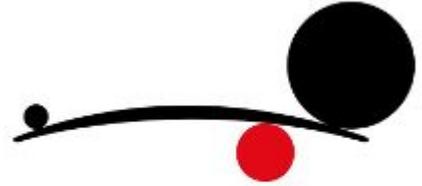


eman ta zabal zazu



Universidad
del País Vasco

Euskal Herriko
Unibertsitatea



Zuzenbide Fakultatea
Facultad de Derecho

**EL USO DE LA TECNOLOGÍA Y LA INNOVACIÓN PARA LA
PREVENCIÓN DE ACCIDENTES EN LOS DEPORTES DE
DESLIZAMIENTO Y SU CONSECUENCIA CON LA
PROTECCIÓN DE DATOS.**

MIKEL MORALEJA MURILLO.

GRADO EN DERECHO, FACULTAD DE DONOSTIA.

TRABAJO DE FIN DE GRADO.

TRABAJO DIRIGIDO POR : SANTIAGO GOÑI ZABALA.

ABSTRACT.

In recent years, the increase in the practice of water sliding sports, especially surfing, is undoubtedly a reality. There is no more to see the influx of surfers in the Basque coast. Another reality is that the surf is a sport of risk. Due to the large number of accidents that occur, high-technology companies are betting on new security systems to prevent them, making use of personal data and health data. This brings consequences for data protection because on May 25 of this year the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, will go into force.

Keywords: Law, regulation, surf, data protection, health data, technology.

LABURPENA.

Azken urteotan, ur-kirolen praktikaren hazkundera, batez ere surfa, zalantzarik gabeko errealitatea da. Euskadiko eta Lapurdiko kostako surflari kantitatea. Beste errealitate bat da kirol arriskutsua dela. Goi teknologiako enpresek, erabiltzaileek jasaten dituzten istripuen kopuru handia dela eta, segurtasun-sistema berrien alde egiten dute hauen prebentzioan, honetarako erabiltzaileen datu pertsonalek erabiliko dituzte. Honek, bere ondorio ditu datu babesarekin eta gainera, urte honetako maiatzean Europako Parlamentuaren eta Kontseiluaren 2016/679 erregelamendu berria (2016ko apirilaren 27koa, pertsona fisikoen babesari buruzkoa) datu pertsonalen tratamenduari eta datu horien doako zirkulazioaren inguruan, sartuko da indarrean.

Hitz gakoak: Zuzenbidea, erregelamendua, surf, datu babesa, osasunari buruzko datuak, teknologia.

RESUMEN.

En los últimos años el incremento de la práctica de deportes de deslizamiento acuáticos, sobre todo el surf, es una realidad indudable. No hay más que ver la afluencia de surfistas la costa vasca y labortana. Otra realidad es que es un deporte de riesgo. Debido a la gran cantidad de accidentes que ocurren las empresas de alta tecnología están apostando por nuevos sistemas de seguridad para la prevención de ellos, haciendo uso de datos personales. Esto trae consecuencias en la protección de datos y encima el 25 de mayo de este año entra en vigor el nuevo 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 al la libre circulación de estos datos.

Palabras clave: Derecho, reglamento, surf, protección de datos, datos de salud, tecnología.

SUMARIO.

I. INTRODUCCIÓN.....	6
1.1 Explicación del proyecto.....	6
1.2 Experiencia personal/posicionamiento.....	10
II. OBJETIVOS DEL TRABAJO.....	11
III. ANÁLISIS DE LA NUEVAS PROPUESTAS DE DIFERENTES ENTIDADES.....	12
1. CLÚSTER GAIA.....	12
2. AZTI TECNALIA.....	15
IV. MARCO CONCEPTUAL.....	17
1. LA PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL.....	17
2. ANÁLISIS DE CONCEPTOS.....	19
2.1 Concepto de intimidad.....	19
2.2 Dato personal.....	20
2.3 Datos relacionados con la salud.....	20
2.4 Consentimiento del interesado.....	22
2.5 Concepto de tratamiento.....	23
2.6 Elaboración de perfiles.....	23
2.7 Seudonimización.....	23
2.8 Concepto de fichero.....	24
2.9 Evaluación de impacto.....	25
2.10 Cesión de datos.....	25
2.11 Tratamiento de datos de salud para la investigación/innovación.....	25

2.12 Responsable del tratamiento.....	26
2.13 Encargado del tratamiento.....	26
3. DIFERENTE TIPOLOGÍA DE DATOS.....	26
3.1 Carácter de los datos.....	26
3.1.1 Datos de carácter anónimo.....	26
3.1.2 Datos seudónimos.....	27
3.1.3 Datos nominativos.....	27
3.2 Tipología.....	28
3.2.1 Historial clínico.....	28
V. REQUISITOS A CUMPLIR POR LAS EMPRESAS A LA HORA DEL TRATAMIENTO DE DATOS PERSONALES.....	31
1. Introducción.....	32
2. Ruta para el correcto tratamiento de datos.....	32
VI. PROBLEMÁTICA DETECTADA Y SOLUCIONES.....	36
1.PROYECTO DE EMERID.....	36
1.1 Problemática del acceso al historial clínico.....	36
1.2 Consentimiento del interesado.....	38
1.3 Legitimación a la hora del tratamiento <i>¿Quién va a realizar el tratamiento?</i>	39
1.4 <i>¿Quién está legitimado para pasar el lector por los trajes?</i>	40
1.5 Posibles sanciones.....	41
2.WOO.....	42
3.AZTI TECNALIA.....	42

3.1 La imagen como dato personal. ¿es la imagen dato personal?.....	42
VII. CONCLUSIÓN.....	44
IX. FUENTES.....	46
1. BIBLIOGRAFÍA.....	46
2. LEGISLACIÓN.....	47
3. JURISPRUDENCIA.....	47
4. ENTREVISTAS.....	47
5. WEBGRAFÍA.....	48
X.ANEXOS.....	48
1. Ficha de entrevista a Jokin Garatea e Itziar Vidorreta.....	48
2. Ficha de entrevista a Juan Ramón Barrena Arriarán.....	51
3. Ficha de entrevista a Julen Mader.....	57
4. Ficha de entrevista Jokin Garatea 2.....	60
5. Anexo número 5: Imágenes.....	62

1. INTRODUCCIÓN

1.1 Explicación del proyecto

En 2015, La Universidad de Burdeos y la Universidad del País Vasco/Euskal Herriko Unibertsitatea lanzaron la iniciativa Plataforma Ocean Experiences (POE) en el contexto del convenio marco de colaboración firmado el 27 de noviembre de 2015. La Plataforma constituye una propuesta de estructuración de las actividades de formación-investigación-transferencia en torno a la actividad de los deportes acuáticos de deslizamiento, que agrupa, además de las universidades participantes a los agentes territoriales públicos y privados del País Vasco a ambos lados de la frontera, agentes públicos y privados, como la Agglomération Sud du Pays Basque, la Fundación Euskampus, el Clúster Eurosima (que reúne 180 empresas, 122 marcas y 58 representantes de servicios), etc.

La iniciativa POE pretende contribuir al eje temático de especialización territorial en relación a la innovación en deportes acuáticos y la promoción del turismo activo, para lo cual cuenta con financiación de la Unión Europea, y se estructura en torno a tres nodos articuladores: una Halle Creative, un Living Lab y un acelerador de start-ups que asocia agentes públicos y privados.

El primer eje de actividad lo constituye la innovación en producto relacionado con el sector de actividad de deportes acuáticos. Su desarrollo físico tiene lugar en el denominado Halle Creative, espacio de innovación que consta de una “materioteca” y semilleros de empresa con el fin de investigar la fabricación de productos innovadores en el sector acuático. Esta iniciativa ayudará a diferentes empresas a crear prototipos innovadores facilitándoles un espacio donde poder diseñar y testar estos productos con diferentes materiales. Recientemente, la asociación ha sido labelizada con el sello de la asociación europea EnoLL, que la reconoce como laboratorio para la innovación abierta donde el usuario representa el centro del desarrollo con el objetivo de diseñar y testear en condiciones reales productos y servicios innovadores.

Y, por último, el tercer eje está representado por el fuerte de Socoa, cuya función principal en el seno del proyecto Ocean Experience consiste en la de organizar y ofrecer formación continua y discontinua en el ámbito de los deportes acuáticos entendidos en su más amplia acepción –desde la vertiente de innovación en producto, pasando por las necesidades de formación continua expresadas por las empresas, como la iniciativa de Plataforma que se inscribe en la prospección jurídica y diagnóstico de los problemas.

Los tres ejes descritos constituyen la base del proyecto de estructuración de una zona atractiva tanto para las empresas innovadoras como para las administraciones territoriales interesadas en atraer usuarios de deportes acuáticos a la zona litoral del País Vasco y la costa de Aquitania. Y es precisamente en este contexto, en el que la práctica de los deportes acuáticos concurre con otros usos lúdicos del litoral en un entorno transfronterizo en el que se plantea un elenco muy rico de cuestiones jurídicas susceptibles de ser estudiadas con una óptica prospectiva, acompañando el desarrollo de la Plataforma y de sus objetivos estratégicos.

La iniciativa Zuzenbideocean que se puso en marcha en el curso 2016/2017, se inscribía en el marco de actividad de la Plataforma Ocean Experiences, constituyendo una experiencia de formación desarrollada en colaboración entre la Clínica Jurídica de la Universidad de Burdeos y la Facultad de Derecho de la UPV/EHU. En esta experiencia participaron seis alumnos de máster 1 de la Universidad de Burdeos y otros seis estudiantes de cuarto curso del Grado de Derecho la UPV/EHU. El equipo internacional de estudiantes, apoyado por profesores y personal perteneciente al POE así como a ambas Universidades, puso su saber jurídico al servicio de la resolución de los problemas jurídicos transfronterizos planteados por la Plataforma.

El dispositivo creado tenía como finalidad crear sinergias entre las necesidades en términos de información jurídica de los agentes agrupados en torno al POE y los imperativos de inserción profesional de los estudiantes universitarios en los cursos avanzados de formación. Ello implicó, por una parte, la puesta en práctica de competencias transversales (técnicas de identificación de problemas a través de entrevistas personales y búsqueda bibliográfica, articulación de conocimientos de

distintas ramas del derecho en torno a problemas complejos, compartir trabajo en equipo en un entorno internacional y multicultural, participación en la co-creación del proyecto identificando las necesidades de aprendizaje y condiciones operativas en las que se desarrolla la iniciativa formativa). En segundo lugar, la formación se desarrolló en entornos de problemas reales donde los estudiantes alcanzaron un importante nivel de implicación y se comprometieron en la identificación y estudio de la casuística propuesta. Por otra parte, la composición del equipo (UB/UPV) y la localización de los trabajos en la zona transfronteriza permitieron estudiar casos desde la óptica de ambos ordenamientos así como de Derecho internacional público y privado, invitando a los estudiantes a apropiarse de la cultura de cooperación transfronteriza en materia jurídica. Finalmente, el proyecto permitió al alumnado participante multiplicar el número de agentes públicos y privados con los que han interactuado, generando así un vivero de reclutamiento profesional de cara al futuro.

La metodología de trabajo en este primer consistió en que el equipo de estudiantes voluntarios experimentó, mediante varias técnicas de investigación, la identificación de problemas jurídicos in situ, con el objetivo común de elaborar un dictamen que recogiera propuestas temáticas para la futura Plataforma Jurídica Zuzenbideocean.

Este curso 2017/2018, la iniciativa Zuzenbideocean ha continuado su curso, teniendo como punto de partida el dictamen final del grupo de estudiantes del curso 2016/2017. Para ello se ha vuelto a constituir otra experiencia de formación desarrollada en colaboración entre la Clínica Jurídica de la Universidad de Burdeos y la Facultad de Derecho de la UPV/EHU. Esta vez, hemos participado en la experiencia cuatro alumnos de Master 1 más dos alumnos de Master 2 de la Universidad de Burdeos y cinco alumnos de cuarto curso del grado de Derecho, junto a Mattin Astigarraga estudiante del Máster de Abogacía de la UPV/EHU y que el año pasado participó en el proyecto. El tema que se nos ha adjudicado este año para el proyecto ha sido el siguiente: “La prevención de accidentes en los que están involucrados los deportes de deslizamiento y garantizar el uso y disfrute de la playa a los usuarios de la playa”. Cabe añadir que este trabajo no hubiera sido posible sin la ayuda de los profesores y personal perteneciente al

POE y los profesores de ambas Universidades, los cuales han puesto su saber jurídico al servicio de nuestra investigación.

La identificación de los problemas en torno al tema citado previamente, ha implicado en primer lugar, la puesta en práctica de competencias transversales (técnicas de identificación de problemas a través de entrevistas personales y búsqueda bibliográfica, articulación de conocimientos de distintas ramas del Derecho en torno a problemas complejos, compartir trabajo en equipo en un entorno internacional y multicultural, participación en la co-creación del proyecto identificando las necesidades de aprendizaje y condiciones operativas en las que se desarrolla la iniciativa formativa). En segundo lugar, la formación se ha desarrollado en entornos de problemas reales (Zarautz, Donostia-Zurriola y Hendaya) donde los estudiantes han alcanzado un importante nivel de implicación y se han comprometido en la identificación y estudio de la casuística propuesta. Por otra parte, la composición del equipo (UB/UPV) y la localización de los trabajos en la zona transfronteriza han permitido estudiar casos desde la óptica de ambos ordenamientos así como de derecho internacional público y privado, invitando a los estudiantes a apropiarse de la cultura de cooperación transfronteriza en materia jurídica.

La metodología de trabajo ha consistido en que el equipo de estudiantes ha experimentado, mediante varias técnicas de investigación, la identificación de problemas jurídicos, con el objetivo común de elaborar un dictamen que proponga soluciones a las causas de los problemas jurídicos identificados, sobre la prevención de accidentes en los que están involucrados los deportes de deslizamiento y garantizar el uso y disfrute de la playa a los usuarios de la playa. Para llevar a cabo este trabajo hemos pasado por diferentes etapas, que son las siguientes:

La primera de ellas fue con los seis alumnos de la Universidad de Bordeaux se convocó en Hendaia como punto medio de encuentro entre las dos universidades. En esta cita pudimos trabajar en la organización de la información para llevar a cabo el proyecto a distancia y fijar las tareas a realizar en las siguientes fechas. Durante las siguientes

semanas continuamos trabajando en el estudio comparado mediante seminarios en Urrugne y reuniones vía Skype.

El primer trabajo que realizamos fue el Contexto; cada universidad en su territorio, y después poniéndolo en común con los estudiantes franceses. Una vez definido este apartado, nos dividimos en tres grupos para realizar diferentes entrevistas a agentes relacionados con las playas de Zarautz y Donostia - San Sebastián.

En segundo lugar, extrajimos de las entrevistas varios problemas jurídicos, de los que cada alumno escogió uno siendo su objeto de estudio: el trabajo de fin de grado. Estos cinco trabajos, unidos con la investigación de los alumnos de Burdeos, forman parte del dictamen final que se presentará el día 15 de junio en Facultad de Derecho de Donostia y el Ayuntamiento de Hendaya.

Para finalizar la experiencia, el dictamen será presentado públicamente ante los ciudadanos de Zarautz y Hendaya, mediante el formato *Street Law*.

1.2 Experiencia personal y posicionamiento

En este punto explicare brevemente mi experiencia personal en el proyecto. El grupo de investigación nos dividimos en tres grupos. Cada grupo abarcó una playa. En mi caso, Gabriela Escámez y yo trabajamos en la playa de la Zurriola analizando la problemática que esta tenía , mediante varias entrevistas a diferentes agentes. Por un lado, a los surfistas y escuelas de surf, por el otro lado a los usuarios de la playa y la Cruz Roja. La metodología utilizada fue la entrevista directa y mediante skype, donde llevábamos unas preguntas anteriormente preparadas y luego las que nos iban surgiendo durante ella. Después de hacerlas, las transcribimos en una fichas técnicas anteriormente preparadas por las dos universidades.

2. OBJETIVOS DEL TRABAJO.

Después de una exhaustiva investigación de la problemática de las playas del litoral guipuzcoano y labortana. El grupo de investigación, nos reunimos en la sede de Tribord (Hendaia) y nos encontramos con diferentes causas por las que ocurren los accidentes en los deportes de deslizamiento acuáticos, mayormente en el surf, dado que es el deporte más practicado.

Con la cantidad de problemas que ocurren las empresas están sacando nuevas propuestas para su prevención. En todas las propuestas se emplearán datos de los usuarios, datos de una sensibilidad y privacidad extrema. Estos datos deben estar seguros y usarlos con el objetivo de salvar vidas. Por eso, uno de los problemas que detectamos fue el de cómo las nuevas tecnologías iban a tratar con estos datos. Es indudable que hoy día estamos sumergidos en un mundo dominado por la tecnología también es indiscutible la importancia que estas tiene a la hora de la prevención de accidentes.

Desde que nacemos tenemos dos datos, el nombre y el apellido y mientras vamos creciendo vamos creando nuevos datos, como el DNI, el email, domicilio etc. Manejamos y facilitamos infinidad de datos durante todo el día, a la hora de hacer compras online, cuando reservamos un vuelo y muchos datos más, muchos de ellos los damos sin darnos cuenta. Estos datos son de gran valor para las empresas, es un tesoro para ellas, damos muchísima información sobre uno mismo, gustos, aficiones. Por eso tenemos que ser responsables con todo los datos que proporcionamos.

Todos, en los que me incluyo, hemos escrito nuestro nombre en Google para ver que aparecía y personalmente me sorprendió toda la cantidad de información que sale sobre uno mismo. Desde un “like” de Facebook, hasta las fotos subidas a Instagram y muchos mas datos.

¿Pero qué ocurre si los datos que hemos proporcionado son para prevenir accidentes? En este caso estamos hablando de datos de gran sensibilidad por lo cual mi reto es determinar los

requisitos y pautas que deberán de tomar estas empresas a la hora del tratamiento de estos datos.

De hecho, esta última semana, ha salido a la luz el escándalo de Facebook. Esta semana Mark Zuckerberg compareció en el Senado de EEUU, por compartir y utilizar alrededor de 86 millones de usuarios sin el consentimiento del dueño de ellos y muchos de ellos con fines políticos. ¿Quién dice que dentro de esa cantidad de datos no están nuestros datos?. Estos datos son vendidos a empresas y estas hacen un perfil de cada uno, no lo cual ya saben cuáles son nuestras aficiones, gustos y entonces sabes que tipo de publicidad nos interesa etc. Estos tipos de datos, sobre todo los médicos, son un banco de oro para las aseguradoras, ya que viendo el estado de salud del interesado pueden asegurarlo o no.

3- ANÁLISIS DE LAS NUEVAS PROPUESTAS TECNOLÓGICAS DE DIFERENTES ENTIDADES.

3.1 GAIA.¹

Antes de empezar a analizar el proyecto, tenemos que contextualizar el proyecto. En primer lugar en España en el 2016 hubo 321 fallecidos entre enero y septiembre, 1,8 ahogamientos por día.² En Euskadi, en el año 2016 hubo 18 muertes en espacios acuáticos³. El perfil del ahogado en Euskadi es hombre de nacionalidad española de más de 55 años (comunidad silver). En cambio solo una mujer murió. Y el 83% de los ahogamientos mortales del año 2016.⁴

¹ Ficha Entrevista Jokin Garatea e Itziar Vidorreta. Realizada por Gabriela Escámez y Mikel Moraleja.

² Informe Nacional de Ahogamientos que elabora la Real Federación Española de Salvamento y Socorrismo.

³Ibidem.

⁴ Ibidem.

En la playa de la Zurriola en Donostia, en el año 2017 en la temporada estival (junio, julio, agosto y septiembre) hubo en 70 rescates a usuarios, teniendo la cifra más alta en julio con 27 rescates⁵. Otro dato de importancia también es que hubo en el mismo año 43 evacuaciones, siendo julio también, el mes con la cifra más alta, con 28 rescates⁶.

En cuanto a las asistencias sanitarias en el mismo año anterior en las cuatro playas de Donostia (la isla incluida) hubo en total 2527 asistencias sanitarias durante la temporada estival de 2017⁷. Siendo la playa de la Zurriola con la mayor cifra, en total 817⁸. Las lesiones más típicas son heridas, traumatismos cerrados, luxaciones, esguinces y fracturas. El resto son picaduras, golpes de calor y quemadura⁹.

Una de las causas de estos accidentes es que la irresponsabilidad de cada uno, es decir, la percepción de riesgo no es muy alta cuando hablamos de deportes y actividades realizadas en el medio acuático, no ocurre lo mismo en la montaña. Juan Ramón Barrena, director Provincial de Salud y Socorros, apuntaba “ *En las playas TIENE QUE PRIMAR LA VIDA Y MINIMIZAR LOS RIESGOS, para esto aparte de la ayuda y del gran labor de la Cruz Roja, hace falta dos cosas. En primer lugar, el segundo común, y en segundo lugar el respeto. El afirma que es posible la convivencia, pero eso sí, teniendo en cuenta el sentido común y el respeto.*”¹⁰ Por lo tanto aparte de incrementar la seguridad, el sentido común es necesario a la hora de la prevención de accidentes. Para ello la tecnología y la innovación son necesarias.

⁵ Informe realizado por la Cruz Roja Gipuzkoa del año 2017.

⁶ *Ibidem*

⁷ *Ibidem*

⁸ *Ibidem*

⁹ Ficha técnica Juan Ramon Barrena. Realizada por Gabriela Escámez y Mikel Moraleja. Anexo número 1.

¹⁰ Ficha técnica Juan Ramon Barrena. Realizada por Gabriela Escámez y Mikel Moraleja. Anexo número 1

Por ello Gaia, ha creado el proyecto llamado “ socorrista virtual”. ¿Pero qué es el socorrista virtual? Es un sistema inteligente e innovador que utilizan las tecnologías más punteras de empresas del País Vasco, pymes, startups, clústers... para ofrecer seguridad en las zonas costera 24 horas al día 365 días al año. El piloto del socorrista virtual consiste en 5 diferentes tecnologías para la prevención de accidentes. A nosotros nos interesa el sistema de seguridad Emerid que es el sistema donde trabaja con datos personales.¹¹ Adentrándonos en la web oficial del sistema de seguridad Emerid así lo define este novedoso proyecto; “ *sistema de identificación para situaciones de emergencia que proporciona los datos de identificación de cada usuario a través de un dispositivo wearable único y personal que contiene una ficha con la información más relevante como el historial médico, datos de contacto o ubicación actual, entre otros.*”

¹²

Este prototipo está basada en tecnología NFC que se incorpora en los textiles de los usuarios. Estos dispositivos emiten y proporcionan datos, estos datos serian, información de carácter personal, datos relacionados con la salud, información de contacto y también la información de la ubicación.

En nuestro caso a la hora de a prevención de accidentes de deportes de deslizamiento puede ser de vital uso, ya que, en los neoprenos de los deportistas y los bañadores se podría implantar este sistema. También, tiene un opción de llamar a la 112.

Otra de las propuestas dentro de socorrista virtual, es WOO (Waima Outrigger Organisation) es una piragua inteligente del futuro. Esta trabaja con datos, pero estos, datos no son de carácter personal.

¹¹ Ficha Entrevista Jokin Garatea e Itziar Vidorreta. Realizada por Gabriela Escámez y Mikel Moraleja. Anexo 1.

¹² Información obtenida de la web oficial de Emerid System. Disponible en: <https://emerid.com>

3.2 AZTI TECNALIA.¹³

Azti Tecnalia (*Transforming Science to Business*), es una empresa que se dedica las nuevas tecnologías. Así dice la web oficial de la entidad “ *En el Centro Tecnológico desarrollan productos, servicios e iniciativas empresariales sostenibles que dinamizan el tejido industrial y recuperan y preservan los recursos naturales. Transformar la ciencia en desarrollo sostenible y saludable para la sociedad presente y futura, es nuestra seña de identidad.*”¹⁴

Gabriela Escámez y Oihane Vadillo, dos componentes del grupo de investigación, entrevistaron a Julien Mader. Este les presentó el proyecto Kostas System, esta aplicación consiste en poner unas cámaras de vigilancia en puntos estratégicos de las playas, para poder investigar tres puntos. El primero sería la morfología de la playa esto es la arena, el segundo sería, la densidad de usuarios que se encuentran en el arenal y por último las corrientes acuáticas. Gracias a estas cámaras se analizarán los tres puntos anteriores.

Por ahora este tipo de cámaras no están implementadas en las playas de Donostia /San Sebastián, pero hay otros municipios como Deba y Hondarribia donde se aplicará este novedoso sistema de seguridad. Ahora, las están aplicando en Bizkaia, en localidades como Bakio, Mundaka y en la playa de Zarautz.

¹³ Ficha de entrevista a Julien Mader, realizada por Oihane Vadillo y Gabriela Escámez. Anexo 3.

¹⁴ Web oficial de Azti Tecnalia.



Diferentes estaciones del proyecto Kostas System.

Fuente: Azti Tecnalia.



Instantánea a tiempo real de la Playa de Zarautz a las 7.17 pm. Fuente: Azti Tecnalia.

Estas imágenes, además de servirles a ellos como instituto de tecnología para sus estudios, son transferidas, además, a los socorristas al instante, y ellos con esto pueden ver las corrientes de ese día, incluso predecir las de los próximos. Es por eso que nos referimos a ellas como métodos de seguridad, porque según Julien, no sólo los socorristas pueden garantizar la seguridad del usuario de la playa, sino que las nuevas tecnologías nos ayudan a tener una información más exacta de las corrientes y mareas, para después balizar la playa de la manera más correcta.¹⁵

¹⁵ Ficha de entrevista a Julien Mader, realizada Por Oihane Vadillo y Gabriela Escámez. Anexo 3.

Estas cámaras tienen que ser fijas, no puede ser drones. Porque en la entrevista mis compañeras le preguntaron si esta podría realizarse con drones y Julien les dijo que no¹⁶.

Para nuestro tema, este proyecto es de vital valor ya que con el uso de estas cámaras puede hacer un gran labor en la prevención de accidentes, en nuestro caso, en los accidentes de deportes de deslizamiento acuático.

4. MARCO CONCEPTUAL.

Para poder llegar a entender el tema del que estamos tratando es necesario definir varios términos fundamentales. Estos términos tienen relación el derecho fundamental a la protección de datos. Estas definiciones están actualizadas, por 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 (Reglamento general de protección de datos)*

1. LA PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL.

La protección de datos es considerada un derecho fundamental derivado del artículo 18 de CE. Esta no nos da una definición de ella, pero gracias a la jurisprudencia del Tribunal Constitucional ha ido configurando el significado de dicho término.

Este concepto es un poco ambiguo, a simple vista parece que este derecho protege a los datos en general, pero no es así, realmente protege a las personas con las que esos datos

¹⁶ Ficha de entrevista a Julien Mader, realizada Por Oihane Vadillo y Gabriela Escámez. Anexo 3.

están relacionados.¹⁷ Por lo cual, no son los datos los que se protegen sino a la persona dueña de ellos.

La RGPD en su Considerando número 1 dice textualmente “ La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental.” Por otro lado este derecho también está recogido por la Carta de Derechos Fundamentales de la Unión Europea en su artículo 8.1 y también, por el TFUE en su artículo 16.1 donde señalan que toda persona tiene derecho a la protección de los datos de carácter personal que les conciernen. El considerando número 4 del RGPD no lo considera como un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.

La sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre definió el concepto de derecho fundamental a la protección de datos y la diferenció del derecho a la intimidad. Así dice “ *En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.*” Por lo tanto el artículo 18.1 tiene como objetivo proteger a las personas frente a cualquier invasión o vulneración que se realizar en el campo de la vida personal y familiar de sujeto¹⁸.

¹⁷ MORTE FERRER, Ricardo. “¿Protección de datos/privacidad en la época del Big Data, IoT, wearables...? Sí, más que nunca.” *Dilemata*, N.º. 24, 2017, pág 224.

¹⁸ STC 292/2000, de 30 de noviembre. Fundamento jurídico número 6.

2. ANÁLISIS DE LOS CONCEPTOS.

2.1 Concepto de intimidad.

La humanidad está obligada a sufrir cambios y la sociedad y el derecho tiene la necesidad y la obligación de dar respuesta y definiciones a estos cambios. Esto les paso a los dos estudiantes de derecho de la universidad de Harvard, Warren y Brandeis. Vieron la necesidad de definir la privacidad y la intimidad, por lo tanto escribieron la monografía llamada “the right to privacy” donde definen que el derecho a la intimidad es un “derecho del individuo a determinar, ordinariamente, en qué medida sus pensamientos, sentimientos y emociones deben ser conocidos por otros”¹⁹. En la doctrina española tenemos al jurista García San Miguel, el que define el concepto de intimidad como “el derecho a no ser conocidos, en ciertos aspectos, por los demás. Es un derecho al secreto, a que los demás no sepan lo que somos y lo que hacemos”²⁰

En España este derecho está recogido en el artículo 18 CE. “*Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*” Por lo tanto, estamos ante un derecho fundamental, este derecho está recogido con el derecho al honor y a la propia imagen.

Por otro lado el Tribunal Constitucional ha definido el derecho a la intimidad de una manera más amplia que en las anteriores . En derecho a la intimidad está vinculado a la parte más personal y reservada de cada individuo, para así estar protegido de las miradas ajenas y preservar el derecho de mantenerse oculto.²¹ Este derecho no solo protege a la personas anónimas, si que también a las personas más expuestas al público

¹⁹ REBOLLO DELGADO, Lucrecio, *El derecho fundamental a la intimidad*, Dykinson, segunda edición, Madrid. 2000.pág.91.

²⁰ GARCIA SAN MIGUEL, Luis, *Estudios sobre el derecho a la intimidad*. Tecnos Madrid, 1992. pág.18.

²¹ Disponible en : <http://www.congreso.es/>

²². La intimidad, no solo está reconocido al individuo como persona individual sino que también abarca el núcleo familiar de él²³.

2.2 Dato personal.

Después de analizar detalladamente el derecho a la intimidad, pasamos a la definir el concepto de dato personal, de este modo vamos podremos entender el significado del derecho a la protección de datos. Así define el artículo 4.1 del RGDP “ *toda información sobre una persona identificada o identificable “el interesado”;* se considera persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo el nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona”. Esto es, los datos personales son los datos información de una persona identificada o puedan llegar identificar a la persona como tal, por ejemplo, el nombre, el apellido, estado civil, edad, datos académicos, profesión, el número de cuenta corriente, las deudas que la persona tiene, póliza de seguro, tendencia sexual. La novedad de este Reglamento europeo es que considera un dato personal relacionado con identificadores que hagan a la persona identificable.²⁴ Otra de las novedades de este reglamento es que a la persona física identificada o identificable se le denomina como “el interesado”.

2.3 Concepto de datos relacionados con la salud.

²² STC 134/1999, de 15 de julio. Fundamento jurídico 7

²³ SSTC 197/1991, de 17 de octubre. Fundamento jurídico 3.

²⁴ALVAREZ HERNANDO, Javier. *Practicum protección de datos*, Thomson Reuters, Primera edición, Cizur menor, 2017. , pág.60.

La definición de este término se encuentra en artículo del 4.15 RGDP así dice, “*datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre la salud*”. Dentro de los datos de la salud existen dos subcategorías. La primera sería datos genéticos y la segunda datos biométricos. Entre los conceptos relativos relativos a la salud debemos incluir este tipo de datos;

En primer lugar datos sobre el estado salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. También se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

Health in data in apps and devices, es trabajo realizado en 2015 por el Grupo del artículo 29²⁵ dice los siguiente sobre los datos de salud;

This may include devices analysing a person's urine and blood, and apps measuring blood pressure or heart rate, regardless whether the testing is

²⁵ Es un órgano consultivo independiente integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea, que realiza funciones de secretariado. Fuente: Agencia Española de Protección de Datos.

*performed by medical professionals or by devices and apps freely available on the commercial market an irrespective whether these devices are marketed as medical devices or not.*²⁶

Según este trabajo, también entran dentro de la categoría de datos sobre la salud los dispositivos que analizan la orina y sangre de una persona y aplicaciones que miden la presión sanguínea o la frecuencia cardíaca, independientemente de si las pruebas son realizadas por profesionales médicos o por dispositivos y aplicaciones disponibles libremente en el mercado comercial e independientemente de si estos dispositivos se comercializan como dispositivos médicos o no.

Cabe destacar, que este tipo de datos tiene un carácter especial debido a la sensibilidad de ellos, por ello el Reglamento en su artículo 9.1 señala que “ *Quedan prohibidos el tratamiento de dato personales que revelen el origen étnico, racial las opiniones políticas, los convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de una manera inequívoca a una persona física, datos relativos con la salud o otros datos relativos a la salud o datos relativos a la vida sexual y orientacion sexules de una persona física.*” Por eso como bien he dicho anteriormente el consentimiento tiene debe de ser explícito.

2.4 Consentimiento del interesado.

El artículo 4.11 del REDP señala; “ *consentimiento del interesado es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea una declaración o una clara acción afirmativa, el tratamiento de datos que le conciernen.*” Es decir, el consentimiento solo lo puede dar el interesado, ese consentimiento tiene que ser libre, informada e inconfundible y lo puede dar mediante una declaración o una clara acción afirmativa. Con lo cual este reglamento

²⁶ Grupo del Artículo 29, *Health in data in apps and devices*, Comision Europea. 2015,

elimina la opción del consentimiento tácito a la otra del tratamiento de estos datos, el consentimiento tiene que ser explícito

2.5 Concepto de tratamiento.

La RGDP en su artículo 4.2 define el concepto de tratamiento. Así dice, *“cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales, ya sea por procedimientos automatizado o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, suspensión o destrucción.”* Por lo tanto, para definirlo en dos palabras sería *el uso de los datos en general.*

2.6. Elaboración de perfiles.

Elaboración de perfiles, este término es muy importante para el tema que nos concierne, el artículo 3.4. del RGDP así lo define *“la elaboración de perfiles es toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.”*

2.7. Seudonimización.

Este concepto está recogido en el artículo 4.5 del RGDP. *“La seudonimización es el tratamiento de datos personales de manera tal que ya no puedan atribuirse al interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuya a una persona física*

identificada o identificable. Estamos ante un concepto jurídico que ha evolucionado gracias al impacto de las nuevas tecnologías". Este término ha evolucionado del antiguo concepto de la anonimización, esta es una herramienta para aplacar los riesgos que la masivo tratamiento de datos. La anonimización se basaba en quitar el nombre o la identificación a los datos personales de cada interesado. Pero hoy día, con el avance de la tecnología, aunque no tengamos el nombre del interesado cotejando un par de datos fácilmente se podría identificar al interesado. La seudonimización tiene origen en el concepto anteriormente definido, tiene como objetivo garantizar que los datos personales del interesado no se le puedan atribuir a sí mismo, es decir, que para relacionar al sujeto con el dato necesiten hacer un esfuerzo desproporcionado.

Finalmente, así aclara Javier Alvarez Hernando *“es la separación de datos identificativos con barreras técnicas u organizativas que impidan su identificación posterior”²⁷*.

Esta medida tiene como fin reducir el riesgo en tratamiento de los datos. así lo dice el considerando número 28 del RGDP: *La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos.*

2. 8 Concepto de fichero.

Esta definición está recogida en la RGDP en su artículo 4.6, donde señala que el término fichero *“es todo el conjunto estructurado de los datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido*

²⁷ ALVAREZ HERNANDO, Javier. *Practicum protección de datos*, pág.68.

o de forma funcional o geográfica". Es decir, en los ficheros se almacenan los datos personales del interesado.

2.9 Evaluación de impacto.

La evaluación de impacto (EIPD) o en inglés *Privacy Impact Analysis*, es una herramienta que permite evaluar de forma anticipada cuáles podrían ser los riesgos potenciales a las que los datos personales de los interesados podrían sufrir a la hora del tratamiento de ellos. Por lo cual, es necesario hacer un análisis exhaustivo posibles riesgos existentes, y así, con el objetivo de bajar el riesgo al mínimo y garantizar los derechos y libertades del interesado.

2.10 Cesión de datos.

La cesión de datos como bien dice su nombre es toda revelación de datos realizada a una persona distinta del interesado. Estos datos se deben de tratar de manera lícita, legal y transparente en relación con el interesado. Teniendo la anterior definición como guía, Alvarez Hernando suma a esta definición dos notas, así dicen; *"La existencia de una voluntad del responsable del fichero de revelar datos a una persona distinta del interesado. La revelación de datos a terceras personas se realiza mediante un tratamiento de datos personales"*²⁸

2.11 Tratamiento de datos de salud para la investigación y la innovación.

Este concepto tiene su definición en el artículo 89 del RGDP, donde dice *"que el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan*

²⁸ ALVAREZ HERNANDO, Javier. *Practicum protección de datos*, pág.68.

alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.”

2.12. Responsable del tratamiento.

El responsable del tratamiento *“es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros”*. Así lo define el artículo 4.7 de RGPD.

2.13. Encargado del tratamiento.

El encargado del tratamiento *“es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable”*, así lo dice 4.7 de RGPD. Esta persona trabaja bajo la responsabilidad del responsable del tratamiento.

3. DIFERENTE TIPOLOGÍA DE DATOS.

3.1 CARÁCTER DE LOS DATOS.

Estos datos, pueden tener el carácter de anónimo, seudónimos o nominativos.

3.1.1 DATOS DE CARÁCTER ANÓNIMO.

Los datos anónimos son, lo que información que no guarda ninguna relación con la persona identificada o identificable. La ley 14/2007, de 3 de julio, de Investigación Biomédica también define que es un dato anónimo, en su artículo 3.h así dice *“dato registrado sin un nexo con una persona identificada o identificable”*.

Por lo tanto esta ley no protege el tratamiento de datos anónimos, incluso si estos datos tienen fines estadísticos o de investigación. Así lo dice el considerando 26 de RGDP. Por lo tanto nosotros no trabajaremos con datos anónimos, sino con datos nominativos.

¿Pero existe el anonimato absoluto? esta es un apregunta que no paro de hacerme durante la redacción del trabajo. Hoy día, los hackers, y expertos en big data, haciendo un gran cotejo de esos datos anónimos podrían identificar a la persona dueña de ellos. Estos datos pasarían de ser anónimos a seudónimos. Este últimos los explicare en el siguiente punto.

3.1.2 DATOS SEUDÓNIMOS.

Anteriormente en el marco conceptual hemos analizado el significado de la seudonimizacion. Los datos seudónimos son aquellos datos personales del interesado que no se le puedan atribuir a sí mismo, es decir, que para relacionar al sujeto con el dato necesiten hacer un desproporcionado cotejo. Esto es, estos datos están seudonimizados para no poderlo relacionar con su dueño.

Por lo tanto, los principios de la protección de datos deben ser aplicados a toda la información relativa a una persona ya identificada o identificable. Por lo cual a este tipo de datos es aplicable el RGDP. Pero en nuestro análisis, no trabajamos con datos seudónimos, sino nominativos.

3.1.3 DATOS DE CARÁCTER NOMINATIVO.

Como bien lo dice el nombre, en este tipo de datos el dueño de ellos está identificado con su nombre y apellido. Estos es, este tipo de datos se caracteriza por la importancia que tiene que estos estén identificado. Por ejemplo en los datos relacionados con la salud, como el historial clínico, es un dato nominativo. Porque cada persona tiene un historial y salud diferente. En nuestro caso, como en el proyecto de Emerid vamos a trabajar con datos nominativos, como bien he dicho antes con el historial clínico.

3.2 TIPOLOGÍA

En todo momento estamos rodeados y creando nuevos datos, pero, ¿Es lo mismo el nombre como dato, o el historial clínico? La respuesta es negativa, todos los datos no son iguales, y esto es debido a la sensibilidad o la información que contengan cada uno. El legislador europeo considera que hay datos más sensibles que otros, y esta sensibilidad se califica teniendo en cuenta el daño que puede crear el tratamiento inadecuado de aquellos datos al interesado.

Bien claro lo deja el RGDP en su artículo 9.1 “ *Quedan prohibidos el tratamiento de dato personales que revelen el origen étnico, racial las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de una manera inequívoca a una persona física, datos relativos con la salud o otros datos relativos a la salud o datos relativos a la vida sexual y orientación sexuales de una persona física.*” Por lo tanto los datos pertenecientes a la esfera más íntima del individuo queda prohibida su tratamiento, al menos que el interesado no dé su consentimiento explícito.

En nuestro proyecto, las empresas analizadas trabajan con dos tipos de datos. En primer lugar Emerid, trabajara con datos relacionados con la salud, esto es, el historial clínico de cada interesado. Azti, en cambio trabaja con la imagen, estas también son considerados datos de carácter personal, pero eso sí, siempre que la persona que aparezcan en dicha imagen sean identificables.

3.2.1. Historial clínico.

Después analizar el proyecto de Emerid, está claro que este sistema necesita el uso de datos relacionados con la salud, esto es, se necesitaría el historial clínico. Como grupo de investigación esto nos propone unos retos en el tema de protección de datos, ya que en mayo entra en vigor el Reglamento de la Unión Europea. Antes de adentrarnos en este tema debemos definir que es un historial clínico. En este punto nos encontramos

con la administración pública y sus leyes. En España, a legislación sobre los derechos de los pacientes es bastante antigua, estos derechos estaban recogidos en la Ley 14/1986, pero esta ley no recoge todos los derechos de los pacientes, por lo tanto los tribunales españoles iban resolviendo la situaciones concretas.²⁹

3.2.1.1 Concepto.

La definición de este concepto no está recogido en el RGDP, si no en la ley 41/2002, de 14 noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de la información y documentación clínica, en su artículo 14. Así dice “ *La historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro.*”. Por lo tanto el historial clínico es el compendio de documentos donde se recogen todos los procesos sanitarios y asistenciales de cada paciente, cada asistencia contará con la identificación del médico o médicos y demás personal sanitario que han tomado parte en ello.

Una definición más amplia es la que recoge la medicina legal, que definen el historial clínico como “ *el documento médico legal donde queda registrada toda relación del personal sanitario con el paciente, todos los actos y actividades médico-sanitarias realizadas con el y todos los datos relativos a salud, que se elabora con la finalidad de facilitar su asistencia, desde su nacimiento hasta su muerte, y que puede ser utilizada por todos los aspectos centros sanitarios donde el paciente acuda.*”³⁰

Continuando con la misma ley su artículo 7.1 dice “*Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.* El historial clínico es una de las herramientas con la que podemos utilizar a la hora de la prevención de accidentes e investigación. El contenido que esta recoge y es sumamente médico así lo recoge el artículo 15 de la Ley 41/2001. En cambio a nosotros nos interesa el historial clínico desde un punto de vista de protección de datos. Por lo tanto tenemos que

²⁹ GOMEZ PIQUERAS, Cristina. *El Derecho a la Protección de Datos en la Historia Clínica y la Receta Electrónica*. Aranzadi, primera edición, Cizur Menor, 2009, págs 127-128

³⁰ Ibidem p. 128.

estudiar el historial clínico del paciente desde el punto de vista de protección de datos. La inspectora instructora de la agencia española de protección de datos, Cristina Gómez Piqueras nos da la respuesta al contenido que el historial clínico debe de tener desde punto que nos concierne.³¹ Así dice;

En primer lugar, los datos recogidos tienen que ser adecuados, pertinentes y no excesivos en relación con el ámbito y la finalidad determinadas, explícitas y legítimas para las que se obtienen. En segundo lugar, no podrá usarse los datos para finalidades incompatibles con aquellas para que los datos han sido recogidos. En tercer lugar, los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación del afectado. En cuarto lugar, si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o impletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificadas o completados. En quinto lugar, los datos de carácter personal serán cancelados cuando hayan dejado de ser necesario para los fines en base a los cuales hubieran sido recabados o registrados. En sexto lugar, los datos no serán conservados en forma que permita la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. En séptimo lugar, los datos de carácter personal serán almacenados de forma que permita el ejercicio del derecho de acceso, salvo que sean legalmente cancelados. En octavo y último lugar, se prohíbe la recogida de datos medio fraudulentos, desleales o ilícitos.

En nuestro sistema, el historial clínico está recogido en los archivos de los hospitales, tanto privado como públicos. Dónde están sumamente protegidos debido a su gran grado de sensibilidad. El historial clínico, nos da una visión detallada del estado de salud del sujeto, es decir en ella estarás recogidos todos los datos relacionados con ella. Esta tiene como finalidad facilitar la asistencia de cada paciente. El médico inicia un historial y durante su vida según las asistencias y los problemas médicos que haya tenido se va agrandando y sumando cosas.

El objetivo de estos proyectos es unir los datos de salud al historial clínico, para así conseguir la finalidad que todos buscamos la prevención de accidentes. Así dice

³¹ GOMEZ PIQUERAS, Cristina. “El Derecho a la Protección de Datos en la Historia Clínica y Receta Electrónica, pág 133.

Cristina Gómez Piqueras, “ *la historia clínica puede considerarse el instrumento básico del buen ejercicio sanitario porque sin ella es imposible que el médico pueda tener una visión completa y global del paciente para prestarle asistencia* ”³². Por ejemplo una persona que se pone el neopreno inteligente de Emerid, en el chip de ese neopreno estarán los datos sanitario y el historial clínico del usuario, por lo tanto ese chip emite una señal a un dispositivo donde se podrán visualizar esos datos.

Aparte de la finalidad anteriormente mencionada, este artículo recoge más de una finalidad, como el historial clínico dirigido a la investigación, una evaluación de la calidad asistencial, finalidad administrativa y por último una finalidad medico legal.

En nuestro caso el historial sólo sería utilizado para la prevención de accidentes y no para otras finalidades recogidas en la ley como la de docencia e investigación, ya que a través de ellos pueden hacerse estudios e investigaciones sobre diferentes patologías, enfermedades etc, y después de hacer esta investigación hacer publicaciones científicas.

Cabe destacar que España está dividida en 17 comunidades autónomas, todas ellas con competencias en materia de sanidad. El artículo 16.7 dice que las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso. Por lo tanto, cada comunidad ha establecido una estructura clínica similar a las demás por lo general pero con diferencias.

V. REQUISITOS A CUMPLIR POR LAS EMPRESAS A LA HORA DEL TRATAMIENTO DE DATOS PERSONALES. (Actualizado con la RGDP).

5.1 Introducción.

El nuevo reglamento de la Unión Europea será aplicable a partir del 25 de mayo del 2018. Este reglamento tiene como objetivo la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de ellas por

³² GOMEZ PIQUERAS, Cristina. “El Derecho a la Protección de Datos en la Historia Clínica y Receta Electrónica, pág 134.

los estados miembros.

Como es un reglamento, es de obligado cumplimiento para todos los estados miembros, con la que Unión Europea pretende unificar todas las diferentes legislaciones en tema de protección de datos. Este reglamento debe aplicarse a la personas físicas, independientemente de su nacionalidad o de su lugar de residencia habitual, pero no regula la protección de datos relativos a las personas jurídicas y en particular a las empresas constituidas como personas jurídicas

En el estado español la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), esta es muy laxa comparándola con la nueva que viene desde Europa, por lo que todas las entidades, tanto privadas como públicas, que trabajen con datos personales deberán adaptarse al nuevo reglamento.

5.2 Ruta para el correcto tratamiento de los datos.

En primer lugar la entidad interesada en el tratamiento y el uso de esos datos deberá establecer la finalidad, es decir, el porque quiere utilizar esos datos. Esta finalidad puede ser para la investigación en el caso de Azti , o en Emerid para la prevención de accidentes en deportes de deslizamiento.

Después de tener clara la finalidad por la que la entidad necesita esos datos, esta deberá hacer una evaluación de impacto. Dentro del siguiente punto explicare detalladamente como se hace una evaluación de impacto. Previamente en el marco conceptual hemos definido que es un evaluacion de impacto, ahora en el siguiente punto explicaremos cuando hay que hacer una evaluación de impacto y cuál es la estructura que se debe de seguir.

Como dice el artículo 35 del RGDP la evaluación de impacto será de carácter obligatorio en los siguientes supuestos;

En primer lugar, cuando el tratamiento, en particular, vaya a crear un alto riesgo para los derechos fundamentales y libertades del interesado. Teniendo en cuenta si para el tratamiento de estos datos se utilicen nuevas tecnologías, por su naturaleza, alcance, contexto o fines.

En segundo lugar, cuando se lleve a cabo una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo parecido.

En tercer lugar, cuando se realice un tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9.1 (RGDP), o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 del RGDP. ¿Pero que se considera como tratamiento a gran escala? La respuesta está recogida en el Considerando número 91 de RGDP, donde dice, *“que el tratamiento de datos a gran escala, es tratar un cantidad considerable de datos personales a nivel regional, nacional, o supranacional y que podrían afectar a un gran número de interesados y que estos sean de alto riesgo.”* En cambio en estos siguientes casos la evaluación de impacto no es necesaria; si el tratamiento de datos personales de pacientes o clientes cuando los hace un solo médico o otro profesional de la salud o un abogado.

Y por último y cuarto lugar, en los casos de observación sistemática a gran escala de acceso público. Por ejemplo el uso de dispositivos optoelectrónicos, así lo dice el El Considerando 91 del RGDP.

A la hora de hacer una evaluación de impacto deberá incluir como mínimo estos requisitos. Esto está recogido en artículo 35.7 del RGDP. Para empezar, la evaluación de impacto deberá recoger, una descripción sistemática de las operaciones de tratamiento previstas y de la finalidad del tratamiento. También, es necesario hacer una evaluación de la necesidad y proporcionalidad del tratamiento respecto a su finalidad. En tercer lugar, la una evaluación de los riesgos para los derechos y libertades del interesado. Y por último, las medidas previstas

para afrontar los riesgos. En este último requisito están incluidas las garantías y las medidas de seguridad y mecanismos que garanticen la protección de datos³³.

La estructura³⁴ de una evaluación de impacto está dividida en cuatro partes, y estas cuatro partes están divididas por diferentes subgrupos. Primero, tenemos el análisis preliminar, la segunda etapa sería la del contexto, en tercer lugar la gestión de riesgos, la quinta etapa sería la conclusión y la validación y por último la supervisión.

En la primera etapa, análisis preliminar, las entidades tienen que analizar la necesidad de hacer una evaluación de impacto.

La segunda etapa es la del contexto, la cual está dividida en dos partes, la primera hay que describir el ciclo de vida de los datos a tratar, esto es, una descripción detallada del ciclo de vida de los datos y el flujo de ellos en el tratamiento. También hay que identificar varios puntos, como por ejemplo, los datos que vas a ser tratados, intervinientes, terceros, sistemas que están implicados en el tratamiento. En resumen, cualquier elemento que sea relevante en el tratamiento de los datos. En la segunda parte, se debe analizar la necesidad y la proporcionalidad del tratamiento. Es decir, analizar la base de legitimación, la finalidad y la necesidad y proporcionalidad del tratamiento.

Después de que la entidad haya cumplido esta segunda etapa, nos encontramos con la gestión de riesgos que el tratamiento de datos podría acarrear. Este punto es de vital importancia para realizar un tratamiento legal y siempre con el objetivo de minimizar los riesgos en el interesado. Esta etapa está dividida en tres subetapas. Como la primera tenemos, la identificación de las amenazas y riesgos potenciales que el tratamiento conlleva. Después de identificar las amenazas y los riesgos tenemos que las entidades deberían de hacer una evaluación de ellos, esto es, evaluación de la probabilidad y el impacto de que se materialicen los riesgos a los que está expuesta la organización. Y por último el tratamiento de los riesgos, esto es, las entidades responsables de tratar o de trabajar con datos personales deberán tener una

³³ Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD. Agencia Española de Protección de Datos. 2018, pág 5.

³⁴ Ibidem, pág 5.

respuesta ante los riesgos previamente identificados con el objetivo de garantizar los derechos y libertades de los interesados, y también minimizar la probabilidad de impacto que el tratamiento pueda crear hacia las personas físicas.

La siguiente etapa después de la gestión de riesgos, son las conclusiones y la supervisión. Las entidades deberán hacer un informe donde se recojan las conclusiones obtenidas de la evaluación de impacto donde esté documentado el resultado y el plan de acción para la gestión de riesgos, y así garantizar los derechos y libertades de los interesados.

Después de hacer la evaluación de impacto, estas deberán recoger los datos de los usuarios. Dicho de otra manera, el consentimiento del interesado. Es obligatorio tener el consentimiento del interesado para poder tratar sus datos. Según el artículo 9.2 del RGDP, el consentimiento para el tratamiento tiene que ser explícito.

Teniendo ya el consentimiento del interesado, a la hora del tratamiento de ellos, hay que tener claro quien va a ser la entidad o responsable del tratamiento. Tenemos dos opciones, la primera sería que el tratamiento lo hiciese la misma empresa interesada en los datos. Y la segunda opción, contratar a una empresa dedicada al tratamiento de datos de la salud. Si optamos por el tratamiento interno de los datos, el responsable del tratamiento tiene que designar a un encargado dedicado al tratamiento de los datos y garantizar y velar por los derechos y libertades del interesado. Si optamos por la segunda, opción, una tercera entidad se encargaría del tratamiento de los datos.

Esta es la ruta que las entidades deberían de seguir para realizar un tratamiento de datos correcto y actualizado a la nueva norma europea³⁵. Pero gracias al ayuda del Clúster Gaia y Azti tecnalia hemos tenido el placer de analizar dos prototipos de ello. En ese proceso, el grupo de investigación y hemos detectamos varios problemas de los que hablaremos en el siguiente punto y daré solución.

³⁵ 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 al la libre circulación de estos datos y por los que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

V. PROBLEMÁTICA DETECTADA y SOLUCIONES.

En este apartado analizaremos los problemas que hemos detectado de los tres proyectos a analizar, en primer lugar analizaremos en el Emerid, luego el de WOO y por último el de Azti Tecnalía.

1.PROYECTO DE EMERID.

Emerid trabaja con datos relacionados con la salud. Estos datos los consiguen de dos fuentes diferentes. La primera es la información directamente obtenida del historial clínico y la segunda fuente es la información obtenida de los trajes gracias a los wearables de los trajes.

1.1 Problemática de acceso al historial clínico.

Anteriormente he definido detalladamente que es el historial clínico. Por un lado he dado una definición de carácter únicamente médico y por el otro lado he explicado el concepto de historial clínico desde el punto de vista de su protección de datos. En la segunda entrevista realizada a Jokin Garatea, le pregunté acerca del acceso a historial clínico, es decir, cómo lo van a conseguir . A la respuesta de esta pregunta Jokin dijo que, que el objetivo de ellos no es que el interesado pida el historial clínico y luego ellos meter esos datos en el chip, si no que crear un sistema informático donde la app y Osakidetza o el IMQ estén alineados, todo vía online.³⁶

Viendo esta intención que tiene la entidad, nos surgen varias preguntas ¿Quién tiene derecho de acceder al historial clínico? ¿Esta Emerid legitimado para pedirla? La respuesta a esta pregunta está recogida en el artículo 18 de la Ley 41/2002, de 14 de noviembre. Esta dice que el paciente tiene el derecho de acceso a su historial clínico y a obtener una copia de ella. Los centros sanitarios regularán el procedimiento que garantice la observancia de estos derechos. En el siguiente artículo en el 18.2 dice, que también se puede ejercer este derecho por representación debidamente acreditada.

³⁶ Entrevista Jokin Garatea 2. Anexo 4.

Por lo tanto, queda claro que Emerid no está legitimado a la hora de ir a la administración sanitaria para pedir el historial clínico, de un cliente de sus productos. Esto está en manos del interesado, del dueño del historial clínico. Para ello tienen que rellenar un formulario los interesados. Hay que hacerlo de una manera formal, esto es, no se puede presentar un día en el hospital y pedirlo directamente. Para ello, tenemos un modelo del formulario para el ejercicio del derecho del interesado.

FORMULARIO PARA EL EJERCICIO DE DERECHO DE ACCESO AL HISTORIAL CLÍNICO (LOPD)

En....., a dede 20...

D./D^a....., con NIF....., con dirección a efectos de notificaciones en C/..... de la localidad de....., en calidad de paciente solicita copia completa de su historial clínico de forma completa, que sobre su persona se mantiene en la Clínica

Solicito que se haga entrega de la documentación mediante fotocopia del historial en el plazo de 10 días desde la recepción de la presente.

Todo ello se exige atendiendo al artículo 18 de la ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de sus derechos y obligaciones en materia de información y documentación clínica; (hacer referencia a la normativa autonómica correspondiente); de la ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos, y del Real Decreto 1720/2007, de 21 de diciembre

En caso de negarse el ejercicio de mi derecho de acceso a la historia clínica, me veré obligada a interponer la oportuna denuncia ante la Agencia Española de Protección de Datos.

Sin otro particular, reciban un cordial saludo.

Fdo.:

Entonces, el interesado tendrá que pedir mediante este formulario a la administración sanitaria de su comunidad la copia de su historial. Después de pedir el historial clínico, este tendrá que ir a instalaciones de Emerid y hacer entrega de ello. Pero, otro de los problemas que nos encontramos es cómo hacer esa entrega y las garantías que la empresa proporciona al usuario, en el siguiente punto analizaremos esto y daremos posibles soluciones.

1.2 Consentimiento del interesado.

Nos encontramos en el punto donde el sujeto ya ha pedido previamente el historial clínico y tiene a copia en sus manos. Como bien he dicho anteriormente, el artículo 9 del RGDP dice que el tratamiento de los datos relacionados con la salud solo puede realizarse con el consentimiento explícito del usuario.

Por lo tanto, Emerid y el usuario deberán firmar un contrato privado donde quede claro el consentimiento explícito del usuario y firmado por los dos. En la LOPD no hacía falta un consentimiento explícito del interesado sino que era suficiente con el consentimiento expreso. Por lo que este contrato tienen que estar actualizado con el Reglamento de la Unión Europea.

En ese contrato deberá aparecer, el nombre del interesado, encargado y responsable del tratamiento de los datos. En segundo lugar, la finalidad, esto es, para que se necesitan estos datos. En tercer lugar, los límites del tratamiento de los datos y por último, en caso de no cumplimiento de las cláusulas estipuladas en el contrato las acciones legales que emprenderá el interesado contra la entidad. (Según el reglamento de Protección de datos de la Unión Europea).³⁷ Este contrato tienen que estar firmado por los tres.

Como bien he definido anteriormente el concepto de historia clínica, dentro de ella entran todos los datos relacionados con la salud del usuario. ¿Pero son todos los datos del historial clínico necesarios? Quiero decir, a esta aplicación no le interesa saber si esa persona tiene VIH etc. La respuesta de esta pregunta nos la dio Jokin Garatea, diciendo que solo harían uso de los datos que sea de interesan a la hora de la prevención de accidentes en el deporte de deslizamiento.

Por último, el responsable y el encargado deberán facilitar información del tratamiento al interesado, esto está recogido en el artículo 13 del RGDP. Ya tenemos solucionado el primer problema sobre la legitimación de acceso de la historia clínica, ahora analizaremos la legitimación a la hora del tratamiento.

³⁷ Entrevista de Jokin Garatea 2

1.3 Legitimación a la hora del tratamiento. ¿ Quien va a realizar el tratamiento?

A continuación otro de los problemas que nos encontramos es cómo van a ser esos datos tratados y la posterior accesibilidad a ellos. Esto es, quien los va a tratar y con qué garantías. Para ello en mi opinión lo más eficaz sería designar a una persona encargada del tratamiento y seguridad de los datos. Esto es, crear una nueva zona en la empresa dedicada a la protección de datos, con expertos en el tema. Para ello habrá que designar a un encargado, este es, la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. En cambio el responsable sería Emerid.

En este caso, nos encontramos en el lugar donde el responsable contrata a un encargado, este último trabaja para el responsable, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado, así dice el artículo 28.11 RGDP. Estas dos figuras se registrarán por un contrato o acto jurídico que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

El encargado deberá garantizar que no ocurra ninguna vulneración de los derechos y libertades del interesado(artículo 32 RGDP): la seudonimización y el cifrado de datos personales;la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Porque, los problemas no se quedan aquí, puede ocurrir si estos datos no son tratados como es debido pueden llegar a manos de farmacéuticas o otras entidades muy interesadas en estos datos y usarlo para el bien económico de ellos. Por ejemplo, un persona que tiene anemia y las farmacéuticas se dan cuenta de eso y le llega publicidad acerca de productos contra la anemia.

1.4. Problemática de la obtención de la información mediante los wearable ¿Quién está legitimado para pasar el lector por los trajes?

Como he dicho antes, una de las fuentes de información es mediante los wearables, esto es, el traje emitirá señales y datos y luego estos se enviarán a un servidor. Esta información se recoge momentáneamente mediante la app. Pero ¿Esa información a donde va? ¿Donde se almacena?

El responsable del tratamiento, tiene que dejar claro cuál es la finalidad de la obtención de los datos mediante los dispositivos wearables. Esta finalidad únicamente tiene ser la de prevención de accidentes, no la de la investigación, dado la gran sensibilidad de los datos. Después de fijar la finalidad del tratamiento, igual que en el historial clínico, tiene que hacer una previa evaluación de impacto.

El responsable del tratamiento (Emerid) tiene que realizar un contrato por escrito con el interesado, fijando así los principios en los que se regirá el presente. En primer lugar, el responsable del tratamiento deberá explicar de manera exacta el tratamiento de los datos, como se va hacer, el destino y almacenamiento de ellos, para que el consentimiento del interesado no esté viciado. El interesado deberá de dar el consentimiento explícito.

La problemática que vemos es que estos datos se van a almacenar en un servidor y el encargado hará el tratamiento de dichos datos. Este servidor está bajo la responsabilidad de Emerid, ya que este es el responsable del tratamiento. Estos datos no pueden salir a la luz, ya que son de gran sensibilidad y pueden caer en manos de las grandes multinacionales, como la farmacéuticas, o las casa de seguros por ejemplo. La responsabilidad del tratamiento inadecuado caerá encima de Emerid.

Otro de los problemas que he detectado es, en caso de accidente quien es legitimado para pasar el lector por el traje y leer los datos? ¿Cualquier usuario podría leer los datos de los demás? ¿Por ejemplo otro usuario podría pasar la app? En este caso nos encontramos ante un problema sobre la privacidad de esos datos, esto es, en caso de accidente quien es legitimado para pasar el lector por el traje. El único legitimado es el responsable del tratamiento, porque es el con el interesado el agente que tiene el contrato firmado.

Otra opción podría ser que estos dispositivos de lectura estén a manos de los socorristas, exclusivamente. Pero esto no lo veo viable ya que los socorristas tendrían que firmar otro contrato con el interesado, para que este autorice el conocimiento de sus datos.

1.5 Posibles sanciones.

Nuestro objetivo es que las empresas con proyectos innovadores que tenga la necesidad del uso de datos personales, se apoyen en este trabajo de buenas prácticas para realizar el tratamiento acorde con el nuevo reglamento de la Unión Europea. Pero en un hipotético caso del no cumplimiento del reglamento este propone unas sanciones para las entidades que no lo cumplan. En el caso hipotético del tratamiento inadecuado de los datos por parte de Emerid, las siguientes sanciones serán aplicables.

Antes de la entrada en vigor del norma europea en España las infracción y sanciones estaban reguladas en la LOPD, en su Título VII. Esta ley establece tres tipo de infracciones y sanciones; la leves, graves y por último, las muy graves. Por lo tanto la multa va establecida en función de la gravedad, desde los 900€ hasta los 600.000€.

En cambio en el RGDP las infracciones y sanciones están recogidas en el artículo 83. Comparándolo con la LOPD, pasamos de tener tres categorías (leve, grave, muy grave) a tener dos categorías. En primer lugar multas administrativas de hasta 10.000.000 de euros y tratándose de una empresa, como puede ocurrir en nuestro caso, una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior. Y siempre se opta por la mayor cuantía, estos es, si el 2% es mayor al 10.000.000 de euros se opta por el dos por ciento y viceversa. En segundo lugar, multas administrativas de hasta 20.000.000 de euros o tratándose de una empresa una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior. Y siempre se opta por la mayor cuantía.

Con lo cual, hemos pasado de una multa máxima de 600.000 euros en la LOPD a un máximo de 20.000.000 de euros o el 4 % de volumen de negocio total anual global del ejercicio financiero del año anterior.

Se ve claramente el endurecimiento que ha tenido el reglamento, comparándolo con la ley española la multas no tienen nada que ver. Por lo tanto, las empresas tienen que hacerlo bien para no caer en estas millonarias multas y porque el objetivo es hacerlo bien, ya que todo no es la multa económica sino también, el daño producido a los interesados.

2. WOO.

La piragua inteligente de WOO sirve para testear tecnologías de salvamento y también, sirve para la investigación del medio acuático, esta última siendo una de las funciones más novedosas del producto. Mediante esta piragua y con la ayuda de otros medios para la investigación, se puede conocer el nivel salinidad, el ciclo de las mareas, el fondo de la mar, la polución de la playa. Pero no trabaja con datos de carácter personal como Emerid.

Estos datos no son de carácter personal son datos públicos. La diferencia entre estos tipo de datos son, que los datos de carácter personal son los datos información de una persona identificada o identificable, por ejemplo, el nombre, el apellido, estado civil, edad, datos académicos etc. En cambio, los tipos de datos como los niveles de salinidad, mareas, son datos públicos y objetivos no identifica a una persona, esto es, no son parte de ella. Por lo tanto estos tipo de datos no están protegidos por ninguna ley, ya que no tienen vinculación con ninguna persona física.

Esto son datos objetivos, que no guardan ninguna sensibilidad para que se an protegidos. Por lo tanto en este caso no es aplicable el Reglamento de la Unión Europea de protección de datos.

3. AZTI TECNALIA.

3.1 La imagen como dato personal. *¿ Es la imagen un dato?*

Todos los días estamos siendo grabados por miles de cámaras de vigilancia, y muchas veces no nos damos cuenta de su existencia. Estas cámaras están constantemente obteniendo y recabando imágenes de personas físicas. ¿Pero es la imagen un dato de carácter personal? Sí, las imágenes captadas por cámaras de video son considerados datos de carácter personal. Así dice Álvarez Hernando “ las imágenes, con independencia del

formato con independencia en el formato en el que se contengan, tiene la consideración de datos de carácter personal.”³⁸

El reglamento europeo define así el dato personal “*toda información sobre una persona identificada o identificable “el interesado”; se considera persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo el nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona”* Por lo tanto dentro de definición entraría el dato recolectado por cámaras de videovigilancia.

Claramente una imagen de una persona física es un dato de carácter personal, y continuando con nuestra investigación y relacionado con este tema, tenemos al empresa de nuevas tecnologías azti, con el novedoso proyecto de Kostasystem esta empresa tiene instaladas varias cámaras por el litoral vasco 24h al día.³⁹ Este fue uno de los problemas de los que detectamos en la entrevistas y tenemos que resolver. Este proyecto trabaja con fotos en ases fotos aparecen personas físicas. ¿Pero son identificables estas persona? En esta pregunta está la clave. Es decir, en la siguientes imágenes⁴⁰ como se puede apreciar, aparecen personas tanto en la playa de Zarautz y de Muskiz pero a primera vista no son personas que se puedan identificar. ¿Son estas capturas identificables?

Como bien se ve en la dos instantáneas, se pueden apreciar personas. ¿Pero son estas personas identificables? A simple parece que no son identificables.

Según la jurisprudencia de la Audiencia Nacional “*se debe partir de la consideración de la fotografías como dato personal requiere que se trate de imagen de persona identificable*”⁴¹.

³⁸ ALVAREZ HERNANDO, Javier. *Practicum protección de datos*, pág 820.

³⁹ Véase el III.2 del trabajo.

⁴⁰ Anexo número 5: Imágenes

⁴¹ SAN 29 de septiembre de 2011.

Y como bien he dicho anteriormente a priori no se puede llegar a identificar a las personas que están en las capturas. ¿Pero qué ocurre si estas cámaras de gran pixelaje tienen un mecanismo de ampliación muy bueno, y gracias a eso se puede identificar a los usuarios de la playa?

La respuesta a esta pregunta la tiene la doctrina, donde dice;

“La doctrina sentada en la citada sentencia es igualmente aplicable al caso ahora planteado siempre y cuando las cámaras a las que la consulta se refiere no dispongan de zoom o de otras herramientas que permitan aproximar la imagen a los transeúntes de forma que los mismos pudieran resultar identificados.”⁴²

Por lo tanto la clave está de este problema está en comprobar si dichas cámaras tienen zoom o otro tipo de herramientas con las que se pueda acercar la imagen y así hacer posible la identificación del individuo. Por lo tanto si las cámaras de Azti tienen zoom o otro tipo de herramientas con las que podría ampliar la imagen y hacer a esa persona, a priori no identificable, identificable estaríamos hablando de datos de carácter personal. Si hacemos una hipótesis de que las cámaras tienen esa capacidad de ampliación, Azti deberá quitar estas cámaras ya que, la legitimación para instalar cámaras en la vía pública es competencia de las Fuerzas y Cuerpos de Seguridad.

VIII. CONCLUSIÓN.

Es indudable la importancia de la nuevas tecnologías hoy día. Estas tienen muchas funciones, una de ellas es la prevención de accidentes. Pero en algunos casos el uso de estas pueden crear un problema jurídico, y la función del derecho es darle respuesta a

⁴² Agencia Protección de Datos, Informe 0153/2014, Gabinete Jurídico, Madrid. págs 3-4.

este. En el presente trabajo he tratado de dar solución a la problemática de la protección de datos en relación con la prevención. Es un tema muy amplio que abarca mucho, ya que en todo momento la sociedad está continuamente creando datos, y esos datos tienen dueño. Por lo tanto a esos datos debemos de tratarlos con sumo cuidado, ya que pueden repercutir mucho en el interesado.

En 25 de mayo de este año, entra en vigor en nuevo Reglamento de la Unión Europea de protección de datos. mediante este van a cambiar muchas cosas, ya que la antigua ley que había en España, LOPD, era muy laxa. Por lo tanto tenemos que buscar la balanza entre los datos y la prevención, con esto no quiero decir que no se utilicen. Todo lo contrario, estoy totalmente a favor de utilizar los datos para fines de prevención de accidentes, como las altas estadísticas de incidencias en la mar. Si no que el tratamiento de estos tiene que ser acorde con la ley y nunca perdiendo el norte, y sabiendo que estos tienen dueño.

Emerid, en este caso la empresa deberá seguir los requisitos anteriormente mencionados para un adecuado tratamiento, y en cuanto a la problemática deberán solucionarla para preservar los derechos y libertades del interesado. Azti Tecnalia, en cambio, deberá comprobar el alcance del zoom de las cámaras y si estas son capaces de identificar a personas. Si esto fuese así, deberá retirarlas ya que el único legitimado para instalar cámaras en la vía pública son las Fuerzas y cuerpos de seguridad. Y por último, Woo hace uso de datos públicos, es decir no tienen ninguna relación con una persona, por lo tanto no tratan con datos de carácter personal.

Para concluir, las personas tenemos derecho a que nuestros datos estén protegidos, y no sean utilizados por otras empresas para auto enriquecerse. Para ello, las entidades deberán seguir las indicaciones recogidas en el trabajo y nunca perdiendo la ética.

IX. FUENTES.

1. BIBLIOGRAFÍA:

- AGENCIA ESPAÑOLA PROTECCIÓN DE DATOS. *Guía práctica para las Evaluaciones de Impacto en la Protección de Los sujetos al RGPD*. 2018. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/comm on/Guias/2018/Guia_EvaluacionesImpacto.pdf.
- AGENCIA ESPAÑOLA PROTECCIÓN DE DATOS, *Informe 0153/2014*, Gabinete Jurídico, Madrid. Disponible en : https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/c ommon/pdf_destacados/2014-0153_C-aa-maras-panor-aa-micas._Inexistencia-d e-datos.pdf
- ALVAREZ HERNANDO, Javier. *Practicum protección de datos*, Thomson Reuters, Primera edición, Cizur menor, 2017.
- GARCIA SAN MIGUEL, Luis, *Estudios sobre el derecho a la intimidad*. Tecnos Madrid, 1992.
- GOMEZ PIQUERAS, Cristina. *El Derecho a la Protección de Datos en la Historia Clínica y la Receta Electrónica*. Aranzadi, primera edición, Cizur Menor, 2009.
- GRUPO DEL ARTÍCULO 29 (Comisión Europea), *Health in data apps and devices*, Bruselas, 2015,
- MORTE FERRER, Ricardo. “¿Protección de datos/privacidad en la época del Big Data, IoT, wearables...? Sí, más que nunca.” *“Dilemadata, N.º. 24, 2017, págs. 219-233.*
- REBOLLO DELGADO, Lucrecio, *El derecho fundamental a la intimidad*, Dykinson, segunda edición, Madrid. 2000.

2. LEGISLACIÓN :

- Constitución de España, año 1978.
- 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 al la libre circulación de estos datos y por los que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley 14/1986, de 25 de abril, General de Sanidad.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de informacion y documentacion clinica.
- Ley 14/2007, de 3 de julio, de Investigación biomédica.

3. JURISPRUDENCIA:

- STS 134/1999, de 15 julio.
- STC 292/2000, de 30 de noviembre
- SSTS 17/1991, de 17 de octubre.
- SAN 29/2011, de 20 de septiembre

4. ENTREVISTA:

- Ficha de entrevista de Jokin Garatea e Itziar Vidorreta.
- Ficha de entrevista Jokin Garatea 2.

- Ficha de entrevista Julien Mader.
- Ficha de entrevista Juan Ramón Barrena.

5. WEBGRAFÍA:

1. AZTI TECNALIA:

- <http://www.kostasystem.com/kostasystem/>
- <https://www.azti.es>

2. EMERID.

- <https://emerid.com>

3. WOO.

- <https://www.woo-outrigger.com/en/>

4. CONGRESO DE LOS DIPUTADOS.

- <http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2>

X. ANEXOS.

**ANEXO NÚMERO 1. Ficha de entrevista a Jokin Garatea e Itziar Vidorreta.
Realizada por Gabriela Escámez y Mikel Moraleja.**

Fiche entretien / Ficha de entrevistas

Date/ Fecha: 16/03/2017

Lieu/ Lugar: Facultad de Derecho de la UPV

Equipe PJO/ Equipo PJO: Gabriela eta Mikel

Nom/ Nombre : Jokin Garatea eta Itziar Vidorreta

Entreprise/organisme : subdirector del Clúster Gaia y Vicepresidente de Ocean Living Lab

Origine du contact/Origen de contacto : Itziar Alkorta

Thème (s) abordé (s)/ élément (s) de contexte abordé/ Tema a abordar : la industria de los deportes de deslizamiento y la estrategia Euskadi Surf

o problèmes soulevés/ Problemas :

- Masificación en la playa

En esta entrevista nos hemos citado con Jokin Garatea, cuyo vínculo con los deportes de deslizamiento es más bien pequeño, esto es, no practica el surf.

Para empezar, le preguntamos sobre la importancia de la industria del surf en la costa vasco-francesa, a lo que nos respondió que él, junto a Itziar Vidorreta, nos podía mandar un informe de Aquitania en cuanto a este tema, donde también podíamos encontrar una referencia al trabajo transfronterizo que se está desarrollando. Así ha sido, por lo que adjuntamos dicho informe en la carpeta de “FICHA DE ENTREVISTAS”.

En segundo lugar, existen diferencias entre Iparralde y País Vasco: sobre todo, en Iparralde existe la gran industria del surf, pero aquí en el País Vasco no; de hecho, la innovación se está dando en empresas de Iparralde, y aquí la especialización es otra, aunque están intentando acoplarse.

Aquí por ejemplo, no hay ninguna regulación en el tema de las escuelas de surf: todos sabemos que se han ido fundando como champiñones a través de asociaciones. Y eso conlleva a la creación de una masificación en la temporada estival. Aún así es más importante el control en invierno, dado que no hay ningún tipo de vigilancia ni seguridad de la Cruz Roja. Resolver este vacío es problema de la administración. Según Jokin, si la percepción de la seguridad fuese mayor, iría más gente a la playa.

Al hilo de lo anterior, Jokin nos explicó de qué trata el SOCORRISTA VIRTUAL: “es un piloto, un programa financiado por el programa transfronterizo POCTEFA, desde Euskadi hasta Cataluña, que trata de incidir en la industria de deslizamiento y de solucionar problemas. Vemos que en invierno es cuando más problemas se dan y la tecnología puede ayudar, no eliminar. Pero sí ayudar. De hecho, no con más policías estamos más seguros. La mayoría de usuarios de playas en invierno son personas “silver” mayores de 55 años. Por eso, las tecnologías están dirigidas a ese tipo de personas. Obviamente son para todo usuario. Pero los “silver” son el segmento de población que más acude a la playa.

Hay que recalcar la importancia que tienen la industria del surf, mueve alrededor de 1,2 billones de euros y trabajan alrededor de 130 marcas. Esta industria está localizada en Lapurdi, es decir en Francia. En el País Vasco no hay industria del surf, lo que tenemos es una gran tecnología que es de vital necesidad para nuestros vecinos en Lapurdi. En Lapurdi están las representaciones de las 6 marcas líderes mundiales, como Tribord,

Quicksilver, Billabong, Volcom etc. Esta industria genera de miles de puestos de trabajo, con que hay que recalcar su importancia.

El Clúster gaia proporciona a este tipo de empresas ayuda en el ámbito de innovación y tecnología, ya que hasta hace poco era una industria muy obsoleta, porque les iba muy bien, pero ahora con la crisis, estas empresas, se han visto en la necesidad de invertir en tecnología e innovación.

Debido al poco interés de Donostia Fomento por nuestro proyecto les preguntamos a ver si ellos sabían que era el Clúster DONOSTIA SURF CITY. Ellos nos facilitaron el contacto de Jokin Arroyo, que es la persona que lleva el tema internacional del Clúster.

Uno de los ambiciosos proyectos que el Clúster está trabajando, como antes se ha expuesto, sería el del “SOCORRISTA VIRTUAL” esto sería una ayuda para evitar los accidentes. Pero esto no es la única solución, si no que también los usuarios tienen que poner de su parte y jugar con el sentido común. Ya que estamos en un momento de mucha comodidad y poco sentido común, sabiendo la cantidad de accidentes que ocurren.

Jokin e Itziar finalizaban la entrevista, recalcando la importancia que el derecho puede tener en este tema, ya que - el derecho puede anticipar algo-.

ANEXO NÚMERO 2. Ficha de entrevista de Juan Ramón Barrena, Director Provincial de Salud y Socorros de la Cruz Roja.

IFiche entretien / Ficha de entrevistas

Date/ Fecha: 23/02/2018

Lieu/ Lugar: Ategorrieta, Cruz Roja Donostia.

Equipe PJO/ Equipo PJO: Gabriela y Mikel

Nom/ Nombre : Juan Ramón Barrena Arriarán

Entreprise/organisme : Cruz Roja

Formation : Licenciado en Medicina

Profession : Director Provincial de Salud y Socorros

Origine du contact/Origen de contacto : Mikel Moraleja

Lien avec les sports de glisse (intérêts)/ Vínculo con deportes de deslizamiento :

Thème (s) abordé (s)/ élément (s) de contexte abordé/ Tema a abordar : Problemas en la playa de la Zurriola, en cuanto a la masificación, zonificación, balizamiento y accidentes entre usuarios de deportes de deslizamiento.

La Cruz Roja gestiona la seguridad de todas las playas de Guipúzcoa y Vizcaya, esto es, las de todo el litoral vasco. En Guipúzcoa tenemos cuatro núcleos donde ocurren la

mayor cantidad de accidentes. Estos son: La playa de la Zurriola (Donostia/ San Sebastián), la playa de Zarautz, la playa de Deba y por último la playa de Itzurun (Zumaia).

Centrándonos en la playa de la Zurriola, se llevan haciendo muchos estudios universitarios; de las corrientes, del fondo del mar, y de la convivencia . Hay que señalar que esta playa tiene todo tipo de usuarios, desde los practicantes de deportes de deslizamientos hasta una señora de 70 años.

Uno de estos estudios analizó las corrientes de dicha playa y se dieron cuenta que las corrientes son vivas, esto es, que no son fijas. También estamos hablando de una playa muy peligrosa, ya que, es muy abierta. Ante estas corrientes la Cruz Roja modifica las banderas según la colocación de ellas, aparte del balizamiento de las corrientes la playa cuenta con una moto de agua que está a todas horas en el mar, hay que apuntar que estos servicios sólo están disponibles en la época estival; junio, julio, agosto y septiembre.

Todos los años se hace una reunión entre las escuelas de surf, el Ayuntamiento de Donostia/ San Sebastián y la Cruz Roja donde se discuten las mayores problemáticas de la playa y buscar soluciones a ellas para que no haya conflictos en verano. Le preguntamos quién tiene la competencia en tema seguridad de la playa, el nos respondió, que la prevalencia tiene la Cruz Roja, ellos son los responsables del balizamiento y la seguridad de las playas.

El ayuntamiento en el 2017 siendo conocedores de la problemática de la playa y queriendo colaborar sacó una instrucción municipal, esta no tiene carácter sancionador solo es una decálogo informativo de buenas prácticas. Y luego por otro lado tenemos la ordenanza municipal. Nosotros después de analizar la ordenanza llegamos a la conclusión que esta está obsoleta y que no soluciona los problemas que tiene la playa

hay día. Sabiendo esto le preguntamos al entrevistado por que no se actualizaba esta, el nos respondió que hay muchos factores. El ayuntamiento de San Sebastián quiere vender la playa de la Zurriola como una playa surfista pero no podemos vender una playa surfista 800m si luego en realidad solo son 100. Este es uno de los mayores problemas.

En las playas TIENE QUE PRIMAR LA VIDA Y MINIMIZAR LOS RIESGOS, para esto aparte de la ayuda y del gran labor de la Cruz Roja, hace falta dos cosas. En primer lugar, EL SENTIDO COMÚN, y en segundo lugar EL RESPETO. El afirma que es posible la convivencia, pero eso sí, teniendo en cuenta el sentido común y el respeto.

La ordenanza de Donostia no obliga a la guardia municipal a sancionar en el arenal. Nosotros le preguntamos qué le parecería que con los socorristas, también estuviese la guardia municipal en el arenal, Juan Ramón Barrena nos respondió “esto seria buenísimo, porque no todo el mundo respeta el balizamiento”

Lesiones más típicas: Heridas, traumatismos cerrados, luxaciones, esguinces y fracturas. El resto son picaduras, golpes de calor y quemaduras ([mirar estadísticas](#)).

¿Qué pruebas hay que hacer para ser socorrista? ¿Es la misma para cualquier playa de Donosti?

No hacen diferencias, en Gipuzkoa se hace la misma prueba; una teórica, otra física y una entrevista personal. Para poder participar en la prueba teórica, hay que tener los cursos de Primeros Auxilios y Socorrismo Acuático en vigor. Con todo ello se puede acceder a la prueba teórica, que después traerá otra física: nadar cerca de 1.600m y correr otros 1.800 por la bahía de la Concha. Aprobado esto, es necesario haber

realizados los cursos de DEA y módulo de playas, así como otro de prevención de riesgos laborales para el día de incorporación al puesto de trabajo.⁴³

Objetivamente, esta prueba de playas es la más exhaustiva y exigente que se pide en toda España, por lo que da igual en qué playa vayan a designar a los socorristas, están preparados para cualquiera de las tres. Y no se necesitan atletas para este puesto, sino gente con características especiales para posibles rescates y salvamentos.

Por supuesto, los seleccionados para socorrer la playa de la Zurriola tienen más experiencia en playas, puesto que es la playa más peligrosa de Donosti. Este año, en concreto, la prueba de socorrismo se realizará el 28 de abril, sin importar las duras condiciones en las que pueda estar el mar esa mañana.

Varios surfistas de la Zurriola, apuntan que los socorristas deberían tener una formación específica a las cualidades de cada playa. ¿Qué opinas al respecto?

Cruz Roja cuenta con dispositivos y cámaras de video con los que consiguen la información más precisa sobre corrientes, mareas etc, para a partir de ello, balizar la playa de la Zurriola correctamente.

¿Es la masificación una de las causas de los accidentes en la playa?

Según Juan Ramón Barrena, más que la masificación, es el clima el factor a tener en cuenta: si el verano va bien, esto es, hay tiempo soleado, se anima más gente a bajar a la playa, y eso trae la masificación. En 2017 durante la Clásica, a pesar del día que salió,

⁴³ <http://www.cruzroja.es/principal/web/provincial-gipuzkoa/prueba-socorristas>

había olas de 2m, y el colapso de gente en 100m para bañarse trajo más riesgos de que hubiera un accidente.

Al hilo de lo anterior, y en relación al tema legislativo, apunta nuestro experto que debería hacerse de la instrucción una ordenanza, dado que la primera no es vinculante. Al final, el trabajo de los socorristas consta de “jugarse la vida por la de los demás”, y eso merece una correcta regulación a la hora de realizar los rescates.

¿Crees que hay demasiadas escuelas de surf?

Las escuelas de surf, hacen su negocio, incluyendo las ilegales, que cuando hay mal tiempo también dan clases a locales y extranjeros. Y claro que hay demasiadas escuelas de surf, y hay que regularlas, controlando que paguen su impuesto municipal, respetando el horario y balizamiento etc.

¿Qué opinas de los socorristas en Francia?

Sabiendo que en Francia los socorristas tienen un perfil de bombero o de guardia urbana, son mucho más respetados, y nuestro experto está a favor de que los socorristas de Donosti tengan ese perfil, puesto que hay que primar por la vida de los usuarios de la playa.

O en todo caso, sería justo poner a la guardia municipal en el arenal.

Por último, Capitanía Marítima es la única que puede sancionar en el agua. Lo más común que es sancionen a embarcaciones, salidas y entradas al puerto y no a usuarios de la playa.

ANEXO NÚMERO 3. Ficha de entrevista a Julien Mader, realizada por Oihane Vadillo y Gabriela Escamez.

Fiche d'entretien / Ficha de entrevistas

Date/ Fecha: 19/03/2018

Lieu/ Lugar: Pasaia

Equipe PJO: Gabriela Escámez y Oihane Vadillo

Nom/ Nombre : Julien Madier

Entreprise/organisme : Azti Tecnalia, Transforming Science into Business.

Formation :

Profession : Coordinador de tecnologías marinas.

Mission/Spécialité : Tecnologías marinas.

Origine du contact/Origen de contacto : Mattin

Lien avec les sports de glisse (intérêts)/ Vínculo con deportes de deslizamiento : Al haber hecho diferentes estudios en nuestros mares, creemos que la aplicación de la ciencia puede ser interesante a la hora de solucionar ciertos problemas identificados en nuestras playas.

Thème (s) abordé (s)/ élément (s) de contexte abordé/ Tema a abordar :

problèmes soulevées/ Problemas : Los estudios y aplicaciones que tienen en Azti.

“En el Centro Tecnológico AZTI desarrollamos productos, servicios e iniciativas empresariales sostenibles que dinamizan el tejido industrial y recuperan y preservan los recursos naturales. Transformar la ciencia en desarrollo sostenible y saludable para la sociedad presente y futura, es nuestra seña de identidad”.

En esta entrevista nos dictamos con Julien Madier, a quien le presentamos el proyecto en el que estamos sumergidos. Julien, lleva desde 2001 aquí en Donosti.

Para empezar, nos habló de una aplicación que usan en las playas llamada KOSTAS SYSTEM que consiste en poner unas cámaras en puntos estratégicos para poder reconocer y poder investigar a cerca de tres cosas : 1. MORFOLOGÍA DE LA PLAYA, LA ARENA. 2. DENSIDAD DE USUARIOS, LOS QUE ESTÁN EN LA ARENA. 3. LAS CORRIENTES, mediante las cámaras sacan varias fotos de una misma imagen durante un tiempo, y así pueden identificar las diferentes corrientes.

Esta última aplicación de las cámaras es la que más nos ha llamado la atención para nuestro proyecto. De momento estas cámaras no están impuestas en Donostia, este año las han empezado a poner en Zarautz y hay interés en nuevos lugares donde se aplicará este método de seguridad como Deba y Hondarribi. Ahora, las están aplicando en Bizkaia. Estas imágenes, además de servirles a ellos como instituto de tecnología para sus estudios, son transferidas, además, a los socorristas al instante, y ellos con esto pueden ver las corrientes de ese día, incluso predecir las de los próximos. Es por eso que nos referimos a ellas como métodos de seguridad, porque según Julien, no sólo los socorristas pueden garantizar la seguridad del usuario de la playa, sino que las nuevas tecnologías nos ayudan a tener una información más exacta de las corrientes y mareas, para después **balizar la playa de la manera más correcta.**

Además, con este sistema, además de la corriente se puede intuir el fondo, y se puede llegar a saber la calidad de la ola. Esto se utilizó en Mundaka para un campeonato muy importante. Así como en Canarias, lugares muy afluentes por surfistas profesionales.

Le preguntamos a ver si este trabajo se podría llevar a cabo mediante Drones, y nos dijo que no, ya que la imagen tiene que ser estática. En cuanto a los Drones, dice que no sabe de ninguna aplicación en las playas que se vaya a hacer ahora, si que lo ha visto en alguna playa como prueba, pero no aquí.

Nos comentó que este mismo sistema se puede hacer mediante el móvil del socorrista, son utilizar móviles para hacer un *timelapse* de la mar (grabar durante unos 20 minutos el oleaje que hay).

Cambiando de tema, abordamos la pregunta del medio ambiente y la calidad del agua. Nos explicó, que hay unos estudios a nivel europeo que analizan las bacterias del agua y nos dice si hay demasiada contaminación o no para el baño. El problema es que estas analíticas dan los resultado en 24h así que este mismo día no se puede cerrar el agua. A pesar de todo esto, y centrándonos en lo que a nosotras nos interesaba, Julien nos afirmó que la práctica del surf en sí, no contamina más el mar. Lo que más contaminan son los usuarios normales de la playa que crean basuras. La única forma de que un surfista puede empeorar el medio ambiente es pasivamente, no mediante la práctica del deporte: mediante el turismo, subida de la densidad de la ciudad y problemas de saneamiento de agua. (GU, del Gobierno Vasco, quien elabora los informes de calidad de agua de las playas).

Siguiendo con el tema del medio ambiente, hablamos de la basura marina. En verano se limpia todos los días aunque sale muy caro. Por ejemplo, en la Concha hay un barco que pesca basura. Nos habló del proyecto LEMA, que es un proyecto cuyo objetivo es limpiar la basura en el mar directamente con barcos.

ANEXO NÚMERO 4. Ficha de entrevista a Jokin Garatea 2. Realizada por Mikel Moraleja.

Fiche entretien / Ficha de entrevistas

Date/ Fecha: 16/03/2017

Lieu/ Lugar: Facultad de Derecho de la UPV

Equipe PJO/ Equipo PJO: Mikel

Nom/ Nombre : Jokin Garatea

Entreprise/organisme : subdirector del Clúster Gaia y Vicepresidente de Ocean Living Lab

Origine du contact/Origen de contacto : Mikel Moraleja

Lien avec les sports de glisse (intérêts)/ Vínculo con deportes de deslizamiento :

Thème (s) abordé (s)/ élément (s) de contexte abordé/ Tema a abordar : tecnología y protección de datos

En esta entrevista nos hemos citado con Jokin Garatea, cuyo vínculo con los deportes de deslizamiento es más bien pequeño, esto es, no practica el surf.

Después de analizar el proyecto de socorrista virtual me surgieron varias dudas sobre los subproyectos, de WOO y EMERID. Ahora mismo estamos analizando la importancia de la tecnología y la innovación a la hora de la prevención de accidentes, y su consecuencia en la protección de datos.

Por lo tanto le hicimos varias preguntas, ya que, en estos prototipos se hace uso de datos de carácter personal de los usuarios, datos relacionados con la salud, concretamente. Estos datos son muy sensibles debido a la información que proporcionan.

Adentrándonos en la entrevista, la primera pregunta fue, cuál era la finalidad de estos proyectos. Jokin, claramente respondió la prevención de accidentes. Le pregunté si era para investigación y dijo que no. Exclusivamente prevención de accidentes.

En mayo, entra en vigor el reglamento de la Unión Europea que es más dura que la española, por lo tanto las cosas tienen que cambiar. En primer lugar, Jokin dice que hay que protocolizar este cambio, esto es, que hay que hacer los cambios debidos.

En Emerid, a la hora de dar el consentimiento, esta les da un cuestionario al usuario donde está recogido la finalidad de los datos. Y después de leer eso, el interesado firma el consentimiento para hacer el tratamiento de sus datos.

Un ejemplo que nos daba Jokin, era si una persona practicando deportes acuáticos, se daba un golpe en la cabeza y está inconsciente y no se le puede identificar, mediante

el lector del chip si. Ya que en ese chip estará su nombre y información sanitaria, alergias etc.

El objetivo de estas empresas no es hacer una cesión de datos, sino que ellos quieren hacer un línea de información con osakidetza e IMQ.

En su opinión esta ley está dirigida más a los ámbitos de comercio internacional y facebook. Ellos harán todos los cambios que la ley pida.

ANEXO NÚMERO 5: Imágenes.

Fotos de varias instantáneas.

Instantánea de la Playa de Muskiz. 2018-04-29 a la 7:20 pm. Fuente: KOSTASYSTEM by Azti.



Instantánea de la Playa de Zarautz. 2018-04-29 a la 7:19 pm. Fuente: KOSTASYSTEM

