EGUZKILORE
Número 21.
San Sebastián
Diciembre 2007
117 - 144

# QUIEBRAS DE LA PRIVACIDAD EN ESCENARIOS DIGITALES: ESPIONAJE INDUSTRIAL

Esther MORÓN LERMA

Profesora de Derecho Penal
Universidad Autónoma de Barcelona

**Resumen:** A medida que la informática y las redes de comunicación se han hecho más convergentes y prestado mayores servicios, también su vulnerabilidad ha aumentado. A pesar de ello, la política de seguridad sigue siendo muy deficiente. Ahora bien, la cifra negra que caracteriza este sector es alta y también son altos los problemas probatorios. El análisis jurídico constata las deficiencias derivadas de la redacción e interpretación de los tipos penales reguladores de estos delitos así como importantes controversias hermenéuticas. Por ello, se aconseja proponer medidas de reforma en el plano legislativo, insistir en la necesidad de tomar conciencia de la problemática, e implantar políticas de seguridad que prevengan y minimicen los daños ocasionados.

**Laburpena:** Informatika eta komunikazio sareak hurbiltzaile eta zerbitzu-emaile bihurtu direnez, bere urrakortasuna handitu da. Hala ere, segurtasun politikak urriak dira. Sektore honen datu beltzak handiak dira eta frogatzeko arazoak ere nabarmenak dira. Analisi juridikoak hainbat urritasun egiaztatzen ditu, tipo penalen interpretazio eta idazketatik eta hermeneutika eztabaidatik datozenak. Horregatik, zenbait aldaketa neurri proposatzen dira legeria mailan, problematika kontutan hartzea, eta kalteak gutxitzeko eta hauei aurre-hartzeko segurtasun politikak ezartzea.

**Résumé:** Au fur et à mesure que l'informatique et les réseaux de communication sont plus convergents et rendent un plus grand service, leur vulnérabilité augmente. Or, la politique de sécurité est encore très déficiente. Le chiffre noir qui caractérise ce secteur est élevé, de même que les problèmes probatoires. L'analyse juridique constate les insuffisances découlant de la rédaction et de l'interprétation des incriminations pénales concernant ces délits ainsi que des importantes polémiques herméneutiques. On recommande des mesures de réforme sur le plan législatif, d'insister sur la nécessité de prendre conscience de cette problématique, et d'implanter des politiques de sécurité qui prévoient et diminuent les dommages provoqués.

**Summary:** As computers and communications networks render more services, its vulnerability increases. In spite of this, the security policy is very deficient. Hidden criminality in this sector is very high as well as the problems concerning crimes evidence. The juridical analysis confirms the difficulties derived from the drafting and interpretation of the articles regarding all these offences, as well as very important hermeneutic controversies. It is advised to adopt some reform measures, and to insist on the need to become aware of these problems as well as the convenience of introducing a security policy suitable for preventing and reducing the damages.

---

(Nota): Contribución a la Jornada sobre "Protección penal de la privacidad en entornos digitales", San Sebastián, 29 noviembre 2007 (subvencionada por el Proyecto DITESEC del programa SAIOTEK, Dpto. de Industria, Comercio y Turismo del Gobierno Vasco).

**Palabras clave:** Derecho penal, Criminología, Política de seguridad, espionaje industrial, Tecnologías de la información y las comunicaciones.

**Gako hitzak:** Zigor zuzenbidea, Kriminologia, segurtasunerako politika, espioitza industriala, Informazioa eta komunikaziorako teknologiak.

**Mots clef:** Droit pénal, Criminologie, Politique de sécurité, espionnage industriel, technologies de l'information et des communications.

**Key words:** Penal Law, Criminology, Security Policy, Industrial espionage, Information and Communication Technologies.

**ÍNDICE:**



## I. EL IMPACTO DE INTERNET EN EL ÁMBITO EMPRESARIAL

Las transformaciones que las nuevas tecnologías de la información generan en el sector empresarial son continuas. Desde hace tiempo se viene subrayando la especial incidencia que la tecnología informática y telemática tiene en el seno de la empresa. Como se sabe, es práctica habitual almacenar electrónicamente la información que la empresa posee (situación financiera, proyectos de celebrar un contrato, listas de impagados, proyectos de reestructuración interna, fusiones, OPAs, aumentos de capital, repartos de beneficios, estudios de mercado, ofertas para futuros concursos públicos, listados de clientes, de proveedores, de trabajadores internos, descubrimientos científicos, invenciones, ensayos e investigaciones, entre otros posibles datos[1]) y resulta también práctica común conectar los ordenadores a redes[2].

---

1. En este trabajo se utilizará la expresión «secreto empresarial» para aludir a toda la información relativa a cualquier parcela de la actividad empresarial, comprensiva, por tanto, de la información industrial, de la comercial y de la meramente organizativa de la empresa. Se ha mantenido, en el comienzo del trabajo, el término "industrial" puesto que se corresponde con la conferencia impartida en estas jornadas, cuyo título fue propuesto por la organización.

2. Acerca del impacto de las nuevas tecnologías en el ámbito económico, vid., entre otros, ROMEO CASABONA, C.M., *Nuevas tecnologías, sociedad y derecho,* Madrid, 1987, pp. 36 y ss. ; GUTIÉRREZ FRANCÉS, M.L., "Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa", en ARROYO ZAPATERO, L. y TIEDEMANN, K. *Estudios de derecho penal económico*, Universidad de Castilla-La Mancha, 1994, p. 184 y MORÓN LERMA, E., *El secreto de empresa: protección penal y retos que plantea ante las nuevas tecnologías*, Navarra, 2002, pp. 171 y ss.

La inmersión de la empresa en el "entorno digital" ha comportado múltiples avances en cuanto al almacenamiento, acceso, manipulación, transmisión y reproducción de los datos. Al efecto, baste pensar en las ventajas derivadas de las conexiones de red de gran ancho de banda, de las redes inalámbricas (Wi-Fi, WiMax), dispositivos móviles (ordenadores portátiles, PDA, telefonía móvil, *smart phones)*, telefonía IP, pen drivers y discos portátiles, servidores virtuales, posibilidad de que cualquier contenido (gráfico o de texto) sea digitalizable y comprimible lo que permite su rápida transmisión, programas (y sitios web) de intercambio de archivos y mensajería, por citar algunas de las herramientas tecnológicas cuyo uso resulta generalizado[3].

Así pues, la integración en Internet de las actividades empresariales –y el proceso de globalización que caracteriza la economía moderna– brinda nuevos modos de investigación y, también, nuevas formas de organización de la producción y de la comercialización, de dimensión transnacional[4]. Esa imbricación entre informática, telecomunicaciones y empresa ha vigorizado el valor económico que ha tenido siempre la información[5]. En la actualidad, puede decirse que la información que una compañía posee representa el activo más importante, llegándose a cifrar en el 70% de su valor medio[6].

En ese sentido, se considera que una de las claves del éxito radica en que la empresa pueda disponer de información actualizada acerca de la evolución de la economía, las actividades de los competidores, los desarrollos tecnológicos y la conveniencia de nuevos productos. Además, la movilidad de la información dentro de la empresa deviene esencial para la agilidad del negocio y la productividad de sus miembros, de modo que resulta indispensable que éstos tengan fácil acceso a la misma.

Por otra parte, destaca la creciente importancia que han cobrado los sistemas informáticos, en cuanto infraestructuras imprescindibles desde las que prestar servicios

---

3. Especialmente reveladores resultan los datos del estudio*"The Confessions Survey: Office Workers Reveal Everyday Behavior That Places Sensitive Information at Risk*", realizado, en noviembre de 2007, por *RSA, The SEcurity Division of EMC*, en el que fueron encuestados empleados y directivos de empresas ubicadas en Boston y en Washington D.C. Los resultados de este estudio indican que el 87% de los trabajadores encuestados gestionan, a menudo, cuestiones laborales de manera remota a través de redes privadas virtuales (VPN) o correo web (Webmail) (vid. p.1); asimismo, el 64% accede a su correo electrónico profesional desde conexiones inalámbricas públicas (por ejemplo, conexiones a Internet desde cafeterías, aeropuertos, hoteles, etc.) (vid. p.2) y el 51% lo hace, además, desde ordenadores públicos (como los ubicados en cibercafés, aeropuertos, hoteles, etc.) (vid. p.1). Por tanto, como se observa, el acceso remoto a datos confidenciales es una práctica frecuente. Puede consultarse dicho estudio en *http://www.rsa.com/company/news/releases/pdfs/RSA-insider-confessions.pdf*.

4. Acerca de los transformaciones y cambios organizativos suscitados en la empresa, vid., entre otros, SÁNCHEZ BRAVO, A., *Internet. Sociedad, empresa y poderes públicos*, Granada, 2000, p.21; TERCEIRO, J.B. *Socied@d digit@l,* Madrid, 1996*,* pp. 213 y ss. y MORÓN LERMA, E., *El secreto de empresa: op. ult. cit.*, pp. 174 ss.

5. En los últimos tiempos, la función de producción se está transformando en un nuevo modelo en el que determinados factores intangibles –hace un tiempo considerados secundarios– adquieren cada vez mayor importancia para el éxito empresarial y empiezan a ser considerados el motor de la economía del futuro. Así, vid. NOMEN, E., "España frente al cambio de reglas contables en la UE para los intangibles", editado por el *Instituto de Análisis de Intangibles y la Sociedad Estatal DDI*, diciembre 2005, pp. 9 y 10.

6. Vid. *Trends in Proprietary Information Loss*, American Society for Industrial Security and PricewaterhouseCoopers, 1999.

y en las que tratar datos. Probablemente, sin las redes telemáticas de comunicación sería difícil para la empresa operar en un mercado definido por su carácter mundial, en cuanto a estructura, estrategia y funcionamiento.

En consecuencia, información y sistemas de información se erigen en un valiosísimo instrumento, imprescindible para subsistir y progresar en un mercado internacional altamente competitivo[7].

Ahora bien, a medida que la informática y las redes de comunicación se han hecho más convergentes y prestado mayores servicios, también su vulnerabilidad ha aumentado, de modo que ambos factores –dependencia y vulnerabilidad– se han ido incrementando progresivamente[8]. Se trata, pues, de una tendencia que implica numerosas utilidades pero que también va acompañada de riesgos. Baste recordar, en este sentido, los peligros derivados de las técnicas de *phishing* y de *pharming*; de las conductas de accesos no autorizados, de la difusión de programas informáticos perjudiciales o de ataques intencionados de «denegación de servicio» (DoS, DDoS), que perturban los servicios ofrecidos por Internet y pueden causar daños a las empresas que cuentan con un portal propio desde el que realizar operaciones con sus clientes[9].

Este relevante foco de riesgos contrasta, sin embargo, con la deficiente política de seguridad reinante en la empresa respecto de sus sistemas de información. En general, las empresas españolas no consideran los sistemas de gestión de la seguridad de la información como una inversión necesaria, se limitan a implementar medidas automatizables e incluso, en algunos casos, mantienen una actitud despreocupada frente a los riesgos. La propia complejidad técnica de los sistemas y la falta de hábitos de seguridad han contribuido a que la seguridad sea concebida como un producto y no como un concepto[10].

En suma, pues, la aparición de esos nuevos peligros, la importancia que para el tráfico económico empresarial posee la información almacenada en soporte digital y

---

7. Hasta tal punto es así que se ha llegado a afirmar que, en un mercado libre y globalizado, sólo pueden sostenerse las ventajas competitivas generadas por creaciones intelectuales. En efecto NOMEN, E., afirma que sólo si una ventaja competitiva se basa en una creación intelectual (activos intelectuales y know-how de difícil asimilación), la suspensión de la competencia derivada permitirá su sostenimiento. Ello no supone, sin embargo, que todas las creaciones intelectuales sean generadoras de ventajas competitivas. Así, en "Creaciones intelectuales y estrategia empresarial", en *Harvard Deusto Business Review*, nº 84, 1998, p. 70.

8. RODRÍGUEZ MOURULLO/ALONSO GALLO/LASCURAÍN SÁNCHEZ, "Derecho penal e Internet", en *Régimen jurídico de Internet* (CREMADES/FERNÁNDEZ-ORDÓÑEZ/ILLESCAS, Coord.), Madrid, 2002, p. 257.

9. Acerca de los riesgos generados por Internet, vid. entre otros, MORÓN LERMA, E., "Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos", en *Delito e informática: algunos aspectos, Cuadernos penales José María Lidón*, nº 4, Bilbao, 2007, pp. 86 y 87.

10. Existe unanimidad por parte de los expertos en seguridad informática en identificar como clave de futuro para la seguridad de la información que las empresas tomen conciencia de la necesidad de adoptar estrategias y hábitos de seguridad. Así, por ejemplo, en la II Jornada Internacional de la Asociación Española para el Fomento de la Seguridad de la Información, *ISMS Forum Spain*, se advertía de la incapacidad de empresas y autoridades para proteger los servidores. En igual sentido, la Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (ASIMELEC) señala que la mayor parte de empresas no están bien protegidas. En general, se insiste en la necesidad de concienciar a los directivos de la importancia de invertir en seguridad e idear sistemas preventivos que garanticen el funcionamiento de la Red en caso de ataques informáticos.

la todavía insuficiente seguridad de los sistemas de información hacen de ellos (información y sistemas) una parcela especialmente vulnerable a conductas ilícitas de diversa índole[11].

A continuación, pues, se examinarán algunos datos relativos a la seguridad informática en la empresa, a fin de poder trazar una primera radiografía de la situación. Ese análisis se centrará en aquellos aspectos que revisten, a los efectos de este trabajo, un especial interés y que se concretan en los siguientes. En primer lugar, se dará cuenta de la repercusión que tienen en el ámbito empresarial los incidentes informáticos vinculados a la seguridad de los datos y, en segundo término, se describirán las peculiaridades del autor de este tipo de amenazas.

Por último, debe ponerse de manifiesto que no se ha perseguido llevar a cabo un exhaustivo estudio criminológico, que hubiera excedido el objeto específico de esta ponencia. Antes bien, las estadísticas recopiladas, sin el rigor y el orden que un estudio de mayor calado hubiera requerido, y la realidad que a través de las mismas se ha puesto de manifiesto, permitirá, más adelante, llevar a cabo un análisis crítico de los preceptos penales referidos a la materia, lo que sí constituía uno de los cometidos de este trabajo.

## II. ALGUNOS DATOS DE INTERÉS: ALCANCE Y PERFIL DEL AUTOR DE INCIDENTES INFORMÁTICOS EN LA EMPRESA

### 2.1. Alcance de los incidentes informáticos relacionados con la seguridad de la información empresarial

Tal como se ha indicado, se trata, en primer lugar, de averiguar cuál es el alcance y la dimensión de los incidentes informáticos que afectan a las empresas y que ponen en peligro la seguridad de los datos que éstas poseen.

Los riesgos para la información empresarial reservada han sido constante fuente de preocupación. Ya en 1999, los incidentes vinculados al espionaje corporativo ocasionaron a las compañías del ranking *Fortune 1000* unas pérdidas cifradas en 45 billones de dólares[12]. Ahora bien, esas amenazas se han visto multiplicadas con la aparición de las nuevas tecnologías. Hasta tal punto es así que, según el informe llevado a cabo, en el año 2006, por la empresa especializada *Lucent Technologies*, el 90% de las empresas, a nivel mundial, sufren ataques informáticos, lo que genera unos daños económicos de 40.000 millones de dólares anuales. En EEUU, la consultora C&A realizó un estudio entre 642 grandes empresas, en el que se señalaba que, en el año 2005, el 84% de las firmas consultadas había sido víctima de algún incidente informático. Asimismo, se hacía constar que, de los encuestados, el 20% admitió que tales incidentes en sus sistemas habían afectado su nivel de ingresos y su cartera de clientes y el 54% reconoció que había perdido productividad.

---

11. Advirtiendo ya respecto de estos riesgos, ROMEO CASABONA, C.M., "Delitos informáticos de carácter patrimonial", en *Informática y Derecho,* nº. 9-11, p.413 y 434 y GUTIÉRREZ FRANCÉS, M.L., "Notas sobre la delincuencia informática", *op. cit.,* p. 184.

12. Así, cfr. *Trends in Proprietary Information Loss*, American Society for Industrial Security and PricewaterhouseCoopers, 1999.

La seguridad informática representa, también, un problema creciente para la pequeña y mediana empresa española, que sufre una media de entre dos y tres ataques anuales en sus equipos informáticos, según una encuesta elaborada por la Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (ASIMELEC), en colaboración con el Ministerio de Ciencia y Tecnología, en el año 2003[13]. Concretamente, seis de cada diez empresas españolas fueron objeto de un incidente informático en el año 2002; un 59% de forma esporádica y el 4% habitualmente. En dicho informe, elaborado sobre una consulta a 250 compañías españolas del sector industrial, se denunciaban las importantes pérdidas económicas que tales incidentes causan, aunque dichas pérdidas no se llegaran a cuantificar. Sin embargo, más recientemente, en el seminario sobre seguridad informática celebrado en abril de 2006, una de las conclusiones alcanzadas cuantificó los costes totales del país debidos a incidentes informáticos en 1.500 millones de euros anuales[14].

El análisis de la situación no ha variado en los últimos tiempos. Según los resultados obtenidos en el Primer Informe Europeo de Seguridad Informática en la Pyme, correspondiente a 2007, realizado por Fundetec con la colaboración de Panda Security, más de la mitad de las Pymes han sido víctimas de ataques informáticos, a pesar de que un 97% creían estar protegidas[15]. Según se recoge en dicho informe, las amenazas detectadas, en el año 2006, se cifran en troyanos (56%), *boots* (15%), *backdoors* (14,1%), gusanos (5,3%), *dialers* (5%), *adware/spyware* (1,7%) y otros (3,1%)[16].

El efecto que estas amenazas suponen para la empresa se cifra en un consumo de recursos tanto a nivel de red como humanos, lo que inevitablemente acaba generando importantes pérdidas económicas. A consecuencia de lo anterior, las empresas se han visto obligadas a interrumpir provisionalmente su actividad durante más de un día en un porcentaje nada desdeñable (el 14% en 2005 y el 8% en 2006) [17], sobre todo si se tiene en cuenta la elevada «cifra negra» reinante en este sector[18].

A tenor de lo expuesto, puede concluirse que el alcance de los incidentes relacionados con la seguridad de los datos es amplio, de dimensión generalizada y de fuerte impacto económico. Actualmente, la gestión de los riesgos de seguridad informática se ha convertido en una de las mayores preocupaciones para la empresa. En un entorno cambiante como el presente, en el que las amenazas vinculadas a las nuevas tecnolo-

---

13. En el ámbito doméstico, el panorama es similar. Según el último estudio llevado a cabo por INTECO (Instituto Nacional de Tecnologías de la Comunicación), el 72% de los hogares españoles tiene algún tipo de código malicioso (más del 50% son troyanos) y el 29,9% de los usuarios reconoce haber sido objeto de algún intento de fraude a través de Internet.

14. Seminario sobre seguridad informática "Cuando el tráfico malicioso bloquea el negocio", celebrado en Madrid, el 27 de abril de 2006, en el que participaron representantes de la empresa (IRC Hispano, Grupo Santander) y de las fuerzas y cuerpos de seguridad (Grupo de Delitos Telemáticos de la Guardia Civil).

15. Así, sobre la situación en España y en las diferentes comunidades autónomas, vid. Primer Informe Europeo de Seguridad Informática en la Pyme, p. 27. Puede consultarse en: http://enegocio.equalmultiplica.net/eNegocio/opencms/enegocio/repositorio/mediateca/documento_digital_1187262514872.html.

16. Vid. Primer Informe Europeo de Seguridad Informática en la Pyme, p. 24.

17. Así, vid. Primer Informe Europeo de Seguridad Informática en la Pyme, p. 30.

18. Como se sabe, las empresas son reacias a admitir que han sufrido una contingencia de este tipo a fin de que no trascienda dicha noticia y no se genere alarma o desconfianza entre su colectivo de clientes.

gías son cada vez mayores y más rápidas y perfeccionadas, la empresa se halla en una situación de vulnerabilidad frente a la seguridad de sus datos y sistemas, lo que suele provocar importantes pérdidas de productividad y desconfianza en los clientes.

Concluido lo anterior, conviene ya analizar lo relativo a las peculiaridades del autor de estos riesgos.

## 2.2. Cuestiones sobre la autoría de los incidentes informáticos relacionados con la seguridad de la información empresarial

### 2.2.1. Origen de los riesgos

Las amenazas relacionadas con la seguridad de los datos pueden proceder del exterior, si quien lleva a cabo la conducta peligrosa es ajeno a la empresa o, por contra, provenir desde dentro de la entidad, si el autor del incidente pertenece a la misma. A continuación, se dará brevísima cuenta de la evolución que han experimentado dichos incidentes, diferenciándolos según el origen del mismo[19].

I) Respecto de los ataques con origen externo, los modos de acceder a los datos o a los sistemas de información de una empresa son cada vez mayores y más sofisticados. Las personas ajenas a la organización suelen explotar los agujeros de seguridad (vulnerabilidades en la codificación de aplicaciones, en las bases de datos, en los sistemas operativos, en las redes, en los equipos de comunicación, técnicas de ingeniería social, ataques de fuerza bruta) para lograr ese objetivo.

Cualquier tecnología implica ventajas pero también peligros, de modo que la presencia de la empresa en la web, la utilización de servicios de mensajería, la navegación por Internet de los empleados, las nuevas herramientas de almacenaje y transmisión de la información se convierten en fuente de riesgos. Según el Primer Informe Europeo antes citado, los asaltos contra las empresas resultan cada vez más específicos, puesto que son creados a medida para intentar burlar los sistemas de seguridad desplegados. El principal foco de entrada es Internet, medio a través del cual se propagan a nivel mundial y en breve espacio de tiempo[20].

Los métodos para entrar en la red de una compañía son múltiples, como, por ejemplo, el descifrado de contraseñas (*password guessing*), las puertas traseras (backdoors), caballos de Troya, trampas y bombas lógicas, "olfateo" de paquetes (*sniffers*), acceso o control remoto, virus y gusanos, entre otros. Según el informe realizado por Symantec España, en el año 2006, los ataques que mayor aumento han experimentado son los vinculados a fugas o filtraciones de información llevados a cabo a través de troyanos y la utilización de "redes bots" (*botnet*)[21]. Concretamente, en el segundo semestre del 2006, el incremento se cifró en el 29% respecto a la primera mitad del año, alcanzando los seis millones el número de ordenadores infectados con *bots* a nivel

19. En este trabajo se ha optado por clasificar los incidentes en función del origen, pero no existe una taxonomía universalmente aceptada en la materia. Al respecto, para una reciente propuesta de un prototipo taxonómico, vid. SIMON HANSMAN, R.H., "A taxonomy of network and computer attacks", en *Computers & Security* (2005), 24, pp. 35 y ss.

20. Así, cfr. Primer Informe Europeo de Seguridad Informática en la Pyme, pp. 27-30.

21. Acerca del concepto de estas redes, vid.http:*//es.wikipedia.org/wiki/Botnet.*

mundial. Como se sabe, el uso de estas redes puede perseguir distintos objetivos entre los que se hallan el acceso a información confidencial de la empresa y la caída de sus servidores (por ejemplo, ataques DDoS).

II) En cuanto a los incidentes con origen interno, se constata la tendencia que, en este sector de la criminalidad, viene siendo habitual, a saber, su predominio como fuente de riesgos frente al origen externo[22].

Especialmente revelador resulta el informe llevado a cabo por el servicio secreto de EE UU y el centro de coordinación CERT, en el que se analiza el impacto real de estos ataques con origen en la propia institución[23]. El estudio, centrado en empresas del sector bancario y financiero y en el periodo comprendido entre los años 1996 y 2002[24], permite extraer interesantes conclusiones. Así, por ejemplo, se observa que, en la casi totalidad de los casos (87%), los autores utilizaron mecanismos plenamente legítimos en la realización del ataque y, concretamente, en el 78%, eran personal autorizado con acceso activo a los sistemas. De ahí que la mayoría de dichos ataques se realizaran físicamente en el interior de las organizaciones y durante el horario habitual de trabajo (83%). Asimismo, se ha comprobado que el principal motivo para su comisión radicaba en la obtención de beneficios económicos (81%). Por último, se hace constar, también, que el impacto económico de tales incidentes fue grave, puesto que en el 30% de los casos, el importe de la pérdida sobrepasó los 500.000 dólares, al margen de otro tipo de daños en las organizaciones afectadas[25].

Poco después, en el año 2004, según datos proporcionados por *ESA Security*, se constata, asimismo, que entre el 60 y 70% de los ataques informáticos fueron obra de los propios empleados e idéntica conclusión se alcanza en el informe de Seguridad Global 2005 realizado por *Deloitte*. Debe advertirse que, en dichos datos, se contabilizan ataques intencionados de los miembros de la empresa y ataques externos acometidos por fallos de seguridad y errores de los empleados.

Sin embargo, aun orillando, en este momento, el segundo bloque de supuestos (accesos de terceros vinculados a conductas negligentes de empleados), parece incontrovertible que, en el ámbito de la empresa, una elevada fuente de peligros para los datos y los sistemas informáticos proviene de quienes se hallan en una situación de fácil acceso a la misma[26]. El *insider* tiene acceso lícito a los recursos de la empresa en virtud

---

22. Así, vid. *United Nations Manual on the prevention and control of computer-related crime*, 1997, item 35.

23. *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, U.S. Secret Service and CERT Coordination Center/SEI. Puede consultarse en: *http://www.secretservice.gov/ntac/its_report_040820.pdf*.

24. El informe analiza un total de 23 incidentes realizados por 26 empleados entre los años 1996 y 2002.

25. Así, vid. *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Secto,* pp. 7 y 8.

26. En este sentido, vid. ROMEO CASABONA, C.M., *Poder informático y seguridad jurídica*, Madrid, 1987, p. 36; GUTIÉRREZ FRANCÉS, M.L., *Fraude informático y estafa*, Madrid, 1991, p.75; ROVIRA DEL CANTO, E. *Delincuencia informática y fraudes informáticos*, Granada, 2002, pp. 106, GALÁN MUÑOZ, A. "Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática", en *Revista de Derecho y Proceso Penal,* nº 15, p. 19, entre otros muchos.

del puesto que desempeña, siendo indispensable que obtenga la información para el correcto ejercicio de sus funciones.

La realidad jurisprudencial corrobora, también, que los ataques informáticos a la empresa suelen ser acometidos por trabajadores que, en la mayor parte de ocasiones, pretenden obtener provecho propio y, en otros más escasos, vengarse tras haber sido despedidos o no recompensados adecuadamente[27].

En suma, pues, la primera conclusión que puede extraerse respecto origen de los riesgos, es que, mayoritariamente, el autor de estos incidentes pertenece a la propia empresa o institución.

### 2.2.2. Perfil del sujeto activo

En los comienzos de Internet, el perfil del sujeto activo de los delitos informáticos se correspondía, en líneas generales, con el de una persona con elevada preparación técnica. Sin embargo, en la actualidad, los estudios criminológicos demuestran que ese perfil ha desaparecido, ampliándose notablemente el círculo de potenciales autores de este tipo de ilícitos.

A ello han contribuido diversos factores. De una parte, la constante aparición en el mercado de técnicas y programas que posibilitan y facilitan la comisión de delitos al "no experto" (esto es, el 99% de la comunidad internauta). Así, por ejemplo, es fácil hallar en Internet o comprar en el mercado programas espía que permiten interceptar información, herramientas para explotar agujeros de seguridad o *bugs* de aplicaciones para lograr accesos no autorizados o depositar programas espía, *dialers* o scaners para localizar servidores, páginas, módems o puertos abiertos de usuarios[28].

Esa nota característica asume tal trascendencia que ha motivado algunas de las recientes reformas en la materia. Obsérvese que el legislador penal ha adelantado su intervención y, progresivamente, ha ido incorporando en el código el castigo de conductas como la fabricación, importación, venta, instalación y mantenimiento de programas o dispositivos, destinados a facilitar la comisión de delitos. Así puede comprobarse cómo, en diversos ámbitos delictivos (delitos contra la propiedad intelectual, falsedades, estafa, piratería de radiodifusión), se hallan previstas todas esas conductas, cerrándose, así, todo el "circuito o ciclo delictivo" en torno a la punición de tales herramientas lógicas.

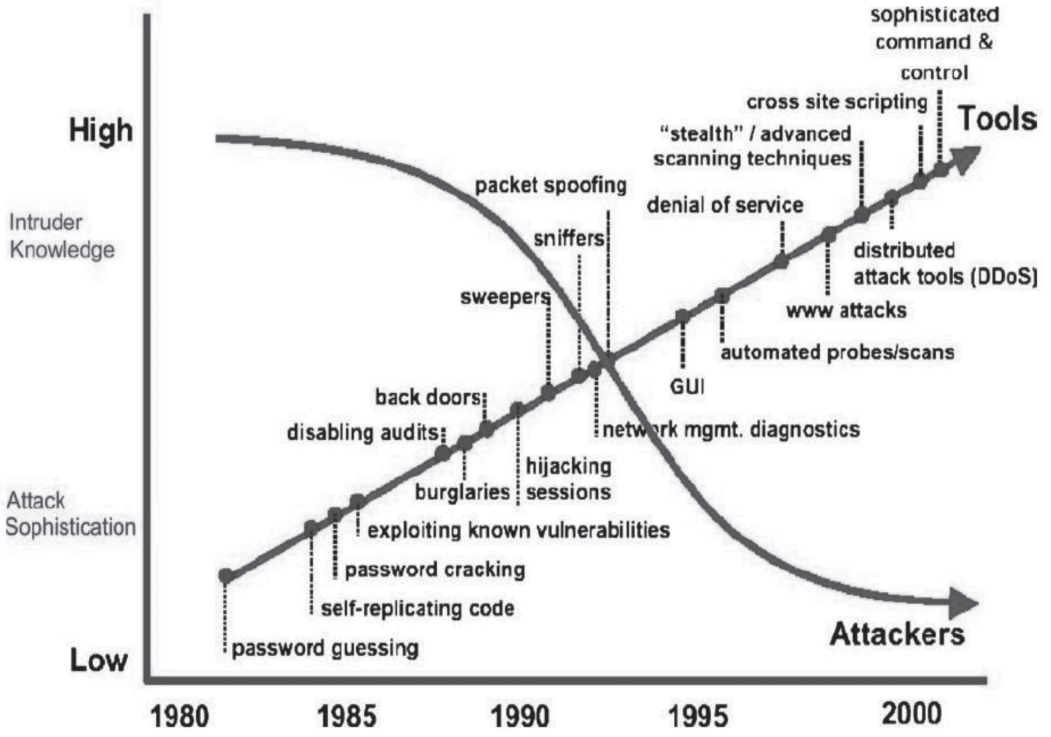
---

27. En algunos casos, dichos incidentes se llevan a cabo cuando el empleado ya ha sido despedido, pero sigue teniendo activas sus cuentas, lo que suele prorrogarse semanas o meses. En esos casos, debería procederse a cancelar los privilegios y cuentas de inmediato, puesto que esos fallos en el protocolo de seguridad son aprovechados por los exempleados.

28. Según un estudio difundido por la empresa de servicios de seguridad *Cyberguardian*, en el año 2000, existían 30.000 páginas *web* en las que era posible encontrar todo tipo de técnicas y herramientas para llevar a cabo ataques informáticos. En la actualidad, tras una sencilla búsqueda a través de google, se han podido encontrar distintos links (*http://www.portalprogramas.com/gratis/sniffers; http://tuwebdeinformatica.ueuo.com/Hacking/Troya.html; http://es.youtube.com/watch?v=r0kpj3qVxlo*), en los que se permite descargar *sniffers*, crear virus e, incluso, contemplar un vídeo sobre cómo conseguir y usar un troyano para acceder a un sistema. Asimismo, en Microsoft es posible obtener el programa *Microsoft Baseline Security Analizer*, que detecta agujeros de seguridad.

De otro lado, el uso generalizado de Internet y el carácter intuitivo de sus interfaces favorece la posibilidad de ser autodidacta, lo que, también, contribuye a esa ampliación del sujeto activo de estos ilícitos.

Sin embargo, debe advertirse que, a pesar de la característica reseñada –esto es, la generalización del sujeto activo y su falta de pericia técnica–, los "ciberdelincuentes" son cada día más rápidos en su actuación y más sofisticados en su diseño de ataques. En efecto, la diversidad y sofisticación de las formas de ataque contra los sistemas de información (intrusiones, virus, ataques contra encaminadores, de denegación de servicios, programas espía, *phishing*, *pharming*) se hallan en constante incremento.




Al respecto, especialmente clarificador resulta el gráfico[29] anterior.

Según puede observarse, la flecha curva (*Intruder knowledge*) alude al conocimiento informático necesario por parte del autor para realizar el ataque y la recta (*Attack sophistication*), a la sofisticación o complejidad de los ataques informáticos.

---

29. Así, vid. SIMON HANSMAN, R.H., "A taxonomy of network and computer attacks", en *Computers & Security* (2005), 24, p. 32.

De forma que, en el año 1980, los conocimientos técnicos de los atacantes eran elevados, pero los ataques resultaban sencillos desde un punto de vista técnico. En cambio, en el año 2000, la preparación o conocimientos informáticos son bajos o, como mínimo, menores que en años anteriores, pero la complejidad de los ataques es notablemente más elevada.

Para explicar esa aparente contradicción tomaremos como ejemplo el primero de los ataques mencionados, el del *password guessing*. En 1980, dicho ataque era sencillo. El fichero de *passwords* en un equipo Unix/Linux podía obtenerse a través de un mensaje de correo electrónico con un comando unix añadido. Conseguido ese fichero y aplicando un programa de fuerza bruta e invirtiendo el tiempo necesario, se lograba descifrar el *password*. Sin embargo, para llevar a cabo la conducta descrita, era necesario conocer bien el sistema operativo (Unix)[30].

Por el contrario, a día de hoy, uno de los ataques más habituales se realiza a través de *rootkits*, conducta que no exige profundos conocimientos por parte de quien la ejecuta. El *rootkit* efectúa múltiples cosas (desconocidas la mayor parte para el atacante) a fin de obtener el acceso al sistema. De ahí que, en la actualidad, sea relativamente sencillo lanzar ataques (con o sin éxito) contra las redes y sistemas informáticos.

Según se deduce, pues, cualquier persona con acceso a un sistema informático es capaz de poner en peligro la información de la empresa. En general, el sujeto activo de estos ilícitos no reúne especiales conocimientos técnicos pero ejecuta ataques cada vez más sofisticados y, por tanto, más peligrosos. De ahí que la esfera de potenciales autores se haya ampliado ostensiblemente, haciéndose estos ilícitos más frecuentes, diversos y peligrosos.

### 2.2.3. Conclusiones

Los estudios e informes consultados revelan que, en su mayoría, los incidentes informáticos sufridos por las empresas tienen como autores a personas vinculadas a las mismas (programadores, directivos, comerciales, operadores y otros empleados de la institución), que, por lo general, actúan movidos por deseos de obtener provecho ilícito o de vengarse.

Además, se ha detectado que el fácil acceso a programas y técnicas para emprender un ataque informático ha favorecido la ampliación y generalización del sujeto activo de los mismos. Esta segunda nota característica, proyectada al ámbito objeto de estudio, suscita un doble orden de efectos.

De una parte, potencia los peligros derivados de la actuación de ese círculo de autores (*insiders*), quienes, sin ostentar especiales conocimientos técnicos, pueden, por ejemplo, reproducir la información a la que tienen lícito acceso, difundirla a través del correo electrónico, modificarla, destruirla e, incluso, vulnerar las posibles medidas de seguridad adoptadas y acceder a datos o sistemas para los que no están autorizados. Piénsese, por ejemplo, en la utilización de programas de interceptación de la informa-

30. Una vez obtenido el fichero /etc/password, se ejecutaba el programa "john the ripper". En la actualidad, ese *modus operandi* ya no sería posible puesto que los sistemas operativos se han protegido contra ese tipo de ataque. Sería necesario operar de otro modo y, conseguir, además del fichero /etc/password, el archivo /etc/shadow.

ción (*e*Blaster[31]), de control remoto[32], dispositivos de almacenamiento portátiles (pen drivers), virus, *etc*. De otro lado, implica la aparición de una nueva fuente de riesgos proyectable, especialmente, sobre la integridad y disponibilidad de la información (por ejemplo, conductas de reproducción, alteración, inutilización, destrucción de la misma), así como sobre los sistemas informáticos de la empresa (ataques de denegación de servicio que provocan la perturbación o inutilización de los servidores)[33].

En suma, pues, todo lo anterior ha permitido constatar e identificar cuál es la esfera de riesgos más frecuentes y graves para la seguridad de la información empresarial de carácter secreto, cuestión que será retomada y tenida en cuenta al analizar la respuesta que, frente a ellos, otorga el legislador penal. Sin embargo, antes de abordar específicamente el ámbito penal, corresponde describir brevemente el marco general de tutela, que nuestro derecho proporciona a la información empresarial reservada.

## III. TUTELA DE LA INFORMACIÓN EMPRESARIAL RESERVADA

Se ha subrayado ya la importancia que, actualmente, reviste la información para el desarrollo económico, sin parangón con la que haya podido tener en cualquier otro periodo histórico. Lógicamente, para las empresas, cuyo desenvolvimiento, organización, capacidad competitiva y posición en el mercado se sustenta en la disposición de informaciones valiosas económicamente, este proceso se ha agudizado. De ahí que la seguridad de ese flujo constante de datos se conforme como una cuestión de crucial importancia para el mantenimiento de su nivel de desarrollo y progreso.

Constatada la significación que asume la seguridad de la información, deben analizarse ya los cauces de tutela existentes en nuestro derecho, a saber, el proporcionado por la Ley de Competencia Desleal[34], de una parte, y el otorgado por el código penal, de otra, que será el que centre nuestra atención.

Sin embargo, pese a su trascendencia económica y frecuente aparición en textos normativos, el secreto empresarial no ha sido objeto de definición en nuestro derecho. Por otra parte, la tutela ofrecida por el código penal es relativamente reciente, puesto que, aunque los secretos de empresa se hallaban regulados en el antiguo art. 499 del

---

31. Recientemente, la STS de 21 de marzo de 2007 condena al acusado por delito contra la intimidad por instalar un programa (eBlaster), de fácil acceso y uso, que monitoriza la actividad informática y de Internet de un PC situado en su domicilio, de forma que, cada 30 minutos, vuelca copia de todas las comunicaciones telemáticas de su esposa a la cuenta de correo del ordenador que el acusado utilizaba en la oficina. Repárese que dicho programa hubiese podido ser utilizado en sentido inverso, esto es, haber sido instalado en el ordenador de la oficina para reproducir la información de la empresa y volcarla en la cuenta de correo personal del acusado.

32. Así, por ejemplo, recientemente, fue detenido un responsable informático, empleado de una agencia inmobiliaria, por haber introducido, antes de marcharse para iniciar su propio negocio, un control remoto en un ordenador de la empresa afectada. Con ese programa, pretendía asegurarse la obtención de toda la información relativa a las nuevas fincas que ofrecían a la venta o alquiler. Puede consultarse esta noticia en: http://www.delitosinformaticos.com/03/2007/proteccion-de-datos/delito-de-descubrimiento-de-secretos-de-una-empresa-inmobiliaria.

33. Sobre esta cuestión, *infra* epígrafe IV.

34. Así, vid. artículos 13 y 14 de la Ley 3/1991, de 10 de enero, de Competencia Desleal, entre otras normas que, también, protegen los secretos de empresa.

CP de 1973, ha sido el código de 1995 el que ha otorgado a estos delitos un mayor protagonismo, adecuado al pujante valor de la información como patrimonio empresarial y el que los ha ubicado, coherentemente, en el ámbito de los delitos contra el mercado y los consumidores.

Así pues, quizá esa falta de definición legal de los mismos y la escasa atención doctrinal merecida hasta el momento, han determinado o influido en la incertidumbre y confusión que todavía predomina respecto de algunos elementos importantes de estos ilícitos. El elevado índice de resoluciones absolutorias en la materia desvela problemas aplicativos que no sólo traen causa de obstáculos probatorios sino también de erróneas interpretaciones de algunos elementos típicos (objeto material, elementos subjetivos, etc.).

De ahí que metodológicamente se opte, en este momento, por formular algunas precisiones conceptuales. En primer lugar, se tratará de acotar cuál es el bien jurídico o valor protegido en estos delitos para, seleccionar, a continuación, qué acciones se desvelan peligrosas para el mismo.

## IV. PRECISIONES CONCEPTUALES: EL OBJETO DE PROTECCIÓN Y LAS CONDUCTAS PELIGROSAS PARA EL MISMO

### 4.1. El bien jurídico objeto de protección

El secreto empresarial representa un bien esencialmente económico, cuya protección jurídica se justifica en la necesidad de preservar los resultados fruto del propio esfuerzo en la libre iniciativa empresarial. Se trata de proteger el interés económico que para el empresario revisten ciertas informaciones, obtenidas por sus propios méritos y cuyo mantenimiento en secreto le proporciona valiosas ventajas competitivas[35].

Por tanto, la tutela de ese bien económico reclama, en primer término, garantizar la seguridad de la información y, dadas las características del actual modelo de empresa, implica, también, garantizar, aunque sea instrumentalmente, la seguridad de sus sistemas, máquinas y redes conectadas a Internet.

Así pues, al objeto de esclarecer las fuentes de peligro para el bien jurídico protegido, parece conveniente determinar, en primer término, cuáles son las características que confieren seguridad a la información o a los sistemas de la empresa y que, por tanto, deberán ser preservadas.

Según se ha insistido ya, las peculiaridades de los sistemas informáticos obligan a pormenorizar el análisis de estos caracteres, a fin de detectar los peligros que se suscitan y, posteriormente, delimitar correctamente las acciones típicas expresamente contempladas en el código e identificar las que se hallan todavía ayunas de previsión. Como muestra de esa necesidad, repárese, por ejemplo, en el hecho de que la comunicación oral, la conservación o grabación en soporte analógico de una estrategia publicitaria será difícilmente alterable y, si se llevase a cabo la supresión de algún fragmento, sería detectado con facilidad; por el contrario, si esa misma información se halla almacenada

35. Vid. extensamente, MORÓN LERMA, E., *El secreto de empresa: protección penal, op.ult.cit.* pp. 128 y ss.

en soporte digital resultará fácilmente modificable y, además, la alteración incluso podría pasar desapercibida para la víctima.

Sometido, pues, a tal objetivo, corresponde ahora proponer una definición técnica de «seguridad». Así, en términos informáticos, se entiende por tal aquella característica que permite saber si un sistema se halla libre de peligros o daños. Debe advertirse que la imposibilidad material de lograr la seguridad o inviolabilidad absoluta de un sistema, ha motivado que se prefiera utilizar el término «fiabilidad» en vez del inalcanzable concepto de seguridad.

Precisado lo anterior, se considera que un sistema es fiable cuando se satisface la confidencialidad, integridad y disponibilidad de los recursos que lo integran[36]. Así, la «confidencialidad» reclama que sólo los usuarios autorizados accedan a los elementos del sistema, en la forma y tiempo determinados; la «integridad» exige que la información sea modificada (incluyendo su creación y borrado) sólo por personal autorizado; y, por último, la «disponibilidad» demanda que los recursos del sistema sean utilizables en el momento y del modo en que lo requieran los usuarios autorizados.

En consecuencia, pues, si se persigue garantizar la seguridad –o fiabilidad– de la información empresarial, será indispensable centrarse en la salvaguardia de esas tres propiedades e identificar las conductas que suponen un peligro para las mismas.

### 4.2. Las conductas peligrosas para la seguridad de la información

En efecto, cualquier acción capaz de provocar una pérdida o daño en la confidencialidad, integridad o disponibilidad de los datos, constituye una amenaza de la seguridad de la información y, en esa medida, una conducta idónea para generar un riesgo sobre el mantenimiento del secreto de empresa como bien esencialmente económico y, por tanto, una conducta con capacidad de afectación del objeto jurídico protegido.

Estas amenazas pueden cifrarse en comportamientos que atenten contra una de dichas características o contra varias de ellas[37]. Así, suponen una amenaza de la «confidencialidad» de los datos, las conductas de acceso inconsentido a la información o de reproducción de la misma; entre las que suponen un riesgo sobre la «integridad» de los datos, se hallan la introducción de algún dato, la alteración, la ocultación, la supresión o borrado; por último, atenta contra la «disponibilidad» de la información la inutilización de la misma, mediante su encriptación o mediante la inserción de alguna subrutina o bomba lógica de actuación retardada. Así, por ejemplo, en marzo de 2002, una "bom-

---

36. Vid. RIBAGORDA GARNACHO, A., "Seguridad de las tecnologías de la información", en *Ámbito jurídico de las tecnologías de la información,* CDJ, CGPJ, 1996, p. 312-313; MARTÍN ÁVILA, A/DE QUINTO ZUMÁRRAGA, F., *Manual de seguridad en Internet. Soluciones técnicas y jurídicas*, A Coruña, 2003, pp. 33 y ss. y COLOBRÁN HUGUET, M., *Introducción a la seguridad informática*, Planeta UOC, Barcelona, 2004, pp. 9 y ss.

37. Atendiendo a la vulneración de dichas cualidades se ha concebido el Convenio sobre Cibercriminalidad, firmado en Budapest, el 23.X.2001. En efecto, ubicado en la Sección I, relativa al derecho penal material, se halla el Título 1, rubricado *Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos,* que comprende, en sus artículos 2 a 6, conductas tales como el acceso ilícito, interceptación ilícita, atentados contra la integridad de los datos, atentados contra la integridad del sistema y utilización abusiva de terminales.

ba lógica"[38], borró 10 billones de archivos de los sistemas informáticos de una empresa de servicios financieros. El incidente, que afectó aproximadamente a 1.300 servidores de la empresa en EE UU, generó pérdidas de 3 millones de dólares[39].

Precisamente, según el reciente informe elaborado por *Recovery Labs*, empresa especializada en recuperación de datos, borrado seguro y peritaje informático[40], más del 60% de los casos para los que se solicita el servicio de peritaje informático están relacionados con el sabotaje[41].

Sentado lo anterior, debe hacerse especial hincapié en la importancia que revisten para la empresa los sistemas informáticos, como infraestructura imprescindible desde la que prestar servicios y operar con datos. En este sentido, cualquier acción idónea para dañar u obstaculizar gravemente el funcionamiento de los sistemas conlleva, también, riesgos para la seguridad de la información.

En estos casos, los incidentes implican comportamientos dirigidos a ocasionar perturbaciones sobre los sistemas de información, por ejemplo, mediante ataques masivos de denegación de servicio (DDoS)[42]. Estos ataques persiguen sobrecargar o saturar, por medio de artificios informáticos (por ejemplo, creando redes de sistemas esclavos), algunos de los recursos limitados del sistema objeto del ataque hasta hacerlo inoperativo, logrando con ello el bloqueo o interrupción temporal de dicho servicio.

Así, según se ha descrito ya anteriormente, los informes consultados revelan el aumento en la creación, divulgación e infección de sistemas a causa de virus –y de los cuantiosos daños económicos provocados por éstos–, así como el incremento de los ataques contra encaminadores y de denegación de servicio, mediante el recurso a las redes *bots*.

Presentada someramente la casuística respecto de incidentes informáticos sobrevenidos en la empresa, en cuanto al alcance y autor de los mismos, identificado el bien jurídico subyacente en la tutela de los secretos de empresa y las acciones con capacidad

---

38. Esta modalidad de destrucción o de sabotaje informático se denomina «*time bombs*» o bomba lógica de actuación retardada. En estos casos, la destrucción de los ficheros se produce, tras un lapso de tiempo, en virtud de indicaciones precisas como la presencia o ausencia de un dato, que puede ser una hora, un código o un nombre (así, vid., entre otros, CORCOY, M., "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", en MIR PUIG, S. (Comp.), *Delincuencia informática,* Barcelona, 1992, p. 151; ROMEO CASABONA, C.M., "Los delitos de daños en el ámbito informático", en *CPC,* nº 43, 1991, pp. 95-96 y GONZÁLEZ RUS, J.J., "Protección penal de sistemas, elementos, datos, informaciones, documentos y programas informáticos", en *Jornadas sobre delincuencia informática*, *Estudios jurídicos del Ministerio Fiscal*, III, Madrid, 1997, p. 526).

39. Así, vid. *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, U.S. Secret Service and CERT Coordination Center/SEI, p.1.

40. *Recovery Labs* es una empresa especializada en el desarrollo y comercialización de aplicaciones y servicios de recuperación de datos, borrado seguro y peritaje informático.

41. En concreto, el 60,20% de los casos respondía a supuestos de sabotaje, el 31,60% a uso indebido de Internet, el 6,10 % a abuso de material informático y el 2,10% a espionaje.

42. Vid., exhaustivamente, MORÓN LERMA, E. *Internet y derecho penal: hacking y otras conductas ilícitas en la red,* Navarra, 2ª ed., 2002, pp. 43 y ss. y RODRÍGUEZ MOURULLO/ALONSO GALLO/LASCURAÍN SÁNCHEZ, "Derecho penal e Internet", en *Régimen jurídico, op.cit.*, pp. 278 y ss.

para ponerlo en peligro, procede ya centrarse en el código penal para comprobar qué respuestas ofrece al respecto.

## V. MARCO NORMATIVO PENAL DE LOS SECRETOS DE EMPRESA

### 5.1. Consideraciones preliminares

La información empresarial reservada encuentra protección en los artículos 278 a 280 del Código Penal, que contemplan gran parte de las posibles modalidades atentatorias de los secretos (así, el apoderamiento, el control audiovisual clandestino y control ilícito de señales de comunicación, la revelación, difusión o cesión y, por último, la utilización). La incorporación *ex novo* de alguna de estas acciones y la nueva redacción otorgada a otras de ellas ya previstas en el anterior código, ha logrado acompasar el derecho penal a las características de modernidad, globalidad e informatización de la actual realidad económica y empresarial.

Ahora bien, como se tendrá ocasión de exponer, algunas de las acciones con capacidad para poner en peligro los datos y los sistemas de la empresa se encuentran todavía ayunas de referencia legal en estos delitos, como, por ejemplo, la reproducción, el "apoderamiento" abusivo y la destrucción, alteración o inutilización de la información y de los sistemas informáticos de la empresa.

Entre las múltiples modalidades mencionadas, nos ceñiremos, en este momento, al análisis de aquellas especialmente vinculadas a los incidentes informáticos[43].

### 5.2. Modalidades atentatorias expresamente previstas

#### 5.2.1. El acceso ilícito a la información

El acceso ilícito a la información se introduce, por primera vez, en el código penal de 1995, en el artículo 278.1, que castiga con pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses a quien:

*«para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197».*

Sin duda, el acceso a la información constituye la modalidad de ataque más importante y su análisis suscita numerosas cuestiones. Sin embargo, a los efectos de este trabajo, interesan esencialmente dos de ellas. De una parte, el estudio de las conductas nucleares que, expresamente, integran la modalidad de acceso ilícito a la información, a saber, el apoderamiento y los medios del artículo 197. Y, de otro lado, la interpretación del elemento típico exigido por el código, cifrado en el ánimo de descubrir un secreto de empresa.

Así pues, al examen de dichos extremos se destinan los epígrafes siguientes.

---

43. Por tanto, resultará orillado el estudio de otras acciones previstas en el código, como son la revelación, difusión o cesión y la utilización ilícita de los secretos.

### 5.2.2. El «apoderamiento» de los datos

El apoderamiento constituye la primera modalidad de acceso ilícito a la información, prevista en el artículo 278.1, primer inciso CP.

El término «apoderarse» debe ser interpretado como la aprehensión, obtención o adquisición de la información constitutiva del secreto de empresa. En este ámbito, pues, el apoderamiento no puede ser dotado de sentido desde un entendimiento clásico del mismo, formulado en los delitos contra el patrimonio y, por tanto, interpretado como un apoderamiento material, con desplazamiento físico de cosa aprehensible[44]. Ello supondría una interpretación sesgada y restrictiva de la acción típica desatenta a las características del objeto del delito, esto es, la inmaterialidad.

Así, el tipo comprenderá conductas de captación mental o intelectual, sin desplazamiento físico (apoderamiento de datos) y conductas de apoderamiento físico subrepticio de los objetos que incorporan el secreto (apoderamiento de documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo).

Centrándonos en el apoderamiento de datos, éste englobará esencialmente captaciones intelectuales o mentales, por ejemplo, por lectura física de los mismos en pantalla o por su memorización[45]. En esta medida, la captación intelectual del secreto se producirá con independencia del soporte en el que se encuentre exteriorizado el secreto.

Mayor complejidad reviste el supuesto en que no sólo se produce el apoderamiento de un documento contenido en cualquiera de las memorias electrónicas del ordenador, sino también la posterior reproducción ilícita del mismo por el sujeto a fin de procurarse certeramente su contenido, cuestión que se retomará al analizar las lagunas legales subyacentes en estos delitos.

En conclusión, el apoderamiento de secretos empresariales constitutivo de delito se verificará tanto con la aprehensión inmaterial de la información como mediante el apoderamiento físico de los documentos o soportes que la contengan.

### 5.2.3. El «control audiovisual clandestino» y el «control ilícito de señales de comunicación»

La segunda de las formas de acceso ilícito a la información se halla integrada por el control audiovisual clandestino y el control ilícito de señales de comunicación.

Esta modalidad se halla en el artículo 278.1, segundo párrafo CP, que, en vez de incorporarla expresamente, la contempla por reenvío a otro precepto del código (art.

---

44. Así, vid. MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial,* Valencia, 1999, p. 73; GUTIÉRREZ FRANCÉS, M.L., "Notas sobre la delincuencia informática…", en ARROYO ZAPATERO, L./TIEDEMANN, K., *Estudios de derecho…, op. cit.,* p. 196 y MORÓN LERMA, E., *El secreto de empresa: protección penal…, op. cit.,* p. 299.

45. En contra, vid. GUTIÉRREZ FRANCÉS, M.L., "Delincuencia económica e informática en el nuevo Código Penal", en *Ámbito jurídico de las tecnologías de la información,* Cuadernos de Derecho Judicial, CGPJ, Madrid, 1996, p. 288 y BAJO FERNÁNDEZ, M./BACIGALUPO, S., *Derecho penal económico,* Madrid, 2001, p. 495.

197.1 CP[46]), que castiga «la interceptación de telecomunicaciones o la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación»[47].

La inclusión de estas dos modalidades –el apoderamiento de datos del primer inciso del art. 278.1 CP y el control ilícito de señales de comunicación–, ha consagrado la tipificación del «espionaje empresarial» acometido por medios informáticos, cuyos efectos económicos, según se ha expuesto, resultan de primera magnitud[48].

Así, la modalidad de acceso relativa al control ilícito de señales de comunicación abrazará cualquier conducta de interceptación ilícita de las comunicaciones a través de una red informática, ya sea de área local (*intranet*) o de área amplia (extranet) (como, por ejemplo, Internet), indistintamente.

I) En las intranets, estas conductas suponen un amplio y problemático sector de riesgos, puesto que suelen ser acometidas por los propios trabajadores, que acceden así a la información con autorización pero no en la forma subrepticia en que se hace, mediante el abuso de cuentas o passwords.

Así, por ejemplo, X, alumno de un *master* en mercados financieros, es contratado en prácticas para desempeñar tareas propias de gestión y análisis de mercados, por una entidad bancaria. X accede informáticamente a otros ordenadores clientes de la red interna y graba ficheros con información confidencial, relativa a documentos elaborados por el propio equipo de análisis de la empresa como soporte de futuras tomas de decisiones, documentos relacionados con valoraciones de inversiones realizadas y un documento con la presentación de una operación bursátil proyectada por dicha empresa y otra del ramo, presentada a los analistas para ser evaluada. Todos estos documentos son reenviados por X a cuentas de correo electrónico suyas abiertas en hotmail.com.

En la determinación de si quien lleva a cabo estas conductas comete espionaje empresarial, debe realizarse un análisis desdoblado. En el caso de que el acceso se haya producido sin autorización, por ejemplo, vulnerando los *passwords* de las otras máquinas, X comete espionaje empresarial. Por el contrario, si X tenía autorización para ejecutar el acceso, al margen de que parezca difícil imaginar que dicha autorización se proyecte a las conductas de reproducción de la información, aun así la presencia del elemento subjetivo cifrado en el ánimo de descubrir el secreto, suscitará serios problemas para afirmar la tipicidad de la conducta.

---

46. El segundo pasaje del art. 197.1 CP, al que reenvía el art. 278.1 CP, establece que «el que, para descubrir sus secretos o vulnerar la intimidad de otro, (…), *intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación*…».

47. Para un análisis exhaustivo de esta conducta, vid., por todos, MORALES PRATS, F., en QUINTERO OLIVARES, (Dir.), *Comentarios al Nuevo Código Penal,* Navarra, 4ª ed., 2005, pp. 1052 y ss.

48. En este sentido, vid. ROMEO CASABONA, C.M., *Poder informático…, op. cit.*, pp. 168 y ss.

En conclusión, por lo que se refiere a la conducta de interceptación en una intranet, no existirán problemas para sancionar penalmente conductas de espionaje, salvo en los supuestos de extralimitación mencionados[49].

II) Asimismo, este precepto resulta proyectable a la interceptación de comunicaciones que se verifiquen en redes telemáticas y, en especial, en Internet. Así, por ejemplo, las que se producen con el empleo de programas rastreadores (*sniffers),* que permiten detectar cierta información en la red y cuyo uso facilita el control y lectura de los mensajes que circulan por Internet[50]. Se trata de modalidades de ataque especialmente insidiosas, que suponen un acceso a la información más penetrante, certero y constante, que además pasa inadvertido para la víctima[51].

Esta previsión resulta merecedora de elogio, puesto que la propia vulnerabilidad de los sistemas informáticos junto con la todavía mayoritaria desprotección material y logística de la empresa española respecto de sus bases de datos, han hecho que la información económica valiosa se haya convertido en una parcela muy vulnerable a la interceptación y a otras modalidades de ataque de diversa índole.

Sin embargo, algunos de esos ataques no resultan subsumibles en el artículo 278.1 CP. Y a esos problemas de encaje típico contribuye, entre otros factores, el elemento subjetivo del injusto presente en estos delitos, a cuyo breve examen se procede a continuación.

### 5.2.4. El problema del elemento subjetivo del injusto: el «ánimo de descubrir el secreto»

El artículo 278.1 CP requiere que las distintas modalidades de acceso ilícito sean llevadas a cabo con el ánimo de «descubrir el secreto de empresa».

Así, para saber si estamos en presencia de apoderamientos e interceptaciones típicas, se revela determinante la función restrictiva que ejercerá el elemento subjetivo del injusto, cuya exégesis –que puede adoptar una doble vertiente– asume especial importancia.

De una parte, el elemento subjetivo cifrado en el ánimo de descubrir un secreto de empresa, puede interpretarse como sinónimo de intención de «revelar», en consonancia con lo propuesto en la sentencia del Tribunal Supremo, de 16 de febrero de 2001 y que ha sido asumido de forma mayoritaria por los tribunales[52]. De ser así, podría decirse que el que sustrae un programa informático, al que tiene acceso legítimamente,

---

49. Así se analizará en detalle más adelante, vid. *infra* epígrafe referente a otras conductas ilícitas asimilables al apoderamiento y, en especial, la conducta de "apoderamiento abusivo".

50. Vid., en este sentido, fundamento de derecho único de la Sentencia de la Audiencia Provincial de LLeida (Sección 1ª), de 12 de febrero de 2001.

51. Así es destacado por MORALES PRATS, F., en QUINTERO OLIVARES, (Dir.), *Comentarios al Nuevo Código…, op. cit.,* p. 1055, respecto a la vulneración de la intimidad.

52. Siguiendo la interpretación sostenida en la STS 16 de febrero 2001, se muestran las SAP Barcelona 29.11.2001, SAP Castellón 15.5.2006; SAP Baleares 26.10.06; SAP Bizkaia, 27.04.2005.

con intención de revelarlo o divulgarlo, al margen de trascendentales problemas probatorios, cometería un acto típico[53].

Sin embargo, existe una segunda opción interpretativa del elemento subjetivo, en la que el ánimo de descubrir un secreto se considera como equiparable a la intención de «conocimiento» del mismo. Con arreglo a esta hermenéutica, la conducta de quien se apodera de una aplicación informática, con intención de divulgarla o explotarla –en definitiva, de usarla de modo contrario a las reglas de la competencia–, no puede ser entendida como un apoderamiento típico, al no ejecutarse la conducta presidida por el ánimo de conocer[54].

Así pues, dependiendo del contenido interpretativo que se otorgue al elemento subjetivo del injusto, el apoderamiento de soportes u objetos referidos al secreto con autorización pero ejecutándolo de una forma indebida, devendrá una conducta típica o, por el contrario, impune.

La inteligencia del elemento subjetivo relativo al ánimo de descubrir el secreto como equiparable al ánimo de divulgarlo cobraba pleno sentido en la regulación prevista en el anterior código penal, que, en su artículo 499, castigaba al empleado que descubría –esto es, revelaba– los secretos de su principal. Sin embargo, esa significación decae por completo en el vigente código. Repárese en que las modalidades típicas incriminadas en uno y otro código son distintas –en el art. 499, revelar y en el art. 278.1, apoderarse, acceder–, de forma que una interpretación lógico-sistemática del elemento subjetivo aconseja su entendimiento como ánimo de conocer y no de divulgar.

En virtud de lo anterior, aunque dé lugar a lagunas indeseables, debe postularse la segunda de las opciones reseñadas, que lo equipara al ánimo de conocer, sin perjuicio de que dicho elemento devenga, sin ningún género de dudas, necesitado de reforma.

### 5.3. Lagunas subsistentes: algunas conductas vinculadas a los abusos informáticos

Junto a las conductas analizadas (apoderamiento e interceptación), que, aun con los problemas indicados, aparecen recogidas en los artículos 278 a 280 CP, existen otros peligros para la información empresarial, como la reproducción, la conducta que se ha denominado "apoderamiento" abusivo y la destrucción, alteración o inutilización del secreto o de los sistemas de información de la empresa.

---

53. La interpretación del elemento subjetivo en ese sentido requiere demostrar la intención de revelar, problema probatorio que, en la mayor parte de casos, conduce a la absolución. Así, por ejemplo, en la SAP Barcelona, 29.11.2001, se absuelve del delito previsto en el art. 278.1 CP a los imputados (oficial administrativo, auxiliar administrativo y director comercial), al no quedar acreditado que, respecto de la información incorporada por los acusados a su nueva actividad laboral y contenida en el ordenador sustraído, hubiese intención de revelar.

54. A salvo de que se considere iniciada la ejecución de la revelación, difusión o cesión (ex art. 278.2 o ex art. 279.1 CP, según sea calificado en el caso concreto el acceso) o la utilización en provecho propio (ex art. 279.2 CP).

Esas modalidades, que poseen una carga lesiva análoga a la del apoderamiento o de la interceptación, adolecen, sin embargo, de refrendo legal. De ahí la necesidad de plantear sucintamente la reflexión en torno a las mismas.

### 5.3.1. La «reproducción» de los datos

Según se anticipó en el análisis del acceso ilícito a la información, especial controversia suscitan los supuestos en que se lleva a cabo una reproducción ilícita de la información a fin de procurarse certeramente su contenido.

Se está haciendo referencia a aquellos casos en que no sólo se produce un apoderamiento de los datos sino que, tras el acceso, se lleva a cabo una reproducción subrepticia de los mismos para utilizarlos posteriormente, en beneficio propio.

Así, por ejemplo, se emplea un dispositivo técnico de entrada y salida (pen driver, disco externo) que permite al sujeto reproducir, en un soporte pequeño y en un lapso de tiempo insignificante, una extraordinaria cantidad de información, concentrada en un espacio reducido; o bien, el sujeto envía dicha información por correo electrónico a una cuenta de la que él es usuario o titular[55].

No se ignora que la disociación de estas acciones –acceso y reproducción– quizá no se produzca siempre, pero pueden llegar a conformarse como dos modalidades de ataque diversas e independientes. Habitualmente, la reproducción se lleva a cabo en casos en que no hay acceso ilícito, ya que no hay previo apoderamiento, sino que simplemente se copia sin estar autorizado o porque se está autorizado para ello, aunque no para los fines con que se hace. Esto es, el empleado de la empresa realiza una copia de los datos para asegurarse su contenido de cara a un posterior uso de los mismos, cifrado, en la mayor parte de casos, en favorecer la constitución y posterior andadura de una nueva empresa, dedicada al mismo objeto social.

Admitido lo anterior, esto es, la relevancia que puede ostentar *per se* la conducta de reproducción, procede ya examinar cómo se regula en el código la punibilidad de esta conducta.

No se recoge la conducta de reproducción como modalidad de ataque independiente, sino que únicamente aparece contemplada en la interceptación, en cuya regulación el código sanciona tal acción y cualquier reproducción posterior. Así pues, sólo

---

55. Así, vid. Sentencia de la Audiencia Provincial de Salamanca (Sección 1ª), de 14 de junio de 2004, en la que el acusado envía, desde uno de los ordenadores de la empresa para la que trabajaba como comercial, a unas direcciones de correo electrónico, de las que era usuario o titular un coacusado, diversos correos electrónicos, en dos de los cuales se adjuntaba un fichero, que contenía la base de los datos de los clientes de tal empresa. Posteriormente, el acusado abandonó dicha empresa y constituyó otra dedicada igualmente a la prestación de servicios de telefonía móvil con un operador distinto. Análogamente, vid. Auto de la Audiencia Provincial de Barcelona (Sección 5ª), de 15 de septiembre de 2006, en la que los hechos objeto de enjuiciamiento se cifran en maniobras de extracción de información (listados de clientes y proveedores, precios de adquisición de productos) por parte de empleados de la empresa antes de su marcha y constitución de su nueva empresa. Dichas maniobras consistieron en el envío de la información por correo electrónico en fichero adjunto al compañero sentimental de una de las imputadas.

podrá subsumirse en esa modalidad típica relativa al control ilícito, cuando la reproducción siga a una previa interceptación[56].

Ahora bien, dicha solución no será posible si se trata de una conducta de reproducción acometida sin previa interceptación, dato que cobra especial relieve si se tiene en cuenta que nos hallamos ante unos delitos cuyo sujeto activo suele ser alguien de la empresa que accede directamente a la información. En estos casos, dado que no hay una incriminación expresa y autónoma, sólo cabría plantearse su posible inclusión en la modalidad del apoderamiento, prevista en el art. 278.1, primer párrafo CP. Desde luego, podrá integrarse en su ámbito de tutela, en la medida en que la conducta de reproducción siempre implicará una conducta previa de acceso, aunque recuérdese que sólo se subsumirán aquellas conductas que impliquen acceso ilícito, quedando el resto de reproducciones exentas de incriminación. Aun así, el apoderamiento puede constituir un medio comisivo menos grave que la reproducción ilícita de la información.

En conclusión, pues, convendría contemplar de forma separada la acción de reproducción ilícita del secreto.

Y esta ausencia de previsión legal se halla estrechamente vinculada con el siguiente ámbito de conflicto que es el relativo a las extralimitaciones, de modo que si se previese la reproducción, en gran parte, también se solventaría el problema del "apoderamiento" abusivo.

### 5.3.2. El «apoderamiento abusivo» de los datos

La segunda de las acciones especialmente problemática alude al apoderamiento acometido con autorización para acceder a los datos o adueñarse de los soportes, pero abusando de dicha autorización –o sea, no en la forma en que debiera hacerse, sino dándole un uso distinto–.

Así, por ejemplo, el supuesto en que un director comercial, con acceso lícito a la información comercial de la empresa (datos sobre productos catalogados con todas sus referencias, fichas de clientes con las modalidades de pago de éstos, volumen y fechas de anteriores compras, listado de precios, listado de vendedores, etc.), se prevale de esa situación de fácil acceso y recopila, en soporte papel e informático, esa información con el fin de favorecer, posteriormente, la andadura profesional de su nueva empresa[57].

Esto es, el sujeto con autorización para acceder a la información (situación lícita, por tanto) se garantiza un conocimiento seguro o duradero del secreto, pero mediante la sustracción (o realización) –ahora ya– no autorizada de una copia de la información o, como mínimo, no autorizada para los fines con que pretende utilizarla[58].

---

56. En el control ilícito de señales de comunicación, ex art. 278.1, segundo párrafo y 197.1, segundo párrafo CP).

57. Así, vid. Sentencia de la Audiencia Provincial de Granada, (Sección 2ª), de 2 de febrero de 2007.

58. Así, por ejemplo, éste sería el conocido caso de López de Arriortúa, Superlópez, al que se le han imputado en EE UU (Detroit, Michigan) los delitos de apoderamiento ilícito de documentos y revelación de secretos industriales. López de Arriortúa, vicepresidente desde principios de los noventa de General Motors, …

Esta modalidad de ataque reconducible al abuso de funciones o a la extralimitación, no se halla prevista ni en el ámbito del apoderamiento ni en el de la interceptación. Y no se halla exento de problemas un posible encaje de estos actos en la modalidad básica de apoderamiento, tal como se halla configurada en el vigente código penal (art. 278.1, primer inciso CP). El problema básico que se suscita al intentar subsumir esta acción en esa modalidad, radica en que en ella el apoderamiento es siempre ilícito y, en estos supuestos, hay una previa situación lícita[59].

En virtud de lo anterior, parece conveniente plantear la posibilidad de acometer una posible reforma de ese tipo penal, en el sentido de que la ilicitud de la conducta no descansase en el mero apoderamiento, sino en que tal conducta no resulte fruto del propio esfuerzo[60].

Desde ese entendimiento de la ilicitud, no sólo se reputarían ilícitos los apoderamientos subrepticios o sin autorización, sino también los cometidos accediendo al

---

…

encargado de ventas, empezó a negociar en secreto con Volkswagen en 1992. Durante meses, según lo demostrado por el gran jurado de Detroit, estuvo acumulando documentos secretos que, en marzo de 1993, se llevó y entregó a Volkswagen. Estos documentos hacían referencia a nuevos modelos, a una nueva planta de montaje, denominada Planta X –que permitía producir coches a gran velocidad y bajo coste– y a los precios de los proveedores. Por tanto, probablemente, López de Arriortúa accedió a los documentos con autorización (no se puede abundar, en este momento, en si era o no el inventor, como Superlópez esgrime) y, en esa medida, se da en una situación de licitud. Ahora bien, se extralimitó en esa autorización y abusó de sus funciones, al acumular los documentos o sustraerlos con la finalidad de aprovecharse o de utilizarlos indebidamente, comportamientos para los que ya no estaba autorizado. Pues bien, a pesar de que, a nuestro juicio, se trata de una conducta asimilable al acceso, puesto que encarna un apoderamiento abusivo, no obstante, no parece que esta conducta sea susceptible de ser calificada como un supuesto de acceso o apoderamiento ilícito, a tenor de la configuración del artículo 278.1 CP. Por tanto, sólo la conducta posterior de revelación a Volkswagen tendría reproche penal por aplicación del art. 279.1 CP. Análogamente, en mayo de 2007, fue condenada por un tribunal de Atlanta a una pena privativa de libertad de 8 años, una ex secretaria de Coca-Cola por hechos análogos. En concreto, J.W. fue acusada de "robo" de secretos de fábrica de Coca-Cola y de conspiración para revelar tales datos a Pepsi. Repárese en que las conductas enjuiciadas son similares a las del caso Superlópez. J.W., secretaria de altos ejecutivos de Coca-Cola probablemente estaba autorizada para acceder a dichos datos (entre otros, muestras de nuevos productos que Coca-Cola todavía no había lanzado), de modo que la conducta de apropiación de esos secretos constituiría lo que, en este trabajo, se ha denominado "apoderamiento abusivo".

59. Así, en el Auto de la Audiencia Provincial de Barcelona (Sección 2ª), de 2 de febrero de 2006, se inadmite a trámite la querella interpuesta por el delito del art. 278.1 CP contra miembros del equipo comercial, por no tratarse de un apoderamiento de la información (cartera de clientes, modelo de presupuestos, datos del equipo comercializado), a la que no tuvieran ya acceso. Análogamente, en el Auto de la Audiencia Provincial de Guipúzcoa (Sección 1ª), de 24 de mayo de 2005, se enjuició la conducta de quienes tenían en su poder correos electrónicos no dirigidos a ellos, con información confidencial (manuales de configuración), remitidos por y para el resto de socios trabajadores de la empresa querellante, cuando los querellados ya no eran socios trabajadores de la misma. No se prueba si dicha información la obtuvieron cuando todavía trabajaban en la empresa o, si por el contrario, la obtuvieron precisamente por no haberlos dado de baja en sus cuentas de correo. En cualquier caso, se sobresee puesto que se considera que la información se ha obtenido lícitamente.

60. Intentando cubrir la laguna denunciada, la Sentencia de la Audiencia Provincial de Tarragona (Sección 2ª), de 4 de abril de 2003, aplica, forzadamente, el artículo 278.1 CP a un supuesto de "apoderamiento abusivo" o "reproducción" de los datos, conductas que no están previstas en el código. El acusado trabajaba para una empresa como administrador de sistemas. En razón de su cometido específico tenía acceso a datos confidenciales (claves de acceso de todos los clientes y empleados de la empresa), de modo que, aprovechando ese acceso lícito a la información, copió e instaló en un ordenador personal en su domicilio diversos códigos fuente creados por la empresa, una base de datos con información sobre cuentas de acceso a internet y correo electrónico de numerosos clientes.

secreto con autorización, pero no en la forma en que debiera hacerse, sino dándole un uso distinto y, por ello, con extralimitación o con abuso de funciones. En definitiva, el acceso ilícito se configuraría como aquella acción de procurarse o asegurarse los datos de forma indebida o abusiva.

A nuestro juicio, pues, estas dos modalidades ayunas de referencia legal (reproducción y "apoderamiento" abusivo)[61], deberían ser asimiladas al apoderamiento, como modalidad de ataque básica, puesto que encarnan, asimismo, supuestos de accesos ilícitos o indebidos.

Por último, procede analizar la tercera modalidad de ataque desprovista de mención específica en estos delitos.

### 5.3.3. La destrucción, alteración o inutilización de los datos o sistemas informáticos de la empresa

La destrucción, alteración o inutilización de los datos o sistemas informáticos de la empresa constituye la tercera de las modalidades de ataque, que no gozan de previsión específica en la regulación de los secretos.

Respecto de los incidentes que se ejecutan sobre los «datos» o «programas informáticos», la conducta de «destrucción» implica la supresión o borrado total de los datos, la «alteración» se integra por comportamientos de inserción de datos, modificación, supresión parcial y la «inutilización» puede llevarse a cabo mediante la ocultación o la encriptación[62]. La destrucción o modificación de datos o programas, puede ejecutarse mediante la introducción en el sistema de algún tipo de virus[63] y, además, pueden asumir especial lesividad si la información confidencial se cifra en un programa de ordenador (así, pongamos por caso, el *software* de control de producción o de gestión de clientes), ya que podrá verse amenazado por otros comportamientos que atentan contra su propio funcionamiento, por ejemplo, haciendo que la ejecución de tales programas sea mucho más lenta, lo que deviene en un perjuicio o daño en sí mismo.

En cuanto a los incidentes que se lanzan contra los «sistemas de información», suelen cifrarse en comportamientos dirigidos a ocasionar perturbaciones sobre los mismos, por ejemplo, mediante ataques masivos de denegación de servicio (DDoS)[64]. Estos

---

61. Según se ha expuesto, el posible encaje de dichas conductas («reproducción» y «apoderamiento abusivo») en el art. 278.1 CP plantea serios obstáculos.

62. Vid. CORCOY, M., "Protección penal del sabotaje…" en MIR PUIG, S. (Comp.), *Delincuencia informática, op. cit.,* p. 166 y GONZÁLEZ RUS, J.J., "Protección penal de…", en *Jornadas sobre delincuencia…, op. cit.,* pp. 532-533.

63. Sobre los tipos de virus (bombas lógicas, gusanos, caballos de Troya, bacterias, virus puros, vid., exhaustivamente, CORCOY BIDASOLO, M., "Protección penal del sabotaje informático…", *op. cit*., pp. 150 y ss., MORÓN LERMA, E., *Internet y derecho penal: hacking…, op.cit.,* pp. 42 y 43 y FERRANDIS CIPRIÁN, D. "Glosario", en ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, Valencia, 2001, pp. 182-183.

64. Vid. exhaustivamente, MORÓN LERMA, E. *Internet y derecho penal: hacking…, op.cit.,* pp. 43 y ss. y RODRÍGUEZ MOURULLO/ALONSO GALLO/LASCURAÍN SÁNCHEZ, "Derecho penal e Internet", en *Régimen jurídico, op.cit*., pp. 278 y ss.

ataques persiguen sobrecargar o saturar, por medio de artificios informáticos (por ejemplo, creando redes de sistemas esclavos), algunos de los recursos limitados del sistema objeto del ataque hasta hacerlo inoperativo, logrando con ello el bloqueo o interrupción temporal de dicho sistema.

Constatado, pues, que estas acciones revisten idoneidad para poner en peligro la seguridad del secreto de empresa, en su reserva, integridad o disponibilidad, así como de los sistemas de información, debe examinarse cuáles son las vías instauradas en el código penal vigente para sancionar tales amenazas.

Las modalidades de acción analizadas (destrucción, alteración e inutilización) tampoco se hallan recogidas en los artículos 278 a 280 CP, destinados a regular la protección del secreto empresarial. Esa ausencia de previsión específica ha obligado a buscar un posible encaje en otros preceptos del código y, en especial, se ha recurrido al artículo 264.2 CP, regulador del denominado «sabotaje informático», como tipo de cobertura de la citada laguna[65].

Sin embargo, las peculiaridades de este ilícito (ubicación sistemática en sede de delitos contra el patrimonio, concreción de la propiedad como bien jurídico protegido, regulación de la conducta en un precepto cuya penalidad se asigna por remisión a la del delito de daños materiales y exigencia de producción de un daño económico superior a 400 euros) generan múltiples escollos y problemas aplicativos, en los que, en este momento, no puede abundarse[66].

Valga advertir que si bien los incidentes contra los datos pueden tener cabida en el art. 264.2 CP, aun con las restricciones que el mismo suscita, por el contrario, el castigo de las intromisiones en los sistemas suscita –en determinadas modalidades de ataques de denegación de servicio y perturbaciones en su funcionamiento–, mayores problemas de encaje por la limitación del objeto material y la demostración del daño evaluable económicamente en cuantía superior a 400 euros.

En conclusión, pues, a tenor de la laguna existente en los art. 278 a 280 CP para reprimir las fuentes de peligro que estos abusos técnicos suscitan sobre el bien jurídico y del encaje forzado e insatisfactorio que tales conductas tienen en el art. 264.2 CP, debería introducirse alguna reforma al respecto. Y, en la configuración de ese precepto, convendría tener en cuenta la circunstancia de que, según se ha advertido, en gran parte de los casos, estas conductas son ejecutadas por empleados de la propia empresa, que gozan de una situación especialmente privilegiada para saber dónde se halla la información y, por tanto, poder alterarla, destruirla o inutilizarla, así como incidir sobre los sistemas de información[67].

---

65. El art. 264.2 CP establece que «La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos».

66. Acerca de los problemas que plantea dicho precepto, vid., extensamente, MORÓN LERMA, E., "Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos", en *Delito e informática: algunos aspectos, Cuadernos penales José María Lidón*, nº 4, Bilbao, 2007, pp. 117 y ss.

67. Así., vid. Sentencia de la Audiencia Provincial de Barcelona, de 9 de marzo de 2006 (JUR 2006/227208), en la que una exempleada lleva a cabo una copia de los archivos relativos a ofertas estudiadas para nuevos concursos públicos, de interés para la competencia, destruyendo los archivos existentes en la empresa para la que había trabajado.

## VI. CONCLUSIONES

La informática y, en general, los avances tecnológicos aumentan vertiginosamente, de modo que los recursos de información y conocimientos se han convertido en fuente de progreso y de negocio a la par que foco de nuevos riesgos de seguridad.

Los informes consultados han puesto de manifiesto que el alcance de los incidentes relacionados con la seguridad de la información en la empresa es amplio y de dimensión generalizada. Se ha comprobado, también, una evolución en la dinámica en los mismos, de forma que, en la actualidad, se producen ataques dirigidos, especializados, de forma oculta y, por todo ello, más peligrosos. Asimismo, se ha constatado que, en su mayoría, estos incidentes tienen como autores a personas pertenecientes a la empresa, que, por lo general, actúan movidos por deseos de venganza o de obtención de provecho ilícito. Esos empleados se prevalen de las facultades de las que gozan, al ostentar un puesto en la empresa que les permite acceder al sistema informático y ejecutar fácilmente la conducta ilícita. Además, el fácil acceso a programas y técnicas para emprender cualquier asalto informático ha potenciado la ampliación y generalización del sujeto activo de los mismos.

El aumento constante de ataques informáticos, junto con una política de seguridad todavía insuficientemente implantada en la empresa, ha determinado la situación de vulnerabilidad en la que ésta se halla frente a la seguridad de sus datos y sistemas. Consecuencia de lo anterior resulta el impacto económico realmente grave que la comisión de esos incidentes genera, en términos de perjuicios económicos, descenso de la productividad, repercusiones en la cartera de clientes, etc.

Sin embargo, la realidad jurisprudencial de nuestro derecho desvela una escasa persecución de estos delitos y, en aquellos casos en que se insta un proceso penal, éste concluye mayoritariamente con resoluciones absolutorias[68]. A ese índice tan escaso de sentencias condenatorias, contribuyen diversos factores. No conviene olvidar la elevada cifra negra que caracteriza este sector y que impide que llegue a noticia de los órganos jurisdiccionales la noticia del crimen ni tampoco los problemas probatorios inherentes a la criminalidad informática, en los que no ha sido posible abundar. Sin embargo, confluyen, además, otras deficiencias derivadas de la redacción e interpretación de los tipos penales reguladores de estos delitos.

En primer lugar, se han identificado diversos ámbitos de deficiencia legislativa y, a los efectos que interesan, fundamentalmente dos. De una parte, la configuración típica de algunas modalidades atentatorias y, en concreto, de la modalidad de apoderamiento, revela una concepción del peligro anclada en los delitos clásicos de apropiación. Ese entendimiento se demuestra inidóneo para aprehender conductas que resultan equiparables al «apoderamiento físico» en cuanto a gravedad y desvalor, como, por ejemplo, la «reproducción» o «aseguramiento» de los datos, pero que no implican apoderamiento ni traslado físico.

El otro desacierto legislativo se anuda a la omisión de ciertas conductas peligrosas para los datos y sistemas informáticos, como resultan la destrucción, alteración o inutilización de los mismos. En efecto, el legislador parece concebir como única fuente de

68. No se ignora la elevadísima cifra negra que reina en este sector de criminalidad.

riesgos el acceso ilícito a los datos y su posible revelación, obviando conductas que suponen similares si no más graves amenazas. Así, por ejemplo, la posible reproducción ilícita del mismo por parte de quien ya lo conoce pero quiere asegurarse su contenido de cara a un posterior uso ilícito (explotación propia o revelación a la competencia), su destrucción o su inutilización o posibles ataques dirigidos a los propios sistemas informáticos que almacenan los datos, conductas todas ellas ayunas de protección en los delitos reguladores de los secretos de empresa. Por último, aunque de menor relevancia, también deviene censurable la presencia en estos ilícitos de un perturbador elemento subjetivo (cifrado en el ánimo de descubrir el secreto) que restringe injustificadamente el ámbito típico y no contribuye a perfilar la tutela del bien jurídico.

En segundo lugar, y estrechamente relacionado con esas deficiencias técnicas, surgen también controversias hermenéuticas respecto de algunos elementos típicos. Destaca, al respecto, la errónea interpretación jurisprudencial del elemento subjetivo del injusto relativo al ánimo de descubrir el secreto como sinónimo de intención de «revelar», cuestión que tampoco ayuda a una aplicación lógica, desde una perspectiva intrasistemática, de estos preceptos.

En suma, el marco normativo de estos delitos se desvela lastrado por una visión analógica de la información empresarial, en la que los soportes resultaban difíciles de copiar, de alterar y, en definitiva, de dañar. Sin embargo, deberían tenerse en cuenta las peculiaridades derivadas de los formatos digitales, copiados, modificados y suprimidos sin dificultad y difundidos sin fronteras gracias a Internet.

En virtud de lo anterior, y dado el imparable y vertiginoso avance de las TIC, conviene proponer medidas de reforma en el plano legislativo tendentes a subsanar las carencias subrayadas. Asimismo, debe insistirse en la necesidad de que, desde la empresa, se tome conciencia de la problemática existente y, por tanto, se implanten políticas de seguridad que prevengan y minimicen los daños ocasionados por los ataques en la red.

## VII. BIBLIOGRAFÍA

BAJO FERNÁNDEZ, M./BACIGALUPO, S., *Derecho penal económico,* Madrid, 2001.

COLOBRÁN HUGUET, M., *Introducción a la seguridad informática*, Planeta UOC, Barcelona, 2004.

CORCOY, M., "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", en MIR PUIG, S. (Comp.), *Delincuencia informática,* Barcelona, 1992.

FERRANDIS CIPRIÁN, D. "Glosario", en ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, Valencia, 2001.

GALÁN MUÑOZ, A. "Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática", en *Revista de Derecho y Proceso Penal,* nº 15.

GONZÁLEZ RUS, J.J., "Protección penal de sistemas, elementos, datos, informaciones, documentos y programas informáticos", en *Jornadas sobre delincuencia informática*, *Estudios jurídicos del Ministerio Fiscal*, III, Madrid, 1997.

GUTIÉRREZ FRANCÉS, M.L., *Fraude informático y estafa*, Madrid, 1991.

GUTIÉRREZ FRANCÉS, M.L., "Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa", en ARROYO ZAPATERO, L. y TIEDEMANN, K. *Estudios de derecho penal económico*, Universidad de Castilla-La Mancha, 1994.

GUTIÉRREZ FRANCÉS, M.L., "Delincuencia económica e informática en el nuevo Código Penal", en *Ámbito jurídico de las tecnologías de la información,* Cuadernos de Derecho Judicial, CGPJ, Madrid, 1996.

MARTÍN ÁVILA, A/DE QUINTO ZUMÁRRAGA, F., *Manual de seguridad en Internet. Soluciones técnicas y jurídicas*, A Coruña, 2003.

MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial,* Valencia, 1999.

MORALES PRATS, F., "Comentario a los delitos contra la intimidad", en QUINTERO OLIVARES, (Dir.), *Comentarios al Nuevo Código Penal,* Navarra, 4ª ed., 2005.

MORÓN LERMA, E. *Internet y derecho penal: hacking y otras conductas ilícitas en la red,* Navarra, 2ª ed., 2002.

MORÓN LERMA, E., *El secreto de empresa: protección penal y retos que plantea ante las nuevas tecnologías,* Navarra, 2002.

MORÓN LERMA, E., "Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos", en *Delito e informática: algunos aspectos, Cuadernos penales José María Lidón*, nº 4, Bilbao, 2007.

NOMEN, E. "Creaciones intelectuales y estrategia empresarial", en *Harvard Deusto Business Review*, nº 84, 1998.

NOMEN, E., "España frente al cambio de reglas contables en la UE para los intangibles", editado por el *Instituto de Análisis de Intangibles y la Sociedad Estatal DDI*, diciembre 2005.

RIBAGORDA GARNACHO, A., "Seguridad de las tecnologías de la información", en *Ámbito jurídico de las tecnologías de la información,* CDJ, CGPJ, 1996.

RODRÍGUEZ MOURULLO/ALONSO GALLO/LASCURAÍN SÁNCHEZ, "Derecho penal e Internet", en *Régimen jurídico de Internet* (CREMADES/FERNÁNDEZ-ORDÓÑEZ/ILLESCAS, Coord.), Madrid, 2002.

ROMEO CASABONA, C.M., *Nuevas tecnologías, sociedad y derecho,* Madrid, 1987.

ROMEO CASABONA, C.M., *Poder informático y seguridad jurídica*, Madrid, 1987.

ROMEO CASABONA, C.M., "Los delitos de daños en el ámbito informático", en *CPC,* nº 43, 1991.

ROMEO CASABONA, C.M., "Delitos informáticos de carácter patrimonial", en *Informática y Derecho,* nº. 9-11.

ROVIRA DEL CANTO, E. *Delincuencia informática y fraudes informáticos*, Granada, 2002.

SÁNCHEZ BRAVO, A., *Internet. Sociedad, empresa y poderes públicos,* Granada, 2002.

SIMON HANSMAN, R.H., "A taxonomy of network and computer attacks", en *Computers & Security* (2005), 24.

TERCEIRO, J.B. Socied@d digit@l, Madrid, 1996.