o error y que puedan causarle algún perjuicio. (Sentencia núm. TC/0024/13)”¹¹²¹.

Con la posición, retornamos al concepto inicial acerca del ámbito de aplicación, fijando una posición para el *habeas data*, el cual no solo aplica para la protección de los datos prestos en dar informes, sino, para aquellos datos personales establecidos en otros medios, aunque no sean los datos dispuestos en los burós de crédito.

La normativa núm. 172-13 contempla el procedimiento para ejercer los derechos dispuestos en el *habeas data* tales como los de modificación, rectificación y cancelación de la información del titular, al mismo tiempo, se establecen las condiciones generales para ejercer los derechos de acceso, rectificación, cancelación y oposición instaurado en la propia ley, considerados como una *acción de protección de los datos personales o de habeas data*, derechos independientes en su ejecución o reclamación.

Una situación que nos permite volver a conectar la Ley núm.172-13 con el órgano de control, producto de la urgente necesidad de tener una autoridad de control destinada y orientada desde sus principios y funciones a la tutela y protección de aquellos datos dedicados no solo a la emisión de informe como se estipula en la sentencia, generando con ello una total protección.

Desde las opiniones del procurador general de la República, el Senado de la República y la Cámara de Diputados, la actual normativa núm.172-13 cumple con lo estipulado en ella incluyendo el órgano de control, dejando en manos del Tribunal Constitucional posibles modificaciones, cambios o transformaciones

¹¹²¹ Sentencia núm. TC/0157/13, p. 14, Disponible en: <https://tribunalsitestorage.blob.core.windows.net/media/7581/sentencia-tc-0157-13-c.pdf>. (Última consulta en línea 20 de diciembre 2018).

realizadas en los articulados dispuestos en ella. En la misma tesitura, el procurador entiende que la capacidad de la Superintendencia para supervisar bancos de datos no financieros es un *mero enjuiciamiento valorativo*.

CONCLUSIONES

En las próximas líneas, planteamos el resultado de los principales hallazgos del trabajo de investigación, una labor orientada en la protección de datos personales y el *habeas data* en la República Dominicana, su vinculación con el órgano de control y las transferencias internacionales de datos, un estudio en el contexto europeo y latinoamericano, acercando las normas europeas al escenario latinoamericano con especial énfasis en la República Dominicana.

La conclusión de la línea de investigación se orienta a los temas desarrollados a lo largo y ancho del trabajo, representado por cinco grandes temas: a) protección de datos; b) hábeas data; c) órgano de control; y d) transferencias internacionales de datos; e) transparencia. Finalizamos con la presentación de la estrategia de implementación del Estándar o Ley Iberoamericana de Protección de Datos, ancladas a las recomendaciones generales del trabajo.

El nacimiento y evolución de la protección de datos no se enmarca en procesos aislados sino en procesos concatenados a lo largo y ancho del Atlántico. Por ello, para ofrecer un aporte de calidad a Latinoamérica, y más concretamente a República Dominicana en esta materia, es necesario ahondar en las raíces del origen conceptual y evolución del derecho a la protección de datos. *privacy* norteamericana, recepción en Europa de la misma, derecho a la autodeterminación informativa. En este sentido sobre tales conceptos cabe concluir:

- Cuando hablamos del origen de la protección de datos debemos remontarnos a finales del siglo XIX y, en concreto a la publicación del artículo de los juristas norteamericanos Warren y Brandeis (*The Right to Privacy*) o el derecho a estar solo. De este modo, en Estados Unidos, -por medio de la IV Enmienda- el concepto de *privacy* se extiende más allá de los derechos de la personalidad y este antecedente marca un hito histórico

generando el nacimiento del derecho a la protección de datos de carácter personal.

- Por su parte, en Europa el derecho a la protección de datos tiene sus orígenes en los derechos de la personalidad /derecho a la intimidad y su recepción de la *privacy* produjo lo que hemos denominado un “encaje distorsionado de la *privacy*”. En el contexto europeo no existe un derecho de amplitud igual a éste lo cual generó: a) una nueva categoría para la protección de datos y b) la asimilación de intimidad y privacidad, cuando, en realidad, la *privacy* no corresponde en Estados Unidos a un concepto unitario.
- La paulatina inclusión de la privacidad con su correlativo encasillamiento *privacy*-intimidad en las legislaciones europeas ha hecho que se desvirtúe el sentido originario que llevaron al nacimiento y construcción de este derecho cuya dinámica por su entorno permite su *aggiornamento*, realidad bien diferente a lo que suele ocurrir en los ordenamientos jurídicos europeos y -como posteriormente concluiremos- latinoamericanos. Esa interiorización de la *privacy* como uno más de los derechos de la personalidad -y vinculado a la intimidad- dejó el terreno abonado para que el Tribunal Constitucional alemán -en su sentencia del Censo de 1983- construyera vía judicial -por primera vez- el derecho a la autodeterminación informativa en base a los preceptos constitucionales del libre desarrollo de la personalidad y la dignidad.
- La construcción alemana del derecho a la autodeterminación informativa penetra en Europa -y también posteriormente se acoge en Latinoamérica- a nivel doctrinal, legislativo y jurisprudencial constituyéndose en el antecedente de impacto en los cimientos y posterior desarrollo del derecho a la protección de datos.
- Por otra parte, el contexto español es otra fuente de aportaciones para el objeto de nuestro estudio. La democracia ha formado parte del origen y evolución de los derechos fundamentales ya que sin ella no hay espacio

para su reconocimiento, tal es el caso también de España. Tras la transición hacia la democracia en 1976 se inicia el reconocimiento de sus derechos fundamentales, logrando una tutela más efectiva de los mismos. Este -como no podía ser de otra manera- también sucede con el derecho que nos ocupa. Por un lado, es de resaltar el definitivo aporte de la doctrina española en la que: a) un sector doctrinal manejó el concepto de autodeterminación informativa que después concluyó en derecho a la protección de datos: b) otro sector, situaba el tema en las coordenadas de los derechos de tercera generación a la que pertenecen una nueva generación de derechos humanos y donde se distinguen tres conceptos diferentes: libertad informática (facultad de conocimiento, acceso y control de las personas sobre la información que le concierne), autodeterminación informativa (facultad sobre lo que se ha revelado y el uso de los datos) y *habeas data* (facultad de las personas a conocer y acceder a las informaciones en los bancos de datos. De otro lado, el Tribunal Constitucional español -y, a su vez, acreedor de dichas corrientes doctrinales- fue paulatinamente perfeccionando el alcance de dicho derecho. Sin embargo, no va ser hasta la STC núm. 292/2000, en donde se reconozca de manera expresa la existencia de un derecho autónomo a la protección de datos que encuentra su sede constitucional en el artículo 18.4 de la Constitución española VACILES. Por tanto, como veremos, las distintas tesis doctrinales y la jurisprudencia españolas han tenido un peso decisivo en la construcción de este derecho en Latinoamérica, y más concretamente, en República Dominicana (posteriores conclusiones).

Igualmente nos ha situado en sus justas coordenadas para este trabajo de investigación destacar cuales han sido y son las aportaciones tanto del ámbito internacional (ONU, OCDE, Consejo de Europa, OEA), como de la Unión Europea y del ámbito español en la construcción *multilevel* del derecho a la protección de datos.

- La Construcción de la protección de la honra y la reputación a lo interno de ONU, no solo se materializa con la Declaración Universal de los

Derechos Humanos del 1948 o el pacto Internacional de los Derechos Civiles y Políticos de 1966, sino que se tejen continuos esfuerzos como las Directrices de protección, el reconocimiento del derecho a la privacidad en la era digital que procuran la instauración de autoridades de supervisión independientes en los Estados, mantener el flujo de información de datos entre los Estados evitando trabas innecesaria, y el reconocimiento de las bondades y peligros que asecha al Internet, tanto para las empresas, gobiernos y personas,

- La OCDE se convierte en una de las instituciones tendentes a la búsqueda de un crecimiento económico de los Estados, disminuyendo posibles obstáculos a las transferencias internacionales de datos e incentivar prácticas sanas de comercio e intercambio de información. Situación que la sumerge en la creación de iniciativas y recomendaciones relacionadas con el cumplimiento de ese objetivo. Tal es el caso de la declaración de flujos transfronterizos del 1985, así como la Recomendación del 2013.
- El Consejo de Europa vía el Convenio Europeo de Derechos Humanos del 1950 reconoce en su artículo 8 el derecho a la vida privada y familiar, unos derechos desarrollados años después con la instauración de los principios básicos de protección de datos personales a ser incorporados en las legislaciones nacionales. Unos principios ampliados y reconocidos en un texto decisivo y unánime en el ámbito legal de la protección de datos personales, nos referimos al Convenio 108 siendo en su momento el único que desarrolla el artículo 18.4 de la Constitución española. En tal sentido, el aumento de los flujos transfronterizos entre los Estados y el deseo manifiesto de evitar obstáculos a los mismos son algunas de las razones que dan pauta a la creación del Protocolo Adicional del Convenio 108 de 2001 relativo a las transferencias internacionales, asignando relevancia a las autoridades de control dotadas de total independencia funcional y económica; en ese sentido y con el interés del Convenio en actualizar su normativa a los cambios y transformaciones

generados en su entorno y relevancia global, surge en el 2018, el Protocolo de modificación del Convenio 108 de 1981 una iniciativa dedicada y orientada a esclarecer los flujos transfronterizos de datos, aumentando la cooperación de las autoridades de protección de datos, con una autoridad de supervisión que goza de poderes de investigación, intervención, independencia, imparcialidad, competencia y la capacidad de imponer sanciones administrativas etc.

- La Organización de los Estados Americanos (OEA) mantiene una preocupación constante en trabajar en post de la construcción de una normativa o Estándar regional en materia de protección de datos personales en aras de homologar la protección en los Estados Latinoamericanos, impulsado y sustentado en diversas propuestas de armonización encaminadas en lograr ese objetivo común, tales son los casos de:
 - (2010) Propuesta de Declaración de Principios de Privacidad y Protección de Datos de las Américas (OEA-RIPD).
 - (2011) Comentarios Preliminares sobre una declaración de Principios para la Protección de la Privacidad y de los Datos Personales en las Américas (OEA).
 - (2011) Proyecto de Principios y Recomendaciones Preliminares sobre la Protección de Datos. (OEA).
 - (2012) Principio de Privacidad y Protección de Datos Personales en las Américas. (OEA).
 - (2012) Estudio Comparativo de Protección de Datos en Las Américas. (OEA)
 - (2014) Proyecto de Ley Modelo sobre Protección de Datos Personales (cuatro principios)
 - (2015) Propuesta ampliada de los 12 Principios. (OEA)
 - (2017) Nuevos Estándares de Protección de Datos Latinoamericana bajo la dirección del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI) de México.

- Por su lado, la Convención Americana de Derechos Humanos contempla la protección de la correspondencia, evitando cualquier tipo de injerencia que pueda colocar en peligro la información contenida en la misma, una protección que va más allá de la tutela de la correspondencia, albergando la protección de otros derechos, como el derecho a la comunicación telefónica amparado en las Sentencias del Tribunal Interamericano de los Derechos Humanos, caso Tristán Donoso Vs. Panamá; Una situación, que nos permite pensar en un acercamiento con las normas legislativas conectadas con el desarrollo tecnológico; con la decisión, se observa y persigue un acercamiento a las normativas internacionales, en especial, las conectadas con el desarrollo tecnológico. Vía el acercamiento, se vislumbra la protección de otros derechos conectados con la tecnología, como es el caso de la protección de la inviolabilidad de la imagen, video vigilancia, datos almacenados en las nubes, medios electrónicos desprovistos del consentimiento de su titular, consumando la protección del honor y la dignidad de las personas.
- La Construcción del derecho a la protección de datos en el ámbito de la Unión Europea, descansa en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, materializando la protección de datos a lo interno de la Unión Europea, amparada en una autoridad que goce de total independencia. La Carta es reconocida y amparada por el Tratado de Funcionamiento de la Unión Europea, convirtiéndose los Trados en los límites de la Carta a lo interno de la Unión. Con la aprobación de la Directiva 95/46/CE se pretende armonizar las legislaciones nacionales en materia de protección de datos, posibilitando la libre circulación de los datos personales entre los Estados Miembros de la Unión Europea, perteneciente a la estructura de Pilares de la Comunidad Europea, desapareciendo con el Tratado de Lisboa, en tanto que con el Reglamento (UE) 2016/679 se persigue la uniformidad de las regulaciones en materia de derecho fundamental a la protección de

datos en un entorno cada vez más global y con ello, alcanzar la seguridad jurídica y garantizar la coherencia en materia de protección de datos de las personas físicas en territorio de la Unión Europea.

- Los derechos fundamentales en España suceden a partir del año 1976 período de transición entre el fin de la dictadura y el nacimiento de la democracia, generándose un ordenamiento jurídico, ya en el año 1977 y siguiente se empieza a distinguir una caterva de derechos entre los que se destacan los derechos de la personalidad, el derecho a la intimidad personal, familiar y social, así como el derecho a la información, unos derechos contemplados en el 18.4 de la Constitución, siendo estos desarrollados en importantes legislaciones como la Ley Orgánica 5/1992 (LORTAD) previo a la firma y ratificación del convenio 108 y la adhesión al Convenio Schengen. Entre tanto y a raíz de la gran cantidad de enmienda vertida a la LORTAD surge la Ley Orgánica 15/1999 (LOPD) luego de la Directiva 95/46/CE. En ese sentido con la intención de adaptar las normas jurídicas españolas al Reglamento se crea ordenamiento español al de acuerdo a lo dispuesto en el Reglamento concretado el Reglamento, una ley que garantiza los derechos digitales en la esfera del Internet y otros derechos complementando el Reglamento.

Todas estas influencias norteamericanas y europeas permean en Latinoamérica de manera desigual. Así se mezcla la privacidad, con la intimidad y con el *habeas data* ofreciendo un panorama nada clasificado. En ese sentido, la garantía judicial; *habeas data* en Latinoamérica se ha mezclado con el derecho, obedeciendo a una serie de justificaciones planteadas a continuación.

- Latinoamérica, basa su visión de la protección de datos en sus realidades políticas, jurídicas y sociales motivadas por su inestabilidad política y jurídica, la inexistencia de tratados internacionales preexistentes que contribuyan a una regulación y unificación de

derechos a la protección de datos, así como la incorporación aislada de dispositivos constitucionales y legales frente al uso de la informática.

- La visión pragmática de Latinoamérica que ha aceptado una visión del Derecho constitucional en términos de Derecho procesal constitucional, asumiendo figuras tales como el amparo, habeas corpus y por último el *habeas data* todo ello por: a) creación de figuras procesales en el ámbito del Derecho constitucional; b) asunción del *habeas data* como nuevo derecho o parte del derecho procesal constitucional.
- Esta concepción anclada en la intimidad (también de alguna manera en la vida privada) se puede ver porque el numeral 2 artículo 44 forma parte del “tronco” del derecho a la intimidad.
- Esto ocasiona, que a menudo, tanto la doctrina, la jurisprudencia, como el legislador se refieran a la intimidad, privacidad, protección de datos (o incluso *habeas data*) sin un deslinde totalmente definido.
- Las regulaciones en el contexto latinoamericano se han realizado de manera aislada en cada país. Además, se ha destacar que si repasamos los distintos textos constitucionales observaremos que, tras la constitucionalización en los años 80 de este derecho en Guatemala, Nicaragua y Brasil, en los 90 se abre una segunda etapa con los Estados de Colombia, Paraguay, Perú, Argentina, Ecuador y Venezuela finalizando en el 2000 con países como Bolivia, Honduras, México y la República Dominicana con su reforma Constitucional del 2010. Pero no todo se queda en el despliegue constitucional, sino que los Estados se abocan en la construcción de leyes generales y específicas, situación de Argentina, Colombia, y Perú. En cambio, otros, poseedores de Constituciones de la era pre informática, no contemplan desarrollos constitucionales en materia de protección de datos o *habeas data*, pero sí han implementado interesantes leyes de protección de datos,

situación de Chile, Costa Rica, Uruguay, un proceso que no se detiene en los Estados Latinoamericanos.

- Los Estados Iberoamericanos realizan ingentes esfuerzos en homologar sus normas nacionales en materia de protección de datos personales, una acción impulsada y bajo el apoyo de los Jefes de Estados vía sus reuniones de jefes de Estados, todo ello con el apoyo europeo en especial España. Así como las organizaciones creadas vía estos esfuerzos para impulsar a los Estados como la Red Iberoamericana de protección de datos, foros económicos entre ellos la Organización de Cooperación y Desarrollo Económico (OCDE) y la Organización de Estados Americanos (OEA).

Todo este acervo es definitorio igualmente en Latinoamérica y, por tanto, también en República Dominicana. El *habeas data* es una garantía judicial que materializa el derecho a la protección de datos. Desde la doctrina dominicana se concluye que esta garantía trata de impedir que se lesione el derecho a la intimidad o que los datos estén siendo manejados sin su consentimiento, pero nosotros discrepamos diciendo que también protege los datos obtenidos con consentimiento y aquellos no íntimos.

El derecho a la protección de datos aparece por primera vez en la Constitución del 2010 y la subsecuente Constitución del 2015, cuyos derechos se mantienen inamovibles en los artículos de la Constitución del 2010 y su reforma, es así como el derecho a la protección si encuentra un acomodo en el numeral 2 del artículo 44 en relación con el artículo 70. Estos preceptos recogen formulas avanzadas, pero presentan algunas deficiencias técnicas.

- El derecho a la protección de datos es un derecho con propia sustantividad por eso hubiera sido más deseable no encuadrarle dentro del epígrafe del derecho a la intimidad. Por ello, la fórmula mejor hubiera

sido la expresión “el derecho a la protección de datos de carácter personal”

- El *habeas data*, al fin y la postre, forma parte del mismo o es un remedio del mismo como garantía de éste, una de las garantías específicas como otras que para este derecho se viene exigiendo en todo el contexto mundial (la autoridad de una autoridad independiente de control)
- No existe una alineación de la tutela judicial efectiva en materia de amparo y *habeas data*, por tanto, acotamos y señalamos, que, desde el punto de vista jurisprudencial, se observan discrepancias y puntos de vistas distintos en materia de amparo, acceso a la información pública, *habeas data*, protección de datos entre el Tribunal Superior Administrativo y el Tribunal Constitucional, Situación observada en las sentencias emanadas por el Alto Tribunal, y presentadas a lo largo y ancho del trabajo
- En tanto que, amparado en las sentencias emanadas por el Tribunal Constitucional de la República Dominicana, destacamos la doble dimensión del *habeas data*. Por un lado, se otorga el derecho de acceso a los datos, y por el otro, protege otros derechos conectados con la información, como el derecho a la intimidad, privacidad, honor, imagen, y el ya mencionado derecho a la autodeterminación informativa, sirviendo de garantía y mecanismo de protección para los mencionados derechos fundamentales establecidos en la carta magna y reflejados en sentencias jurisdiccionales evacuadas por el Tribunal Constitucional.
- El Tribunal Constitucional mediante la evacuación de sus sentencias, y amparados en el principio de oficiosidad que le otorga la referida Ley núm. 137-11 en su respectivo artículo 7 numeral 11, recalifica la acción de amparo ordinario en un *habeas data* (STC/0475/18). A raíz de ello,

entendemos que, desde el punto de vista Constitucional, el Tribunal reconoce, modifica y asume como tal, la acción de *habeas data* figurada en el Derecho Procesal Constitucional, una acción capaz de proteger el derecho fundamental a la autodeterminación informativa, posibilitando el desarrollo de la legitimación activa, accionando el *habeas data*. Es decir, podemos categorizar diciendo que, *el habeas data* desde la óptica del Tribunal Constitucional, es una acción de amparo con sustantividad propia, siendo reconocido o tipificado como un amparo con su propio apellido, capaz de proteger aquellos derechos para el cual fue concebido, o llamado a proteger. Con tales decisiones, el Tribunal Constitucional hace pleno uso de la tutela efectiva otorgada por la Constitución y el principio rector de efectividad contenido en la *Ley Orgánica núm. 137-11 del Tribunal Constitucional y de los Procedimientos Constitucionales*

- La República Dominicana, debe estrechar sus lazos de cooperación con los Estados, tejiendo normativas legislativas conjuntas en materia de protección de datos personales, repercutiendo en un aumento de los flujos de mercancías. Una situación sobrevenida por los efectos de la globalización, adquiriendo una connotación de doble vía, por lo que, un aumento en la protección de datos, repercute en un aumento de los flujos transfronterizos y viceversa, fortaleciendo la economía de los Estados involucrados.
- El desarrollo del Internet y el aumento de las TIC, revisten una gran conexión con la protección de datos personales durante el proceso de ejecución de transferencias internacionales de datos entre los Estados. Situación considerada al momento de concebir los proyectos normativos en materia de protección de datos en el Estado dominicano, previo a la promulgación de la Ley núm.172-13. Desarrollos normativos al alcance de las legislaciones europeas, caso de las pasadas legislaciones españolas vistas (LORTAD y LOPD); siendo considerado, motivos suficientes y necesarios al momento de concebir los proyectos normativos en materia de

protección de datos en el Estado dominicano previo a la promulgación de la Ley núm.172-13.

- La actual ley de protección de datos personales (Ley núm. 172-13), es el resultado de los proyectos resultantes de la Cámara de Diputados y el Senado de la República, materializándose en la actual Ley núm. 172-13, una ley alejada de ambos proyectos y conectadas con la *Ley núm. 288-05, del 18 de agosto del 2005 que regula las Sociedades de Información Crediticia y Protección del Titular de la Información*, derogada en su totalidad e integrada en la *Ley núm. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros público, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados*.
- La Ley núm. 172-13 nace desprotegida, careciendo de un órgano de control dotado y rodeado de total independencia funcional y económica, al margen de las normas legislativas expuestas y que, a su vez, apelan por la creación e instauración de la figura del órgano de control rodeado de la independencia añorada por estos.
- La normativa (Ley 172-13), no cuenta con una estructura que permita su adhesión al Convenio 108 del Consejo de Europa del 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y, su Protocolo Adicional al Convenio 108 relativo a las autoridades de control y transferencias internacionales y formar parte de los Estados reconocidos por la Unión Europea como Estados con legislaciones adecuadas, tales son los casos de la República de Argentina y Uruguay. De ahí, la urgente necesidad de readecuar la normativa núm. 172-13 mediante la elaboración de una ley de protección de las personas físicas en relación con la protección de datos, permitiendo a su vez, la inserción del Estado al Convenio 108, y con ello, obtener la

certificación de la Unión Europea, contribuyendo con el aumento de los flujos transfronterizos hacia los Estados europeos y como no, de la Unión Europea en su conjunto, retribuyendo en una mejora del comercio de la República Dominicana, protegiendo los datos personales involucrados en las transferencias.

- Durante la exposición del trabajo, hemos denotado y evidenciado un fuerte compromiso del Gobierno dominicano por la transparencia y búsqueda de institucionalidad y seguridad jurídica en las instituciones gubernamentales. Situación materializada en la estructura compuesta por: a) las Oficinas de Acceso a la Información pública (OAI) establecidas en todo el territorio nacional y en franco crecimiento cada año, superando los 300 puntos de atención distribuidos en toda la geografía nacional, representadas por Responsables de Acceso a la Información Pública (RAI) conectados con la Dirección General de Ética e Integridad Gubernamental (DIGEIG), capaz de orquestar Comisiones de Ética Pública (CEP) a nivel nacional y, b) la estructura tecnológica conformada por el Portal Único de Solicitud de Acceso a la Información Pública (SAIP), adscrito a la Dirección General de Ética e Integridad Gubernamental (DIGEIG) dependencia del Ministerio de la Presidencia.
- La DIGEIG la conforma un director general y un director ejecutivo bajo la dependencia del Ministerio de la Presidencia, signatario de una independencia comprometida, producto de la conexión existente entre el director general y el partido de gobierno, y más, cuando nos referimos a la Dirección General de Ética e Integridad Gubernamental (DIGEIG), una institución responsable del aseguramiento de la transparencia e integridad en la administración pública. Situación por las que recomendamos crear los mecanismos necesarios que nos conduzcan a la obtención de una adecuada selección, logrando contribuir con la tan anhelada transparencia gubernamental.

- En búsqueda de la transparencia en la administración pública y su vinculación con el libre acceso a la información pública, el Gobierno dominicano hace ingentes esfuerzos en conectar la tecnología de información y comunicaciones con la administración gubernamental. La iniciativa permite el acceso de sus nacionales a las informaciones de las oficinas públicas o instituciones dependientes de ella, vía los diferentes puntos de conexiones virtuales y físicas establecidos en el territorio nacional, situación del Portal Único de Solicitud de Acceso a la Información Pública (SAIP). Cuyo resultado es la creación de instituciones provistas de independencia económica y funcional, tales son los casos de la Dirección General de Ética e Integridad Gubernamental (DIGEIG) y la Oficina Presidencial de Tecnología y Comunicaciones (OPTIC), vinculadas a la presidencia, conformando el gobierno electrónico. El escenario planteado nos permite sugerir y exhortar una vez más la vinculación del órgano de control instituido en el artículo 29 de la Ley núm. 172-13 con la presidencia.
- República Dominicana no cuenta con planes de verificación o programas de supervisión para las sociedades de información crediticias (SIC)
- Desde la Oficina de Servicio y Protección al Usuario (PROUSUARIO), no se han realizado campañas de verificación, más allá de una ligera promoción de los derechos y deberes contemplados en la ley por medio a la estrategia de educación contemplada por la Superintendencia de Bancos (SIB) vía la exposición en redes sociales, charlas.
- La actual Ley núm. 172-13 deposita en manos de la Ley de Función Pública y la Ley General de Libre Acceso a la Información Pública, la responsabilidad de crear, modificar o suspender los archivos de datos correspondientes a la administración pública. De entrada, nos referimos a disposiciones legislativas previas a la actual Ley núm. 172-13, que, a su vez, no incorpora las funciones o atribuciones reconocidas y otorgadas en la referida ley. En cambio, la administración pública asegura la protección de

los archivos de datos públicos, por medio al uso y empleo de servidores de repartos y unidades departamentales internas, responsables de asegurar y tutelar los archivos de datos personales en manos de la administración pública, convirtiéndose en juez y parte de la situación ante la inexistencia de un órgano de control capaz de asegurar, auditar, velar, y proteger las informaciones, garantizando la implementación de medidas preventivas y proactivas, asegurando tales derechos.

Estandarización Normativas Latinoamericanas

En la actualidad, no ha sido posible la implementación de una Ley Modelo en materia de protección de datos personales en los Estados Iberoamericanos, a pesar de los continuos esfuerzos realizados por múltiples organizaciones internacionales. Tales son los casos del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) México, la Organización de los Estados Americanos (OEA), entre otras; en ese sentido, presentamos la siguiente propuesta de implementación de la Ley Latinoamericana.

Propuesta de implementación Ley Latinoamericana

Para soportar y asegurar el proceso de implementación de la Ley Latinoamericana en los Estados, será necesario:

- Crear mecanismos de controles independientes, siendo necesario el reconocimiento, aporte y colaboración de los mismos en el establecimiento e instauración de una Ley de Protección de Datos Personales Latinoamericana, situación de la actual propuesta de “*Estándares de Protección de Datos Personales para los Estados Iberoamericanos*”, asegurando una adecuada implementación, vía la creación de mecanismos de controles, garantizando la colaboración entre los organismos instituidos en los Estados, dotados de la capacidad necesaria para solucionar posibles desavenencias entre los organismos, maximizando la colaboración entre ellos. En resumen, estamos delante de tres situaciones: a) la creación del

Estándar o norma legislativa; b) el establecimiento de organismos o instituciones en los Estados, capaces de realizar las adecuaciones necesarias para cumplir con la implementación de la norma legislativa; c) la instauración de un mecanismo capaz de coordinar; y d) colaborar con los organismos instituidos en los Estados.

- Con la implementación de la normativa en los Estados Latinoamericanos, se plantea la posibilidad de disponer de leyes equivalentes en los mismos, y con ello, equiparar el nivel de protección en los Estados, elevando la protección existente. En igual contexto, con la creación de autoridades independientes en los Estados, se apuesta por una supervisión coherente al momento de realizar tales implementaciones, logrando alcanzar un nivel congruente de protección, evitando divergencias en la creación e implementación de la norma por los organismos asignados, siendo homologadas en cada uno de los Estados, creando marcos sólidos y coherentes en lo que a materia de protección de las personas físicas se refiere en relación al tratamiento automatizado de datos personales, reforzando la seguridad jurídica y la transparencia en la zona, aumentando a su vez el nivel de confianza, imprescindible y necesario para los operadores económicos en el área conformada por los países iberoamericanos.
- En tal sentido, se contempla la creación de un organismo coordinador de los órganos de control, asegurando la cooperación efectiva entre las autoridades de control, otorgando poderes equivalentes entre las autoridades y, aplicando sanciones equivalentes a las infracciones cometidas en el espacio iberoamericano. En tanto, el órgano coordinador deberá ser capaz de solucionar posibles desavenencias entre los Estados, por tanto, su conformación deberá estar compuesta por representantes de los Estados Iberoamericanos con capacidades y amplios poderes de toma de decisiones delegadas por los Estados.

- Por otra parte, y guardando la distancia, el nivel de penetración y tendencia tecnológica de Latinoamérica, se encuentra a la altura de los Estados europeos. En esa medida debe contemplarse su proceso regulatorio, a pesar de no contar con idénticas realidades económicas, sociales y políticas como las existentes en los Estados europeos o en aquellos Estados pertenecientes a la Unión Europea, poseedores de estándares legislativos vanguardistas en materia de protección de datos. En ese sentido, es de vital importancia disponer de autoridades de control independientes en los Estados, dirigidas por una autoridad general de control a nivel supranacional, sustentada económicamente por el aporte proveniente de los Estados a raíz de los beneficios obtenidos por el aumento de las transacciones comerciales de bienes y servicios generados por el crecimiento internacional de datos, producto de la cooperación entre los Estados, sin dejar de lado otros aportes provenientes de sanciones impuestas. Por su parte, el órgano general de control estará adscrito y bajo la administración de un organismo supranacional, tal es el caso de la Organización de Estados Americanos (OEA), considerado un organismo de vocación regional , ejerciendo el papel del Comité contemplado en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo de 27 de abril de 2016, disponiendo de una normativa general y homogénea en materia de protección de las personas físicas en lo que respecta al tratamiento de datos personales y su libre circulación.
- En ese sentido, los órganos de control independientes de los Estados Latinoamericanos se conectarán a un mecanismo u órgano de control general, dirigido por un representante o director general elegido por los Estados, con la capacidad de realizar los procesos propios de las actividades de control referida en anteriores capítulos.

Requisitos para implementar la Ley de Protección de Datos Latinoamericana

Como se ha evidenciado y comentado durante la exposición del trabajo, el modelo europeo es parte integral de los modelos más representativos tomados

en cuenta por los Estados Latinoamericanos al momento de crear u homologar sus normas legislativas en materia de protección de datos. A pesar de ello, no son el núcleo de nuestro análisis, debido a que independiente de su gran fortaleza, no todos los Estados Latinoamericanos cuentan con una estructura capaz de reproducir e implementar en sus normas de protección de datos el modelo europeo, siendo necesario disponer de:

- El apoyo económico suficiente para crear, implementar y llevar a cabo la normativa europea,
- b) La cultura existente en los Estados,
- c) El desarrollo e influencia tecnológica que impacta los Estados,
- d) La intención o voluntad de los gobiernos,
- e) La infraestructura jurídica existente,
- f) La inexistencia de una Unión de Estados Iberoamericanos con plenos derechos y deberes como los Estados que son parte de la Unión Europea,
- g) La fortaleza y capacidad de materializar la implementación.

Todo ello, formando parte de los requisitos necesarios, pero no suficientes para completar el proceso de implementación de la ley. Por el momento, no más de dos Estados Latinoamericanos han sido reconocidos por decisiones de la Comisión como Estados con normativas adecuadas en materia de protección de datos, situación que nos permite desarrollar una secuencia de eventos que propicie concluir con el proceso de implementación del Estándar o Ley Modelo para los Estados Iberoamericanos en materia de protección de datos.

Propuesta de secuencia de eventos sugeridas para el proceso de homologar las normativas latinoamericana en materia de protección de datos en el espacio iberoamericano

- Crear una Ley Modelo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- Elaborar un tratado regional vinculante para los Estados Latinoamericanos relativo a la Ley Modelo, referente a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Establecer un mecanismo de implementación y seguimiento del proceso de instauración de la Ley Modelo.
- Concebir mecanismos de controles formado por autoridades independientes en los Estados.
- Instituir un mecanismo de control general conformado por una autoridad de control supranacional seleccionada por los Estados y adscrita a un organismo supranacional con poderes de decisión, coordinación y sanciones.
- Instaurar un organismo supranacional de alto nivel, responsable de la administración general del proceso; en ese sentido, es necesario disponer de una estructura con capacidad económica, administrativa y jurídica, provista de la experiencia y fortaleza necesaria para soportar la propuesta. Tal situación nos permite seleccionar a la OEA como mecanismo integrador, ya que, a pesar de las desavenencias históricas existentes entre la OEA con alguno de sus Estados miembros, viabilizamos la posibilidad de asumir el rol de liderar el desarrollo de la implementación y gestión del proceso, convirtiéndose en su máxima autoridad.

Luego de presentar la propuesta de implementación del Estándar, pasamos a plantear las siguientes recomendaciones conectadas con los temas tratados durante el trabajo de investigación, incluida sus conclusiones y expuestas a continuación.

Recomendaciones

- Crear e implementar una cultura de protección de datos, dotada de mecanismos de control, posibilitando las transferencias de datos personales entre y desde los Estados Latinoamericanos.
- Instaurar órganos de control en los Estados Iberoamericanos, provistos de independencia funcional y económica, bajo la dependencia y administración de los Estados Latinoamericanos quienes le otorgan capacidad y amplios poderes de toma de decisiones.
- Otorgar poderes equivalentes entre las autoridades de control de los Estados Latinoamericanos.
- Incorporar un órgano de control Latinoamericano, responsable de la coordinación de los órganos de control implementados en los Estados Latinoamericanos, asegurando la cooperación efectiva entre las autoridades de control dispuestas en los Estados.
- Disponer de autoridades de control independientes en los Estados, dirigidos por una autoridad general de control a nivel supranacional, sustentada económicamente por el aporte proveniente de los Estados. A raíz de los beneficios obtenidos por el aumento de las transacciones comerciales de bienes y servicios generados por el crecimiento internacional de datos, producto a la cooperación entre los Estados, sin dejar de lado otros aportes, como los obtenidos vía las sanciones impuesta. Por otro lado, el órgano general de control, estará adscrito y bajo la administración de un organismo supranacional, tal es el caso de la Organización de Estados Americanos (OEA), considerado un organismo de vocación regional, ejerciendo el papel del Comité contemplado en el *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016*, disponiendo de una normativa general y homogénea en materia de protección de las personas físicas en lo que respecta al tratamiento de datos personales y su libre circulación.

- Solucionar posibles desavenencias existentes entre los órganos de control creados y en proceso de implementación en los Estados Latinoamericanos bajo la estructura de la propuesta del órgano de control Latinoamericano instaurado en la propuesta.
- Aplicar sanciones homogéneas en el espacio Iberoamericano en materia de protección de datos y *habeas data* tras la implementación de la propuesta.
- Reforzar las garantías adecuadas que permitan completar, realizar y asegurar transferencias de datos con la Unión Europea (UE) y terceros países sin requerir o necesitar autorización previa de las autoridades de control.
- Continuar con el proceso de homologación de la Ley Iberoamericana de Protección de Datos del INAI en los Estados Iberoamericanos, miembros de la Organización de los Estados Americanos (OEA).
- Instaurar la figura y la guía del delegado de protección de datos (DPO) fungiendo como interlocutor entre el órgano de control y las instituciones provistas de la figura en los Estados Latinoamericanos, con la iniciativa se aboga por una interacción proactiva entre el órgano y las instituciones conformadas y comprometidas con los delegados de protección de datos (DPO).
- Reunir bajo una misma estructura económica, funcional, organizativa y normativa, los temas de transparencia, acceso a la información pública y protección de datos personales, siendo necesario su inserción en la República Dominicana y los demás Estados que componen Latinoamérica, logrando la tan anhelada eficacia y eficiencia.
- Crear normas nacionales en los Estados capaces de impedir posibles vulneraciones de los derechos de sus ciudadanos, unos derechos conectados con el desarrollo tecnológico, requiriendo su protección ante el

acceso sin consentimiento de la información almacenada en medios electrónicos que están más allá de la correspondencia o comunicación telefónica contemplado en la convención americana. Tales son los casos de las informaciones privadas almacenadas en medios electrónicos ubicados en discos, tarjetas de memorias, almacenamiento en las nubes o informaciones contenidas en correos etc.

- Estrechar los lazos de cooperación entre los Estados Latinoamericanos, tejiendo normativas legislativas conjuntas en materia de protección de datos personales, repercutiendo en un aumento de los flujos de mercancías, una situación sobrevenida por los efectos de la globalización, adquiriendo una connotación de doble vía, por lo que, un aumento en la protección de datos, repercute en un aumento de los flujos transfronterizos y viceversa, fortaleciendo la economía de los Estados involucrados.
- Fortalecer el proceso de transferencias de datos personales contemplado en la Ley núm. 172-13 (artículo 80), mediante la incorporación de garantías adecuadas ante la ausencia de niveles de protección adecuados que permitan y garanticen transferencias de datos personales entre los Estados. Situación por las que se recomienda la incorporación de mecanismos de aseguramiento de transferencias de datos como: a) las cláusulas contractuales; b) instrumentos jurídicos; c) mecanismos de certificación; y d) otras alternativas, previa validación del órgano de control.
- Crear en la República Dominicana un órgano de protección de datos personales, dotado de independencia funcional y económica, adscrito al Ministerio de la Presidencia de la República Dominicana.
- Elaborar y establecer un plan estratégico del órgano de control, implementando las acciones a considerar y a tomar en cuenta por el referido órgano de control de protección de datos personales para los próximos 10 años, convirtiéndose en la base de su línea de actuación.

- Incluir la protección de datos personales en el Plan Nacional del 2030 de la República Dominicana.
- Diseñar los ejes estratégicos que sustentarán el plan estratégico al 2030, enfocado y conectado con los ciudadanos, los responsables, las instituciones públicas, los delegados de protección de datos, y el propio órgano de control conformado por su personal.
- Instituir un portal único de quejas y reclamaciones a la violación de la privacidad y los datos personales bajo la sombrilla del órgano de protección de datos de la República Dominicana.
- Realizar encuestas de satisfacción de la situación e incidencia de la protección de datos personales en la población dominicana.
- Establecer campañas de difusión masiva por medio al empleo de medios de comunicaciones radiales, televisivos, redes sociales (Facebook, Instagram, Twitter, etc.), destinados al conocimiento, prevención y protección de los datos personales de las personas, asegurando la protección física de estas, incluido el sector más vulnerable y menos favorecido del cual forman parte los menores de edad.
- Impulsar la cooperación del órgano de control con las instituciones públicas y privadas entre ellas: a) el Defensor del Pueblo; b) el Consejo del Poder Judicial; c) el Ministerio Público; d) la administración estatal, incluido los distintos ministerios, universidades privadas, públicas (Universidad Autónoma de Santo Domingo (UASD)), industrias, asociaciones, grupos profesionales de protección de datos y su acercamiento al órgano de control, etc.
- Despertar la necesidad del consumidor en relación a la protección de datos personales, mediante el establecimiento de charlas en las asociaciones u organismos destinados a la protección del consumidor.

- Fomentar e implementar una cultura de protección de datos, creando formadores de protección de datos, multiplicando el conocimiento de los mismos en la sociedad en especial con los menores de edad. Con la medida, se procura obtener adultos responsables en un mundo digital, siendo la educación la materia prima del crecimiento del germen de la protección de datos en la población.
- Crear mecanismos de protección de datos en la República Dominicana desde el diseño y por defecto.
- Homologar la propuesta de “*Estándares de Protección de Datos Personales para los Estados Iberoamericanos*” del INAI con la Ley núm. 172-13 en materia de protección de datos.
- Reformar y readecuar la normativa *Ley núm. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados* con las normas internacionales, aplicando e insertando las adecuaciones necesarias que les permitan estar al alcance de los nuevos estándares internacionales en la materia, así como la creación del ya comentado órgano de control dotado de independencia económica y funcional.
- Adecuar la actual Ley núm. 172-13 en los temas de órgano de control, delegado de protección de datos, derecho al olvido y otros temas, con el objetivo de lograr un acercamiento a los estándares existentes en materia de protección de datos, integrando y haciendo suya las últimas tendencias en materia de protección de datos orientada a la protección de las personas físicas, cuyos datos sean sometidos a tratamientos automáticos o no automáticos.

En ese sentido, los Estados deben continuar tejiendo normativas legislativas encaminadas a la protección de las personas físicas ante los constantes

embates a la intimidad y la privacidad, originados por una incesante evolución tecnológica y, un crecimiento de la globalización, aumentando los flujos transfronterizos entre los Estados y con ello, un incremento de los movimientos de mercancías entre los Estados de la Unión y terceros Estados, incluido los Estados Latinoamericanos.

Es así, como las conclusiones propuestas no cierran los temas expuestos, una situación sobrevenida por los constantes cambios acaecidos en el campo tecnológico, legislativo y comercial, conectados con la globalización y el aumento de los flujos transfronterizos, siendo necesario otorgar una real protección de las personas físicas en lo que respecta al tratamiento de datos personales y su libre circulación en los Estados, situación puesta en contexto en la introducción del trabajo y reflejado a continuación.

Propuesta de investigación para próximos desarrollos

El trabajo de investigación, no concluye con su presentación, sino más bien, es el grano que pronto germinará, dando paso a la ampliación de las actuales propuestas o el surgimiento de nuevos planteamientos encaminados a la conformación de una real, efectiva y eficaz normativa internacional de protección de las personas físicas en materia de protección de datos respecto al tratamiento de los datos personales y las transferencias internacionales para la República Dominicana y Latinoamérica.

A raíz de ello, presentamos los puntos a considerar en los próximos desarrollos para la República Dominicana y Latinoamérica.

República Dominicana.

- Viabilizar la creación de un órgano de control con total independencia económica y funcional.
- Analizar las sentencias de los tribunales ordinarios de la República Dominicana en materia de protección de datos, *habeas data*, intimidad.

- Adecuar y presentar una propuesta normativa de la *Ley núm. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados*, por una normativa adecuada a los últimos adelantos en materia de:
 - Órgano de control incluida su competencia, funciones, poderes, sin dejar de lado los derechos y funciones del director del órgano de control.
 - Derecho de supresión (el derecho al olvido).
 - Protección de datos desde el diseño y por defecto.
 - Delegado de protección de datos.
 - Transferencias internacionales.
- Realizar una nueva propuesta normativa para la República Dominicana en materia de protección de datos, incorporando los nuevos conceptos internacionales existentes, entre ellos: a) derecho al olvido; b) protección de datos por defecto y por diseño; c) Delegado de Protección de Datos (DPO); d) mecanismo de control y e) órgano de control independiente.

Latinoamérica

- Crear una normativa general o Ley Modelo Latinoamericana en materia de protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación, capaz de agrupar bajo una misma norma a los Estados Iberoamericanos, siendo capaz de formar parte del Convenio del Consejo de Europa.
- Presentar un Reglamento de implementación de la Ley Modelo.
- Crear un Sistema de Coherencia para los órganos de control.

A pesar de todo el esfuerzo realizado y logros alcanzados, entendemos que falta camino por recorrer en la búsqueda o establecimiento de un Estándar internacional en materia de protección de las personas físicas en relación al

tratamiento automático o no, de datos personales y su libre circulación, el cual asegurará y garantizará una mayor protección que la obtenida en los actuales momentos. Ante tal situación, somos partícipe de crear normativas supranacionales con la finalidad de formar o dar paso a una normativa de alcance global.

Los Estados Iberoamericanos mantienen un continuo desarrollo de sus normas legislativas desde el orden constitucional y sus normativas generales y específicas, a pesar de su cercanía territoriales y culturales, no se observa una homologación entre las mismas, a pesar de mantener una estrecha cooperación e incorporación de sus procesos normativos, en ese sentido desde la óptica del *habeas data* se observan homogeneidad desde el punto constitucional con algunos Estados y en otros a nivel de sus legislaciones generales.

BIBLIOGRAFÍA

Libros

THILL, E., *La tecnología y su rol en la protección de datos personales. Biometría, firma digital, identificación electrónica: claves para la implementación de políticas sociales, Régimen Jurídico de los Datos Personales*, tomo I, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

ABOGADOS, E., *Factbook protección de datos personales*, 2ª ed. Aranzadi, S. A., Navarra, 2008.

ABRAMOVICH, V. M. y COURTIS, C., *El acceso a la información y derechos sociales como derechos exigibles*, Trotta, Madrid, 2002.

ACADEMIA ESPAÑOLA, R., *Diccionario de la lengua española*, 22ª ed. Espasa Calpe, S. A., Madrid, 2001.

ACADEMIA ESPAÑOLA, R., *Diccionario de la lengua española*, 21ª ed. Espasa Calpe, S. A., Madrid, 1991.

ALMAZARA ALMAIDA, C. (Coordinador), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed. Lex Nova, Valladolid, 2007.

AMIANA, M., *Notas de Derecho Constitucional*, Tiempo, S. A., Santo Domingo, 1995.

ARENAS RAMIRO, M., *El Derecho fundamental a la protección de datos personales en Europa*, Tirant Lo Blanch, Valencia, 2006.

ARENAS RAMIRO, M. y ORTEGA GIMÉNEZ, A. (Directores), *Protección de Datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)*, 1ª ed. Sepín, S. L. Madrid, 2019.

ARGUELLO TELLEZ, F., *Protección de datos personales: La Directiva Comunitaria, su influencia y repercusiones en Latinoamérica, protección de datos de carácter personal en Iberoamérica, II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala 2-6 de junio de 2003*, Tirant Lo Blanch, Valencia, 2006.

ARZOZ SANTISTEBAN, X., *Derecho al respeto a la vida privada y familiar*, visto en LASAGABASTER HERRARTE, I. (Director), *Convenio Europeo de Derechos Humanos*, 3ª ed. Aranzadi S.A., Pamplona, 2015.

BAJO FERNÁNDEZ, M., *Protección del Honor y la Intimidad, comentarios a la legislación penal*, tomo I, Madrid, 1982.

BALDASARRE, A., *Privacy e Costituzione, L'esperienza statunitense*, Bulzoni, Roma, 1974.

BARBA MARTÍNEZ, G. P., *Curso de Derechos Fundamentales*, Teoría General, Boletín Oficial del Estado, Universidad Carlos III de Madrid, Madrid, 1999.

BARNICHTA GEARA, E., *Jurisprudencia constitucional dominicana*, 1ª ed. Centenario SRL, Santo Domingo, 2014.

BASTIDA, F., VILLAVERDE, I., REQUEJO, P., ÁNGEL PRESNO, M., ALÁEZ, B. F. y SARASOLA, I., *Teoría general de los derechos fundamentales en la Constitución Española de 1978*, Tecnos, Madrid, 2004.

BAZÁN, V., *El habeas data y el derecho a la autodeterminación informática en el escenario latinoamericano*, en *Constitución y Democracia: Ayer y Hoy (libro homenaje a Antonio Torres del Moral)*, Vol. I, Madrid, 2012.

BEATRIZ CALLE, S., *Apuntes jurídicos sobre la protección de datos personales a la luz de la actual norma de habeas data en Colombia*, Colombia, 2009.

BEATRIZ SBDAR, C., *Amparo de derechos fundamentales*, 1ª ed. Buenos Aires, 2003.

BELL, MALLÉN., CORREDOIRA y ALFONSO, I. (Coordinadores), *Derecho de la información*, 1ª ed. Ariel, S. A., Barcelona, 2003.

BELLAMY, C. y CHILD, G., *Derecho de la competencia en el mercado común*, 1ª ed. Civitas, S. A., Madrid, 1992.

BENNETT, C. D. y RAAB, C., *the governance of privacy, policy instruments in global perspective*, 2ª ed. London, 2006.

BENNETT, C., *Regulating privacy (Data Protection and Public Policy in Europe and the United State)*, 1ª ed. Cornell University Press, United States of America, 1992.

BENNETT, D. y RAAB., *The Governance of privacy (Policy Instruments in Global Perspective)*, The MIT Press Massachusetts, United States of America, 2006.

BENHAM, F., *Ayuda económica y subdesarrollo*, 1ª ed. Hobbs-Sudamericana, S. A., Buenos Aires, 1965.

BETEGÓN, J., LAPORTA, F. J., RAMÓN DE PÁRAMO, J. y PRIETO SANCHÍS, L. (Coordinadores), *Constitución y derechos fundamentales*, Ministerio de la Presidencia, Secretaría General Técnica, Centro de Estudios Políticos y Constitucionales, Madrid, 2004.

BHAGWATI, J., *En defensa de la Globalización*, 1ª ed. Random House Mondadori, S. A., (DEBATE), Barcelona, 2005.

BREA FRANCO, J., *El sistema constitucional dominicano (Tomo I)*, 1ª ed. UNPHU, Santo Domingo, 1983.

BOSCH., *Cómo sobrevivir al GDPR*, 1ª ED. Wolters Kluwer, S. A., Madrid, 2018.

CABANELLAS DE TORRES, G., *Diccionario Jurídico Universitario*, Heliasta S. R., Argentina, 2000.

CAMPOS FARÍAS, F., *Estudio comparado de las constituciones políticas nacionales latinoamericanas*, Santo Domingo, 2002.

CARLOS PEREIRA, J. (Coordinador), *Diccionario de relaciones internacionales y política exterior*, Ariel S. A., Barcelona, 2008.

CARLOS PEREIRA, J. (Coordinador), *Historia de las relaciones internacionales contemporánea*, Ariel S. A., Barcelona, 2009.

CARRASCOSA LÓPEZ, V. (Director), *Informática y Derecho*, 1ª ed. Universidad Nacional de Educación a Distancia (UNED), Centro Regional de Extremadura Mérida, Sevilla, 1992.

CARRASCOSA LÓPEZ, V., *Informática y Derecho 1*, 1ª ed. Universidad Nacional de Educación a Distancia, Mérida, Sevilla, 1992.

CARRASCOSA LÓPEZ, V. (Director), *Informática y Derecho 6-7 La Protección de Datos Personales*, 1ª ed. Universidad Nacional de Educación a Distancia (UNED) Centro Regional de Extremadura Mérida, Sevilla, 1994.

CARRASCOSA LÓPEZ, V. (Director), *Informática y Derecho (II Congreso Internacional de Informática y Derecho)*, 1ª ed. Universidad Nacional de Educación a Distancia (UNED), Centro Regional de Extremadura Mérida, Sevilla, 1994.

CARRERAS SERRA, L., *Régimen Jurídico de la Información*, Ariel S. A., Barcelona, 1996.

CASAL, J., *El nuevo Derecho Constitucional venezolano (IV Congreso de Derecho Constitucional en homenaje al Doctor Humberto La Roche*, Caracas, 2001.

CASTAÑEDA GONZÁLEZ, A. (Coordinador), *Derecho tecnológico respuesta legales a nuevos retos*, 1ª ed. Experiencia, S. L., Barcelona, 2004.

CASTILLO MOTA, S. P., KARINA BELLO, H. y BURÓ GUTIÉRREZ, J., *La acción de habeas data y su aplicación en la República Dominicana*, Santo Domingo, 2004.

CENTRAL DE INFORMÁTICA., *Informática Leyes de Protección de Datos*, Documentación Informática, núm. 2, serie Verde /Legislación, 1ª ed. Presidencia del gobierno, Madrid, 1977.

CENTRAL DE INFORMÁTICA., *Informática Leyes de Protección de Datos*, Documentación Informática, núm. 3, serie Verde /Legislación, 1ª ed. Presidencia del gobierno, Madrid, 1983.

CÉSAR MATOS, J., *Introducción al estudio del derecho*, 1ª ed. Santo Domingo.

CISNAL DE UGARTE, E. S., FERNÁNDEZ LIESA, C. R. y MOREIRA GONZÁLEZ, C., *Descripción, análisis y comentarios al Tratado de la Unión Europea*, 1ª ed. McGRAW-HILL / INTERAMERICANA DE ESPAÑA, S. A., Madrid, 1993.

CHEZ CHECO, J., *La Telefónica, presencia y desarrollo en la República Dominicana*, Amigo de Hogar, Santo Domingo, 2000.

COLLADO, G. y LAJARA, E., *Protección de datos de carácter personal*, 1ª ed. Comares, S. L., Granada, 2000.

CONDE ORTIZ, C., *La protección de datos personales*, Dykinson, Madrid, 2005.

COTINO, L., *Derechos humanos, Internet y TICs*. En Rey (dir). *Los derechos humanos en España, un balance crítico*, Tirant Lo Blanch, Valencia, 2015.

COUDHRY, S., *Commentary to article 7: Right to respect for Private and Family life (Family Life Aspects)*. En PEERS S., HARVEY, T., KENNER, J. & WARD, A. (Eds.). *The EU Charter of Fundamental Rights. A Commentary*. Oxford and Portland: Hart Publishing, 2014.

CRESPO LÓPEZ, A. (Coordinador), *La protección de datos en los centros de enseñanza*, 1ª ed. Aranzadi, S. A., Navarra, 2007.

DARANAS, M., *Jurisprudencia constitucional y extranjera. Tribunal Constitucional Alemán. Ley del Censo*, Boletín de Jurisprudencia Constitucional, núm. 33, 1984.

DAVARA RODRÍGUEZ, M., *Manual de protección de datos para abogados*, 2ª ed. Aranzadi, S. A., Pamplona, 2008.

DAVARA RODRÍGUEZ, M., *XVII encuentros sobre Informática y Derecho*, 1ª ed. Aranzadi, S. A., Navarra, 2003.

DAVARA RODRÍGUEZ, M. A. (Coordinador), *XVII encuentro sobre Informática y Derecho*, Universidad Pontificia Comillas, Madrid, 2002-2003.

DAVARA RODRÍGUEZ, M., *XIV encuentros sobre Informática y Derecho*, 1ª ed. Aranzadi, S. A., Navarra, 2001.

DAVARA RODRÍGUEZ, M., *XIII encuentros sobre Informática y Derecho*, 1ª ed. Aranzadi, S. A., Navarra, 2000.

DAVARA RODRÍGUEZ, M., *X encuentros sobre Informática y Derecho*, 1ª ed. Aranzadi, S. A., Navarra, 1997.

DAVARA RODRÍGUEZ, M. A., *La Protección de datos personales en el sector de las telecomunicaciones*, Fundación Airte, Madrid, 2000.

DAVARA RODRÍGUEZ, M. A., *Las Telecomunicaciones y las Tecnologías de la Información en la Empresa: Implicaciones Socio-Jurídica*, visto en CARRASCOSA LÓPEZ, V. (Director), *Informática y Derecho I*, 1ª ed. Universidad Nacional de Educación a Distancia, Mérida, Sevilla, 1992.

DAVARA RODRÍGUEZ, M. A., *Manual de Derecho Informático*, 3ª ed. Aranzadi, S. A., Madrid, 2001.

DAVARA RODRÍGUEZ, M. A., *Normativa para la protección de la intimidad: planteamiento general*, nota 3, p. 22, tomado de IX encuentro 1991, *implicaciones socio-jurídicas de las tecnologías de la información*, CITEMA, Madrid, 1991.

DE ABREU DALLARI, D., “*El Habeas data en Brasil*”, *Ius ET Praxis* (año 3 núm.1), Facultad de Ciencias Jurídicas y Sociales (Universidad de Taica), Chile, 1997.

DE AZEVEDO CUNHA, M. V., *Protección de Datos en el Mercosur: Hacia un Marco Común*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

DE LA MATA, J. (Coordinador), *Protección de datos comentarios al Reglamento*, 1ª ed. Lex Nova, Valladolid, 2008.

DEL CASTILLO VÁZQUEZ, I. C., *Protección de datos: cuestiones constitucionales y administrativas*, 1ª ed. Aranzadi, S. A., Madrid, 2007.

DÍAZ ROJO, J. A., Privacidad, *El cajetín de la lengua*. Disponible en: <http://pendientedemigracion.ucm.es/info/especulo/cajetin/privacid.html>. (Última consulta en línea 14 de agosto 2013).

DÍEZ PICAZO, L. M., *Sistema de Derechos Fundamentales*, 3ª ed. Thomson Civitas, España, 2008.

DÍEZ DE VELASCO, M. A., *Instituciones de Derecho Internacional Público*, 15ª ed. Tecnos, S. A., Madrid, 2005.

DÍEZ DE VELASCO, M. A., *Instituciones de Derecho Internacional Público*, 13ª ed. Tecnos, S. A., Madrid, 2001.

DOCUMENTACIÓN INFORMÁTICA., *Flujo Internacional de Datos, recomendación de la OCDE de 23 de septiembre de 1980*, tratados Internacionales núm. 2, 1ª ed. Presidencia del Gobierno, serie amarilla, servicio central de publicaciones, Madrid, 1982. Disponible en: <http://www.oecd.org/centrodemexico/paisesmiembros.htm>. (Última consulta en línea 7 de diciembre 2017).

DUCOURTIEUX, C., *Comunicaciones en tiempo real, el atlas de las mundializaciones, le monde diplomatique en español*, Uned, Madrid, 2012.

DURÁN CARDO, B., *El Delegado de Protección de Datos en el RGPD y la nueva LOPDGDD*, 1ª ed. Wolters Kluwer España, S. A. Madrid, 2019,

DURÁN CARDO, B., *La figura del responsable en el derecho a la protección de datos*, La Ley, Wolters Kluwer, Las Rozas (Madrid), 2016.

DURÁN RIBERA, W. R., *Contenido y alcances del habeas data en Bolivia*, Anuario de Derecho Constitucional Latinoamericano, 2006.

EBERT, F., *Relaciones económicas entre América Latina y la Comunidad Económica Europea (seminario sobre las relaciones de América Latina y la CEE)*, 1ª ed. Fundación Friedrich Ebert, Madrid, 1988.

EKMEKDJIAN, M. y PIZZOLO, C., *Habeas Data (El derecho a la intimidad frente a la revolución informática)*, De Palma, Buenos Aires, 1998.

ENÉRIZ OLAECHEA, F. J., *La protección de los derechos fundamentales y las libertades públicas en la Constitución Española*, editora Universidad Pública de Navarra, Navarra, 2007.

ESTADELLA YUSTE, O., *La protección de la intimidad frente a la transmisión internacional de datos*, 1ª ed. Tecnos, S. A., Madrid, 1995.

FALCON, E. M., *Que es la informática jurídica*, ABELEDOPERROT S. A., Buenos Aires, 1992.

FARRIAS CAMPOS, F., *Estudio comparado de las constituciones políticas nacionales latinoamericanas*, 1ª ed. Universidad del Caribe, Santo Domingo, 2002.

FAÚNDEZ LEDESMA, H., *El Sistema Interamericano de Protección de los Derechos Humanos, Aspectos institucionales y procesales*, 3ª ed. Instituto Interamericano de Derechos Humanos, San José, 2004.

FERNÁNDEZ DELPECH, H., *Internet: problemática jurídica*, ABELEDOPERROT S. A., Buenos Aires, 2001.

FERNÁNDEZ ESTEBAN, M. L., *Nuevas tecnologías, Internet y derechos fundamentales*, 1ª ed. Susana Santos Prieto, Madrid, 1998.

FREIXAS GUTIÉRREZ, G., *La protección de los datos de carácter personal en el derecho español*, 1ª ed. Bosch, S. A., Barcelona, 2001.

FROSINI, V., *Cibernética, Derecho y Sociedad*, 1ª ed. Tecnos, S. A., Madrid, 1982.

FROSINI, V., *Derechos humanos y constitucionalismo ante el tercer milenio (Los derechos humanos en la era tecnológica)*, Monografías Jurídicas, Marcial Pons Jurídicas Sociales, Madrid, 1996.

FUNDACIÓN INSTITUCIONALIDAD Y JUSTICIA INC. (FINJUS), F., *Constitución comentada*, 3ª ed. Búho, Santo Domingo, 2012.

GAIERO GUADAGNA, B. y SOBA BRACESCO, I. M., “*El proceso de habeas data en Uruguay (protección de datos personales y acceso a la información pública)*”, *Anuario de Derecho Constitucional Latinoamericano*, año XVI, Konrad Adenauer Stiftung, Montevideo, Uruguay, 2010.

GALINDO, F., *Derecho e Informática*, La Ley-Actualidad, S. A., Madrid, 1998.

GALINDO, J. y ROVER (EDS), *Derecho, Gobernanza y Tecnologías de la Información en la sociedad del conocimiento*, 1ª ed. LEFIS, Zaragoza, 2009.

GAMBOA SERAZZI, F., *Manual de Derecho Internacional Público*, 4ª ed. Lom, Santiago, 1997.

GARCÍA BELAUNDE, D., *Derecho Procesal Constitucional*, Temis S. A., Bogotá, 2001.

GARCÍA LAJARA, E. C., *Protección de datos de Carácter Personal*, 1ª ed. Comares, Granada, 2000.

GARCÍA MADARIA, J., *Preparador Código de legislación informática*, 1ª ed. BOE (Boletín Oficial del Estado), Madrid, 1998.

GARCÍA VITORIA, A., *El derecho a la intimidad, en el derecho penal y en la Constitución de 1978*, 1ª ed. Aranzadi, S. A., Pamplona, 1983.

GARZÓN, G., *El marco jurídico del flujo de datos transfronteras*, IBI, Doc. TDF 102, Roma, 1981.

GOIG MARTÍNEZ, J. (Coordinador), *El sistema constitucional de derechos y libertades según la jurisprudencia del Tribunal Constitucional*, Universitas Internacional, S. L., Madrid, 2006.

GOMES CANOTILHO, J. J. & MOREIRA, V., *Constituição da República Portuguesa. Anotada*, 1ª ed. COIMBRA, 1980.

GÓMEZ, E. y CRESPO LÓPEZ, A., *La protección de datos en los centros de enseñanzas*, 1ª ed. Aranzadi S. A., Navarra, 2007.

GÓMEZ RIVERO, M.^a del C. (Directora), *Nociones Fundamentales de Derecho Penal*, Volumen 1, 3ª ed. Tecnos, Madrid, 2018.

GONZÁLEZ MURUA, A. R., “Protección de datos de carácter personal” en *La Carta de los Derechos Fundamentales de la Unión Europea*, Ugartemendia Eceizabarrena, J. I. Thomson Reuters Aranzadi, Cizur Menor, 2012.

GONZÁLEZ MURUA, A. R., “Las competencias de las defensorías del pueblo estatal y autonómicas y su relación con la protección de datos”, en *la protección de los derechos humanos por las Defensorías del Pueblo*. Escobar Roca, G., Dykinson, Madrid, 2013.

GONZÁLEZ MURUA, A. R., “Unión Europea y protección de datos personales”, Grupo de Investigación G1184, *Derechos Fundamentales y Unión Europea*, 2010.

GOZAINI, O., *EL Derecho de amparo*, 2ª ed. De Palma, Buenos Aires, 1998.

GOZAINI, O., *Introducción al Derecho Procesal Constitucional* Rubinzal-Culzoni, Buenos Aires, 1998.

GRANERO, H., *La protección de datos personales y la responsabilidad objetiva en Internet*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo I, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

GROSSO, C. P., *Algunos aspectos de la protección de la privacidad en el ámbito de las empresas*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

HALSALL, F., *Data Communications, Computer Networks and OSI*, Addison-Wesley Publishing Company, United States of America, 1988.

HERRERO HIGUERAS, M., *Panorama General de la Legislación Mundial sobre protección de datos*, CITEMA, España, p. 35, tomado de IX encuentro implicaciones socio-jurídicas de las tecnologías de la información, CITEMA, España, 1991.

HEREDERO HIGUERAS, M. y ÁLVAREZ RICO, M. (Preparadores), *Legislación informática*, 1ª ed. Tecnos, S. A., Madrid, 1994.

HERNANDO, I., *Contratos informáticos*, 1ª ed. Librería Carmelo, San Sebastián, 1995.

HERNANDO, I., *Contratos informáticos, derecho informático Legislación y Práctica*, 1ª ed. Librería Carmelo, San Sebastián, 20009.

HONDIUS F, A., *Decade of International Data Protection*, Netherlands of International Law Review, Vol. 30, núm. 2, 1983.

JIMÉNEZ DE PARGA, M., *La Información y los derechos penales*, prólogo de C. MOLINERO, 1ª ed. Dirosa, Barcelona, 1977.

JORDÁN GALDUF, J. M.^a (Coordinador), *Economía de la Unión Europea*, 1^a ed. Civitas, Madrid, 1994.

JORGE PRATS, E., *Derecho Constitucional, Volumen I*, Iusnovum, Santo Domingo, 2012.

JORGE PRATS, E., *Derecho Constitucional, Volumen II*, Iusnovum, Santo Domingo, 2012.

QUESADA RODRÍGUEZ, A., *Protección de datos y telecomunicaciones convergentes*, 1^a ed. Agencia Española de protección de datos, Madrid, 2014.

LASAGABASTER HERRARTE, I. (Director), *Convenio Europeo de Derechos Humanos*, 3^a ed. Aranzadi S.A., Pamplona, 2015.

LESMES SERRANO, C. (Coordinador), *La ley de protección de datos análisis y comentario de su jurisprudencia*, 1^a ed. Lex Nova, Valladolid, 2008.

LOBATO, A., KABBAS, D. y DE LUCIO, L., *Computación en la nube. Desafíos de los Estados y de los ciudadanos. La privacidad de la información personal*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo I, 1^a ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

LÓPEZ CARBALLO, D. (Coordinador), *Protección de datos y habeas data: una visión desde Iberoamérica*, imprenta nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2015.

LÓPEZ GUERRA, L., *El Derecho Constitucional español. Origen y características de la Constitución*, visto en *Derecho Constitucional*, volumen I, 8^a ed. Tirant Lo Blanch, 2010.

LÓPEZ MUÑIZ M. G., *Los derechos de la persona en la ley de protección de datos personales*, visto en CARRASCOSA LÓPEZ, V. (Director), *Informática y*

Derecho, II Congreso internacional de Informática y Derecho, 1ª ed. Universidad Nacional de Educación a Distancia, Mérida, Sevilla, 1996.

LORCA NAVARRETE, J. F. y LORCA MARTÍN DE VILLODRES, M. I., *Derechos fundamentales y jurisprudencia*, 4ª ed. PIRÁMIDE, Madrid, 2010.

LOSANO y MARIO, G., *para una teoría general de las leyes sobre la protección de los datos personales*, CITEMA, vemos en IX encuentro, *implicaciones socio-jurídicas de las tecnologías de la información*, CITEMA, España, 1991.

LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales (cuadernos y debates)*, 1ª ed. Centro de estudios constitucionales, Madrid, 1993.

LUCAS MURILLO DE LA CUEVA, P., *La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad en el derecho a la autodeterminación informativa*, dirigido por Lucas Murillo de la Cueva, P. y Piñar Mañas, J. L., Fundación Coloquio Jurídico Europeo, Madrid, 2009.

LUCAS MURILLO DE LA CUEVA, P., *El Derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990.

LUCHAIRE, F., *La ayuda a los países subdesarrollados*, 1ª ed. Oikos-Tau, S. A., Barcelona, 1971.

LUIS MARÍA, B., *Disertación pronunciada en el Seminario Iberoamericano sobre la acción de "habeas data"*, Talca (Chile), 8 al 11 de abril de 1997 visto en PUCCINELLI, O., *El Habeas data en Indoiberoamérica*, Temis, Bogotá, 1999.

MANGAS MARTÍN, A. y LIÑAN NOGUERAS, D. J., *Instituciones y Derecho de la Unión Europea*, 4ª ed. Tecnos, S. A., Madrid, 2004.

MARTÍN RETORTILLO, L., DE OTTO, y PARDO, I., *Derechos fundamentales y constitución*, 1ª ed. Civitas S. A., Madrid, 1988.

MARTÍNEZ DE PISÓN, J., *Las generaciones de Derechos Humanos*, Visto en BETEGÓN, J., LAPORTA, F. J., RAMÓN DE PÁRAMO, J. y PRIETO SANCHÍS, L. (Coordinadores), *Constitución y derechos fundamentales*, Ministerio de la Presidencia, Secretaría General Técnica, Centro de Estudios Políticos y Constitucionales, Madrid, 2004.

MARTÍNEZ SOSPEDRA, M. (Coordinador), *La Constitución Española de 1978 después de su trigésimo Aniversario*, editora Tirant Lo Blanch, Valencia, 2010.

MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica a la autodeterminación informativa*, Thomson-Civitas, Madrid, 2004.

MAZZONI, A., *Protección de datos y videovigilancia*, visto en TRAVIESO, J. A., *Régimen Jurídico de los Datos Personales*, tomo I, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

MIGUEL A., E. y CALOGERO, P., “*Habeas data*” *El derecho a la intimidad frente a la revolución informática*, Buenos Aires, Depalma, 1996, pp. 33 y 34, visto en PUCCINELLI, O., *El Habeas data en Indoiberoamérica*, Temis, Bogotá, 1999.

MILLER, A. R., *The assault on Privacy*, The University of Michigan Press Ann Arbor, 1971.

MILLÉ, A., *informaciones de carácter personal Derecho Comparado y prospectiva*, visto en CARRASCOSA LÓPEZ, V. (Director), *Informática y Derecho, II Congreso internacional de Informática y Derecho*, 1ª ed. Universidad Nacional de Educación a Distancia, Mérida, Sevilla, 1996.

MIR, P., *Poema nacionales*, editora Búho, Santo Domingo, 1984.

MOLINERO, C., *La información y los Derechos Personales*, 1ª ed. Dirosa, Barcelona, 1977.

MUÑOZ CONDE, F., *Derecho penal parte especial*, 18ª ed. Tirant Lo Blanch, Valencia, 2010.

MUÑOZ FRANCO, G., *La Protección de Datos Personales en México*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

MURILLO VILLAR, A. y BELLO PAREDES, S. (Coordinadores), *Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías*, 1ª ed. Servicio de Publicaciones Universidad de Burgos, Burgos, 2005.

NOGUEIRA ALCALÁ, H., *Autodeterminación informativa y habeas data en Chile e información comparativa*, Anuario de Derecho Constitucional Latinoamericano, 2005.

NUGTER, A. M. C., *Transborder Flow of Personal Data within the European Community*, Kluwe, Deventer, 1990.

OTHON SIDOU, J. M., *Las nuevas figuras del derecho procesal constitucional brasileño: mandato de injucao y habeas data*, Boletín Mexicano de Derecho Comparado (Traducción de Flx Zamudio, H), núm. 70, UNAM, México, 1991.

OCDE., *Tratados Internacionales Flujo Internacional de datos (Recomendación de la OCDE de 23 de septiembre de 1980)*, 1ª ed. Presidencia del gobierno, Madrid, 1982.

PASTOR RIDRUEJO, J. A., *Curso de Derecho Internacional Público y Organizaciones Internacionales*, Tecnos, Madrid, 2009.

PATRÓN BEDOYA, P. y BUENO DE MATA, F. (Coordinadores), *Nuevas tecnologías y justicia 2.0*, 1ª ed. Parlamento de Extremadura, Extremadura, 2013.

PEARSON, F. S., *Relaciones Internacionales*, McGraw-Hill, Bogotá, 2003.

SAGÜÉS, N. P., *Subtipos de habeas data*, en jurisprudencia argentina, 1995, pp. 31 y ss.; tomado de NOGUEIRA ALCALÁ, H., *Autodeterminación informativa y habeas data en Chile e información comparativa*, Anuario de Derecho Constitucional Latinoamericano, 2005.

PEERS S., HARVEY, T., KENNER, J. & WARD, A. (Eds.), *The EU Charter of Fundamental Rights. A Commentary*. Oxford and Portland: Hart Publishing, 2014.

PENDÁS, B. y BALSEGA, P., *El Derecho a la Intimidad*, Civitas, Madrid, 1995.

PEREIRA, J., *Diccionario de Relaciones Internacionales y Política Exterior*, Ariel S. A., Barcelona 2008.

PÉREZ GÓMEZ, E. y CRESPO LÓPEZ, A., *La protección de datos en los centros de enseñanzas*, 1ª ed. Aranzadi S. A., Navarra, 2007.

PÉREZ LUÑO, A., *Derechos humanos, Estado de derecho y constitución*, Tecnos, Madrid, p. 354; visto en BEATRIZ CALLE, S., *Apuntes sobre la protección de datos personales a la luz de la actual norma de habeas data en Colombia*, Colombia, 2009.

PÉREZ-LUÑO, A. E., *Internet y los Derechos Humanos*, Derecho y conocimiento, vol. 2, Facultad de Derecho. Universidad de Huelva, España. Disponible en: <https://core.ac.uk/download/pdf/60638165.pdf>. (Última consulta en línea 26 de junio 1018).

PÉREZ-LUÑO, A. E., *Internet y la garantía de los derechos fundamentales, visto en* MURILLO VILLAR, A. y BELLO PAREDES, S. (Coordinadores), *Estudios Jurídicos sobre la sociedad de la información y nuevas tecnologías*, 1ª ed. Servicios de Publicaciones Universidad de Burgos, Burgos, 2005.

PÉREZ-LUÑO, A. E., *Intimidad y protección de datos personales: Del habeas Corpús al habeas data*, edición a cargo de Luís García San Miguel Rodríguez-Arango, estudio sobre el derecho a la intimidad, Tecnos, Madrid., 1992.

PÉREZ LUÑO A. E., *El derecho a la intimidad*, Visto en BETEGÓN, J., LAPORTA, F. J., RAMÓN DE PÁRAMO, J. y PRIETO SANCHÍS, L. (Coordinadores), *Constitución y derechos fundamentales*, Ministerio de la Presidencia, Secretaría General Técnica, Centro de Estudios Políticos y Constitucionales, Madrid, 2004.

PÉREZ-LUÑO, A. E., *Libertad informática y leyes de protección de datos personales*, edición a cargo de LOSANO, M., Pérez Luño, A. y Guerrero Mateus, M., *Centro de Estudios Constitucionales*, Madrid, 1989.

PÉREZ LUÑO, A. E., *Panorama general de la legislación española sobre protección de datos*, 1991, p. 25, tomado de *IX encuentro implicaciones socio-jurídicas de las tecnologías de la información*, CITEMA, España, 1991.

PÉREZ-LUÑO, A. E., *La LORTAD: Entre las luces y las sombras (Conferencia impartida del 14 al 16 de julio de 1993, durante el XXII Curso de Informática y Derecho, celebrado en el Centro Regional de la UNED)*, visto en CARRASCOSA LÓPEZ, V. (Director), *Informática y Derecho 6-7*, 1ª ed. Universidad Nacional de Educación a Distancia, Mérida, Sevilla, 1994.

PÉREZ-LUÑO, A. E., *Manual de Informática y Derecho*, Ariel, Barcelona, 1996.

PÉREZ MIRAS, J., *El derecho a la protección de datos y a la privacidad. Una perspectiva comparada entre la Unión Europea y Estados Unidos*, Universidad de Sevilla, España, 2018.

PÉREZ PONTE, M., *Facultades y atribuciones del órgano de control de la ley nacional de protección de datos personales 25,326*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo I, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

PERUZZOTTI, M., *El impacto de la ley de protección de los datos personales en el sector público*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

PEYDRO, F., *Privacidad: una mirada desde el marketing.*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

PIERINI LORENCE, T., *Habeas Data derecho a la Intimidad*, Universidad de Buenos Aires, Buenos Aires, 1999.

PINTO, M. (Compiladora), *Las fuentes del Derecho Internacional en la era de la Globalización*, 1ª ed. Editorial Universitaria de Buenos Aires, Buenos Aires, 2009.

PIÑAR MAÑAS, J. L. y RECIO GAYO, M., *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, 1ª ed. Wolters Kluwer España, S. A., Madrid, 2018.

PIÑAR MAÑAS, J. L., *La Red Iberoamericana de Protección de Datos: Declaraciones y Documentos*. Editorial Tirant Lo Blanch, Valencia, 2006.

PIÑAR MAÑAS, J. L., *El derecho fundamental a la protección de datos personales. Contenido esencial y retos actuales. En torno al nuevo Reglamento de protección de datos. Legislación de protección de datos.* Iustel. Madrid 2008.

PIÑAR MAÑAS, J. L., *Protección de datos: origen, situación actual y retos de futuro en el Derecho a la autodeterminación informativa*, dirigido por LUCAS MURILLO DE LA CUEVA, P. y PIÑAR MAÑAS, J. L., Fundación Coloquio Jurídico Europeo, Madrid, 2009.

PIÑOL RULL, J. L., “*Los flujos internacionales de datos: aproximación a su regulación jurídica*”, UNED, t.IV, Barbastro, 1987.

PUCCINELLI, O., *El habeas data en Indoiberoamérica*, 1ª ed. Temis S. A., Bogotá, 1999.

PUCCINELLI, O., “Versiones, tipos, subtipos y subespecies de habeas data en el derecho latinoamericano (Un intento clasificador con fines didácticos)”, *Revista Iberoamericana de derecho procesal constitucional (Proceso y Constitución*, núm. 1, editorial Porrúa / Instituto Iberoamericano de Derecho procesal Constitucional, México, 2004.

QUESADA RODRÍGUEZ, A., *Protección de datos y telecomunicaciones convergentes*, 1ª ed. Agencia Española de Protección de Datos, Madrid, 2015.

RAMÍREZ MORILLO, B., *Derecho Constitucional Dominicano, Centenario*, S. A., Santo Domingo, 2010.

RAY GUEVARA, M., *Opinión constitucional*, 1ª ed. Amigo del Hogar, Santo Domingo, 2014.

RECALDE DIEZ, J. R. y AUSEMS, E., *Presentación 27 Informática judicial y protección de datos personales*, 1ª ed. Servicio central de Publicaciones del Gobierno Vasco, Vitoria –Gasteiz, 1994.

RECALDE DIEZ, J. R., (Presentación), *Informática Judicial y Protección de Datos Personales*, 1ª ed. Servicio Central de Publicaciones del Gobierno Vasco, Vitoria- Gasteiz, 1994.

REBOLLO DELGADO, L., y SERRANO PÉREZ, M. M., *Manual de protección de datos*, 2ª ed. Dykinson, Madrid, 2017.

REMOLINA ANGARITA, N., *Recolección internacional de datos personales: un reto del mundo Post modernos*, 1ª ed. Agencia Española de Protección de Datos, Madrid, 2015.

REMOLINA ANGARITA, N., *Insuficiencia de la regulación latinoamericana frente a la recolección internacional de datos personales a través de Internet*, Quaestiones Disputatae 2, Pontificia Universidad Javeriana, Facultad de Ciencias Jurídicas, Colección Doctorado en Ciencias Jurídicas, Bogotá, 2011.

REMOLINA ANGARITA, N., *realidades y reflexiones sobre el tratamiento de datos personales en Latinoamérica*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

RIPO y CARULLA, S. (Coordinadores), *La protección de los datos personales: regulación nacional e internacional de la seguridad informática (jornadas organizadas por la Universidad Pompeu Fabra)*, 1ª ed. Generalitat de Catalunya, Catalunya, 1993.

ROBINSON, P., *Legal Issues Raises by TDF*, CUSLJ, vol.11, 1986.

RODRÍGUEZ ABASCAL, L., *El derecho de autodeterminación en la España constitucional*, visto en BETEGÓN, J., LAPORTA, F. J., RAMÓN DE PÁRAMO, J. y PRIETO SANCHÍS, L. (Coordinadores), *Constitución y derechos fundamentales*, Ministerio de la Presidencia, Secretaría General Técnica, Centro de Estudios Políticos y Constitucionales, Madrid, 2004.

RODRÍGUEZ VILLAR, P., *La protección de datos personales y la esfera de actuación de las autoridades de control*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo I, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

ROCHA VALENCIA A. y PRECIADO CORONADO, J. (Coordinadores), *Proyectos y Estrategias de integración América Latina y el Caribe en el contexto de América del Norte y Europa*, 1ª ed. Cucsh-UdeG, Guadalajara, Jalisco, México, 2008.

RODRÍGUEZ, N., *Derecho de la información*, 2ª ed. Media byte, S. A., Santo Domingo, 2008.

RODRÍGUEZ, N., *Elementos de derecho de la información*, 1ª ed. Santo Domingo, 2004.

ROMERO COLOMA, A. M., *Libertad de Información frente a otros Derechos en conflicto, Honor, Intimidación y presunción de Inocencia*, 1ª ed. Civitas, Madrid, 2000.

ROTONDO, F., *Protección de Datos Personales en la República de Uruguay*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

SACHS, J., *El fin de la pobreza*, 2ª ed. Random House Mondadori, S. A., (DEBATE), Barcelona, 2005.

SAGÜÉS, N. P., *Derecho Procesal Constitucional. Acción de Amparo*, Astrea, Buenos Aires, 1995.

SANTIAGO RIPOL, I. C. (Coordinador), *La protección de los datos personales: regulación nacional e internacional de la seguridad informática (jornadas*

organizadas por la Universidad Pompeu Fabra), 1ª ed. Generalitat de Catalunya, Catalunya, 1993.

SASSEN, S., *Los espectros de la globalización*, 1ª ed. (en español) Fondo de cultura económica de Argentina, S. A., Buenos Aires, 2003.

SEGURA, P., *Internet de las cosas*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo I, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

SEMPERE RODRÍGUEZ, C., *Artículo 18 CE*, visto en O. ALZAGA VILLAMIL (Director), *Comentarios a la Constitución española de 1978*, Tomo II, Edersa, Madrid, 1997.

SEN, A. y KLIKSBURG, B., *primero la gente*, 1ª ed. Deusto, Barcelona, 2007.

SERRANO PÉREZ, M. M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Cívitas-Thomson, Madrid, 2003.

SERVICIO CENTRAL DE INFORMÁTICA., *Informática Leyes de Protección de Datos*, Documentación Informática núm. 2, serie Verde /Legislación, 1ª ed. Presidencia del gobierno, Madrid, 1977.

SERVICIO CENTRAL DE INFORMÁTICA., *Informática Leyes de Protección de Datos (II)*, Documentación Informática, núm. 3, serie Verde /Legislación, 1ª ed. Presidencia del gobierno, Madrid, 1983.

STEINER, C. & URIBE, P. (Coordinadores), *Convención Americana sobre Derechos Humanos*, comentada, 1ª ed. D. R. Konrad Adenauer Stiftung, República Federal de Alemania. Disponible en:

<http://www.corteidh.or.cr/tablas/30237.pdf>. (Última consulta en línea 5 de febrero 2019).

SOSA PÉREZ, R., *Constitución comentada*, Fundación Institucionalidad y Justicia inc. (FINJUS), Santo Domingo, 2011.

TANENBAUM, A., *Estructuras de datos en C*, Prentice Hall Hispanoamericana S. A., México, 1993.

TÉLLEZ AGUILERA, A., *La protección de datos en la Unión Europea: Divergencias normativas AS y anhelos unificadores*, EDISOFER S. L, Madrid, 2002, p. 329.

TEAHAN, M., *La protección de datos: Marketing y publicidad*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

TRAVIESO, J. A., *Régimen Jurídico de los Datos Personales*, tomo I, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

TRAVIESO, J. A., *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

TREVIJANO SÁNCHEZ, P. G. (Presidente consejo de redacción), *Constitución y Derechos Fundamentales*, editora La Ley, edición septiembre 2009.

TRONCOSO REIGADA, A., *La protección de datos personales en busca del equilibrio*, Tirant Lo Blanch, Valencia, 2011.

TRONCOSO REIGADA, A. (Director), *Comentario de la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno*, 1ª ed. Aranzadi, S.A.U, Pamplona, 2017.

ULL PONT, E., *Derecho público de la informática (Protección de datos de carácter personal)*, 1ª ed. Uned, Madrid, 2000.

ULL PONT, E., *Derecho público de la informática (Protección de datos de carácter personal)*, 2ª ed. Uned, Madrid, 2003.

URBAYEN, M., *Vida Privada e Información, un conflicto permanente*, Eunsa, Pamplona, 1997.

VASAK, K. (Editor general), *Las dimensiones internacionales de los derechos humanos*, 1ª ed. Ediciones Serbal, S. A., Barcelona, 1984.

VELASCO SAN PEDRO, L., *MERCOSUR y la Unión Europea: dos modelos de Integración económica*, 1ª ed. Lex Nova, Valladolid, 1988.

VERITAS FORMACIÓN, B., *Ley de protección de datos personales*, 1ª ed. Fundación Confemetal (F. C.), Madrid, 2010.

VIETOR, R., *Cómo compiten los países, estrategia, estructura y gobierno en la economía global*, 1ª ed. Deusto, Barcelona, 2008.

VILA, J., *La protección de datos personales: responsabilidad social empresarial con controles y auditorías*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

VIZCAÍNO CALDERÓN, M., *Comentario a la ley orgánica de protección de datos de carácter personal*, 1ª ed. Cívitas Ediciones, S. L., Madrid, 2001.

WARREN, S. & BRANDEIS, L., *The Right to Privacy*, *Harvard Law Review*, vol. IV, núm. 5, 15 diciembre 1980. Una traducción castellana del mismo se puede encontrar en PENDÁS, B. Y BALSEGA, P., *El derecho a la Intimidad*, Civitas, Madrid, 1995.

WENCESLAO, V., *Historia del derecho dominicano*. Santo Domingo, 2006.

WHITAKER, R., *El fin de la privacidad*, 1ª ed. Paidós Ibérica, S. A., Barcelona, 1999.

WIONCZEK, M., *Inversión y tecnología extranjera en América Latina*, 1ª ed. Joaquín Mortiz, S. A., Tabasco, México, 1971.

ZAMBRANO, F., *El procedimiento de amparo constitucional (colección de textos legislativos venezolanos, núm.2)*, Atenea, Caracas, 2001.

ZAMUDIO SALINAS, D. L., *La Ley de Protección de Datos Personales Peruana. Reflexiones Comparativas.*, visto en TRAVIESO, J. A. (Director), *Régimen Jurídico de los Datos Personales*, tomo II, 1ª ed. ABELEDOPERROT S. A., Buenos Aires, 2014.

Habeas data en bancos de datos., privacidad, personalidad e ciudadanía no Brasil actual., 1ª ed. Lumen Juris, Rio de Janeiro, 2002.

Artículos en Revistas

ACOSTA DE LOS SANTOS, H., “Protección de Datos en la República Dominicana”, en *Revista iberIUS*, monográfico dedicado a *la protección de datos personales*, núm.2, agosto, 2006. Disponible en:

http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/Centro AnalisisDocumentacionJudicial/revista%20iberius/IberIUS_02.pdf. (Última

consulta en línea 24 de agosto 2013).

ALDECOA, F., “Por un mayor compromiso de la Comunidad Europea con América Latina, seminario sobre las relaciones económicas entre América Latina y la Comunidad Económica Europea (CEE)”, fundación Friedrich Ebert, Madrid, 1988.

ÁLVARE CARO, M., “Reflexiones sobre la sentencia del TJUE en el asunto Mario Costeja (C-131/12) sobre derecho al olvido”, *Revista española de Derecho Europeo*, núm. 51, Julio-Septiembre, Thomson Reuters, 2014.

ÁLVARE CARO, M. y RECIO GAYO, M., “la declaración de invalidez del Acuerdo Puerto Seguro entre la UE y los EEUU por el TJUE (C-362/14)”, *Revista española de Derecho Europeo*, núm. 57, Enero-Marzo 2016, Thomson Reuters, 2016.

ANSELMO MARTINO, A., “Asecho del derecho a la privacidad en América Latina”, *Revista Internacional de Protección de Datos personales*, núm. 1 Julio, universidad de los Andes, Bogotá, 2012.

BAZÁN, V., “El habeas data, su autonomía respecto del amparo y la tutela del derecho fundamental de autodeterminación informativa”, *Anuario de Derecho Constitucional Latinoamericano*, Año XVIII, Bogotá, 2012.

BAZÁN, V., “El habeas data, su autonomía respecto del amparo”, *Anuario de Derecho Constitucional Latinoamericano* año XVIII, Bogotá, 2012. Disponible en: <http://www.corteidh.or.cr/tablas/r29666.pdf>. (Última consulta en línea 23 de marzo 2018).

BEATRIZ CALLE, S., “Apuntes jurídicos sobre la protección de datos personales a la luz de la actual norma de *habeas data* en Colombia”, *Revista Anuario Jurídico*, Colombia, 2009.

BURRI, E., “Discurso inaugural presidente de CODETEL”, *Revista Noticias CODETEL*, mayo 1992.

CALATAYUD SORIANO, D., “Deconstruyendo al Leviat@n: hacia un sistema de gobernanza digital”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 33, Septiembre - Diciembre, 2013.

CIFUENTES, M., “El Habeas data en Colombia”, en Derecho PUC. *Revista de la Facultad de Derecho de la Pontificia Universidad Católica del Perú*, núm. 51, diciembre de 1997, publicado en 199, Lima, p. 122 tomado de BAZÁN, V., “El habeas data, su autonomía respecto del amparo”, *Anuario de Derecho Constitucional Latinoamericano año XVIII*, Bogotá, 2012. Disponible en: <http://www.corteidh.or.cr/tablas/r29666.pdf>, (Última consulta en línea 23 de marzo 2018).

DÍA DÍAZ, E., “El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones”, *Revista Aranzadi doctrinal*, núm. 6, 2016.

FERNÁNDEZ W, A., *El derecho a saber*, Diario Libre, 2013.

FROSINI, V., “Bancos de datos y tutela de la persona”, *Revista de Estudios Políticos (Nueva Época)*, núm. 30, Noviembre-Diciembre 1982. Disponible en: <file:///C:/Users/pc/Downloads/Dialnet-BancosDeDatosYTutelaDeLaPersona-26724.pdf>. (Última consulta en línea 12 de noviembre 2019).

GARCÍA DE PABLOS, J., “La transferencia de datos fuera de la Unión Europea”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 40, Enero-Abril 2016, Madrid, 2016.

GARECA PERALES, P., “El habeas data en la Constitución de Bolivia”, *Anuario de Derecho Constitucional Latinoamericano*, 2005.

GARRIGA DOMÍNGUEZ, A., “La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento general de protección de datos de la Unión Europea”, *Revista Derechos y Libertades*, núm. 38, Época II, enero 2018, Madrid, 2016.

GONZÁLEZ MURUA, A. R., “Comentarios a la STC 254/1993, de 20 de Julio. Algunas reflexiones en torno al art. 18.4 de la Constitución y la protección de datos personales”, *Revista Vasca de Administración Pública*, núm. 37.

GUILLÉN CATALÁN, R., “La vulneración de la protección de datos personales por las redes sociales”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 45, Septiembre-Diciembre, Madrid, 2017.

HEREDERO HIGUERAS, M., “La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la ley del Censo de población de 1983”, *Revista de Documentación Administrativa (1958-2005)*, núm. 198.

LÓPEZ BOFILL, H., “Reforma estatutaria y protección de datos personales”, en *Revista digital Datos personales*. núm. 19, enero 2006.

LÓPEZ JIMÉNEZ, D. y VARGAS, P., “La autorregulación del comercio electrónico en el ámbito de América Latina”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 40, Enero-Abril, 2016, Madrid, 2016.

MARCOS DEL RINCÓN, J., “La administración electrónica en las leyes 39 y 40/2015 de 1 de octubre. Una visión de conjunto”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 45, Septiembre-Diciembre, Madrid, 2017.

MAYORGA JÁCOME, T. C., GARCÍA JIMÉNEZ, M., CARRIÓN JUMBO, J. L., YARAD JEADA, P. V. y DURET GUTIÉRREZ, J. F., “Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos”, *Revista Científica, Dominio de la Ciencia*, vol. 5, núm. 1, 2019 Disponible en: [file:///C:/Users/pc/Dropbox/Documentos/Dialnet-HistoriaDeLaNormativaReguladoraDeLaProteccionDeDat-6869937-1%20\(1\).pdf](file:///C:/Users/pc/Dropbox/Documentos/Dialnet-HistoriaDeLaNormativaReguladoraDeLaProteccionDeDat-6869937-1%20(1).pdf). (Última consulta en línea 23 de Octubre 2019).

NOGUEIRA ALCALÁ, H., *Autodeterminación Informativa y habeas data en Chile e información comparativa*, Anuario de Derecho Constitucional Latinoamericano, 2005.

PAVÓN PÉREZ, J. A., “La Protección de Datos Personales y el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos Personales”, *Anuario de la Facultad de Derecho*, 2001. Disponible en:

<https://dialnet.unirioja.es/servlet/articulo?codigo=831270>. (Última consulta en línea 24 de octubre 2017).

PÉREZ LUÑO, A. E., “Informática y Libertad. Comentario al artículo 18.4 de la Constitución Española”, *Revista de Estudios Políticos (Nueva Época)*, núm. 24, Noviembre-Diciembre, 1981.

PÉREZ-LUÑO, A. E., “La protección de la intimidad frente a la informática en la Constitución Española de 1978”, *Revista de Estudio Político*, Nueva Época, núm. 9, mayo-junio 1979.

PÉREZ LUÑO, A. E., “Las generaciones de derechos Humanos”, *Revista del Centro de Estudios Constitucionales*, núm. 10, Septiembre-Diciembre 1991.

PLAZA PENADÉS, J., “El nuevo modelo de protección de datos personales europeo y el modo de obtener un consentimiento lícito”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 44, Mayo-Agosto 2017, Madrid, 2017.

PLAZA PENADÉS, J., “Doctrina del tribunal de justicia de la Unión Europea sobre protección de datos y derecho al olvido”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 35, Mayo-Agosto, 2017, Madrid, 2014.

PLAZA PENADÉS, J., “Implementando el nuevo reglamento general europeo de protección de datos”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 43, Enero-Abril, 2017, Madrid.

PLAZA PENADÉS, J., “Los derechos fundamentales en Internet”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 36, Septiembre-Diciembre, Madrid, 2014.

PLAZA PENADÉS, J., “El proyecto de la nueva ley orgánica de protección de datos de carácter personal”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 46, Enero-Abril, Madrid, 2018.

PLAZA PENADÉS, J., “Doctrina del tribunal de justicia de la unión europea sobre protección de datos y derecho al olvido”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 35, Mayo-Agosto, Madrid, 2014.

PUCCINELLI, O., “Versiones, tipos, subtipos y subespecies de habeas data en el derecho latinoamericano (Un intento clasificador con fines didácticos)”. *Revista Iberoamericana de derecho procesal constitucional* (Proceso y Constitución, núm. 1), Editorial Porrúa / Instituto Iberoamericano de Derecho procesal Constitucional, México, 2004.

PUCCINELLI, O., “Tipos y subtipos de habeas data en América Latina”. Disponible en: <https://www.astrea.com.ar/resources/doctrina/doctrina0158.pdf>. (Última consulta en línea 1 de julio 2018).

RALLO LOMBARTE, A., “Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma”, UNED, *Revista de Derecho político* núm. 85, Septiembre-Diciembre 2012.

REMOLINA ANGARITA, N., “Ámbito Jurídico”, núm. 326, julio-agosto de 2011.

SÁNCHEZ DE DIEGO, M., “El «día después» de la ley de transparencia”, *Revista Jurídica de Castilla y León*, núm. 33, 2014.

SERRANO MAÍLLO, I., MARTÍNEZ PASTOR, E. y BELTRÁN ORENES, P., “Una revisión crítica de la Ley española 19/2013”, *Revista Transparencia & Sociedad*, núm. 5-Diciembre 2017.

TRONCOSO REIGADA, A., “El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio en los modelos de protección de datos a nivel internacional”, *Revista Internacional de Protección de Datos Personales*, Universidad de los Andes, Bogotá, núm.1, Julio-Diciembre 2012.

VILLAVERDE MENÉNDEZ, I., “Protección de datos personales, derecho a ser informado y autodeterminación informática a propósito de la STC 254/1993”, *Revista de Derecho Constitucional*, Mayo-Agosto 1994.

VÁZQUEZ DE CASTRO, E., “Derecho al honor en Internet, anonimato y responsabilidad de los prestadores de servicios: ¿evolución e involución?”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 44, Mayo-Agosto, Madrid, 2017.

VÁZQUEZ DE CASTRO, E., “La autonomía del paciente y la protección de datos personales sensibles. Especial referencia a la historia clínica electrónica”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 36, Septiembre-Diciembre, Madrid, 2014.

WILLMAN RUPERTO, W. R., “Contenido y alcances del habeas data en Bolivia”, *Anuario de Derecho Constitucional Latinoamericano*, 2006.

Congresos

BARINAS UBIÑAS, B., *Los derechos fundamentales de acceso a la información pública y protección de datos personales: una aproximación a la pertinencia de su vinculación normativa en República Dominicana*, Congreso

Internacional Protección Internacional de los Derechos Fundamentales: dimensión pública y privada, Governance, Donostia, 2012.

GONZÁLEZ FUSTER, G., *El Comité Europeo de Protección de Datos*, exposición en la mesa redonda *autoridades de control e implementación de la normativa en materia de protección de datos*, Congreso Internacional sobre el Impacto del Reglamento Europeo de Protección de Datos: análisis nacional y comparado, Castellón de la Plana, Universitat Jaume I, 17 y 18 de mayo 2018.

GARCÍA MAHAMUT, R., discurso Inaugural, Congreso Internacional sobre “*el Impacto del Reglamento Europeo de Protección de Datos: análisis nacional y comparado*”, Universitat Jaume I, Castellon, 17 y 18 de mayo de 2018.

MEDINA GUERRERO, M., *La posición de las autoridades de control en el nuevo marco regulador de la protección de datos*, Congreso Internacional sobre el Impacto del Reglamento Europeo de Protección de Datos: Análisis Nacional y Comparado, Universitat Jaume I, Castellón de la Plana, 18 de mayo 2018.

LUCAS MURILLO DE LA CUEVA, P., *Marco Jurídico Europeo en la Protección de Datos*, exponente cursos de Verano UPV/EHU nuevo escenario tras la aprobación del Reglamento General de Protección de Datos, Palacio Miramar, Donostia, San Sebastián, 22 de junio, 2017.

PIÑAR MAÑAS, J. L., *Adecuación de la legislación española al nuevo escenario de la protección de datos.*, exponente cursos de Verano UPV/EHU Nuevo escenario tras la aprobación del Reglamento General de Protección de Datos, Palacio Miramar, Donostia, San Sebastián, 22 de junio, 2017.

RALLO, A., *El impacto del reglamento europeo de protección de datos en España*, mesa redonda Análisis comparado del impacto del RGPD en los Estados miembros, Congreso Internacional sobre el Impacto del Reglamento Europeo de Protección de Datos: análisis nacional y comparado, Universitat Jaume I, Castellon, 17 y 18 de mayo de 2018.

URIA ETXEBARRIA, M., *Protección de datos y transparencia: Compañeros de viaje.*, Discurso inaugural curso de verano, Agencia Vasca de Protección de Datos, Donostia, San Sebastián, 21 de junio, 2018. Disponible en: <http://www.avpd.euskadi.eus/webcast/s04-5273/es/>. (última consulta en línea 10 de agosto 2018).

Tesis doctorales

PÉREZ MIRAS, J., *El derecho a la protección de datos y a la privacidad. Una perspectiva comparada entre la Unión Europea y Estados Unidos*, Universidad de Sevilla, España, 2018.

RODRÍGUEZ MARCANO, E. R., *El Derecho a la autodeterminación Informativa en Venezuela*, Tesis doctoral, Universidad nacional de educación a distancia, Madrid, 2013.

GONZÁLEZ MURUA, A. R., *La Agencia Vasca de Protección de Datos y el Estado de las Autonomías. Estudio de su naturaleza jurídica y sus funciones en una perspectiva de Derecho comparado*, Servicio editorial UPV/EHU, Leioa, 2010.

Conferencias, Asambleas, Declaraciones, Propuestas

(2017) *Taller nuevo marco normativo para la protección de los datos personales: los estándares iberoamericanos*. Disponible en:

http://www.redipd.es/actividades/talleres/CartagenadeIndias_2017/index-ides-idphp.php. (Última consulta en línea 14 de junio 2017).

(2017) Red Iberoamericana de Protección de Datos., *Estándares de protección de datos personales para los Estados Iberoamericanos*, Santiago de Chile, 20 de junio 2017. Disponible en:

http://inicio.inai.org.mx/nuevo/Estandares%20PDP_Ibero.pdf. (Última consulta en línea 29 de junio 2017).

(2016) *Cumbre Internacional de la Alianza para el Gobierno Abierto*. Disponible en: <http://datos.gob.es/es/eventos/cumbre-internacional-de-la-alianza-para-el-gobierno-abierto-2016>. (Última consulta en línea 30 de mayo 2018).

(2016) *XIV Encuentro Iberoamericano de Protección de Datos, celebrado el 8 de junio en Santa Marta, Colombia 2016*. Disponible en:

http://www.redipd.es/documentacion/common/Declaracion_RIPD_XV_encuentro.pdf. (Última consulta en línea 06 de julio del 2017).

(2015) *27º Conferencia Internacional de Comisionados de Protección de Datos; La protección de datos personales y de la intimidad en un mundo globalizado: un derecho universal que respeta diversidades*. Disponible en:

https://icdppc.org/wp-content/uploads/2015/06/montreux_declaration-Spanish.pdf. (Última consulta en línea 06 de julio del 2017).

(2015) *86 Periodo Ordinario de Sesiones, Informe del Comité Jurídico Interamericano, privacidad y protección de datos personales*, OEA/Ser.Q. CJI/doc. 474/15 rev.2, 26 marzo 2015, Río de Janeiro, Brasil. Disponible en: http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf. (Última consulta en línea el 15 de agosto 2017).

(2014) *84 Períodos Ordinarios de Sesiones., privacidad y protección de datos*, OEA/Ser.Q, CJI/doc.450/14, 25 de febrero de 2014, Río de Janeiro, Brasil. Disponible en:

http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_documentos_referencia_CJI_doc_450-14.pdf. (Última consulta en línea 14 de agosto 2017).

(2014) BARIÑAS UBIÑAS, B., Taller Impulso normativo de la Protección de Datos Personales en Centroamérica y el Caribe, *Historial Ley Orgánica sobre protección de datos de carácter personal 2013*, Antigua, Guatemala, 14 de febrero de 2014. Disponible en:

http://www.redipd.org/actividades/talleres/La_Antigua_02_2014/common/Ponencias_Taller_La_Antigua./REPUBLICA_DOMINICANA..pdf. (Última consulta en línea 14 de agosto 2017).

(2013) *35 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad*: 23-26, septiembre, Varsovia, Polonia 2013. Disponible en: <http://www.a pep.es/wp-content/uploads/downloads/2013/10/resoluciones-35-conferencia-autoridades-PD.pdf>. (Última consulta en línea 14 de junio 2017).

(2013) *Asamblea General, Cuadragésimo Tercer Período Ordinario de Sesiones*, OEA/Ser.P, AG/RES. 2811 (XLIII-O/13), 6 de junio 2013, La Antigua, Guatemala. Disponible en: www.oas.org/es/sla/docs/ag06222s04.pdf. (Última consulta en línea 11 de agosto 2017).

(2012) *Propuesta de Declaración de principios de privacidad y protección de datos personales en las Américas*, CJI/doc. 402/12 rev.2, 9 de marzo 2012. (Última consulta en línea 13 de agosto 2017).

(2012) *Estudio Comparativo: protección de datos en las Américas Diversos regímenes jurídicos, políticas y mecanismos de aplicación existentes para la protección de datos personales, incluidas leyes, reglamentos y autorregulación nacionales*, Consejo Permanente de la Organización de los Estados Americanos, comisión de asuntos jurídicos y políticos, OEA/Ser.G, CP/CAJP-3063/12, 3 abril 2012. Disponible en: www.oas.org/es/sla/ddi/docs/cp-cajp-3063-12.pdf. (Última consulta en línea 13 de agosto 2017).

(2012) *Declaración del X Encuentro de la Red Iberoamericana de Protección de Datos*, 22 de octubre, Punta del Este, Uruguay, 2012. Disponible en:

www.redipd.es/documentacion/common/declaracion_2012_X_encuentro_es.pdf
 (Última consulta en línea 16 de julio del 2017).

(2012) *Declaración del X Encuentro de la Red Iberoamericana de Protección de Datos*, 22 de octubre, Punta del Este, Uruguay, 2012. Disponible en: <http://www.redipd.es/actividades/encuentros/X/common/pdfs/DeclaracionXEIPD.pdf>. (Última consulta en línea 12 de junio 2017).

(2012) *Propuesta de Declaración de principios de privacidad y protección de datos personales en las Américas*, OEA/Ser. Q/CJI/RES.186 (LXXX-O/12), 9 de MARZO 2012. México, D.F., México. Disponible en: www.oas.org/es/sla/cji/docs/CJI-RES_186_LXXX-O-12.pdf. (Última consulta en línea 12 de agosto 2017).

(2012) *XXII Conferencia Internacional de Jefe de Estado., Declaración de Cádiz*, 16 y 17 de noviembre 2012, Colombia. Disponible en: <http://www.oei.es/histórico/xxiicumbredec.htm> . (Última consulta en línea 12 de abril 2017).

(2011) *33 Conferencia Internacional de Comisionados de Privacidad y Protección de Datos*. Disponible en: http://www.redipd.es/documentacion/common/declaracion_2011_IX_encuentro_es.pdf. (Última consulta en línea 09 de mayo 2017).

(2011) *Propuesta de Declaración de principios de privacidad y protección de datos personales en las Américas*, 26 mayo San Salvador, El Salvador, 2011; Disponible en: http://www.oas.org/es/sla/cji/docs/CJI-doc_402_12_rev2.pdf. (Última consulta en línea 12 de agosto 2017).

(2011) *Comentarios preliminares sobre una declaración de principios para la protección para la protección de la privacidad y de los datos personales en las Américas*, Documento CJI/doc.382/11. Disponible en:

http://www.oas.org/es/sla/cji/docs/CJI-doc_382-11.pdf. (Última consulta en línea 12 de agosto 2017)

(2011) *Comisión de asuntos jurídicos y políticos, consejo permanente de la organización de los Estados americanos, cuestionario de legislación y prácticas sobre privacidad y protección de datos*, CP/CAJP-3026/11, 31 octubre 2011. Disponible en: www.oas.org/dil/esp/CP-CAJP-3026-11_esp.pdf. (Última consulta en línea 11 de agosto 2017).

(2011) *Comisión de asuntos jurídicos y políticos, principios y recomendaciones preliminares sobre la protección de datos*, OEA/Ser.G, CP/CAJP-2921/10 REV. 1 corr. 1, 17 octubre 2011. Disponible en: http://www.oas.org/dil/esp/cp-cajp-2921-10_rev1_corr1_esp.pdf. (Última consulta en línea 12 de agosto 2017).

(2011) *Consejo permanente de la Organización de los Estados americanos, principios y recomendaciones preliminares sobre la protección de datos (la protección de datos personales)*, OEA/Ser.G, CP/CAJP-2921/10 rev.1 corr.1, 17 de octubre 2011. Disponible en: www.oas.org/dil/esp/cp-cajp-2921-10_rev1_corr1_esp.pdf. (Última consulta en línea 14 de agosto 2017)

(2011) *Principios y recomendaciones preliminares sobre la protección de datos*, OEA/Ser.G, CP/CAJP-2932/11 rev.1, 13 abril 2011. Disponible en: http://www.oas.org/es/sla/ddi/docs/CP-CAJP-2921-10_rev1_corr1.pdf. (Última consulta en línea 11 de agosto 2017).

(2010) *Proyecto de principios y recomendaciones preliminares sobre la protección de datos (la protección de datos personales)*, CP/CAJP-2921/10 rev.1 corr.1, 17 octubre 2011. Disponible en: http://www.oas.org/dil/esp/cp-cajp-2921-10_rev1_corr1_esp.pdf. (Última consulta en línea 12 de agosto 2017).

(2010) *VIII Encuentro Iberoamericano de Protección de Datos., Declaración de México*, México 2010. Disponible en:

<http://www.redipd.es/actividades/encuentros/VIII/index-ides-idphp.php>. (Última consulta en línea 12 de junio 2017).

(2010) *VIII Encuentro Iberoamericano de Protección de Datos, Declaración de México*, México 2010. <http://www.redipd.es/actividades/encuentros/VIII/index-ides-idphp.php>. (Última consulta en línea 18 de agosto 2017).

(2009) *31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad*. Disponible en: <http://www.privacyconference2009.org/home/index-ides-idweb.html>. (Última consulta en línea 16 de julio 2017).

(2009) *Declaración conjunta de Madrid sobre la Protección de Datos Personales, Madrid*, 3 de noviembre de 2009. Disponible en: http://www.redipd.es/documentacion/common/declaracion_2009_VII_encuentro_es.pdf. (Última consulta en línea 08 de junio 2017).

(2009) *XIX Cumbre Iberoamericana, Declaración de Lisboa*, 30 de noviembre y 1 de diciembre de 2009. Disponible en: <http://www.oei.es/histórico/ixiiicumbreddec.htm>. (Última consulta en línea el 11 de abril 2017).

(2008) *XVIII Cumbre Iberoamericana, Declaración de El Salvador, 29 a 31 de octubre, San Salvador, El Salvador*. Disponible en: <http://www.oei.es/histórico/ixiiicumbreddec.htm>. (Última consulta en línea el 11 de abril 2017).

(2007) *V Encuentro Iberoamericano de Protección de datos, Declaración de Lisboa*. Disponible en: <http://www.redipd.es/actividades/encuentros/V/index-ides-idphp.php>. (Última consulta en línea 08 de junio del 2017).

(2005) *Declaración de Montreux "La protección de datos personales y de la intimidad en un mundo globalizado: un derecho universal que respeta diversidades"*, Suiza 14-16 de septiembre de 2005. Disponible en:

https://icdppc.org/wp-content/uploads/2015/06/montreux_declaration-spanish.pdf . (Última consulta en línea 17 de mayo 2017).

(2005) *IV Encuentro Iberoamericano de Protección de datos., Informe de Viabilidad de creación de autoridades de control en el entorno Iberoamericano*, Huixquilucan (Estado de México), 4 de noviembre de 2005. Disponible en: <http://www.redipd.es/actividades/encuentros/IV/index-ides-idphp.php>. (Última consulta en línea 6 de mayo 2017).

(2005) *27 International Conference of Data Protection and Privacy Commissioners, declaración de Montreux*, 14 y 16 de septiembre 2005. Disponible en: https://icdppc.org/wp-content/uploads/2015/06/montreux_declaration-Spanish.pdf. (Última consulta en línea 17 de mayo 2017).

(2004) *III Encuentro Iberoamericano de Protección de Datos, Declaración de Cartagena de Indias* Colombia, 2004. Disponible en: <http://www.redipd.es/actividades/encuentros/III/index-ides-idphp.php>. (Última consulta en línea 18 de mayo 2017).

(2003) *II Encuentro Iberoamericano de Protección de Datos, Declaración de San Lorenzo del Escorial*, España, 2003. Disponible en: http://www.redipd.es/documentacion/common/declaracion_2003_II_encuentro_es.pdf. (Última consulta en línea 18 de mayo 2017).

(2003) *XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, Declaración de Santa Cruz de la Sierra*, 14 y 15 de noviembre de 2003. Disponible en: <http://www.oei.es/historico/xiiicumbredec.htm>. (Última consulta en línea 11 de abril 2017).

(2003) *XIII Cumbre Iberoamericana de Jefes de Estado y Presidentes de Gobierno.*, 14 y 15 de noviembre 2003, San Carlos Bariloche (Argentina).

Disponible en: <http://www.oei.es/histórico/ixiicumbredec.htm>. (Última consulta en línea 11 de abril 2017).

(2002) *I Encuentro Iberoamericano de Protección de datos, Declaración de San Lorenzo del Escorial-España*, 2002. Disponible en: https://icdppc.org/wp-content/uploads/2015/06/montreux_declaration-Spanish.pdf. (Última consulta en línea 17 de mayo 2017).

(2002) *I Encuentro Iberoamericano de Protección de Datos, Declaración de San Lorenzo del Escorial-España*. Disponible en: http://www.redipd.es/documentacion/common/declaracion_2002_I_encuentro.pdf. (Última consulta en línea 03 de abril 2017).

(2002) *Primer Encuentro Iberoamericano de Protección de Datos celebrado en San Lorenzo del Escorial (España)*. Disponible en: https://icdppc.org/wp-content/uploads/2015/06/montreux_declaration-Spanish.pdf. (Última consulta en línea 17 de mayo 2017).

(1999) *Primera Cumbre entre los Jefes de Estado y de Gobierno de América Latina y el Caribe y la Unión Europea., Declaración de Río de Janeiro, Río de Janeiro, Brasil, 28 y 29 de junio de 1999*. Disponible en: <http://www.oei.es/histórico/cumbrerio.htm>. (Última consulta en línea 3 de abril 2017).

(1998) *Declaración relativa a la protección de la intimidad en las redes globales, conferencia “un mundo sin fronteras: comprender el potencial del comercio electrónico global”*. Disponible en: http://www.oas.org/es/sla/ddi/docs/Declaracion_OCDE_Proteccion_Intimidad_r edes.pdf. (Última consulta en línea 3 de diciembre 2017).

(1997) *VII Cumbre Iberoamericana de Jefes de Estado y Presidentes de Gobierno, Declaración de Margarita, 08 y 09 de noviembre 1997, Margarita, República de Venezuela*. Disponible en:

<http://www.oei.es/histórico/iviicumbre.htm>. (Última consulta en línea 3 de abril 2017).

(1995) *Cuadragésimo Quinto período de Sesiones, Asamblea General*. Disponible en: <http://www.un.org/es/comun/docs/?symbol=A/RES/45/95>. (Última consulta en línea 1 de diciembre 2017).

(1995) *V cumbre Iberoamericana de Jefes de Estado y Presidentes de Gobierno, 16 y 17 de octubre 1995*, San Carlos Bariloche (Argentina). Disponible en: <http://www.oei.es/histórico/ivcumbre.htm>. (Última consulta en línea 9 de abril 2017).

(1995) *V Cumbre Iberoamericana de Jefes de Estado y Presidentes de Gobierno, 16 y 17 de octubre 1995*, San Carlos Bariloche (Argentina). Disponible en: <http://www.oei.es/histórico/ivcumbre.htm>. (Última consulta en línea 9 de abril 2017).

(1994) *IV Cumbre Iberoamericana de Jefes de Estado y Presidentes de Gobierno, 14 y 15 de junio 1994*. Disponible en: <http://www.oei.es/histórico/ivcumbre.htm>. (Última consulta en línea 9 de abril 2017).

(1993) *II Cumbre Iberoamericana de Jefes de Estado y Presidentes de Gobierno.*, 15 y 16 de Julio 1993. Disponible en: <http://www.oei.es/histórico/iicumbr.htm> . (Última consulta en línea 7 de abril 2017).

(1992) *II Cumbre Iberoamericana de Jefes de Estado y Presidentes de Gobierno, Declaración de Madrid, 23 y 24 de Julio 1992*, Madrid. Disponible en: <http://www.oei.es/histórico/iicumbre.htm>. (Última consulta en línea 7 de abril 2017).

(1991) *IX Encuentro implicaciones socio-jurídicas de las tecnologías de la información*, 1ª ed. Citema, España, 1991.

(1991) *I Cumbre Iberoamericana de Jefes de Estado y Presidentes de Gobierno, Declaración de Guadalajara*, 18 y 19 de Julio 1991, México. Disponible en: <http://www.oei.es/histórico/icumbr.htm>. (Última consulta en línea 7 de abril 2017).

(1977) *Instrumento de Ratificación de España del Pacto Internacional de Derechos Civiles y Políticos, hecho en Nueva York el 19 de diciembre de 1966*. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1977-10733>. (Última consulta en línea 23 junio 2017).

Cumbres Iberoamericanas de Jefes de Estado y de Gobierno. Disponible en: <http://www.oei.es/histórico/cumbres2.htm>. (Última consulta en línea el 6 de abril 2017).

(1960) *Convención de la OCDE*. Disponible en: <http://www.oecd.org/centrodemexico/laocde/convenciondelaocde.htm>. (Última consulta en línea 20 de junio 2017).

Sentencias

(2018) *Sentencia núm. TC/0475/18. Expediente núm. TC-05-2016. Relativo al recurso de revisión constitucional de sentencia de amparo interpuesto por Ricardo Sosa Filoteo contra la Sentencia núm.00125-2015, dictada por la Tercera Sala del Tribunal Superior Administrativo el veintiocho (28) de septiembre de dos mil quince (2015)*. Disponible en: <https://www.tribunalconstitucional.gob.do/consultas/secretar%C3%ADa/sentencias/tc047518/>. (Última consulta en línea 14 de noviembre 2018).

(2018) Caso no. 8691/79, *MALONE v. THE UNITED KINGDOM*, Council of Europe., Case law of the European Court of Human Rights Concerning the protection of personal data Strasbourg, june 2018. Disponible en: <https://rm.coe.int/t-pd-2018-15-case-law-on-data-protection-may2018-en/16808b2d36>. ((Última consulta en línea 19 de octubre 2018).

(2018) Council of Europe., Case law of the European Court of Human Rights Concerning the protection of personal data Strasbourg, june 2018. Disponible en: <https://rm.coe.int/t-pd-2018-15-case-law-on-data-protection-may2018-en/16808b2d36>. ((Última consulta en línea 19 de octubre 2018).

(2016) *Sentencia núm. TC/0484/16*, p. 53. Disponible en: <https://www.tribunalconstitucional.gob.do/sites/default/files//documentos/TC-0484-16.pdf>. (Última consulta en línea 14 de octubre 2016).

(2016) *Sentencia núm. TC/0404/16. Recurso de revisión constitucional en materia de habeas data incoado por la sociedad comercial Boreo, S. R. L. contra la Sentencia núm. 052-2014, dictada por la Segunda Sala de la Cámara Penal del Juzgado de Primera Instancia del Distrito Nacional el once (11) de marzo de dos mil catorce (2014)*, p. 14. Disponible en: <https://www.tribunalconstitucional.gob.do/consultas/secretar%C3%ADa/sentencias/tc040416/>. (Última consulta en línea 16 de noviembre 2018).

(2015) *Sentencia núm. TC/478/15 Recurso de revisión constitucional en materia de amparo interpuesto por el señor José Rafael Diloné Estévez contra la Sentencia núm. 365-14-01904, dictada por la Primera Sala de la Cámara Civil y Comercial del Juzgado de Primera Instancia del Distrito Judicial de Santiago el once (11) de noviembre de dos mil catorce (2014)*. Disponible en: <https://www.tribunalconstitucional.gob.do/consultas/secretar%C3%ADa/sentencias/tc047815/>. (Última consulta en línea 14 de noviembre 2018).

(2014) *Sentencia núm. C-362/14, Maximillian Schrems / Data Protection Commissioner*. Disponible en:

<https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150106es.pdf>. Comunicado de prensa n.º 106/15. (Última consulta en línea 14 de marzo 2018).

(2014) *Sentencia núm. C-362/14, Maximillian Schrems / Data Protection Commissioner*. Disponible en:

<https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf>. Comunicado de prensa n.º 117/15. (Última consulta en línea 14 de marzo 2018).

(2014) *Sentencia núm. TC/0050/14. Recurso de revisión constitucional en materia de amparo incoado por el señor Melvin Velázquez Then, contra la Sentencia núm. 088-2011, dictada por la Segunda Sala del Tribunal Superior Administrativo, en fecha diez (10) de agosto de dos mil once (2011)*. Disponible en:

<https://www.tribunalconstitucional.gob.do/consultas/secretar%C3%ADa/sentencias/tc005014/>. (Última consulta en línea 14 de noviembre 2018).

(2014) *Sentencia núm. TC/0039/14. Expediente núm. TC-05-2012-0114, relativo al recurso de revisión constitucional en materia de amparo incoado por Reemberto José de Jesús Pichardo Juan contra la Sentencia núm. 114-2012, de fecha treinta y uno (31) de agosto de dos mil doce (2012), dictada por la Segunda Sala del Tribunal Superior Administrativo*. Disponible en: <https://www.tribunalconstitucional.gob.do/content/sentencia-tc003914>. (Última consulta en línea 27 de enero 2016).

(2013) *Acción directa de inconstitucionalidad contra la Ley Orgánica sobre protección de datos de carácter personal 172-13*. Disponible en:

<http://www.prensayderecho.org/descargas/category/2-acciones-procesales#>.

(Última consulta en línea 14 de octubre 2016).

(2013) *Sentencia núm. TC/0084/13. Expediente núm. TC-04-2012-0045, relativo a recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Alejandro Alberto Paulino Vallejo contra la Sentencia*.

núm. 105 dictada por la Tercera Sala de lo Laboral, Tierras, Contencioso Administrativo y Contencioso Tributario de la Suprema Corte de Justicia, en fecha veintinueve (29) de febrero de dos mil doce (2012). Disponible en: <https://www.tribunalconstitucional.gob.do/node/1544>. (Última consulta en línea 27 de enero 2016).

(2013) Sentencia núm. TC/0062/13. Expediente núm. TC-04-2012-0041, relativo al recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Allan de Jesús Tiburcio Andrickson contra la Sentencia núm. 60, dictada por la Tercera Sala de la Suprema Corte de Justicia, en fecha quince (15) de febrero de dos mil doce (2012). Disponible en: <https://www.tribunalconstitucional.gob.do/sites/default/files/documentos/Sentencia%20TC%200062-13%20C.pdf> . (Última consulta en línea 27 de enero 2016).

(2013) Sentencia núm. TC/0052/13, relativo al recurso de revisión constitucional de Decisiones Jurisdiccionales incoado por la Asociación Nacional de Pilotos, contra la Sentencia núm. 130, dictada por la Tercera Sala de la Suprema Corte de Justicia, en fecha siete (07) de marzo de dos mil doce (2012). Disponible en: <https://www.tribunalconstitucional.gob.do/node/1330>. (Última consulta en línea 25 de enero 2016).

(2013) Sentencia núm. TC/0024/13, relativo al recurso de revisión de sentencia de Habeas Data incoado por Fior D'Alisa Recio Tejada, Procuradora Fiscal Adjunta del Distrito Nacional, Coordinadora del Departamento de Investigaciones de la Procuraduría Fiscal del Distrito Nacional, en contra de Mario Pérez García, Agustín Abreu Galván, Manuel Mario Pérez. Disponible en: <https://www.tribunalconstitucional.gob.do/node/1223>. (Última consulta en línea 29 de enero 2016).

(2013) Sentencia núm. TC/0010/13. Expediente núm. TC-04-2012-0039, relativo al Recurso de Revisión Constitucional de Decisiones Jurisdiccionales incoado por la Asociación Nacional de Pilotos, contra la Sentencia núm. 86,

dictada por la Tercera Sala de la Suprema Corte de Justicia, en fecha doce (12) de abril de dos mil doce (2012). Disponible en:

<https://tribunalsitestorage.blob.core.windows.net/media/7434/sentencia-tc-0010-13-c.pdf>. (Última consulta en línea 27 de enero 2016).

(2013) *Sentencia núm. TC/0157/13 Referencia: Expediente núm. TC-05- 2012-0067, relativo al recurso de revisión constitucional incoado por Michelle Carolina Reyes Vicioso contra la Sentencia núm. 013/2012, dictada por la Presidencia del Juzgado de Trabajo de la Provincia de Santo Domingo, en fecha veintitrés (23) de julio del año dos mil doce (2012).* Disponible en:

<https://tribunalsitestorage.blob.core.windows.net/media/7581/sentencia-tc-0157-13-c.pdf>. (Última consulta en línea 20 de diciembre 2018).

(2013) *Sentencia núm. TC/0204/13, recurso de revisión constitucional en materia de amparo, incoado por Rosa Elena Rijo, contra la Sentencia núm. 404/2012, dictada en fecha veinticuatro (24) de mayo de dos mil doce (2012), por la Cámara Civil y Comercial del Juzgado de Primera Instancia del Distrito Judicial de La Altagracia.* Disponible en:

<https://www.tribunalconstitucional.gob.do/consultas/secretar%C3%ADa/sentencias/tc020413/>. (Última consulta en línea 29 de enero 2016).

(2012) *Sentencia núm. TC/0011/12, acción de amparo incoada por Gary Gresko, S. A., contra la Dirección General de Migración.* Disponible en:

<http://www.tribunalconstitucional.gob.do/sites/default/files/documentos/Sentencia%20TC%200011-12%20C.pdf>. (Última consulta en línea 22 de enero 2016).

(2012) *Sentencia núm. TC/0042/12, recurso de revisión en materia de amparo incoado por la Cámara de Diputados de la República Dominicana y el Estado Dominicano contra el señor Manuel Muñoz Hernández.* Disponible en:

<https://www.tribunalconstitucional.gob.do/node/582>. (Última consulta en línea 25 de enero 2016).

(2012) *Sentencia núm. TC/0062/13, recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Allan de Jesús Tiburcio Andrickson contra la Sentencia núm. 60, dictada por la Tercera Sala de la Suprema Corte de Justicia, en fecha quince (15) de febrero de dos mil doce (2012).* Disponible en:

<https://www.tribunalconstitucional.gob.do/sites/default/files/documentos/Sentencia%20TC%200062-13%20C.pdf>. (Última consulta en línea 27 de enero 2016).

(2012) *Sentencia núm. TC/0039/14, relativo al recurso de revisión constitucional en materia de amparo incoado por Reemberto José de Jesús Pichardo Juan contra la Sentencia núm. 114-2012, de fecha treinta y uno (31) de agosto de dos mil doce (2012).* Disponible en:

<https://www.tribunalconstitucional.gob.do/content/sentencia-tc003914>. (Última consulta en línea 27 de enero 2016).

(2012) *Sentencia C-131/12 Google Spain, S.L., Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González.* Disponible en: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070es.pdf>. *Comunicado de prensa n.º 70/14.* (Última consulta en línea 14 de marzo 2018).

(2012) *Conclusiones del Abogado General en el asunto C-131/12 Google Spain, S.L. y Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González.* Disponible en:

<https://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077es.pdf>. *Comunicado de prensa n.º 77/13.* (Última consulta en línea 14 de marzo 2018).

(2009) Corte IDH. *Caso Tristán Donoso vs. Panamá.* Excepción preliminar, fondo, reparaciones y costas. Sentencia de 27 de enero de 2009 Serie C N.º 193. pp. 1 y ss. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_193_esp.pdf. (Última consulta en línea 5 de febrero 2019).

(2007) Corte IDH. Caso Escué Zapata Vs. Colombia, Fondo, Reparaciones y Costas, Sentencia de 4 de julio de 2007. pp. 1 y ss. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_165_esp.pdf. (Última consulta en línea 5 de febrero 2019).

(2005) *Sentencia núm. C-981/05. Reserva de Ley estatutaria - Criterios para su determinación respecto de derechos fundamentales*. Disponible en: <http://www.corteconstitucional.gov.co/relatoria/2005/c-981-05.htm>. (Última consulta en línea 24 de marzo 2018).

(2004) *Sentencia núm. C-993/04. Habeas data, Corte Constitucional República de Colombia*. Disponible en: <http://www.corteconstitucional.gov.co/relatoria/2004/C-993-04.htm>. (última consulta en línea 24 de marzo 2018).

(2003) *Sentencia núm. TC/0084/13, Recurso de revisión constitucional de decisiones jurisdiccionales incoado por el señor Alejandro Alberto Paulino Vallejo contra la Sentencia núm. 105 dictada por la Tercera Sala de lo Laboral, Tierras, Contencioso Administrativo y Contencioso Tributario de la Suprema Corte de Justicia, en fecha veintinueve (29) de febrero de dos mil doce (2012)*. Disponible en: <https://www.tribunalconstitucional.gob.do/node/1544>. (Última consulta en línea 27 de enero 2016).

(2003) Sentencia del TJUE de 6 de noviembre de 2003, Bodil Lindqvist, C-101/01, EU: C:2003:596. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN> (Última consulta en línea 24 de octubre 2019).

(2000) *Fundamento jurídicos número 8 de la Sentencia 290/2000, de 30 de noviembre de 2000 del Tribunal Constitucional*. Disponible en: <https://www.agpd.es/portaIwebAGPD/canaIdocumentacion/sentencias/tribunaI>

[constitucional/common/pdfs/Sentencia290.pdf](#). (Última consulta en línea 25 de agosto 2017).

(2001) *Sentencia núm. 290/2000, de 30 de noviembre de 2000. Recursos de inconstitucionalidad acumulados 201/93, 219/93, 226/93 y 236/93. Promovidos por el Consejo Ejecutivo de la Generalidad de Cataluña, el Defensor del Pueblo, el Parlamento de Cataluña y por don Federico Trillo-Figueroa Conde, Comisionado por 56 Diputados del Grupo Parlamentario Popular, contra diversos artículos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Competencia sobre derechos fundamentales y la Agencia de Protección de Datos. Voto particular.* Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-T-2001-330>. [BOE-T-2001-330](#). (Última consulta en línea 25 de agosto de 2017).

(2000) *Recursos de inconstitucionalidad acumulados y reflejados en la STC 290/2000.* Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-T-2001-330> [4 de enero de 2001](#). (Última consulta en línea 25 de agosto de 2017).

(1993) *Sentencia núm. 254/1993 del 20 de Julio de 1993.* Disponible en: <https://www.boe.es/boe/dias/1993/08/18/pdfs/T00028-00034.pdf>.

(Última consulta en línea 19 de junio 2018).

Direcciones de Internet

(2018) Comisiones de Ética Pública (CEP) conformadas a nivel nacional, de Julio 2017 a junio 2018. Disponible en:

<https://digeig.gob.do/transparencia/images/docs/estadisticas/2018/%20JUNIO%202018/CEP%20Conformadas-Junio2018.pdf>. (Última verificación en línea, 22 de mayo 2019).

(2018) *Consejo Nacional, 2018, Sistema Nacional de Transparencia México.* <http://snt.org.mx/index.php/consejo-nacional>. Disponible en: (Última consulta en línea 23 de julio 2018).

(2018) SANTILLAN, O., *Falla Inai en protección de datos personales, Eje Central*, 2018. Disponible en: <http://www.ejecentral.com.mx/falla-inai-en-proteccion-de-datos-personales/>. (Última consulta en línea 26 de mayo 2018).

(2018) *The United States and OECD partners for better live*. Disponible en: <http://www.oecd.org/washington/oechandus/>. (Última consulta en línea 7 de diciembre 2017).

(2018) *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)*. Disponible en: <http://inicio.inai.org.mx/SitePages/Transparencia/GobiernoAbierto.aspx>. (Última consulta en línea 16 de julio 2018).

(2018) *Marco Normativo, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)*, México 2018. Disponible en: <http://inicio.inai.org.mx/SitePages/marcoNormativo.aspx>. (Última consulta en línea 23 de junio 2018).

(2018) *Oficina Presidencial de Tecnologías de la Información y Comunicación*. Disponible en: <http://www.optic.gob.do/index.php/sobre-nosotros/quienes-somos>. (Última consulta en línea 29 de mayo 2018).

(2018) *Open Government Partnership*. Disponible en: <https://www.opengovpartnership.org/countries/dominican-republic>. (Última consulta en línea 31 de mayo 2018).

(2018) *Portal Oficial del Estado Dominicano, Seguridad y Delito Electrónico (Cyber Security and Crime)*. Disponible en: <http://www.gob.do/index.php/seguridad-y-delito-electronico>. (Última consulta en línea 29 de mayo 2018).

(2018) *Portal Oficial del Estado Dominicano*. Disponible en: www.dominicana.gob.do. (Última consulta en línea 28 de mayo 2018).

(2018) *Portal Oficial del Estado Dominicano, e-Transparencia, Gobierno y Datos Abiertos (Open Government)*. Disponible en: <http://www.gob.do/index.php/e-sociedad/2014-12-17-20-08-19/2014-12-17-20-09-52>. (Última consulta en línea 4 de julio 2018).

(2018) *Portal de transparencia, estructura orgánica ministerio de la presidencia*. Disponible en: <https://minpre.gob.do/transparencia/estructura-organica-ministerio-de-la-presidencia/>. (Última consulta en línea 16 de julio 2018).

(2018) *Sistema Nacional de Transparencia*. Disponible en: <http://snt.org.mx/>. (Última consulta en línea 23 de julio 2018).

(2018) *Salvadoreños serán multados si no cumplen nueva ley de protección de datos de la UE*, *elsalvador.com*, 2018. <https://www.elsalvador.com/noticias/negocios/salvadorenos-seran-multados-si-no-cumplen-nueva-ley-de-proteccion-de-datos-de-la-ue/484160/2018/>. (Última consulta en línea 18 de noviembre 2019).

(2018) *Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales*. Disponible en: <http://www.snt.org.mx/>. (Última consulta en línea 23 de julio 2018).

(2017) *Derechos de los ciudadanos al Libre Acceso a la Información Pública*. Disponible en: <http://transparencia.dicom.gob.do>. (Última consulta en línea 30 de mayo 2018).

(2016) *Instructivo para las Sociedades de Información Crediticia (SIC)*. Disponible en: <https://www.sib.gob.do/pdf/vistaspublicas/2016-07-29-Instructivo-para-las-sociedades-de-informacion-creditiaversion-final.pdf>. (Última consulta en línea 12 de marzo 2018).

(2016) *Panorama Económico y Social de la Comunidad de Estados Latinoamericanos Y caribeños*. Disponible en:

<https://www.cepal.org/es/publicaciones/40916-panorama-economico-social-la-comunidad-estados-latinoamericanos-caribenos-2016>. (Última consulta en línea 28 de noviembre 2018).

(2016) OCDE/CEPAL/CAF (2016), *Perspectivas Económicas de América Latina 2017: Juventud, competencias y emprendimiento*, OECD Publishing, Paris. Disponible en: <http://dx.doi.org/10.1787/leo-2017-es>. (Última consulta en línea 4 de octubre 2018).

(2016) *Panorama Económico y Social de la Comunidad de Estados Latinoamericanos y Caribeños*. Disponible en: <https://www.cepal.org/es/publicaciones/40916-panorama-economico-social-la-comunidad-estados-latinoamericanos-caribenos-2016>. (Última consulta en línea 24 de noviembre 2018).

(2016) *Superintendencia de Bancos de la República Dominicana*. Disponible en: <https://www.sib.gob.do/pdf/Memoria-Institucional-SIB-2016.pdf>. (Última consulta en línea 12 de marzo 2018).

(2015) *Constitución de la República Dominicana del 2015*. Disponible en: <https://www.tribunalconstitucional.gob.do/sites/default/files//documentos/TC-0484-16.pdf>. (Última consulta en línea 14 de octubre 2016).

(2015) *El artículo 29 sobre protección de datos.*, Nota de prensa, *Independencia de las autoridades de protección de datos*, 06/18/2015. Disponible en: http://ec.europa.eu/justice/data-protection/article-29/press-aterial/press-release/art29_press_material/2015/20150618_wp29_press_release_on_the_independence_of_data_protection_authorities.pdf. (Última consulta en línea 28 de febrero 2017).

(20015) Fundéu BBVA., *¿Finalmente cómo se debe escribir hábeas data o habeas data?*, 2015. Disponible en:

<https://www.fundeu.es/noticia/habeas-data/>. (Última consulta en línea 14 de noviembre 2019).

(2015) *Tribunal Constitucional de la República Dominicana*. Disponible en: <https://www.tribunalconstitucional.gob.do/node/2504>. (Última consulta en línea 14 octubre de 2016).

(2015) *Portal de Transparencia, Superintendencia de Bancos*. Disponible en: <https://www.sib.gob.do/transparencia/servicio-al-publico>. (Última consulta en línea 3 de marzo 2018).

(2015) *Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales*. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5436072&fecha=04/05/2016. [DOF 04 Mayo 2015](#). (Última consulta en línea 23 de julio 2018).

(2014) *e-Transparencia, Gobierno y Datos Abiertos (Open Government)*. Disponible en: <http://www.gob.do/index.php/e-sociedad/2014-12-17-20-08-19/2014-12-17-20-09-52>. (Última consulta en línea 4 de julio 2018).

(2013) CEPALSTAT., *Bases de Datos y Publicaciones Estadísticas, Infográficos de América Latina y el Caribe*. <http://www.cepal.org/estadisticas>. (Última consulta en línea 28 de noviembre 2018).

(2013) REMOLINA ANGARITA, N., *Informe Latinoamérica y Protección de Datos Personales en Cifras, 1985-2012*. Disponible en: http://www.redipd.org/noticias_todas/2013/tribuna/common/Latinoamericaypden cifras19852012NRemolina.pdf. (Última consulta en línea 14 de agosto 2013).

(2013) *Organigrama Superintendencia de Bancos*. Disponible en: https://www.sib.gob.do/oai/Organigrama_Oficial_Aprobado_CI_06_13.pdf. (Última consulta en línea 3 de marzo 2018).

(2013) MÁRQUEZ, W., *Lo que Snowden ha revelado hasta ahora del espionaje de EE.UU.*, Periódico BBC NEWS, 2 JULIO 2013. Disponible en: https://www.bbc.com/mundo/noticias/2013/07/130702_eeuu_snowden_revelaciones_espionaje_wbm. (Última consulta en línea 29 de octubre 2019).

(2013) MEJÍA MARIELA, M. R., *Más de 600 personas acuden a Data Crédito al final de la tarde*, Periódico Diario Libre, 2013. Disponible en: <https://www.diariolibre.com/economia/ms-de-600-personas-acuden-a-data-crédito-al-final-de-la-tarde-MNDL368765>. (Última verificación en línea 29 de abril 2019).

(2011) AG/RES-2661 (XLI-O/11)., *Acceso a la información pública y protección de datos personales*. Disponible en: http://www.oas.org/es/sla/cji/docs/CJI-doc_402_12_rev2.pdf. (Última consulta en línea 16 de agosto 2017).

(2011) *Alianza para el Gobierno Abierto (OGP)*. Disponible en: http://www.opengovpartnership.org/sites/default/files/OGP_Booklet_Spanish_Digital.pdf. (Última consulta en línea 30 de mayo 2018).

(2011) *Open Government Partnership*. Disponible en: <https://www.opengovpartnership.org/countries/dominican-republic>. (Última consulta en línea 31 de mayo 2018).

(2011) *Hacia una gestión pública más efectiva y dinámica en México*, OECD. Disponible en: <https://www.oecd.org/gov/regulatory-policy/48808023.pdf>. (Última consulta en línea 6 de agosto 2018).

(2010) *Usuarios de Internet.*, Comisión Económica para América Latina y el Caribe, Infográficos de América Latina y el Caribe, División de Estadísticas. Disponible en: <http://www.cepal.org/estadisticas/>. (Última consulta en línea 24 de noviembre 2018).

(2002) *The Working Group, Roadmap for E-Government in the developing World*, April 2002. Disponible en:

<http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan005030.pdf>.

(Última consulta en línea 29 de julio 2018).

(1985) *Resumen Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, Declaración sobre flujos de datos transfronterizos* (1985). Disponible en:

<http://www.oecd.org/sti/ieconomy/15590267.pdf>. (Última consulta en línea 4 de

diciembre de 2017):

(1969) *Preámbulo Convención Americana sobre Derechos Humanos (Pacto de San José)*, 1969. Disponible en:

https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm. (Última consulta

en línea 24 de enero 2019).

Carta de la Organización de los Estados Americanos. Disponible en:

http://www.oas.org/dil/esp/afrodescendientes_manual_formacion_lideres_anexos.pdf. (Última consulta en línea 24 de enero 2019).

(1948) *Preámbulo Carta de la Organización de los Estados Americanos*. (1948). Disponible en:

http://www.oas.org/dil/esp/afrodescendientes_manual_formacion_lideres_anexos.pdf. (Última consulta en línea 24 de enero 2019).

(1945) *Carta de las Naciones Unidas*. Disponible en:

<http://www.un.org/es/documents/charter/index.shtml>. (Última consulta en línea 30 de noviembre 2017).

Agencia Española de Protección de Datos, directrices protección de datos de la ONU. Disponible en:

https://www.agpd.es/portaleswebAGPD/canaldocumentacion/legislacion/organismos_internacionales/naciones_unidas/common/pdfs/D.3BIS-cp--Directrices-de-Proteccion-de-Datos-de-la-ONU.pdf. (Última consulta en línea 30 de octubre 2017).

Corpus Iuris Internacional y Nacional. Disponible en: <http://corpusiurispdp.inai.org.mx/Pages/home.aspx>. (Última consulta en línea 25 de mayo 2018).

Catálogo General de Publicaciones Oficiales. Disponible en: <http://publicaciones.administracion.es>. (Última verificación en línea 22 de abril 2018).

Defensor del Pueblo, Informe anual de gestión 2017-2018, del 1 de mayo de 2017 al 30 de abril de 2018. República Dominicana. Disponible en: http://defensordelpueblo.gob.do/transparencia/phocadownload/PlanEstrategico/informe_de_gestion/Informe%20de%20gestion%202017-2018.pdf. (Última verificación en línea 20 de mayo 2019).

Dirección General de Ética e Integridad Gubernamental., *Instituciones públicas con Responsables de Acceso a la Información (RAI), junio 2018*. Disponible en: <https://digeig.gob.do/transparencia/images/docs/estadisticas/2018/%20JUNIO%202018/RAI%20Designados-Junio2018.pdf>. (Última verificación en línea, 22 de mayo 2019).

Emoji de los ojos de WhatsApp. Disponible en: <https://emojiterria.com/es/ojos/>. (Última consulta en línea 11 de agosto 2017).

Legislación República de Costa Rica. Disponible en: <http://www.redipd.org/legislacion/costarica-ides-idphp.php>. (Última consulta en línea 18 de noviembre 2019).

Histórico Telecomunicaciones 1996 al 2011. Disponible en: <https://www.indotel.gob.do/transparencia/publicaciones->

[oficiales/estad%C3%ADsticas-telecomunicaciones/otros/](#). (Última consulta en línea 20 de noviembre 2018).

Reforma de las normas de protección de datos de la UE. Disponible en: http://ec.europa.eu/justice/data-protection/reform/index_en.htm. (Última consulta en línea 28 de enero 2017).

Portal Superintendencia de Bancos. Disponible en: <https://www.sib.gob.do/transparencia/servicio-al-publico>. (Última consulta en línea 3 de marzo 2018).

Portal Cámara de Diputado Mexicano. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_150917.pdf. (Última consulta en línea 23 de julio 2018).

Resumen ejecutivo 2017, reforma de las administraciones públicas, Comisión para la Reforma de Administraciones públicas (CORA), Ministerio de Hacienda y Administraciones públicas, Ministerio de la presidencia. Disponible en: <http://transparencia.gob.es/transparencia/dam/jcr:b1c69477-9882-41a5-9f6d-5cbb46fa12b4/reforma-AAPP.PDF>. (Última consulta en línea 24 de agosto 2017).

Portal Único de Solicitudes de Acceso a la Información Pública (SAIP), *Estadísticas Generales*. Disponible en: <https://saip.gob.do/estadisticas-generales>. (Última consulta en línea 25 de mayo 2019).

REMOLINA ANGARITA, N., *Informe Latinoamericano y Protección de datos personales en cifras, 1985-2012*, Bogotá Colombia, 2013. Disponible en: http://www.redipd.org/noticias_todas/2013/tribuna/common/Latinoamericaypden cifras19852012NRemolina.pdf. (Última Consulta en línea 14 de agosto 2013).

Organisation for Economic Co-operation and Development (OECD). Disponible en: <http://publicaciones.administracion.es>. (Última consulta en línea 7 de diciembre 2017).

Organigrama Dirección General de Ética e Integridad Gubernamental (DIGEIG), organigrama directivo. Disponible en: <https://digeig.gob.do/index.php/sobre-nosotros/organigrama>. (Última verificación en línea, 22 de mayo 2019).

Organización de las Naciones Unidas (ONU), *informe general*., Disponible en: <https://www.un.org/es/sections/about-un/overview/index.html>. (Última consulta en línea 18 de octubre 2019).

El derecho a la privacidad en la era digital. Disponible en: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_34_L7_rev1.pdf. (Última verificación en línea 18 de octubre 2019).

Constituciones

(2011) *Constitución de Venezuela*. Disponible en: <http://www.minci.gob.ve/wp-content/uploads/2011/04/CONSTITUCION.pdf> . (Última consulta en línea 23 de marzo 2018).

(2010) Constitución de la República Dominicana del 2010. Disponible en: <http://www.senado.gob.do/senado/Portals/0/Documentos/Constituciones/const.%202010.pdf>. (Última consulta en línea 22 de enero 2018).

(2009) *Constitución de Bolivia*. Disponible en: https://www.oas.org/dil/esp/Constitucion_Bolivia.pdf. (Última consulta en línea 23 de marzo 2017).

(2009) *Constitución de Bolivia*. Disponible en:

https://www.oas.org/dil/esp/Constitucion_Bolivia.pdf. (Última consulta en línea 21 de marzo 2018).

(2008) *Constitución de la República de Ecuador*. Disponible en:

http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf.

(Última consulta en línea 13 de abril 2018).

(2004) *Constitución de Bolivia*. Disponible en:

<https://www.lexivox.org/norms/BO-CPE-20040413.html#idm4333904>. (Última

consulta en línea 19 de marzo 2017).

(2002) *Constitución de la República Dominicana del 2002*. Disponible en:

[http://www.consultoria.gov.do/Documents/GetDocument?reference=529f0575-](http://www.consultoria.gov.do/Documents/GetDocument?reference=529f0575-b936-4a51-b403-b9d8eb905288)

[b936-4a51-b403-b9d8eb905288](http://www.consultoria.gov.do/Documents/GetDocument?reference=529f0575-b936-4a51-b403-b9d8eb905288). (Última consulta en línea 27 de junio 2018).

(1999) *Constitución de la República Bolivariana de Venezuela*. Disponible en:

https://www.oas.org/dil/esp/constitucion_venezuela.pdf. (Última consulta en

línea 05 de abril 2018).

(1999) *Constitución de Venezuela 1999*. Disponible en:

<http://www.minci.gob.ve/wp-content/uploads/2011/04/CONSTITUCION.pdf>.

(Última consulta en línea 23 de marzo 2018).

(1998) *Constitución de la República de Ecuador*. Disponible en:

http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf.

(Última consulta en línea 13 de abril 2018).

(1994) *Constitución de la República Argentina*, 22 de agosto de 1994.

Disponible en:

<http://pdba.georgetown.edu/Parties/Argentina/Leyes/constitucion.pdf>.

(Última consulta en línea 26 de abril de 2018).

(1994) *Proyecto sustitutorio de reforma constitucional sobre la Acción de Habeas Data Peruana*. Disponible en:

<http://www4.congreso.gob.pe/dgp/constitucion/Const93DD/reforconst/Ley26470.pdf>. (Última consulta en línea 24 de abril 2018).

(1993) *Constitución de la República de Guatemala*. Disponible en: https://www.oas.org/juridico/mla/sp/gtm/sp_gtm-int-text-const.pdf. (Última consulta en línea 7 de octubre 2019).

(1993) *Constitución política de Perú*. Disponible en: <http://pdba.georgetown.edu/Parties/Peru/Leyes/constitucion.pdf>. (Última consulta en línea 20 de marzo del 2018).

(1993) *Constitución política del Perú*. Disponible en: http://www.oas.org/juridico/spanish/per_res17.pdf. (Última consulta en línea 20 de abril 2018).

(1992) *Constitución de Paraguay*. Disponible en: https://www.oas.org/juridico/spanish/par_res3.htm. (Última consulta en línea 20 de marzo 2018).

(1988) *Constitución Política de Brasil*. Disponible en: <http://www.wipo.int/edocs/lexdocs/laws/es/br/br117es.pdf>. (Última consulta en línea 19 de marzo 2018).

(1982) *Constitución política de la República de Honduras*. Disponible en: https://www.oas.org/dil/esp/Constitucion_de_Honduras.pdf. (Última consulta en línea 25 de marzo 2018).

(1978) *Constitución española*. Disponible en: <https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf>. (Última consulta en línea 19 de junio 2018).

(1972) *Constitución de Panamá*. Disponible en:

<http://pdba.georgetown.edu/Constitutions/Panama/vigente.pdf>. (Última consulta en línea 23 de marzo 2018).

(1917) *Constitución política de los Estados Unidos Mexicanos del 5 de febrero de 1917*, que reforma la constitución del 5 de febrero de 1857. Disponible en: <http://www.ordenjuridico.gob.mx/Constitucion/1917.pdf>. (Última consulta en línea 23 de julio 2018).

Tribunal Constitucional de la República Dominicana. Disponible en: <https://www.tribunalconstitucional.gob.do/node/2504>. (Última consulta en línea 14 de octubre 2016).

Tribunal Constitucional de la República Dominicana. Disponible en: <https://www.tribunalconstitucional.gob.do/transparencia/estad%C3%ADsticas-institucionales/2019/enero-marzo-2019/>, Última verificación en línea, 22 de mayo 2019).

Leyes / Proyectos de Ley / Decreto / Normas / Comunicado / Iniciativas

(2019) *Directrices de Protección de Datos de la ONU de 14 de diciembre de 1990*. Disponible en: <http://www.informatica-juridica.com/anexos/directrices-de-proteccion-de-datos-de-la-onu-de-14-de-diciembre-de-1990/>. (Última verificación en línea 18 de octubre 2019).

(2018) *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-16673. (Última verificación en línea 26 de julio 2019).

(2018) *Normas sobre Tecnologías de Información y Comunicaciones. NORTIC*. Disponible en: <http://optic.gob.do/nortic/index.php/documentos/category/normativas>. (Última consulta en línea 16 de julio 2018).

(2018) *Normas sobre tecnologías de la información y comunicación (NORTIC) 2018*. Disponible en: <http://optic.gob.do/nortic/index.php/nortic>. (Última consulta en línea 30 de mayo 2018).

(2018) *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Disponible en: <https://www.coe.int/it/web/conventions/search-on-treaties/-/conventions/rms/09000016808ac918>. (Última consulta en línea 14 de octubre 2018).

(2017) *Resumen ejecutivo 2017, reforma de las administraciones públicas, Comisión para la Reforma de Administraciones Públicas (CORA)*. Disponible en: <http://transparencia.gob.es/transparencia/dam/jcr:b1c69477-9882-41a5-9f6d-5cbb46fa12b4/reforma-AAPP.PDF>. (Última consulta en línea 24 de agosto 2017).

(2017) DOF: 26/01/2017. *Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017. (Última consulta en línea 28 de julio 2018).

(2017) *Decreto 143-17 proceso de actualización Comisión de Ética Pública (CEP)*. Disponible en: <https://es.scribd.com/document/346596887/Decreto-143-17>. (Última consulta en línea 9 de julio 2018).

(2017) *Decreto 234-17 que designa al Director Ejecutivo DIGEIG*. Disponible en: <https://digeig.gob.do/images/docs/DECRETO%20234-17.%20Designaci%C3%B3n%20Director%20Ejecutivo%20DIGEIG.pdf>. (Última consulta en línea 8 de julio 2018).

(2017) *Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, XII Legislatura*. Disponible en:

http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF. (Última consulta en línea 22 de mayo 2018).

(2017) *Legislación Cámara de Diputados Mexicana*. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_150917.pdf. (Última consulta en línea 23 de julio 2018).

(2017) *Informe sobre el anteproyecto de ley de protección de datos para adaptarla al Reglamento Comunitario*. Disponible en:

http://www.lamoncloa.gob.es/consejodeminstros/referencias/documents/2017/r_efc20170623.pdf#page=12. (Última consulta en línea 15 de julio 2018).

(2016) Comisión Europea, *¿Como simplificará la reforma de la protección de datos en la UE la normativa vigente?* Disponible en:

ec.europa.eu/newsroom/document.cfm?doc_id=41593. (Última consulta en línea 28 de febrero 2017).

(2016) *Decreto 246-16 que designa al Lic. Lidio Cadet Jiménez, Director General de la Dirección General de Ética e Integridad Gubernamental (DIGEIG)*. Disponible en: <https://digeig.gob.do/index.php/despacho-del-director>. (Última consulta en línea 9 de julio 2018).

(2016) *¿De qué modo adaptará la reforma de la protección de datos en la UE la normativa vigente a la evolución tecnológica?* Disponible en: ec.europa.eu/newsroom/document.cfm?doc_id=41597. (Última consulta en línea 28 de febrero 2017).

(2016) Iniciativa núm. 03346-2010-2016-CD. Disponible en: <https://www.camaradediputados.gov.do/masterlex/mlx/docs/2e/2/53DD/5888.pdf>. (Última consulta en línea 1 de mayo 2018).

(2016) Instructivo para las Sociedades de Información Crediticia (SIC). Disponible en: <https://www.sib.gob.do/pdf/vistaspublicas/2016-07-29-Instructivo-para-las-sociedades-de-informacion-crediticiaversion-final.pdf>.

(Última consulta en línea 12 de marzo 2018).

(2016) *Comunicación de la Comisión al Parlamento Europeo con arreglo al artículo 294, apartado 6, del Tratado de Funcionamiento de la Unión Europea sobre la posición del Consejo acerca de la adopción de un Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) y por el que se deroga la Directiva 95/46/CE*. Disponible en: <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016PC0214&from=ES>.

(última consulta en línea 14 Octubre de 2016).

(2016) *Protección de Datos, Normas para la protección de datos personales dentro y fuera de la UE*. Disponible en: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

(Última consulta en línea 20 de noviembre 2017).

(2016) *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*. Disponible en:

<https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807>. (Última consulta en línea 8 de marzo 2018).

(2015) *Comunicado de prensa n.º 117/15*. Disponible en: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070es.pdf>. (Última consulta en línea 24 de octubre 2017).

(2015) *El artículo 29 sobre protección de datos.*, Nota de prensa, independencia de las autoridades de protección de datos. Disponible en: http://ec.europa.eu/justice/data-protection/article-29/press-aterial/press-release/art29_press_material/2015/20150618_wp29_press_release_on_the_independence_of_data_protection_authorities.pdf. (Última consulta en línea 28 de febrero 2017).

(2015) *Ley núm. 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.* Disponible en: <https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10566-consolidado.pdf>. (Última consulta en línea 24 de agosto 2018).

(2015) *Ley núm. 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.* Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565>. (Última consulta en línea 24 de agosto 2018).

(2015) *Comunicado de prensa n.º 106/15.* Disponible en: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077es.pdf>. (Última consulta en línea 20 de octubre 2017).

(2015) *Comunicado de prensa n.º 117/15.* Disponible en: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070es.pdf>. (Última consulta en línea 22 de octubre 2017).

(2015) DOF: 26/01/2017. Decreto por el que se expide la Ley General de protección de Datos Personales en posesión de Sujetos Obligados. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017. (Última verificación en línea 28 de julio 2018).

(2014) *Declaración relativa a la protección de la intimidad en las redes globales*, conferencia “un mundo sin fronteras: comprender el potencial del comercio electrónico global”. Disponible en:

http://www.oas.org/es/sla/ddi/docs/Declaracion_OCDE_Proteccion_Intimidad_r edes.pdf. (Última verificación en línea 3 de diciembre 2017).

(2014) *Ley núm. 550-14 que establece el código penal de la República Dominicana*. Disponible en: <https://oig.cepal.org/sites/default/files/251865974-ley-no-550-14-que-establece-el-codigo-penal-de-la-republica-dominicana.pdf>. (Última verificación 11 de mayo 2018).

(2014) Albrecht y Droutsas: *La reforma de la protección de datos entra en la recta final*. Disponible en: <http://www.europarl.europa.eu/news/es/news-room/20140310STO38525/albrecht-y-droutsas-la-reforma-de-protecci%C3%B3n-de-datos-entra-en-la-recta-final>. (Última consulta en línea 01 de octubre 2016).

(2014) *Comunicado de prensa n.º 70/14*. Disponible en: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf>. (Última verificación en línea 30 de octubre 2017).

(20013) *Ley núm. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados*. Disponible en: <http://www.gob.do/index.php/recursos/2014-12-16-21-02-56/category/3-constitucion-y-leyes-rd?download=58:ley-no-172-13&start=20>. (Última verificación en línea 22 de marzo 2018).

(2013) *Ley núm. 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno*. Disponible en: <https://www.boe.es/boe/dias/2013/12/10/pdfs/BOE-A-2013-12887.pdf>. (Última verificación en línea 3 de septiembre 2018).

(2013) *Ley núm. 20/2013, de 9 de diciembre, de garantía de la unidad de mercado*. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-2013-12888>. (Última verificación en línea 24 de agosto 2018).

(2013) *Iniciativa núm. 01367-2013-PLO-SE*. Disponible en: <http://www.informatica-juridica.com/ley/iniciativa-01367-2013-plo-se-ley-organica-proteccion-datos-caracter-personal>. (Última consulta en línea 1 de mayo 2018).

(2013) *Recomendación del Consejo relativa a Pautas para la protección de la privacidad y flujos transfronterizos de datos personales*. Disponible en: <https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>. (Última consulta en línea 3 de diciembre 2017).

(2013) *The OECD Privacy Framework*. Disponible en: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. (Última consulta en línea 3 de diciembre 2017).

(2013) *Comunicado de prensa n.º 77/13*. Disponible en: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077es.pdf>. (Última consulta en línea 21 de octubre 2017).

(2013) GABRIEL GARCÍA, C., *Proyecto busca regular uso datos personales*, Periódico Hoy, 30 de julio 2013. Disponible en: <https://hoy.com.do/proyecto-busca-regular-usodatos-personales/>. (Última verificación en línea 14 de agosto 2017).

(2013) *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*. Disponible en: <https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>. (Última consulta en línea 3 de diciembre 2017).

(2012) *Decisión de Ejecución de la Comisión de 19 de diciembre de 2012 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales por Nueva Zelanda (notificada con el número C (2012) 9557)*. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415703506367&uri=CELEX:32013D0065_2013/65_/UE. (Última consulta en línea 14 de septiembre 2017).

(2012) *Decisión de Ejecución de la Comisión de 21 de agosto de 2012 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales por parte de la República Oriental del Uruguay con respecto al tratamiento automatizado de datos personales (notificado con arreglo al documento C (2012) 5704)*. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32012D04842012/484/UE>. (Última consulta en línea 14 de septiembre 2017).

(2012) *Ley estatutaria 1581 del 17 de octubre del 2012 por la cual se dictan disposiciones generales para la protección de datos personales, art. 26*. Disponible en: <https://www.sisben.gov.co/Documents/Informaci%C3%B3n/Leyes/LEY%20TRATAMIENTO%20DE%20DATOS%20-%20LEY%201581%20DE%202012.pdf>. (Última consulta en línea 18 de abril 2018).

(2012) *Ley núm. 787 de protección de datos personales, Nicaragua*. Disponible en: <http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d>. (Última consulta en línea 18 de abril 2018).

(2012) *Decreto. N.º 486-12 que crea la Dirección General de Ética e Integridad Gubernamental (DIGEIG). G. O. N.º 10693 del 31 de agosto de 2012*. Disponible en:

http://www.poderjudicial.gob.do/documentos/PDF/decretos/Dec_486-12.pdf.

(Última consulta en línea 6 de julio 2018).

(2012) *Decreto. N.º 486-12 que crea la Dirección General de Ética e Integridad Gubernamental (DIGEIG). G. O. N.º 10693 del 31 de agosto de 2012.*

Disponible en:

http://www.poderjudicial.gob.do/documentos/PDF/decretos/Dec_486-12.pdf.

(Última consulta en línea 6 de julio 2018).

(2012) *Decreto 490-12, mediante el cual se crea la Dirección General de Comunicaciones (DICOM).* Disponible en:

[https://presidencia.gob.do/themes/custom/presidency/docs/microsite-](https://presidencia.gob.do/themes/custom/presidency/docs/microsite-dicom/decreto_490_12.pdf)

[dicom/decreto_490_12.pdf](https://presidencia.gob.do/themes/custom/presidency/docs/microsite-dicom/decreto_490_12.pdf). (Última consulta en línea 29 de mayo 2018).

(2012) *Decreto 469-12 que designa al Ing. Armando García como Director General de la Oficina Presidencial de Tecnología de la Información y Comunicación.* Disponible en: <https://www.optic.gob.do/index.php/marco-legal-m>. (Última consulta en línea 9 de julio 2018).

(2012) Biblioteca del Congreso Nacional de Chile., *Historia de la Ley* núm. 19.812. Disponible en: <https://www.bcn.cl/historiadelaley/historia-de-la-ley/vista-expandida/5947/>. (Última consulta en línea 3 de abril 2018).

(2012) *Reforma de las normas de protección de datos de la UE.* Disponible en: http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

(Última consulta en línea 28 de enero 2017).

(2011) *Decisión de la Comisión de 31 de enero de 2011 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales por parte del Estado de Israel con respecto al tratamiento automatizado de datos personales (notificada en el documento C 332).* Disponible en:

<https://eur-lex.europa.eu/legalcontent/EN/TXT/?qid=1415701992276&uri=CELEX:32011D00612011/61> / UE. (Última consulta en línea 14 de septiembre 2017).

(2011) *Ley núm. 8968 de protección de la persona frente al tratamiento de sus datos personales*. Disponible en:

<http://www.tse.go.cr/pdf/normativa/leydeprotecciondelapersona.pdf>. (Última consulta en línea 18 de abril 2018).

(2011) *Ley núm. 2/2011, de 4 de marzo, de Economía Sostenible*. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2011-4117>. (Última consulta en línea 24 de agosto 2018).

(2011) *Ley núm. 137-11 Orgánica del Tribunal Constitucional y de los procedimientos constitucionales*. Disponible en:

<https://www.tribunalconstitucional.gob.do/transparencia/base-legal-de-la-institucion/ley-no-137-11/>. (Última verificación en línea 22 de mayo 2019).

(2010) *Decisión de la Comisión de 19 de octubre de 2010 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales en Andorra (notificada con el número C (2010) 7084) Texto con EEE pertinencia*. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32010D0625_2010/625 / UE. (Última consulta en línea 14 de septiembre 2017).

(2010) *Decisión de la Comisión de 5 de marzo de 2010 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada proporcionada por la Ley de Feroe sobre tratamiento de datos personales (notificada con el número C (2010) 1130*. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415701435417&uri=CELEX:32010D0146_2010/146 / UE. (Última consulta en línea 14 de septiembre 2017).

(2010) *Ley modelo Interamericana sobre Acceso a la Información Pública*. La resolución AG/RES. 2607 (XL-O/10. Disponible en: www.oas.org/dil/esp/ag-res_2607-2010.pdf. (Última consulta en línea 12 de junio 2017).

(2010) *Versión consolidada del Tratado de Funcionamiento de la Unión Europea (TFU)*. Disponible en: <https://www.boe.es/doue/2010/083/Z00047-00199.pdf>. (Última consulta en línea 8 de marzo 2018).

(2010) *Versión consolidada del Tratado de la Unión Europea*. Disponible en: <https://www.boe.es/doue/2010/083/Z00013-00046.pdf>. (Última consulta en línea 8 de marzo 2018).

(2010) *Carta de los Derechos Fundamentales de la Unión Europea*. Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003>. (Última consulta en línea 21 de abril 2018).

(2010) Protocolo Adicional al Convenio n.º 108, Artículo 1-Autoridad de Control Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-2010-14380>. (Última consulta en línea 7 de marzo 2018).

(2009) *Ley núm. 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio*. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2009-18731&p=20131210&tn=2>. (Última consulta en línea 24 de agosto 2018).

(2009) Decreto núm. 414/009, Protección de Datos Personales – Acción de Habeas Data, Disponible en: https://www.agesic.gub.uy/innovaportal/v/295/1/agesic/decreto-n%C2%B0-414_009-de-31-agosto-de-2009.html. (Última consulta en línea 5 de abril 2018).

(2008) *Ley núm. 41-08 de Función Pública del dieciséis (16) de enero del año dos mil ocho (2008)*. Disponible en:

<http://unpan1.un.org/intradoc/groups/public/documents/icap/unpan029758.pdf>.

(Última consulta en línea 24 de abril 2018).

(2008) *Decisión de la Comisión de 8 de mayo de 2008 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales en Jersey (notificada con el número C (2008) 1746)*. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415703064772&uri=CELEX:32008D0393_2008/393_/CE. (Última consulta en línea 18 de septiembre 2017).

(2008) *Ley núm. 1266 del 31 de diciembre de 2008 Colombia*. Disponible en: <http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/Ley%201266%20de%2031%20de%20diciembre%202008.pdf>. (Última consulta en línea 23 de marzo 2018).

(2008) *Ley núm. 18.331, de protección de datos personales y acción de habeas data de 11 de agosto de 2008, art. 23*. Disponible en: <https://www.agesic.gub.uy/innovaportal/v/302/1/agesic/ley-n%C2%B0-18331-de-11-de-agosto-de-2008.html>. (Última consulta en línea 18 de abril 2018).

(2008) *Ley estatutaria núm. 1266 del 31 de diciembre de 2008 por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones*. Disponible en: <http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/Ley%201266%20de%2031%20de%20diciembre%202008.pdf> . (Última consulta en línea 23 de marzo 2018. (Última consulta en línea 23 de marzo 2018).

(2007) *Ley núm. 37/2007 de 16 de noviembre*. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-19814. (Última consulta en línea 10 de agosto 2017).

(2007) *Ley núm. 53-07 sobre Crímenes y Delitos de Alta Tecnología*. Disponible en: https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf. (Última consulta en línea 22 de mayo 2019).

(2007) *Decreto N.º 229-07 ratifica el decreto N.º 1090-04 que creó la Oficina Presidencial de las Tecnologías de la Información y Comunicaciones (OPTIC)*. Disponible en: <https://optic.gob.do/index.php/marco-legal-m?download=12:decreto-229-07-instructivo-de-aplicacion-gobierno-electronico>. (Última consulta en línea 9 de julio 2018).

(2007) *Decreto N.º 297-07 ratifica el Decreto N.º 1090-04*. Disponible en: <https://www.google.com/search?q=Decreto+No.+229-07&oq=Decreto+No.+229-07&aqs=chrome..69i57j69i59.2033j0j7&sourceid=chrome&ie=UTF-8>. (Última consulta en línea 31 de mayo 2018).

(2007) *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2008-979>. (Última consulta en línea 23 de agosto 2018).

(2006) *Ley núm. 27/2006 del 18 de Julio*. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2006-13010>. (Última consulta en línea 10 de agosto 2017).

(2006) *Decreto N.º 323-06 que crea e integra la Comisión encargada de preparar las consultas que fueren necesarias tendentes a modificar la Constitución de la República*. Disponible en: http://www.camaradediputados.gob.do/serve/listfile_download.aspx?id=1121&num=1. (Última consulta en línea 11 de marzo 2018).

(2006) Ley *núm.* 340-06 sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones. Disponible en:

http://www.oas.org/juridico/PDFs/Mesicic5_RepDo_RespuestaC_Ane6.pdf.

(Última consulta en línea 24 de abril 2018).

(2005) *Decreto N.º 101-05 que crea la Comisión de Ética y Combate a la Corrupción*. Disponible en:

http://www.hacienda.gov.do/images/docs/marco_legal/decretos/decreto_101-05.pdf. (Última consulta en línea 5 de julio 2018).

(2005) *Decreto N.º 101-05 de 16 de febrero que crea la Comisión de Ética Pública y Combate a la Corrupción*. Disponible en:

http://www.hacienda.gov.do/images/docs/marco_legal/decretos/decreto_101-05.pdf. (Última consulta en línea 5 de julio 2018).

(2005) *Código Unión Europea*, la Ley-Actualidad, S. A., Edición septiembre 2005, Madrid, 2005.

(2004) *Decisión de la Comisión de 28 de abril de 2004 sobre la protección adecuada de los datos personales en la Isla de Man*. Disponible en: [https://eur-lex.europa.eu/legal-](https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415702956426&uri=CELEX:32004D0411_2004/411_/CE)

[lex.europa.eu/legal-](https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415702956426&uri=CELEX:32004D0411_2004/411_/CE)

[content/EN/TXT/?qid=1415702956426&uri=CELEX:32004D0411_2004/411_/](https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415702956426&uri=CELEX:32004D0411_2004/411_/CE)
[CE](https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415702956426&uri=CELEX:32004D0411_2004/411_/CE). (Última consulta en línea 14 de septiembre 2017).

(2004) *Con la decisión 2004/915/CE de 27 de diciembre de 2004 por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países, notificada con el número C 2004/5271*. Disponible en:

<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32004D0915>.

(Última consulta en línea 14 de septiembre 2017).

(2004) *Decreto 1090-04 presidencia de la República Dominicana*. Disponible en: <http://www.optic.gob.do/phocadownload/Marco-Legal/DECRETO%201090-04.pdf>. (Última consulta en línea 31 de mayo 2018).

(2003) *Decisión de la Comisión de 30 de junio de 2003 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales en Argentina*. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415636698083&uri=CELEX:32003D0490_2003/490_/CE. (Última consulta en línea 20 de septiembre 2017).

(2003) *COM (2003)*, Bruselas, 26/9/2003. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52003DC0567&from=ES>. (Última consulta en línea 26 de junio 2018).

(2003) *Decisión de la Comisión de 21 de noviembre de 2003 sobre la protección adecuada de los datos personales en Guernsey (Texto pertinente a efectos del EEE) [notificada con el número C (2003) 4309]*. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415701941268&uri=CELEX:32003D0821_2003/821_/CE. (Última consulta en línea 14 de septiembre 2017).

(2003) *Dictamen 8/2003 sobre el proyecto de cláusulas contractuales tipo presentado por un grupo de asociaciones empresariales («The alternative model contract»)*, Grupo del artículo 29 sobre protección de datos, adoptado el 17 de diciembre de 2003. 11754/03/ES WP 84. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp84_es.pdf. (Última consulta en línea 27 de noviembre).

(2002) *Ley núm. 183-02 que aprueba la Ley Monetaria y Financiera, regula junto a la Constitución el Sistema Monetario y Financiero de la República Dominicana*. Disponible en:

<http://www.omg.com.do/files/Uploads/Documents/Ley%20No.%20183-02.%20Que%20Aprueba%20la%20Ley%20Monetaria%20y%20Financiera.pdf>.

(Última consulta en línea 17 de abril 2018).

(2001) *Ley núm. 19-01 que instituye el Defensor del Pueblo*, participación ciudadana, República Dominicana, p. 5. Disponible en:

http://www.oas.org/juridico/spanish/mesicic2_reptom_sc_anexo_12_sp.pdf.

(Última consulta en línea 6 de mayo 2018).

(2001) *Decisión de la Comisión de 20 de diciembre de 2001 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales prevista en la Ley Canadiense de Protección de Datos Personales y Documentos Electrónicos (notificada en el documento número C (2001) 4539)*. Disponible en: [https://eur-](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002D0002&qid=1415699250815_2002/2/CE)

[lex.europa.eu/legal-](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002D0002&qid=1415699250815_2002/2/CE)

[content/EN/TXT/?uri=CELEX:32002D0002&qid=1415699250815_2002/2/CE](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002D0002&qid=1415699250815_2002/2/CE).

(Última consulta en línea 14 de septiembre 2017).

(2001) *Decisión 2001/497/CE de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE*, notificada con el número c (2001) 1539. Disponible en:

<https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32001D0497>.

(Última consulta en línea 14 de septiembre 2017).

(2001) *Decreto 1558/2001 de 29 de noviembre de 2001. Reglamentación de la ley de protección de datos personales*. Disponible en:

[http://www2.congreso.gob.pe/sicr/cendocbib/con2_uibd.nsf/983EC5385CB1658E052577B9006C2DB7/\\$FILE/Decreto_1558_Reglamenta_Ley_25.326.pdf](http://www2.congreso.gob.pe/sicr/cendocbib/con2_uibd.nsf/983EC5385CB1658E052577B9006C2DB7/$FILE/Decreto_1558_Reglamenta_Ley_25.326.pdf).

(Última consulta en línea 20 de abril del 2018).

(2001) *Reglamento N.º 45/2001 del Parlamento Europeo y del Consejo de 1 de diciembre de 2000 relativo a la protección de las personas físicas en lo que*

respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. Disponible en: <https://www.boe.es/doue/2001/008/L00001-00022.pdf>. (Última consulta en línea 25 de mayo 2018).

(2001) *Reglamento N.º 45/2001 del Parlamento Europeo y del Consejo de 1 de diciembre de 2000.* Disponible en: <https://www.boe.es/doue/2001/008/L00001-00022.pdf>. (Última consulta en línea 25 de mayo 2018).

(2001) *Ley núm. 120-01 del 20 de Julio del 2001 que instituye el Código de Ética del Servidor Público.* Disponible en: <http://www.contraloria.gob.do/Sitecontraloria/images/docs/ley-no-120-01.pdf>. (Última consulta en línea 7 de julio 20018).

(2001) *Decreto. N.º 783-01 que crea e integra el Consejo Asesor en Materia de Lucha Anticorrupción de la Presidencia de la República.* Disponible en: http://www.oas.org/juridico/spanish/dna_res2.pdf. (Última consulta en línea 5 de julio 2018).

(2000) *Decisión de la Comisión de 26 de julio de 2000 de conformidad con la Directiva 95/46 / CE del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales facilitada en Suiza [notificada con el número C (2000) 2304].* Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415700329280&uri=CELEX:32000D0518_2000/518_/CE. (Última consulta en línea 15 de julio 2018).

(2000) *Ley núm. 25326 Argentina de Protección de Datos Personales.* Disponible en: https://www.agpd.es/porta1webAGPD/canaldocumentacion/legislacion/iberoamerica/leyes_nacionales/common/pdfs/LEY-25.326-Proteccion-de-los-datos-personales.pdf. (Última consulta en línea 23 de marzo 2018).

(2000) *Carta de los Derechos Fundamentales de la Unión Europea*. Disponible en: http://www.europarl.europa.eu/charter/pdf/text_es.pdf. (Última consulta en línea 14 de agosto 2018).

(1985) *Resumen Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*. Disponible en: <http://www.oecd.org/sti/ieconomy/15590267.pdf>. (Última consulta en línea 4 de diciembre 2017).

(1999) *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750>. (Última consulta en línea 16 de noviembre 2017).

(1999) *Ley núm. 19.628 de protección de datos de carácter personal chilena publicada el 28 de agosto del 1999*, Chile. Disponible en: <https://www.leychile.cl/Navegar?idNorma=141599&idVersion=2011-07-23>. (Última consulta en línea 18 de abril 2018).

(1999) *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750>. [BOE-A-1999-23750](https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750). (Última consulta en línea 21 de septiembre de 2017).

(1999) *Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal*. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1999-13967>. [BOE-A-1999-13967](https://www.boe.es/buscar/doc.php?id=BOE-A-1999-13967). (Última consulta en línea 25 de septiembre de 2017).

(1999) *Resumen Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, Declaración sobre flujos de datos transfronterizos (1985)*. Disponible en:

<http://www.oecd.org/sti/ieconomy/15590267.pdf>. (Última consulta en línea 4 de diciembre de 2017).

(1999) *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*. Disponible en:

<https://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf>. (Última consulta en línea 16 de noviembre 2017).

(1998) *Código penal de la República Dominicana*. Disponible en:

https://www.oas.org/juridico/mla/sp/dom/sp_dom-int-text-cp.pdf.

(Última consulta en línea 11 de mayo 2018).

(1998) *Decreto 149-98 que crea las Comisiones de Ética Pública*. Disponible

en: http://www.sisalril.gob.do/pdf/transparencia/decreto_149_98.pdf. (Última verificación en línea 3 de septiembre 2018). (Última consulta en línea 3 de septiembre 2018).

(1997) *Decreto N.º 322-97 del 24 de julio de 1997 que crea el Departamento de Prevención de la Corrupción Administrativa*. Disponible en:

http://www.oas.org/juridico/pdfs/mesicic4_reptom_dec322.pdf. (Última consulta en línea 5 de julio 20018).

(1996) *Real Decreto 156/1996, de 2 de febrero, por el que se modifica el Estatuto de la Agencia de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo, para designar a la Agencia de Protección de Datos como representante español en el grupo de protección de personas previsto en la Directiva 95/46/ce, de 24 de octubre*. Disponible en:

<https://www.boe.es/buscar/doc.php?id=BOE-A-1996-2991>. (Última consulta en línea 25 de junio del 2017).

(1995) *Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos*

datos. Disponible en: www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678. (Última consulta en línea 8 de marzo 2018).

(1995) *Capítulo VI Autoridad de Control y grupo de protección de las personas en lo que respecta al tratamiento de datos personales*. Disponible en: www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678. (Última consulta en línea 8 de marzo 2018).

(1994) *Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal*. (Última consulta en línea 18 de junio 2017).

(1993) *Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos*. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1993-11252>. [BOE-A-1993-11252](https://www.boe.es/buscar/doc.php?id=BOE-A-1993-11252). (Última consulta en línea 23 de agosto 2017).

(1993) *Sentencia 254/1993 del 20 de Julio de 1993*. Disponible en: <https://www.boe.es/boe/dias/1993/08/18/pdfs/T00028-00034.pdf>. (Última consulta en línea 19 de junio 2018).

(1992) *Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal*. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189>. (Última consulta en línea 23 de junio 2018).

(1990) *Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales*. Disponible en: <http://www.un.org/es/comun/docs/?symbol=A/RES/45/95>. (Última consulta en línea 1 de diciembre 2017).

(1988) BOE, *Código de legislación Informática*, Madrid, 1988.

(1985) *Resumen Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*. Disponible en: <http://www.oecd.org/sti/ieconomy/15590267.pdf>. (Última consulta en línea 4 de diciembre 2017).

(1982) *Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-1982-11196>. (Última consulta en línea 23 de agosto 2017).

(1981) *Convenio n.º 108 del Consejo de Europa*. (Última consulta en línea 20 de septiembre 2018).

(1981) *Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447>. (Última consulta en línea 20 de septiembre 2018).

(1980) *Recomendación del consejo relativa a las directrices que regulan la protección de la privacidad y el flujo transfronterizo de datos personales (23 de septiembre de 1980)*. (Última consulta en línea 7 de diciembre de 2017).

Rules for the protection of personal data inside and outside the EU. Disponible en:

http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm. (Última consulta en línea 20 de noviembre 2017).

Decisiones de la Comisión sobre la adecuación de la protección de datos personales en terceros países. Disponible en: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm. (Última consulta en

línea 20 de noviembre 2017). Protección de datos, reglas para la protección de datos personales dentro y fuera de la UE.

El derecho a la privacidad en la era digital. *Resolución 68/167*. Disponible en: <https://undocs.org/es/A/RES/68/167>. (Última verificación en línea 18 de octubre 2019).

Entrevistas (videos)

(2019) AMER, K., NOUJAIM, J., *El gran hackeo*, Netflix, 2019.

(2018) URÍA ETXEBARRIA, M., *Protección de Datos y Transparencia: Compañeros de Viaje*, discurso inaugural curso de verano 2018. Disponible en: <http://www.avpd.euskadi.eus/webcast/s04-5273/es>. (Última consulta en línea 10 de agosto 2018).

(2018) SANTILLAN, O., *Falla Instituto Nacional de Transparencia (INAI) en protección de datos personales*. Disponible en: <http://www.ejecentral.com.mx/falla-inai-en-proteccion-de-datos-personales>. (Última consulta en línea 26 de mayo 2018).

(2016) HERZOG, W., *Lo and Behold: Reveries of the Connected World*, NETFLIX, 2016.

(2015) REMOLINA ANGARITA, N., *Protección de datos personales y proactiva empresarial*. Disponible en: <http://m.youtube.com>. (Última consulta en línea 16 de junio 2017).

(1997) ORWELL, G., *1984 George Orwell en español*. Disponible en: <https://www.youtube.com/watch?v=sxnMQ97YLvU>. (Última consulta en línea 11 de agosto 2017).

(1984) *El ojo que todo lo ve, eso es el Gran Hermano*, extracto del video 1984 George Orwell en español, Disponible en:

<https://www.youtube.com/watch?v=sxnMQ97YLvU>. (Última consulta en línea 11 de agosto 2017); Gran Hermano (Big Brother): el brazo omnipotente del gobierno: término extraído de la novela 1984. De Georges Orwell (N. del T).

(1984) ORWELL, G., *George Orwell 1984*, Disponible en: <http://www.formarse.com.ar/libros/Libros-recomendados-pdf/1984%20de%20G.Orwell.pdf>. (Última verificación en línea 02 de agosto 2017).

(1979) BENTHAM, J., *Genealogía del poder el Panóptico*. Disponible en: <https://iedimagen.files.wordpress.com/2012/02/bentham-jeremy-el-panoptico-1791.pdf>. (Última consulta en línea 02 de agosto 2017).

BENTHAM, J., *el Panóptico*, las ediciones de la piqueta, Madrid, 1979, p. 75. Disponible en: <https://iedimagen.files.wordpress.com/2012/02/bentham-jeremy-el-panoptico-1791.pdf>. (Última consulta en línea 02 de agosto 2017).

Tablas / gráficas / diagramas

Figura 1. TRONCOSO REIGADA, A., *Mapa Latinoamericano sobre la protección de datos personales: constituciones y normas generales (1985-2012*

Disponible en:

<https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Latinoamerica-proteccion-datos-en-cifras-1985-2012-Remolina.pdf>. (Última consulta en línea 24 de febrero 2017).

Figura 2. *Sentencias recibidas Tribunal Constitucional de la República Dominicana, desde su creación al 31 de marzo 2019*, (gráfico, construcción propia).

Figura 3. *Sentencias emitidas Tribunal Constitucional de la República Dominicana, desde su creación al 31 de marzo 2019*, (gráfico, construcción propia).

Figura 4. *Estudio Comparativo proyectos de ley y actual ley de protección de datos*. (cuadro, construcción propia).

Figura 5. *Vinculación: tecnología, normas jurídicas, globalización* (diagrama, construcción propia).

ANEXO