VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

TRABAJO FIN DE GRADO

Grado en Derecho

Curso 2013/2014

PRIVACIDAD EN LA RED: APROXIMACIÓN A LAS VÍAS DE PROTECCIÓN

AUTOR: María del Carmen Blanco Hernández

TUTOR: María Luz Gutiérrez Francés

Julio de 2014

ÍNDICE DE CONTENIDOS

INTRODUCCIÓN

A principios del año pasado, se publicaba una noticia en el diario digital El País[1] con un titular no muy alentador para los asiduos a las altas tecnologías de la información y comunicación: ***"Internet lo sabe (casi) todo de usted"***. Entre sus fragmentos más llamativos se leía: *"Cuánto se gasta en ropa, qué juegos prefiere, sus creencias religiosas, tendencia política, dónde pasó sus últimas vacaciones, su color favorito, o si es de tomar cerveza, vino o agua en las comidas. Muchos de estos detalles sobre usted están en Internet. Algunos los habrá publicado usted mismo, otros se pueden inferir de su actividad en la Red, qué páginas visita, qué aplicaciones se descarga en el móvil o simplemente de lo que otros dicen de su persona. La información está ahí y no hace falta ser malintencionado para encontrarla, aunque puede ser usada con malas intenciones"*.

No es difícil advertir que las palabras anteriores hacen referencia a una realidad que acompaña al hombre moderno, el *hombre transparente del siglo XXI*, que ha sucumbido a las múltiples ventajas que reporta la revolución tecnológica, pero que, como contrapunto, ha de soportar su dimensión pervertida y abusiva, sus lacras y sus riesgos (realidad criminal vinculada al uso abusivo de las Tecnologías de la Información y Comunicación –en adelante TICs-, que generalmente se viene conociendo con expresiones como "Ciberdelincuencia" o "Criminalidad informática")[2].

Obviamente, las características del presente estudio impiden abordar con un mínimo de rigor los problemas que plantean las diversas vertientes de la Criminalidad informática, tanto en el ámbito *doméstico* nacional como en la esfera internacional.[3] Es

---

[1] Nota de prensa del diario digital El País, 17 de marzo de 2013, firmado por AGUDO, Alejandra, http://sociedad.elpais.com/sociedad/2013/03/17/actualidad/1363555505_736818.html

[2] Entendemos que aciertan quienes optan por esta terminología porque da idea del carácter plural, heterogéneo y multidimensional de esta categoría, resaltando su componente criminológico; se rechaza, por consiguiente, la expresión "delito informático", que aún conservan algunas legislaciones como la venezolana o colombiana, y a la que siguen recurriendo algunos autores. Vid. ampliamente GUTIÉRREZ FRANCÉS, *Fraude informático y estafa*, Ministerio de Justicia, Madrid, 1991, pp. 49 ss.

[3] Habría que ahondar en parcelas bien distantes, desde el ámbito de la delincuencia patrimonial y socioeconómica a los delitos de falsedades, desde los delitos contra la libertad e indemnidad sexual, a los atentados contra la seguridad del Estado, por sólo citar algunos. Y ningún estudio quedaría completo sin una referencia a los principales problemas que las TICs plantean en el ámbito procesal, o las repercusiones que la emergencia de la criminalidad en el *espacio virtual* representan para principios

por ello que circunscribimos nuestro estudio a una de las parcelas que más interés nos ha despertado: Incidencia de las TICs en la llamada "privacidad", terminología ésta con la que aludiremos a los bienes personalísimos del sujeto (desde la intimidad al honor, derecho a la propia imagen, la dignidad personal o el libre desarrollo de la personalidad). El atractivo de esta materia radica, a nuestro juicio, en dos aspectos fundamentales: Primero, desde una perspectiva social, estamos ante una cuestión que, seamos más o menos conscientes, nos concierne a todos los ciudadanos sin excepción, en la actualidad y en el futuro, y la preocupación creciente que genera se observa con facilidad en las noticias que con frecuencia nos llegan a través de los medios de comunicación o las denuncias ante la Agencia de Protección de Datos; pero, además, en segundo término, para el estudioso ofrece el atractivo adicional de implicar cuestiones nucleares de la disciplina, como el nacimiento de un nuevo bien jurídico, las fronteras entre el Derecho Penal y otros instrumentos de control social (en especial, en este caso, el Derecho Administrativo), los límites al *ius puniendi* estatal, entre otros. Así pues, asumiendo nuestras limitaciones, nos proponemos aproximarnos al contenido de este nuevo interés social tan valioso para el ciudadano actual, identificando después los riesgos que inciden en el mismo y las vías previstas para su protección.

El trabajo se ha estructurado siguiendo las pautas que a continuación referimos:

En primer lugar, dedicamos la **Parte inicial** a la identificación de la "privacidad" como interés social de nuevo cuño, vinculado al desarrollo y masiva utilización de las TICs. Se trata, en esta sede, de justificar su presencia, su existencia, y delimitar su contenido (que excede y supera materialmente la idea tradicional de la intimidad). A tal efecto, se examinarán las previsiones constitucionales como telón de fondo, con las inevitables referencias de carácter internacional y la interpretación jurisprudencial de las mismas. Se pone fin a esta primera parte con una sintética relación de las principales amenazas que la privacidad soporta en nuestros días, ya procedan de actuaciones abusivas de otros ciudadanos o de compañías privadas, ya procedan de entidades u organismos públicos, nacionales o internacionales.

---

clásicos, como el de territorialidad de la ley penal. Todo ello resultaría, desde luego, inabarcable en estas líneas.

La **segunda parte** del trabajo se centra en los cauces propuestos para proteger la privacidad frente a este elenco de riesgos. Llegados a este punto, con carácter preliminar, se ha de mencionar la vía posiblemente más eficaz y práctica para preservar en lo posible este nuevo bien: la vía *extrajurídica*, integrada por un amplio compendio de medidas lógicas y/o técnicas de marcado carácter preventivo, en la línea propuesta por SIEBER.[4] A continuación, se abordan los cauces *jurídicos* establecidos en el Derecho español vigente para combatir los potenciales ataques a la privacidad, lo que remitirá, primero, a la Ley Orgánica de Protección de Datos de 1995 (en adelante LOPD) y, finalmente, como instrumento *último* de control social, al Código Penal, especialmente, aunque no sólo, a su art.197, introducido en la reforma penal de 1995 y sometido a sendas adiciones en 2003 y 2010. Será el momento para analizar críticamente las decisiones adoptadas por nuestro legislador y para valorar, con el apoyo de la doctrina penal, aspectos como los siguientes: técnica legislativa empleada, grado de sometimiento de estas medidas a las garantías constitucionales frente al poder punitivo estatal, la eventual coherencia entre la vía extrapenal y la penal, nivel de armonización con las legislaciones próximas, o pronóstico estimado de eficacia en la práctica.

Por último, debemos advertir que en la elaboración del presente estudio se han manejado, sobre todo, **fuentes bibliográficas** (textos jurídicos, doctrina y jurisprudencia) en castellano, si bien hemos podido acceder a resoluciones, normas y trabajos sobre la materia desarrollados más allá de nuestras fronteras. Ello resulta plenamente justificado, no sólo por el carácter transnacional de esta manifestación de la criminalidad, sino también por las exigencias derivadas de nuestra pertenencia a la Unión Europea y, en fin, por ser parte de la *aldea global*.

[4] SIEBER, "Criminalidad informática: Peligro y prevención", (traducción de Elena Farré Trepat), *Delincuencia Informática*, AA.VV., Santiago Mir Puig (comp.), PPU, Barcelona, 1992.

PRIMERA PARTE:
DESARROLLO TECNOLÓGICO Y
EMERGENCIA DEL BIEN PRIVACIDAD

I. Realidad social: Impacto de las TICs en los bienes personalísimos.

La relevante incorporación de las TICs a lo largo de las últimas tres décadas en la sociedad ha estado encaminada a favorecer el tratamiento y la gestión de la información de la manera más eficaz posible. La capacidad de almacenamiento y circulación que las caracteriza, unido a su fácil acceso, operación exacta y fiable a tiempo real, eliminación de las barreras espaciales, su enorme adaptabilidad a las necesidades humanas, entre otras, han hecho de las TICs un instrumento imprescindible para las administraciones públicas, las empresas privadas de prestación de servicios, así como para la producción industrial y el desarrollo tecnológico y de la investigación. Hablando de modo técnico, con las TICs se produce el cambio de la información analógica a la información digital[5].

En los últimos años las TICs se han convertido en un instrumento de la vida cotidiana de los particulares como medio de comunicación con otras personas (a través de las redes sociales o blogs), de adquisición de productos y contratación servicios y, en un sentido amplio, de difusión y acceso a la información más diversa y abundante que se pueda imaginar.

Si hay algo que podamos destacar del empleo de las TICs sería, en efecto, el intercambio y la comunicación de la información, que no se circunscribe a un ámbito de dimensiones reducidas sino que, como bien aludimos en la Introducción de este trabajo, alcanza un carácter global o internacional.

Aunando todas estas características, cabe afirmar que las TICs han ido generando una revolución multidimensional, con incidencia tanto en las estructuras como en los valores sociales vigentes. No podemos obviar que las mismas se han convertido en un instrumento poderoso de influencia cultural, cuyos efectos más profundos a medio plazo no son fáciles de evaluar.

---

[5] ROMEO CASABONA, *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Comares, Granada, 2006.

Las comunicaciones a través de la Red no sólo nos permiten acceder a información, sino también, como usuarios, podemos crearla, cederla y difundirla, encontrándose a disposición del resto de usuarios como una manifestación cotidiana de la libertad de expresión y de comunicación. La Red en este sentido se ha convertido en un nuevo y gran espacio de libertad y, por consiguiente, en un excelente marco para el ejercicio de tan importante derecho fundamental.

Por otro lado, posicionándonos en la vertiente negativa del acceso, uso, apropiación, manipulación o distribución de esa información, estas conductas pueden ser en sí mismas abusivas para los derechos fundamentales y libertades públicas de otras personas, requiriendo, en un último término, una respuesta jurídico-penal. A esto se refería QUINTERO OLIVARES[6], a finales de los ochenta, cuando afirmaba que "la tecnología moderna (…) y la informática proporciona, a la vez que grandes ventajas al desarrollo social y cultural, grandes riesgos que no por necesarios deben ser asumidos hasta el punto de dejar los derechos individuales expuestos a cualquier agresión, pues el progreso auténtico también pasa por el respeto profundo a la libertad".

Es cierto que pueden verse afectados múltiples derechos fundamentales y libertades públicas por el uso indebido de las TICs; sin embargo, por la concreción del trabajo, según se advirtió, no podremos abordar cada una de las afecciones a los diversos bienes y e intereses concernidos. Por ello centráramos nuestra atención en un interés social tan valioso que denominamos "privacidad" y que aúna en su fuero interno una serie de derechos fundamentales tales como: la intimidad, el honor, la propia imagen, el libre desarrollo de la personalidad e incluso la misma dignidad de la persona.

II. Previsiones constitucionales y referencias en la esfera internacional.

Para iniciar este apartado, entendemos necesaria una advertencia previa en lo que respecta a la posición que adoptaremos en torno al concepto de "bien jurídico" o "bien jurídico-penal". Siguiendo la posición masivamente aceptada por la doctrina desde el S. XIX hasta nuestros días, la categoría dogmática de "bien jurídico" no puede confundirse con el concepto de "derecho fundamental" ni con la idea de "derecho subjetivo".

---

[6] MORALES PRATS, *La tutela penal de la intimidad: privacy e informática*, "Prólogo" de QUINTERO OLIVARES, 1ª ed., Ediciones Destino S.A., Barcelona, 1984.

Siguiendo la concepción cedida por VON LISZT, aún de plena vigencia, el objeto jurídico es "el interés vital para el desarrollo de los individuos de una sociedad determinada, que adquiere reconocimiento jurídico". De esta definición se puede destacar que el objeto jurídico, en primer lugar, es un interés vital y preexistente, anterior a un ordenamiento jurídico, pues el Derecho no crea esos intereses sino que les otorga un reconocimiento que los convierte en bienes jurídicos[7].

En segundo lugar, cabe señalar la mención a una "sociedad determinada", esto es, un determinado interés, bien por sus características o bien por cualquier otro motivo, puede llegar a adquirir especial relevancia dentro de un grupo social y en un momento determinado. Al mismo tiempo ese interés puede no tener valor para otros grupos sociales o en otros momentos históricos. Por último, de este concepto básico que nos aportó VON LISZT, podemos inferir que lo que hace o convierte a un interés en bien jurídico es su reconocimiento jurídico; por tanto, cabe preguntarse qué rama del ordenamiento jurídico es la creadora de tales bienes y qué papel juega la Carta Magna en el proceso de *juridificación* o traslado a la norma de un interés valioso para la vida en sociedad.[8] Al respecto, y sin pretensión de afrontar desde estas líneas un debate que nos excede, nos adherimos a las posiciones que sitúan a la Constitución en el papel de establecer un marco esencial de valores, principios y derechos, expresión consensuada de los valores sociales en la sociedad. En dicho texto, y cada vez más en las normas de Derecho Internacional, con las aportaciones de la doctrina y la jurisprudencia constitucional, debe encontrar el Derecho penal su referencia y sus límites al tiempo de tipificar las conductas más reprobables contra los intereses más relevantes.[9].

---

[7] En palabras del propio LISZT: "Nosotros llamamos bienes jurídicos a los intereses protegidos por el Derecho. Bien jurídico es el interés jurídicamente protegido. Todos los bienes jurídicos son intereses vitales del individuo o de la comunidad. El orden jurídico no crea el interés, lo crea la vida, pero la protección del derecho eleva el interés vital a bien jurídico". VON LISZT, *Tratado de Derecho penal*, trad. de la 20ªed. alemana por Luis Jiménez de Asúa, adicionado con el Derecho penal español por Quintilliano Saldaña, t. II, 4ª ed., Reno, Madrid, 1999, p.6.

[8] Vid. GARCÍA RIVAS, *El poder punitivo en el Estado democrático*, Ediciones de la Universidad de Castilla-La Mancha, Cuenca, 1996, pp.46-43.

[9] Conf. ZAFFARONI, –ALAGIA–SLOKAR, *Derecho penal. Parte general*, 2ª ed., Ediar, Buenos Aires, 2002 (1ª ed., 2000), pp. 98 y ss., 486 y ss.: "…la legislación penal no crea bienes jurídicos, sino que éstos son creados por la Constitución, el derecho internacional y el resto de la legislación. (…) La ley penal sólo eventualmente individualiza alguna acción que lo afecta de cierto modo particular, pero nunca puede brindarle una tutela amplia o plena, dada su naturaleza fragmentaria y excepcional" (p. 486)

De las anteriores reflexiones se desprende, en suma, que entendemos el bien jurídico como un producto histórico desde un punto de vista material, es decir, no es propio de la sociedad sin más, sino que es el resultado de un conjunto de relaciones sociales en un periodo determinado. Es obvio, que en un Estado democrático el bien jurídico es fruto de la sociedad civil, surgiendo de los conflictos y discusiones que se producen en toda sociedad[10].

Por tanto, atendiendo a los principios o postulados que marca la Constitución no necesariamente hay que encontrar en ella los contornos exactos de un bien jurídico. Sin embargo, la relevancia o demanda social frente a los eventuales riesgos de las TICs para los bienes e intereses personalísimos, lo que llamamos "privacidad", ya tuvo su reflejo en el año 1978, en la redacción del art. 18 de la Carta Magna. Si bien es cierto, el precepto centra su atención en el derecho a la intimidad, algunas sentencias del Alto Tribunal dejan constancia de que no es el único derecho afectado por el uso masivo de las TICs. En tal sentido, sirva la sentencia de 5 de mayo de 2000 (STC 115/2000), en cuyo fundamento jurídico cuarto se establece que "…el derecho fundamental a la intimidad reconocido por el artículo 18.1º de la Constitución española tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona (artículo 10), frente a la acción y el conocimiento de los demás, sean estos poderes públicos o simples particulares. De suerte que el derecho a la intimidad atribuye a su titular el poder de resguardar ese ámbito reservado, no sólo personal sino también familiar". Este fragmento del Tribunal Constitucional, nos da la clave de que este derecho sólo es predicable de las personas físicas (como todos los derechos fundamentales, lógicamente), e incluso se atreve a concretar que su objeto o finalidad es garantizar el "ámbito reservado" de la vida del individuo, esto es, su "privacidad".

Ahora bien, queda claro que el objeto jurídico que se protege es la intimidad, que abarca las manifestaciones concretas a que se refiere el art. 18 de la Constitución Española (en adelante CE) y que se extiende a diversos ámbitos de aplicación: intimidad corporal, intimidad económica y secreto bancario, intimidad de correspondencia, intimidad informática, etc.

---

[10] "Los bienes jurídicos tienen un carácter dialectico. Surgen de la base de la relación social y constituyen una superación en la síntesis de la confrontación social". HORMAZÁBAL MALARÉE, *Bien jurídico y Estado social y democrático de Derecho*, 1ª ed., PPU, Barcelona, 1991, p. 152.

No obstante, frente a esta "privacidad" se encuentra el derecho fundamental de la libertad de información, consagrado en el art. 20 apartado primero, letra d) de la CE referida a la comunicación de hechos mediante cualquier medio de difusión general. El precepto constitucional exige la veracidad, lo cual se ha interpretado como necesidad de veracidad subjetiva, es decir que el informante haya actuado con diligencia, haya contrastado la información de forma adecuada a las características de la noticia y a los medios disponibles[11], puesto que de exigirse una verdad objetiva eso haría imposible o dificultaría en extremo el ejercicio de la libertad de información[12].

Como ya hemos señalado en el párrafo anterior esta libertad de información, con frecuencia, entra en colisión con los derechos al honor, a la intimidad y la propia imagen, que incluso aparecen como límite expresamente reconocido en el precepto constitucional. Ahora bien, en caso de que se produzca este conflicto, deberá llevarse a cabo la correspondiente ponderación de bienes[13], teniendo que analizar cada una de las circunstancias concurrentes, de forma tal que cada caso necesitará de un examen concreto, sin que tenga cabida la aplicación automática de reglas generales.

No obstante, existen unas pautas de las que se sirve la jurisprudencia, que será necesario tener presentes a la hora de analizar cualquier conflicto entre los derechos del artículo 18.1 y los del artículo 20:

a) En ningún caso resultará admisible el insulto o las calificaciones claramente difamatorias[14];

b) El cargo u ocupación de la persona afectada será un factor a analizar, teniendo en cuenta que los cargos públicos o las personas que por su profesión se ven expuestas

---

[11] CARRILLO, "Derecho a la información y veracidad informativa", en *Revista española de derecho constitucional*, Nº 23 (1988), pp. 187-206.

[12] Véase SSTC, entre otras, 6/1988, de 21 de enero, 240/1992, de 21 de diciembre; 47/2002, de 25 de febrero; 75/2002, de 8 de abril.

[13] DOMINGO, *¿Conflictos entre derechos fundamentales?: un análisis desde las relaciones entre los derechos a la libre expresión e información y los derechos al honor y la intimidad*, Centro de Estudios Políticos y Constitucionales, Madrid, 2001, p. 402.

[14] Véase, entre otras, las SSTC 204/2001, de 15 de octubre y 20/2002, de 28 de enero; STC 181/2006.

al público tendrán que soportar un grado mayor de crítica o de afectación a su intimidad que las personas que no cuenten con esa exposición al público[15];

c) Las expresiones o informaciones habrán de contrastarse con los usos sociales, de forma tal que, por ejemplo, expresiones en el pasado consideradas injuriosas pueden haber perdido ese carácter o determinadas informaciones que antes pudieran haberse considerado atentatorias del honor o la intimidad ahora resultan inocuas;

d) No se desvelarán innecesariamente aspectos de la vida privada o de la intimidad que no resulten relevantes para la información[16].

Sin embargo, más allá de estos aspectos de naturaleza subjetiva, el Tribunal Constitucional ha destacado el carácter prevalente o preferente de la libertad de información por su capacidad para formar una opinión pública libre, indisolublemente unida al pluralismo político propio del Estado democrático. Al mismo tiempo, se requiere tener presente que esa prevalencia no juega de forma automática sino sólo en supuestos en los que no concurran otros factores, como pueda ser la presunción de inocencia, en los que la ponderación lleve a primar intimidad, honor o propia imagen sobre las libertades de expresión o, en particular, de información.

Visto y planteado cómo aparece en el marco constitucional configurada la "privacidad" (recordemos que no nos referimos a un derecho fundamental) a través de los diversos derechos que la conforman, es necesario profundizar de modo concreto en aquellos instrumentos jurídicos que sirvieron de inspiración al legislador constitucional, o incluso que sin servir a ese fin, asentaron las bases de una problemática que cada vez se agudizaba en mayor medida y que pretendían establecer una uniformidad en el tratamiento del problema a nivel internacional.

Hemos de referirnos, en primer lugar, a la Declaración Universal de los Derechos Humanos[17]. Esta Resolución adoptada por la Asamblea General de las Naciones Unidas recoge en su artículo 12 que "Nadie será objeto de injerencias

---

[15] Véase la STC 101/2003, de 2 de junio.

[16] Véase la STC 185/2002, de 14 de octubre.

[17] Resolución 217 (III) de la Asamblea General de las Naciones Unidas, adoptada en Nueva York el 10 de Diciembre de 1948.

arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". Por lo tanto, es evidente la necesidad de una regulación concreta (a través de mecanismos que se ajusten al desarrollo tecnológico del momento) que tenga como finalidad la protección de la vida privada de cualquier persona y frente a cualquier tipo de ataque.

En segundo lugar, el Convenio 108 del Consejo de Europa[18], ratificado por España en 1984, fue el pionero de la legislación específica sobre esta materia. No es derecho directamente aplicable, pues se compone de criterios a los que se debe ajustar las legislaciones internas de los Estados que lo ratifiquen[19].

La exigencia[20] de este Convenio se fundamenta en la necesidad de que los datos se obtengan y elaboren de modo lícito, su registro tenga una finalidad legítima y que su utilización no sea incompatible con esa finalidad.

En tercer lugar, a nivel comunitario, la Unión Europea dispone de la Directiva 95/46/CE[21] que, dentro del marco europeo, es el texto modelo en lo referente a la protección de datos personales. Con el objetivo de alcanzar un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales (dentro de la Unión Europea), la Directiva establece una serie de límites al almacenamiento y empleo de esos datos personales, solicitando además la creación de un organismo nacional dentro de cada Estado miembro, que se encargue de aplicar la protección de esos datos.

Los datos a los que resulta de aplicación esta Directiva son: los datos tratados por medios automatizados y los datos contenidos en un fichero no automatizado o que

---

[18] Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales.

[19] El Convenio 108 exige a los ordenamientos internos de los Estados que el desarrollo que lleven a cabo del mismo esté inspirado en el principio de territorialidad, para así proteger a los extranjeros del mismo modo que a los nacionales del Estado en cuestión.

[20] SANTOS GARCÍA, *Nociones generales de la Ley Orgánica de Protección de Datos y su Reglamento*, 2ª ed., Tecnos (Grupo Anaya, S.A.), Madrid, 2012, p. 28.

[21] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

vayan a figurar en él. Por su parte, se excluye la aplicación de la Directiva en los siguientes casos de tratamiento de datos[22]:

- Efectuado por una persona física en el ejercicio de actividades exclusivamente particulares o domésticas;

- Aplicado al ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, tales como la seguridad pública, la defensa o la seguridad del Estado.

Podemos concluir, por tanto, que la Directiva tiene como finalidad proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo una serie de principios de orientación capaces de determinar si dicho tratamiento es o no lícito. Estos principios fundamentales de la protección de datos personales son: La calidad de los datos; la legitimación del tratamiento; la información a los afectados por dicho tratamiento; el derecho de acceso del interesado a los datos; el derecho del interesado a oponerse al tratamiento; la confidencialidad y la seguridad del tratamiento y la notificación del tratamiento a la autoridad de control.

En último lugar y, no por ello menos importante pues nos detendremos de modo conciso en su estudio, se encuentra el Convenio sobre Ciberdelincuencia del Consejo de Europa, hecho en Budapest el 23 de noviembre de 2001. Este instrumento jurídico, ratificado recientemente por España[23], tiene como objetivo prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, mediante la tipificación de esos actos y la asunción de poderes suficientes para luchar de forma efectiva contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación internacional rápida y fiable. (Huelga decir que el Convenio se ocupa de las otras parcelas de la *Ciberdelincuencia* que no se abordan en el presente estudio).

---

[22] http://europa.eu/legislation_summaries/information_society/data_protection/l14012_es.htm

[23] A través del Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, el 1 de octubre de 2010.

En lo que concierne al acceso a los datos personales, el propio Convenio regula lo relativo a las medidas que deben adoptarse a nivel nacional, destacando los siguientes preceptos dentro del propio articulado:

En primer lugar, los art. 4.1º y 5 se refieren a la interferencia directa en los datos y a la interferencia en los sistemas que provoquen daños, alteración o supresión de datos informáticos.

> ***Artículo 4 Interferencia en los datos***
>
> *1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.*

> ***Artículo 5 Interferencia en el sistema***
>
> *Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.*

En segundo lugar, en el art. 6.1º letra a) se establece una serie de actos de disposición de los datos que impliquen un abuso de los dispositivos.

> ***Artículo 6 Abuso de los dispositivos***
>
> *1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:*
>
> *a) la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:*
>
> *(...)*
>
> *ii) una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático.*

Ahora bien, en el título II de la Sección 2ª se regula la manera con la que han de proceder los Estados Parte para la conservación rápida de los datos informáticos almacenados (de especial relevancia para generar un nivel mínimo de confianza entre los Estados en los múltiples casos en que resulta imprescindible la colaboración judicial

y policial para la investigación y persecución de conductas abusivas con impacto transnacional). El título se compone de los arts. 16 y 17, relativos a la conservación rápida de datos informáticos almacenados y conservación y revelación parcial rápidas de datos sobre el tráfico, respectivamente.

Sin embargo si hay algo que caracteriza a este Convenio es el *peligroso* sistema de contacto permanente entre los Estados Parte. En efecto, nos referimos al Mecanismo 24/7 regulado en el art. 35 del Convenio. Este precepto establece en su apartado primero que cada Estado Parte designará un punto de contacto disponible las veinticuatro horas del día, los siete días de la semana, con la finalidad de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito.

La asistencia a la que se refiere el precepto debe incluir los actos tendentes a facilitar una serie de medidas o su adopción directa, conforme a la legislación y la práctica internas. Las medidas son las siguientes: el asesoramiento técnico; la conservación de datos en aplicación de los artículos 29 y 30; la obtención de pruebas, el suministro de información jurídica y la localización de sospechosos.

El apartado segundo del precepto delimita los puntos de contacto que conectan a ambos Estados Parte del Convenio. Así, el punto de contacto de una Parte estará capacitado para mantener comunicaciones con el punto de contacto de otra Parte con carácter urgente. No obstante, si el punto de contacto designado por una Parte no depende de la autoridad o de las autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, el punto de contacto velará por garantizar la coordinación con dicha autoridad o autoridades con carácter urgente.

En resumen, el contexto en el que se ejercitan los derechos a los que nos venimos refiriendo, y en concreto al bien "privacidad", es el de una sociedad donde la informática se ha convertido en un símbolo emblemático de nuestra cultura, hasta el punto de que para designar el marco de nuestra convivencia se puede aludir a las expresiones: "sociedad de la información" o "sociedad informatizada".

A esto aludía PÉREZ LUÑO[24] cuando afirmaba que en la sociedad que vivimos, la información es poder y este poder adquiere relevancia cuando, en virtud de la informática, convierte informaciones parciales y dispersas en informaciones en masa y organizadas. Es en ese preciso momento cuando la reglamentación jurídica de la informática reviste un interés prioritario.

III. Delimitación de la "privacidad" como objeto de protección.

1. Insuficiencia de los bienes y derechos clásicos.

Hemos venido constatando en los anteriores apartados que ni los instrumentos internacionales ni la propia Carta Magna son suficientes para tutelar los bienes y derechos fundamentales eventualmente afectados por las conductas ilícitas o abusivas que se desarrollan a través de las TICs.

No debemos conformarnos simplemente con aplicar el ámbito de protección de los derechos reconocidos en el art. 18 de la CE, pues es evidente que los distintos ataques que se pueden producir a la "privacidad" van más allá de cualquier solución dada al respecto. No obstante, debemos preguntarnos dónde se encuentra en verdad el problema, cuando disponemos de un amplio catálogo de derechos fundamentales, libertades públicas y bienes jurídicos objeto de tutela penal, ¿por qué decimos que los bienes y derechos clásicos son insuficientes para dar amparo satisfactorio a la "privacidad"?

La respuesta ya había sido dada por PÉREZ LUÑO en la década de los ochenta cuando afirmaba que el "riesgo reside en la pretensión de sustituir la racionalidad humana por una racionalidad artificial tecnológica, es decir, en convertir la lógica del desarrollo tecnológico en el principio supremo del vivir social"[25].

---

[24] PÉREZ LUÑO, "Las generaciones de derechos fundamentales" en *Revista del Centro de Estudios Constitucionales*, Nº 10 (Septiembre - Diciembre 1991), p. 209.

[25] PÉREZ LUÑO, *Nuevas tecnologías, sociedad y derecho. El impacto socio-jurídico de las N.T. de la información*, FUNDESCO, Madrid, 1987, p. 21.

Por tanto, sirviéndonos de jurisprudencia, doctrina y otros materiales, intentaremos dar un contenido material a la "privacidad" para entender qué queremos o pretendemos proteger, quiénes deben protegerse y cómo han de hacerlo.

2. Contenido material de la privacidad.

En 1992, con la promulgación de la Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal[26] (en adelante LORTAD), vemos como el legislador desarrolla en su Exposición de Motivos el art. 18 de la Constitución, asimilando, el derecho a la protección de datos de carácter personal con el Derecho Fundamental al Honor, la Intimidad personal y familiar, y la propia imagen, afirmando:

"...hasta el presente, las fronteras de la privacidad estaban defendidas por el tiempo y el espacio. El primero procuraba, con su transcurso, que se desvanecieran los recuerdos de las actividades ajenas, impidiendo, así, la configuración de una historia lineal e ininterrumpida de la persona; el segundo, con la distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. El tiempo y el espacio operaban, así, como salvaguarda de la privacidad de la persona.

Uno y otro límite han desaparecido hoy: las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, por distante que sea el lugar donde transcurrieron los hechos, o remotos que fueran éstos.

Los más diversos datos relativos a las personas podrían ser, así, compilados y obtenidos sin dificultad. Ello permitiría a quien dispusiese de ellos acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas; a aquélla a la que sólo deben tener acceso el individuo y, quizás, quienes le son más próximos, o aquellos a los que él autorice.

---

[26] Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, vigente hasta el 14 de enero de 2000.

Aún más: el conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor; y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos...".

Así pues, el legislador dejó constancia en el artículo primero de la LORTAD cuál era su objetivo primordial: limitar el uso de la informática y otros medios de tratamiento automatizados, para proteger así el derecho al honor, la intimidad y la propia imagen y además pudiéndose aplicar la norma sobre los ficheros automatizados o bases de datos tratadas a través de medios informáticos.

Volviendo a los párrafos transcritos de la Exposición de Motivos, podemos apreciar la preocupación que invade al legislador el prominente desarrollo de las TICs, pues como bien afirma, consiguen superar los límites del tiempo y del espacio, viéndose amenazadas por tanto, la intimidad personal y familiar, la propia imagen, la libertad individual, el derecho al libre desarrollo de la personalidad e incluso la dignidad del individuo, sin que él mismo sea capaz de controlar todos los datos que componen "su vida privada", aquello que va más allá de lo que quiere que se sepa.

Cabe destacar de entre los derechos "amenazados" la intimidad personal y familiar, propia imagen y el derecho al honor que se encuentran desarrollados por una Ley orgánica[27] en cuyo primer artículo se determina la protección civil de estos derechos frente a todo género de injerencia o intromisión ilegítima (sin obviar que algunos de estos derechos gozan de protección penal. Tal es el caso del derecho al honor amparado por los artículos que componen el libro II, título X del presente Código Penal[28]). La relevancia de los mismos se plasma no sólo en el desarrollo de esta ley, sino que además la doctrina jurídica los ha encuadrado en la categoría de derechos de la

[27] Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

[28] En los casos que exista la protección penal tendrá ésta preferente aplicación, por ser sin duda la de más fuerte efectividad, si bien la responsabilidad civil derivada del delito se deberá fijar de acuerdo con los criterios que esta ley establece.

personalidad, siendo por tanto una calificación de la que se desprende el carácter irrenunciable de estos derechos.

Por tanto, paralelamente al desarrollo de estos derechos fundamentales, se aprecia junto a la "privacidad" el tratamiento de los datos de carácter personal como un derecho autónomo, en concreto, la STC 254/1993 declaró en su fundamento jurídico séptimo que "el art. 18.4 CE incorpora un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad. La garantía de la intimidad adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático *(habeas data)* y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención". De esta manera, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención.

En lo que respecta al avance en las TICs y el uso masivo de Internet, el Tribunal Constitucional también se pronunció en la STC 143/1994, afirmando que "es un hecho también admitido en la jurisprudencia de este Tribunal que el incremento de medios técnicos de tratamiento de la información hace precisa la ampliación del ámbito de juego del derecho a la intimidad, que alcanza a restringir las intromisiones en la vida privada puestas en práctica a través de cualquier instrumento, aun indirecto" (…) "y a incrementar las facultades de conocimiento y control que se otorgue al ciudadano, para salvaguardar el núcleo esencial de su derecho".

Ahora bien, para salvaguardar ese núcleo[29], se debe establecer una serie de garantías que hagan frente al acceso, uso, transmisión de los datos personales que integren la vida privada de cualquier individuo. En este punto, entra a funcionar el *habeas data* o derecho fundamental a la protección de los datos (art. 18.4 CE).

El Alto Tribunal ha perfilado las singularidades del derecho a la protección de datos, indicando de modo expreso en su STC 292/2000, fundamento jurídico sexto, que

[29] HERNÁNDEZ RAMOS, "El derecho al olvido digital en la Web 2.0" en *Cuaderno Red de Cátedras Telefónica*, Mayo 2013, pp. 16 a 19.

"su objeto es más amplio que el del derecho a la intimidad", puesto que "el derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado". En consecuencia, el objeto de protección del derecho fundamental a la protección de datos que se deriva del art. 18.4 CE "no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos que, por el hecho de serlo, al ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos".

3. Titularidad y valor del consentimiento.

Antes de entrar a analizar cómo se configura el consentimiento de la persona en lo relativo al acceso y tráfico de sus datos personales, es preciso estudiar de modo breve el carácter de los derechos a los que nos hemos venido refiriendo. Así el derecho a la intimidad, el honor, la propia imagen o la libertad son derechos de carácter personal, individual y disponible. Como bien señala GUTIÉRREZ FRANCÉS[30], la disponibilidad del derecho es lo que "determina que el consentimiento de su titular adquiera una incuestionable trascendencia en la calificación jurídica de las actividades que puedan incidir sobre el mismo".

Sin embargo, somos conscientes de que esa disponibilidad con la que en su día se calificó a los derechos nombrados no puede equipararse a la disponibilidad de la que venimos haciendo uso hoy en día, sobre todo porque aunque seamos nosotros mismos los que pongamos a disposición del resto de usuarios de la Red nuestros datos personales, no podemos imaginarnos hasta quiénes pueden llegar o, posicionándonos en lo peor, no imaginamos qué perjuicios nos pueden causar con ellos.

---

[30] GUTIÉRREZ FRANCÉS, "La privacidad en el espacio virtual (riesgos y cauces de protección)" en *Cuaderno Red de Cátedras Telefónica*, Septiembre, 2011, p. 13.

Es cierto que la mayoría de los datos que circulan por la Red han sido cedidos por nosotros mismos, de modo voluntario o inconsciente, ya sea a través de redes sociales, foros, grupos… Otras veces, alguna clase de datos personales son requeridos en ciertos ámbitos privados o públicos, más allá de lo que quiera el titular de los mismos, porque son imprescindibles para acceder a algún tipo de prestación o de servicio[31]. Obviamente no todos los datos son prestados de modo voluntario, y en concreto están aquellos datos que en verdad tampoco requieren un consentimiento expreso por tratarse de imágenes, comentarios, vídeos que proporcionan personas cercanas a nosotros o a nuestro entorno.

Por otro lado, se encuentran aquellos datos que recopilan de nosotros cuando llevamos a cabo determinadas actividades (sirva como ejemplo, cuando realizamos alguna búsqueda para realizar un viaje de fin de semana y estamos comparando precios y páginas *webs* de alojamientos. A partir de ese momento, recibiremos *emails* a nuestros correos sobre las ventajas que nos oferta una determinada página *web* especialista en alojamientos, o simplemente mientras navegamos por la Red, a ambos lados de la pantalla salen imágenes sobre casas rurales, ofertas de apartamentos, etc…) Quizás esto sirva para amenizar nuestra búsqueda o facilitarnos la vida de cara a simplificar las opciones de compra o alquiler, pero hay algo cierto y es que en ningún momento hemos prestado un consentimiento para que terceros ajenos a nuestro entorno recaben información sobre nuestras actividades y gustos y las empleen para captar nuestra atención y así operar económicamente.

En último lugar se encontrarían aquellos datos que bajo ninguna circunstancia quisiéramos que fuesen conocidos o que accediesen a ellos. Es, en este punto, donde entran en juego aquellos terceros que, sin nuestro consentimiento, acceden o sistemas informáticos y ordenadores sin autorización, ya sea físicamente o por medio de programas informáticos especializados, bien para capturar, borrar o manipular la información y datos ajenos, bien para suplantar identidades o bien para controlar y espiar a otros. En verdad, este tipo de delitos pueden ser cometidos no sólo por "*hackers*" individuales, sino que actualmente la problemática adquiere relevancia a nivel internacional como una de las expresiones modernas de la criminalidad organizada

[31] En este aspecto la LOPD exige en su artículo 6 que el consentimiento del afectado tiene que ser inequívoco.

transnacional (como es el caso del movimiento internacional de ciberactivistas, ANONYMOUS).

Analicemos ahora cómo se plantea el consentimiento en la LOPD y la prestación del consentimiento en el caso de los menores de edad. Dentro de la LOPD el consentimiento se refleja:

- En lo que respecta al tratamiento de datos especialmente protegidos de salud, vida sexual y origen racial: se requiere el consentimiento expreso del afectado, además a modo de garantía conviene que conste por escrito. En el caso de tratamiento de datos especialmente protegidos de ideología, afiliación sindical, religión y creencias es obligatorio que el consentimiento sea expreso y aparezca por escrito.

- El resto de datos que no se encuentren incluidos en el art. 7 de la LOPD requieren un consentimiento inequívoco tal y cómo se exige en el art. 6 de la misma Ley. No se necesita que sea expreso o conste por escrito.

- Conforme al art. 11 de la LOPD los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado, por tanto, basta con que el consentimiento sea inequívoco.

- El consentimiento no puede concederse de modo general, sino que hay que atender al caso concreto en cuestión.

- La ley prevé además que el consentimiento puede ser revocado[32] en cualquier momento siempre que medie causa justificada.

Un problema a nuestro juicio especialmente sensible es el relativo al consentimiento otorgado por los menores, pues la propia LOPD no se pronuncia al respecto. Sí lo ha hecho, en cambio, la Memoria de la Agencia Española de 2000[33], que

[32] El artículo 6.3 de la LOPD establece que el consentimiento puede ser revocado en cualquier momento, aunque la Ley introduzca la expresión "cuando exista causa justificada".

[33]http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2000-0000_Consentimiento-otorgado-por-menores-de-edad.pdf

diferencia entre los menores mayores de catorce años (a los que la Ley atribuye capacidad para la realización de determinados negocios jurídicos) y aquellos menores que no alcanzan esta edad.

a) Menores mayores de catorce años: se ha de tener en cuenta que el artículo 162.1 del Código Civil exceptúa de la representación legal del titular de la patria potestad a "los actos referidos a derechos de la personalidad u otros que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, pueda realizar por sí mismo", es por ello, que la AEPD considera que "el menor tiene condiciones suficientes de madurez para prestar su consentimiento al tratamiento de los datos (…) toda vez que nuestro ordenamiento jurídico viene, en diversos casos, a reconocer a los mayores de catorce años la suficiente capacidad de discernimiento y madurez para adoptar por sí solos determinados actos de la vida civil".

Se ha de tener en cuenta, además, lo afirmado por la DGRN en su resolución de 3 de marzo de 1989: "no existe una norma que, de modo expreso, declare su incapacidad para actuar válidamente en el orden civil, norma respecto de la cual habrían de considerarse como excepcionales todas las hipótesis en que se autorizase a aquél para obrar por sí; y no cabe derivar esa incapacidad ni del artículo 322 del Código Civil, en el que se establece el límite de edad a partir del cual se es capaz para todos los actos de la vida civil, ni tampoco de la representación legal que corresponde a los padres o tutores respecto de los hijos menores no emancipados".

Por tanto, se puede afirmar que la minoría de edad no supone una causa de incapacitación (artículo 200 del CC), por lo que aquélla habrá de ser analizada en cada caso concreto para analizar si el menor dispone de capacidad suficiente para la prestación de su consentimiento.

b) Menores que no han cumplido aún los catorce años: en este caso la AEPD no da una solución favorable, remitiendo al artículo 162.1 del CC, donde se deberá tener en cuenta la condición de madurez del menor en cuestión.

Concluye la AEPD afirmando que "será necesario recabar el consentimiento de los menores para la recogida de sus datos, con expresa información de la totalidad de los extremos contenidos en el artículo 5.1 de la Ley, recabándose, en caso de menores de

catorce años cuyas condiciones de madurez no garanticen la plena comprensión por los mismos del consentimiento prestado, el consentimiento de sus representantes legales".

4. Amenazas a la privacidad en la sociedad globalizada.

El fenómeno de la globalización es un hecho con un detonante económico: surge vinculado a la necesidad de los medios de producción, con la finalidad de abrir nuevos mercados y abaratar los costes, pero entendemos que el fenómeno resultaría de todo punto incomprensible sin la palanca impulsora que ha representado la revolución tecnológica digital. Por lo demás, cabe afirmar que el proceso de globalización no implica necesariamente un efecto negativo o positivo. Depende de quién y cómo se controle el proceso. Parte de la doctrina se posiciona a favor[34] del aprovechamiento de este fenómeno en un proyecto humanista, aunque en otros ámbitos se pone mayor acento en los efectos perversos. la verdad es que hoy en día la globalización es una forma específica de mundialización de la actividad económica[35] desarrollada conforme a unas políticas neoliberales que están dañando el bienestar de las clases menos favorecidas[36].

Así pues, dentro de este contexto, la generalidad y el empleo masivo de la Red configuran esta realidad que sea un fenómeno más del proceso de la globalización. Sin embargo, como bien sostiene ROMEO CASABONA[37], no debemos obviar que las comunicaciones telemáticas por medio de sistemas informáticos también han contribuido a extender este fenómeno.

---

[34] AMÍN sostiene que "la realización de ese proyecto implica construir un sistema político global que no esté al servicio del mercado global", en *El capitalismo en la era de la globalización*, Paidós, Barcelona, 1999, p. 19.

[35] MATELLANES RODRÍGUEZ, "La criminalidad informática como manifestación del fenómeno de la globalización" en *Revista Penal*, Nº 22, LA LEY, (Julio 2008), p.53.

[36] NAVARRO LÓPEZ, *Bienestar insuficiente, democracia incompleta: sobre lo que no se habla en nuestro país*, Anagrama, Barcelona, 2003, p. 149.

[37] ROMEO CASABONA, "De los delitos informáticos al Cibercrimen. Una aproximación conceptual y político-criminal", *El Cibercrimen. Nuevos retos jurídico-penales…* ob., cit., p. 1.

Importa destacar que a finales del pasado año, la Asamblea General de las Naciones Unidas adoptaba la Resolución 68/167[38] en la que defiende el derecho a la privacidad y llama a los Estados a tomar medidas para poner fin a las actividades que violen ese "principio de la sociedad democrática".

El texto, adoptado por consenso subraya que el derecho a la privacidad es una garantía fundamental y afirma que debe protegerse como tal cuando las personas utilicen el Internet y otros medios de comunicación digitales. Por ello, la resolución insta a los Estados a establecer o mantener sistemas de vigilancia nacional independientes y transparentes, que rindan cuentas sobre sus operaciones, incluidas la interceptación de comunicaciones y la recolección de datos personales.

Al tiempo que se desarrollaba y adoptaba la Resolución por parte de la Asamblea General de la ONU, el exanalista de la Agencia de Seguridad Nacional de Estados Unidos (NSA) Edward Snowden advertía de la amenaza global a la privacidad, recordando que el inglés George Orwell "ya advirtió del peligro de este tipo de información" en su novela "1984", donde los datos se recogían con micrófonos, cámaras de vídeo y televisiones "que observan". Sin embargo, Snowden señaló que esos mecanismos no son nada comparado con lo que existe en la actualidad, afirmando que "tenemos sensores en nuestros bolsillos que nos siguen a cualquier lugar al que vayamos".

Para Snowden, la importancia que se le dé a la privacidad hoy en día abrirá un debate que permitirá juzgar no sólo el grado de confianza que nosotros, los usuarios, depositemos en la tecnología, sino también la confianza que recae en los Gobiernos nacionales y su manera de regular las TICs.

[38] Resolución aprobada por la Asamblea General el 18 de diciembre de 2013 [sobre la base del informe de la Tercera Comisión (A/68/456/Add.2)]

SEGUNDA PARTE:
CAUCES PARA LA PROTECCIÓN DE LA PRIVACIDAD

I. Introducción: Medidas de prevención y de autoprotección.

Tras señalar sucintamente las principales amenazas que se ciernen sobre este bien de nuevo cuño que denominamos "privacidad", procede ahora abordar los cauces a los que puede recurrirse, dentro de nuestro contexto, para procurar su protección. Obviamente, nuestro objetivo prioritario se centra en las vías de naturaleza jurídica, extrapenales y penales. No obstante, consideramos importante mencionar, siquiera brevemente, otras medidas sobre las que vienen insistiendo los especialistas en el ámbito interno y en la esfera internacional. Se trata de las medidas de prevención y de autoprotección. Aunque pudieran parecer obvias estas reflexiones, y por tanto innecesarias (al ser de aplicación a cualquier otra modalidad delictiva la *advertencia* genérica sobre la necesidad de prevención y la adopción de medidas de autoprotección), en la parcela que aquí nos ocupa está singularmente justificada tal referencia. Ello conecta con las especiales notas criminológicas que, debido a las posibilidades que ofrecen las TICs y su modo de operar, caracterizan a todas las parcelas de la *Ciberdelincuencia*, incluida ésta.

Desde los primeros estudios sobre delincuencia informática (de PARKER, NYCUM, BEQUAI o SIEBER, entre otros)[39], se ha destacado la elevada "cifra negra" o "zona oscura" en el ámbito referido, derivado de las extraordinarias dificultades que se plantean en términos de detección, prueba y persecución de los hechos. Las razones son de sobra conocidas: relativa facilidad de comisión, con la posibilidad de separación espacio/temporal entre la conducta y el resultado; facilidad para borrar todo rastro del ilícito desde lugares remotos, con frecuencia traspasando las fronteras de varios Estados y actuando con un ordenador ajeno (de cualquier ciudadano en cualquier lugar del mundo) infectado por un programa *troyano (bot),* mediante el que se controla a distancia toda la actividad de ese ordenador; dificultades para coordinar actuaciones policiales y judiciales en las actuaciones contra delitos en el *espacio virtual*, problemas para la investigación de los hechos y para el aseguramiento de las pruebas…, entre otras causas.

[39] Vid., con amplia bibliografía, GUTIÉRREZ FRANCÉS, *Fraude informático y estafa*, cit. pp.

Si partimos de una realidad así, la idea de combatir eficazmente el *cibercrimen*¸ resulta una utopía; y ello, pese a lo completa y rigurosa que sea la legislación propia y la de los demás países de la comunidad internacional incorporados a la *era digital*, y por elevado que sea el nivel de formación y capacitación en la Justicia y en la Policía.

Así se explica que desde distintas instancias se inste a los ciudadanos y a las instituciones públicas y privadas a que adopten toda clase de medidas preventivas frente a esta delincuencia *silenciosa.* Entre las mismas, destacamos aquellas que nos parecen más relevantes para preservar en lo posible la privacidad:

- Respecto al ciudadano particular, se recomienda cuidar la información que se suministra y dónde. Todo lo que se deja en la Red, queda para siempre en la Red, por más que quisiéramos creer que sólo nos comunicamos con nuestro círculo de seleccionados. Correos electrónicos, videos y fotos privadas, opiniones vertidas en periódicos digitales y foros, noticias y anuncios que son de nuestro interés, movimientos de nuestra tarjeta de crédito, datos médicos informatizados en centros médicos y farmacias… Debemos ser conscientes de que toda esa información está, de hecho, disponible a otros sujetos individuales o grupos organizados, a servidores nacionales e internacionales, y a compañías e instituciones públicas y privadas; es una información que, al saltar a la Red, se ha ido de nuestro control, de tal suerte que ya no está en nuestras manos el uso/maluso que se pueda hacer de ella. Convendría ponderar qué estamos dispuestos a sacrificar en términos de privacidad en el uso de redes sociales, foros y grupos, e, incluso, en la utilización sin límites de las comunicaciones electrónicas.

- Se añaden medidas de carácter físico (preservar instalaciones y equipos informáticos, el lugar donde estos se encuentren y las personas con acceso a los mismos) y medidas de carácter lógico (cortafuegos, antivirus y antitroyanos actualizados, contraseñas encriptadas, etc).

- Adicionalmente, para empresas, instituciones públicas y privadas, y para los encargados y responsables de archivos y bancos de datos informatizados, se aconsejan, además de las medidas anteriormente indicadas, otras relativas a la selección del personal de forma adecuada, división de trabajo entre los que tienen acceso a los sistemas y manejan la información –a fin de evitar que un

solo trabajador controle todo el proceso-, cambios frecuentes de contraseñas y claves, incorporación de mecanismos para el rastreo de la actividad de los empleados, etc.

Para terminar este apartado, recordamos que estas medidas acaso pueden minimizar riesgos, pero no van a ser el cauce suficiente para evitar los ataques a la privacidad de *hackers*, organizaciones y entidades gubernamentales, nacionales e internacionales.

II. Medidas administrativas.

1. Antecedentes: De la LORTAD a la LOPD.

Con la redacción de la Carta Magna España fue uno de los países europeos (junto con Portugal) que reconoció la necesidad de otorgar una protección a las personas frente al desarrollo de las TICs. Fruto de la problemática que venía asomando (Caso Publi Gest[40]) y quizás de un modo precipitado y urgente se promulgó en 1992 la LORTAD encargada de regular el tratamiento automatizado de datos personales.

---

[40] En el año 1991 despertó la alarma social un hecho ilícito que, aun no encontrándose tipificado, daba señas a la doctrina sobre la importancia de la positivización del tratamiento de los datos de carácter personal. Aquello que abrió la caja de Pandora, se gestó en un simple "chivatazo" o "yo acuso" por parte del Director Técnico de una empresa. El 11 de julio de 1991 O.G., Director Técnico de la empresa "Leisa", presentó una denuncia contra J.G.L., representante de la empresa "Publigest", en la cual afirmaba que J.G. era arrendatario de los locales de "Leisa" y que éste hizo uso de las máquinas instaladas en ellos con la finalidad de reproducir bancos de datos informáticos de distintas dependencias oficiales (Hacienda, Tráfico, Censo electoral, etc.). Esos datos eran vendidos a diferentes empresas y facilitados a J.G. por funcionarios de los centros oficiales correspondientes. Tras las oportunas diligencias el Juzgado de Instrucción núm. 2 de Móstoles dictó el 1 de septiembre de 1992 un Auto de sobreseimiento, motivado por la falta de indicios de la comisión de algunos de los delitos tipificados en el Código Penal, excepto lo recogido en el fundamento jurídico quinto que establecía que «de las diligencias obrantes en autos sí parece desprenderse la comisión de un delito de cohecho, previsto y penado en el art. 391 del Código Penal , que viene configurado por gestiones llevadas a cabo por J.G., a través de una funcionaria de la Junta de Andalucía».
En el propio Auto de sobreseimiento se explican las distintas maneras por las que se conseguía la información: desde la compra o intercambio de ficheros con otras empresas del sector, pasando por una serie de datos relativos a la Seguridad Social o aportados por censos y padrones, pues eran solicitados con la finalidad ficticia de emplearlos en trabajos de informatización para festejar fines públicos, siendo empleados con fines privados e incluso se solicitaban a las instancias públicas u organismos encargados de la recogida y almacenamiento de este tipo de información.
Ahora bien, cabe destacar que la mayoría de la información proporcionada por los datos que se encargaba de recopilar PUBLIGEST S.L. no era una información secreta, pues se trataban de datos públicos al alcance de cualquiera que los solicitara. Entonces, ¿dónde se encuentra la problemática? Este caso, nos permite analizar dos lagunas que inundaban nuestro ordenamiento jurídico en aquellos años: 1º no había norma alguna que regulase todo lo relativo al tráfico de datos personales; y 2º el Código Penal del

La LORTAD fue aprobada con errores en sus planteamientos y con una remisión constante a otras normas para regular supuestos concretos, y ello conllevo una cierta diversidad normativa. Puede citarse entre sus errores:

- Dentro de su contenido se citaba normativa que restringía el uso de la informática y obligaba a inscribir todos los ficheros automatizados, además de instaurar medidas cautelares que los protegieran.

- Disponía de un tratamiento desigual a la hora de aplicar las sanciones por infracciones cometidas por los responsables de los ficheros, siendo más restrictivas las aplicadas a las que atentaban contra los ficheros privados y más suaves con los responsables de los ficheros públicos.

- Atribuía al Ejecutivo[41] la posibilidad de regular cuestiones de carácter trascendental como es el caso del nombramiento del Director de la Agencia Española de Protección de Datos.

No obstante, siete años después la LORTAD fue sustituida por la Ley orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (en adelante LOPD), que si bien se tenía expectativas muy altas sobre su regulación[42], esta Ley no ha implicado cambios importantes respecto de la regulación anterior.

Estudiemos de manera detenida[43], cuál es el objeto de la Ley y su ámbito de aplicación para entender el funcionamiento de la misma.

2. Ámbito de la LOPD.

Acudiendo al artículo primero de la LOPD podemos apreciar de modo sintético y breve cuál es el objeto: "garantizar y proteger, en lo que concierne al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas

---

momento únicamente se refería en sus artículos 286, 390 y 391 a los casos de ofrecimiento o solicitud de dádivas o cualquier efecto a los funcionarios públicos encargados de la custodia de esos datos.

[41] ARTECHE alude a un alto grado de "administrativización".

[42] GARRIGA DOMÍNGUEZ, *Tratamiento de datos personales y derechos fundamentales*, 2ª ed., Dykinson S.L., Madrid, 2009, p. 49.

[43] No analizaremos, por falta de espacio, la Ley Orgánica 1/1982, de Protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

físicas, y especialmente su honor e intimidad personal". En la redacción del precepto se observa claramente la influencia que ejerce la Directiva 95/46/CE y también nos sirve a modo de comparación para ver en qué difiere de la regulación contenida en la LORTAD.

Así pues, en la anterior regulación se seguía lo establecido en el artículo 18.4 de nuestra Constitución, siendo el objeto de la LORTAD la limitación del uso de la informática con la finalidad de garantizar los derechos de los ciudadanos. En la actual LOPD el objetivo es la garantía y protección de las libertades públicas y derechos fundamentales de las personas, en lo que concierne al tratamiento de datos de carácter personal.

No obstante, ambas Leyes orgánicas coinciden en el establecimiento de un conjunto de principios y garantías que tratan de asegurar ese respeto a los derechos y libertades fundamentales, a los que aludimos en el párrafo anterior.

Volviendo a la lectura del primer precepto de la LOPD, se deduce que el legislador pretendía ir más allá de la limitación de la informática y de las TICs. Lo que en verdad buscaba era ofertar un abanico amplio de garantías que tutelasen los derechos fundamentales del cualquier individuo. Sin embargo, la limitación del uso de la informática de la que se servía la anterior LORTAD tenía también como objetivo garantizar esos derechos; por tanto, aunque se ha mejorado la redacción del precepto, como bien afirma GARRIGA DOMÍNGUEZ, "en nada se habrá avanzado si los derechos de los afectados no gozan de plena eficacia frente a la anterior regulación caracterizada por las numerosas excepciones de aquellos".

Hemos hecho alusión a libertades públicas y derechos fundamentales objeto de garantía y protección, pero ¿a qué libertades y derechos nos referimos? De la lectura del artículo primero de la LOPD se deduce que se refiere a todos los derechos constitucionalmente reconocidos, en concreto y como nos hemos venido refiriendo a lo largo de este trabajo, el derecho a la intimidad (con todas sus variantes) y el derecho al honor, pero si únicamente nos centrásemos en estos derechos, estaríamos pretendiendo la protección de aquellos datos personales con un carácter íntimo, dejando fuera de protección el resto de datos personales de la persona en cuestión.

En conclusión, el bien jurídico que pretende garantizar la LOPD es un derecho fundamental autónomo, una garantía que tutela las libertades públicas y derechos fundamentales, en concreto y de suma importancia es la dignidad de las personas.

En el art. 2 de la Ley se establece que la LOPD será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado y, por tanto, se incluyen los datos contenidos en los ficheros manuales, diferenciándose en este punto de la antigua LORTAD.

Como consecuencia de la promulgación de la Directiva 95/46/CE, la LOPD incluye los ficheros no automatizados, algo que no se reflejaba en la LORTAD, aunque en la Disposición Final Segunda de esta última Ley se preveía la extensión de su aplicación a los ficheros convencionales.

En conclusión, las normas contenidas en esta Ley se aplicarán a aquellos datos personales que se contengan en ficheros privados o públicos, como automatizados o no automatizados.

El precepto, además, nos proporciona unos criterios de carácter territorial, es decir, la Ley resulta de aplicación: cuando el tratamiento se lleve a cabo en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento; o bien cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público; y, en tercer lugar, cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

3. Principios y derechos consagrados.

La LOPD consagra en su Título II los "principios de la protección de datos" incluyendo en el mismo tanto los principios que hacen referencia a la calidad de los datos como determinados derechos de los afectados (aunque en el siguiente Título de la LOPD se regule de modo teórico los derechos de los titulares de los datos personales).

El encargado de abrir el Titulo II es el art. 4 relativo al *principio de calidad de los datos*. El precepto establece que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, siempre que sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades para las que se hayan obtenido. Así mismo, estos datos no podrán ser emplearse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

En el apartado tercero del precepto se establece la siguiente exigencia: Los datos serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado, pues si resultasen ser inexactos (en todo o en parte) la solución que propugna la Ley es que sean cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados.

La cancelación de los datos se produce cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recabados. El almacenamiento de los mismos tendrá como finalidad el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

En último lugar, el precepto señala la prohibición de la recogida de los datos a través de medios fraudulentos, desleales o ilícitos.

El Título II se compone de otros ocho preceptos (arts. 5 a 12) que se encargan de regular: el derecho de información en la recogida de datos[44] –art. 5-; el consentimiento del afectado (tratado en la primera parte del trabajo); los datos especialmente protegidos –art. 7.-; los datos relativos a la salud –art. 8-; la seguridad de los datos –art. 9-; el deber de secreto –art. 10-; la comunicación de los datos –art. 11-; y el acceso a los datos por cuenta de terceros[45] –art. 12.

Junto a estos principios son de gran importancia social y para el tratamiento de los datos de carácter personal, los derechos ARCO (acceso, rectificación, cancelación y

[44] El art. 5 de la LOPD exige que los individuos a los que se requieran sus datos, deben de ser informados "de modo expreso, preciso e inequívoco".

[45] Se exige que, para la realización del tratamiento de los datos por cuenta de terceros, ha de "estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido".

oposición) regulados en los arts. 15 a 17. De modo concreto cada uno de estos derechos consiste:

Derecho de acceso

Derecho que la LOPD reconoce en su art. 15 a los ciudadanos para que puedan controlar por sí mismos el uso que se hace de sus datos personales, y en particular, el derecho a obtener información sobre si éstos están siendo objeto de tratamiento y la finalidad del mismo, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

Su ejercicio es personalísimo, por lo que sólo podrá solicitarlo la persona interesada, quién deberá dirigirse a la empresa u organismo público del que sabe o presume que tiene sus datos, pudiendo optar por visualizarlos directamente en pantalla u obtenerlos por medio de escrito, copia, fotocopia o cualquier otro sistema adecuado al tipo de fichero de que se trate.

Sólo se podrá acceder a la información pretendida si se trata de información sobre los datos personales del interesado y no sobre datos de terceros.

Derecho de rectificación

Es otro derecho reconocido por la LOPD, en su art. 16, a los ciudadanos a fin de que puedan defender su privacidad controlando por sí mismos el uso que se hace de sus datos personales, y en particular, el derecho a que éstos se modifiquen cuando resulten inexactos o incompletos.

Al igual que el anterior derecho, sólo podrá solicitarlo la persona interesada, quién deberá dirigirse a la empresa u organismo público que sabe o presume que tiene sus datos, indicando a qué datos se refiere y la corrección que se solicita, y aportando al efecto la documentación que lo justifique.

Derecho de cancelación

Este derecho recogido en el art. 16 apartado tercero de la LOPD permite a los ciudadanos defender su privacidad controlando por sí mismos el uso que se hace de sus datos personales, y en particular, el derecho a que éstos se supriman cuando resulten inadecuados o excesivos.

También se trata de un derecho personalísimo y el particular interesado deberá operar de la misma manera que con el derecho de rectificación, es decir, acudiendo a la empresa u organismo público que sabe o presume que tiene sus datos, indicando a qué datos se refiere, y aportando al efecto la documentación que lo justifique.

La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas, transcurrido el cual deberá procederse a la cancelación.

Derecho de oposición

Este derecho otorga al ciudadano la tutela para que no se lleve a cabo el tratamiento de sus datos personales o se cese en el mismo cuando no sea necesario su consentimiento para el tratamiento, por la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, y siempre que una Ley no disponga lo contrario.

Su ejercicio es personalísimo (regulado en el art. 17 de la LOPD), por lo que sólo podrá hacerlo la persona interesada mediante solicitud dirigida al responsable del tratamiento, en la que deberán hacerse constar los motivos fundados y legítimos que lo justifican.

4. Infracciones y sanciones.

Las infracciones y sanciones aparecen tipificadas a lo largo del Título VII de la LOPD. Importa destacar el art. 43, donde el legislador hace una diferencia entre los responsables de los ficheros de titularidad privada y los de titularidad pública. Así, los primeros se encuentran sujetos al régimen sancionador que aparece establecido en la LOPD, mientras que para los ficheros de titularidad pública el procedimiento y sanciones a los que se encuentran sujetos depende de lo establecido en los arts. 46 y 48 de la LOPD.

Las infracciones se clasifican en leves, graves y muy graves, siendo el art. 44 el encargado de remitir en un listado todas las infracciones contenidas en cada una de las tres categorías y las sanciones varían conforme sea la gravedad de la infracción.

5. La Agencia Española de Protección de Datos[46].

La LOPD regula en su Título VI la Agencia Española de Protección de Datos (en adelante AEPD) que sustituye al correspondiente Título de la LORTAD, con el que se adoptó en nuestro país el sistema de *Ombudsman*, al confiar la proteccion general de los datos personales a un órgano especial creado para garantizar los derechos y libertades de los ciudadanos. La AEPD "nace y existe para hacer efectivo el derecho a la autodeterminación informativa, libertad informática o derecho a la intimidad"[47]. Este modelo supone la importante ventaja de ofrecer un sistema de protección de carácter preventivo, antes de que se produzca lesión alguna en los derechos de las personas. Sin embargo, haciendo una comparación con el modelo americano, este último encomienda a los Tribunales ordinarios la tutela de estos derechos, exige que se haya producido un "daño o perjuicio imputable a la recogida y el uso indebido de los datos". PEREZ LUÑO[48] destaca las ventajas de una opción como ésta por "su función dinamizadora, adaptadora y de reciclaje de los derechos fundamentales", que realiza principalmente por medio de una serie de informes que estas autoridades han de presentar de manera periódica a los Parlamentos y señala además "su función orientadora de los ciudadanos, agilizando y clarificando los procedimientos de tutela de las libertades".

Tal y como nos indica GARRIGA DOMÍNGUEZ[49], podría pensarse que las funciones protectoras que lleva a cabo la AEPD respecto de los datos de carácter personal, y realmente se planteó así en un principio, fuesen asumidas por el Defensor del Pueblo. No obstante, si se hubiese adoptado esta postura, ¿qué sentido tendría la institución de la AEPD al ampliar el campo de actuación de las Administraciones Públicas a los sujetos privados? Tengamos en cuenta que la Constitución en su art. 54,

---

[46] http://www.agpd.es/

[47] LUCAS MURILLO DE LA CUEVA, "Las funciones de la Agencia de Protección de Datos" en *Jornadas sobre el Derecho Español de la Protección de Datos Personales*, Agencia de Protección de Datos, Madrid, 1996, p. 265.

[48] PÉREZ LUÑO, "Intimidad y protección de datos personales: del Habeas Corpus al Habeas Data", en GARCÍA SAN MIGUEL, *Estudios sobre el derecho a la intimidad*, Tecnos, Madrid, 1992, p. 43.

[49] GARRIGA DOMÍNGUEZ, *Tratamiento de datos personales…*ob., cit., p. 190.

le encomienda al Defensor del Pueblo la defensa de los derechos del Título I respecto de la actuación de la Administración Pública[50].

La Ley configura la AEPD como un ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada, que actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones. Entre las mismas, destaca una de carácter general: Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

Otras funciones serían: Velar por la publicidad en los tratamientos; Cooperación Internacional; Representación de España en los foros internacionales en la materia; Control y observancia de lo dispuesto en la Ley reguladora de la Función Estadística Pública y la elaboración de una Memoria Anual, presentada por conducto del Ministro de Justicia a las Cortes.

Si por algo se caracteriza la actuación de la AEPD en los últimos años es en lo referente al "Derecho al olvido" en Internet, intenso en la teoría y con poca fuerza en la práctica. Es sabido que el profundo desarrollo de Internet y el aumento de los usuarios en las redes sociales, han permitido que se produzca un acceso ilimitado, cesión, transmisión de todo tipo de datos, principalmente, de carácter personal. Todo ello, ha implicado el planteamiento sobre el tema de la validez y de la eficacia jurídica de la normativa europea en lo relativo a la protección de datos, pero al ciudadano de hoy en día no le interesa ver sus derechos plasmados en papel, sino que su intención es hacer uso de la protección que le ampara, es decir, ejercitar el derecho de supresión de sus datos en todo soporte y medio, sobre todo de carácter informático.

Al hilo de lo que venimos comentando, no podemos pasar por alto que nos encontramos en los albores del s. XXI y en menos de veinte años el empleo de Internet ha pasado de la era llamada "web 2.0." a la prominente "web 3.0.", viéndose la doctrina y legislación comprometida para afrontar los nuevos retos de la sociedad, pues es obvio que la actual legislación en materia de protección de datos quizás sirva para cubrir o

[50] En este sentido, PÉREZ LUÑO, *Derecho Humanos, Estado de Derecho y Constitución*, 8ª ed., Tecnos, Madrid, 2003, p.372.

atender las necesidades actuales, pero no aseguran una protección que a corto plazo implican los rápidos avances en las TICs[51].

> *"Mientras la Web 2.0. está gestionada por el propio usuario humano, la Web 3.0. gestionada en la nube o cloud computing y ejecutada desde cualquier dispositivo, constituye un nuevo tipo de Web en la que se añade contenido semántico a los documentos que la forman y ello conlleva que la ejecución de la misma sea realizada por maquinas que, basándose en nuestros perfiles en la Red, descubren información para nosotros"*[52]

Unido a lo dicho anteriormente, se encuentra el empleo de Internet para ejercer dos simples acciones: acceso a las redes sociales[53], un acceso cada vez más generalizado, y la ya mencionada nube o *cloud computing*[54]. Esto explica la preocupación por parte de la Comisión Europea en la citada Comunicación de 2010, donde advirtió la necesidad de un derecho al olvido, para mitigar los efectos negativos o perjudiciales que puedan conllevar las dos actividades mencionadas.

---

[51] En noviembre de 2010 la Comisión Europea a través de una Comunicación ha asegurado que la rapidez de la evolución tecnológica y la globalización han modificado profundamente nuestro medio y ha lanzado nuevos retos en materia de protección de datos personales. Véase la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre un enfoque global de la protección de los datos personales en la Unión Europea, de 4 de noviembre de 2010. COM (2010) 609 final.

[52] KÜSTER, -HERNÁNDEZ-, "De la Web 2.0 a la Web 3.0: antecedentes y consecuencias de la actitud e intención de uso de las redes sociales en la web semántica" en *Universia Business Review*, Primer trimestre 2013.

[53] El quinto estudio anual de redes sociales del IAB destaca que el 70% de los usuarios de redes sociales en Internet accedió a través de su teléfono móvil en 2013 (un 25% más que en el 2012). Además el estudio refleja que las redes sociales más utilizadas fueron Facebook (94% de uso) y YouTube (69%), seguidas de Twitter (49%) y la red social de Google, Google+ (41%). A la cola de la lista se sitúan Tuenti (22%), la red para buscar trabajo Linkedin (22%) o la plataforma para escuchar música Spotify (20%). En cuanto a conocimiento de redes sociales en general, el estudio subraya que son los jóvenes de entre 18 y 30 años los que más destacan. FUENTE: http://www.rtve.es/noticias/20140401/70-usuarios-redes-sociales-se-conecto-traves-del-movil-2013/908881.shtml.

[54] La AEPD nos facilita una definición del término *cloud computing*: también conocido como computación en nube. "Es una nueva forma de prestación de los servicios de tratamiento de la información, válida tanto para una empresa como pata un particular y, también, para la Administración Pública. Una solución *cloud computing* permite al usuario optimizar la asignación y el coste de los recursos asociados a sus necesidades de tratamiento de información. (…) En un entorno de *cloud computing* la gestión de la información esta de forma virtual en manos del cliente que contrata los servicios de la nube, que la trata a través de Internet accediendo a soluciones de bases de datos, correo electrónico, nominas o gestión de recursos humanos de acuerdo a sus necesidades. (…) El proveedor del servicio puede encontrase en, prácticamente, cualquier lugar del mundo y su objetivo último será proporcionar los servicios citados optimizando sus propios recursos a través de, por ejemplo, prácticas de deslocalización, compartición de recursos y movilidad o realizando subcontrataciones adicionales." *Guía para clientes que contraten servicios de Cloud Computing*.

En conclusión, los riesgos tecnológicos para la intimidad o la privacidad encuentran su punto de partida en las bases de datos, que unido al uso de las redes sociales y el *cloud computing* han producido el nacimiento de una nueva demanda, el derecho al olvido. No obstante, en qué consiste la misma. Empecemos dando un concepto: " es aquél derecho que tiene el titular de un dato a que éste sea borrado o bloqueado, cuando se produzcan determinadas circunstancias y, en particular, que no sea accesible a través de la red Internet"[55].

En definitiva, aquel interesado dispone de un derecho que ejercitándolo obliga al responsable del tratamiento de datos personales (los que conciernen al interesado) a suprimirlos, evitando así su posterior difusión. En este término, resulta de aplicación el art. 17 de la propuesta de Reglamento europeo[56], en lo que respecta a los datos personales proporcionados por el interesado siendo niño[57], cuando concurra alguna de las circunstancias siguientes:

a) Los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados;

b) el interesado retira el consentimiento en que se basa el tratamiento de conformidad con lo dispuesto en el artículo 6, apartado 1, letra a)[58], o ha expirado el plazo de conservación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos;

c) el interesado se opone al tratamiento de sus datos personales ejerciendo su derecho de oposición[59];

---

[55] DAVARA RODRÍGUEZ, "El derecho al olvido en Internet", *Diario La Ley, Sección Tribuna*, Nº 8137, LA LEY, 30 de julio de 2013, Año XXXIV.

[56] El artículo 17 establece el derecho del interesado al olvido y de supresión. *Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), COM (2012) 11 final*.

[57] En el art. 4 apartado18 del citado Reglamento se define la figura del niño como "toda persona menor de 18 años".

[58] El tratamiento de datos personales es lícito cuando el interesado ha dado su consentimiento para el tratamiento de sus datos personales para uno o más fines específicos.

[59] Artículo 19 del Reglamento europeo.

d) el tratamiento de datos no es conforme con el presente Reglamento por otros motivos.

Además la propuesta de Reglamento europeo[60] especifica el derecho de supresión[61] y establece las condiciones del derecho al olvido, incluida la obligación del responsable del tratamiento que haya difundido los datos personales de informar a los terceros sobre la solicitud del interesado de suprimir todos los enlaces a los datos personales, copias o réplicas de los mismos[62].

El régimen jurídico de la AEPD se regula con carácter general, como señalamos al principio de este apartado, en el Título VI de la LOPD y de modo supletorio por la Ley 6/97 de 14 de abril de Organización y Funcionamiento de la Administración General del Estado (Disposición Adicional 10ª). Y como todo ente público el ejercicio de sus competencias se regula a través de la Ley 30/92, de 26 de noviembre del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

III. Medidas penales de protección.

1. Introducción.

Antes de analizar cómo se configuran en nuestro Código Penal los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, es preciso

---

[60] Para entender la propuesta del Reglamento, véase STJUE 13 de mayo de 2014, as. C-131/12, *Google Spain, S.L. y Google Inc. vs. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González*.

[61] Artículo 12 letra b), Directiva del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[62] Sin embargo, la publicación en una página web de datos personales no supone ninguna dificultad para aplicar la Directiva europea sobre protección de datos, pues traigamos a colación lo que el Tribunal de Justicia de la Unión Europea señaló en la sentencia del caso Lindqvist. En concreto, en el párrafo primero de la parte dispositiva establece el Tribunal que "La conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales» en el sentido del artículo 3, apartado 1, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos". *Sentencia de 6 de noviembre de 2003 (Petición de decisión prejudicial planteada por el Göta hovrätt): Bodil Lindqvist (C-101/01, Rec. p. I-12971).*

tener en cuenta dos de los principios básicos o pilares del Derecho Penal en un Estado social y democrático de Derecho como el nuestro: la función de prevención y el principio de intervención mínima o *ultima ratio*.

En primer lugar, el Derecho Penal se caracteriza por tener una función preventiva, que es el *modus operandi* que la norma penal tiene para cumplir su función de protección[63]. Así pues, en un Estado moderno el Derecho penal tiene que encontrarse respaldado por un consenso de la sociedad y es por ello que la prevención no puede alcanzarse a través de la intimidación[64], como una amenaza de la pena para aquellos que realizan la conducta ilícita, sino que ha de crear en la conciencia de la sociedad un sentimiento o pensamiento acorde a los valores que la guían.

Por otro lado, la función del Derecho en general (no sólo del Derecho Penal) es la tutela de los bienes jurídicos con la finalidad de alcanzar una convivencia social pacífica. Para que esto sea posible, los distintos sectores del ordenamiento jurídico disponen de diversos medios de reacción[65]: por ejemplo, las sanciones civiles en el Derecho privado; las fiscales, disciplinarias y gubernativas en el Derecho Administrativo y, en último lugar, las sanciones punitivas en el Derecho Penal. Son estas últimas las que tienen un carácter drástico y de gran dureza para la sociedad, pues afecta a bienes imprescindibles como la libertad (sin olvidar el nada desdeñable "efecto estigmatizador", que distingue la reacción penal de cualquier otra). Esto explica por qué el Derecho Penal sólo debiera operar cuando resulte imprescindible.

De esta forma, llegamos al principio de intervención mínima, que SAINZ CANTERO[66] entiende en una triple dimensión: El Derecho Penal debe aparecer como la "*ultima ratio*", debe de encontrarse en último lugar, y entrar en juego únicamente cuando resulten insuficientes o inservibles para el mencionado cometido otros medios de reacción y tutela menos gravosos.

---

[63] MORILLAS CUEVA, *Curso de Derecho Penal Español. Parte General*, Madrid, 1996.

[64] MIR PUIG, *Función de la pena y teoría del delito en el Estado Social y Democrático de Derecho*, BOSCH, Casa Editorial S.A., Barcelona, 1982, p. 30.

[65] GARCÍA-PABLOS DE MOLINA, "Reflexiones sobre el actual saber jurídico-penal y criminológico", en *Revista de Legislación y Jurisprudencia*, agosto de 1981.

[66] SAINZ CANTERO, *Lecciones de Derecho penal, Parte general*, Barcelona, 1980, 1982 y 1985.

En segundo lugar, sólo protegerá los bienes jurídicos más fundamentales para el individuo y para la sociedad, tutelándolos contra los ataques más intensos, más intolerables: y, por último, para la sanción de tales hechos, se ha de optar por las penas que, sin dejar de ser adecuadas, resulten menos onerosas.

Por tanto, su significado se ajusta a que el Derecho Penal sólo debe intervenir en aquellos ataques que se caractericen por ser muy graves contra bienes jurídicos. Ello lleva a una parte de la doctrina a aludir a la "subsidiariedad" del Derecho Penal. Sin embargo, autores como MUÑOZ CONDE[67] discrepan al respecto por considerar que el término subsidiariedad "(…) no es más que una de las consecuencias que se derivan del principio de intervención mínima". Con todo, más allá de matices, advertido nuestro punto de partida, debemos mantener que, en la parcela que nos ocupa, sólo acudiríamos a la vía penal una vez que el ataque a la privacidad ha sido demasiado grave y no hay norma extrapenal capaz de tutelar satisfactoriamente dicho bien.

Dentro del ámbito nacional, el legislador ha optado por regular los "ciberdelitos" contra la intimidad, privacidad y el honor dentro del texto del Código Penal, evitando así una Ley penal especial[68] (a nuestro entender con acierto, por razones de seguridad jurídica fundamentalmente)

Cabe destacar que ni el Código Penal de 1995 ni sus sucesivas reformas (hasta la operada por la Ley Orgánica 5/2010, de 22 de junio, en adelante CP) incluían referencia alguna a los eventuales ataques que afectasen a los datos informatizados de carácter personal, a pesar de recoger otras previsiones en materia de criminalidad informática (v.gr. el concepto de documento electrónico, a los efectos de las falsedades; la estafa mediante manipulación informática, espionaje informático contra valores de contenido económico empresarial, daños y sabotaje informático…). Tampoco aludían a una norma común que facilitare el tratamiento y la sanción; sin embargo, como bien afirma MESTRE DELGADO[69], el empleo de las TICs para realizar actos delictivos es un

---

[67] MUÑOZ CONDE, *Introducción al Derecho penal*, BdeF, Montevideo-Buenos Aires, 2001, p. 107

[68] MOISÉS BARRIO, "Los delitos cometidos en internet. Marco comparado, internacional y derecho español tras la reforma penal de 2010" *La Ley Penal, Sección Legislación aplicada a la práctica*, Nº 86, LA Ley, Octubre 2011.

[69] MESTRE DELGADO, "Reformas legales contra el cibercrimen", *La Ley Penal, Sección Editorial*, Nº 105, LA LEY, 2013.

nuevo y grave reto al que ha de hacer frente nuestro Derecho Penal, pues no podemos olvidar que la delincuencia informática va superando constantemente toda revisión o actualización que se realice sobre el Código Penal y sobre la Ley de Enjuiciamiento Criminal. No deja de llamar la atención que no fuera aprovechado por el legislador español el momento inmejorable de la gran reforma penal que cuajó en 1995 para actualizar y modernizar las diversas manifestaciones de la criminalidad informática, incluyendo la que aquí nos ocupa: los atentados contra la intimidad.[70] La consecuencia de perder esa oportunidad la estamos viviendo con las sucesivas reformas que se han llevado a cabo desde entonces, reformas en las que, acaso de forma precipitada, se adicionan nuevas figuras en el ámbito que examinamos. Un claro ejemplo lo hallamos en el art. 197 CP, del que nos ocuparemos a continuación.

2. Previsiones del CP de 1995 en materia de privacidad y aportaciones de la reforma de 2010.

El CP de 1995 en el Título X del Libro II regulaba los "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio" de la siguiente manera:

El art. 197 "Del descubrimiento y revelación de secretos", equipara los mensajes electrónicos con el concepto de documento[71]: así en su apartado primero se establece que "El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento se apodere de papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos papeles, cartas personales o intercepte sus telecomunicaciones (…) será castigado con la pena de prisión de uno a cuatro años y multa de doce a veinticuatro meses".

La pena aumentaría (prisión de dos a cinco años) "si se difunden, revelan o ceden a terceros los datos o hechos descubiertos" o las imágenes captadas a las que se refieren los dos apartados anteriores. El apartado tercero concluye aplicando la misma pena de prisión de dos a cinco años a aquel que teniendo conocimiento del origen ilícito

---

[70] GUTIÉRREZ FRANCÉS, *Fraude informático y estafa*, op. cit., pp. 599 ss.

[71] ÁLVAREZ-CIENFUEGOS SOTO, "Informática y Derecho penal. Los delitos relativos a la informática" en *El Código Penal de 1995: Parte Especial*, 1ª ed., Consejo General del Poder Judicial, Catalunya, 1996, p. 202.

realizare las conductas descritas en el apartado segundo, sin necesidad de que participara en su descubrimiento.

El cuarto y último apartado del art. 197 regulaba la imposición de la pena de prisión de tres a cinco años a las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros[72] que realizasen las conductas descritas en los apartados primero y segundo del precepto objeto de análisis.

Las circunstancias agravantes del tipo que preveía el CP de 1995 se concentraban en dos conductas:

a) "Cuando los hechos descritos afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o incapaz"[73].

b) Que los hechos ilícitos o conductas típicas se realicen con fines lucrativos.

El art. 198, por lo demás, agrava la sanción "Cuando el autor tenga la condición de funcionario público" y actúe fuera de los casos permitidos por la Ley y sin mediar causa por delito.

Con la reforma operada por Ley Orgánica 5/2010, de 22 de junio, al art. 197 se le incorpora un tercer párrafo: "El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años".

Atendiendo a la lectura de un precepto tan amplio y farragoso,[74] de discutible técnica legislativa según se ha reiterado por la doctrina penal, cabe preguntarse por el

---

[72] Podemos observar como el CP de 1995 equipara los ficheros y soportes informáticos con los archivos y registros tradicionales.

[73] En este caso, se trata de datos especialmente protegidos por la antigua LORTAD y por la actual LOPD, cuyo tratamiento informático requiere un consentimiento expreso del afectado.

alcance de la protección que otorga y, a continuación, por el sentido de la nueva redacción del texto. Con carácter general, aunque de forma sintética, podemos reseñar:

- A pesar de la rúbrica del Título ("Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio"), y a pesar del anticuado encabezamiento del Capítulo en que se inserta ("Del descubrimiento y revelación de secretos"), consideramos inexactas las referencias al bien jurídico (primero) y a la modalidad de conducta y objeto material (el segundo). Como hemos reflejado a lo largo de esta exposición, al aludir a la intimidad y a la propia imagen como objeto de protección, el legislador se queda corto, porque lo que está en juego supera ampliamente el contenido de la intimidad y propia imagen. Es más, si añadimos la segunda rúbrica relativa a la modalidad de conducta y el objeto material, en puridad restringiríamos incomprensiblemente la potencialidad del precepto. (No olvidemos la función exegética del bien jurídico ni la restricción que implicaría interpretar que sólo se protege en esta sede lo que tiene carácter "desconocido por la generalidad"). Cuando hablamos de "privacidad", justamente lo hacemos para superar las lagunas del planteamiento y redacción tradicional, obsoletos en gran medida por el impacto de las TICs.

- De partida, parece que estamos ante un bien jurídico de carácter personalísimo (por ello mismo disponible, en el sentido ya examinado; esta idea se completa con la exigencia de denuncia por parte del agraviado o representante legal, salvo el caso de menores, incapaces y personas desvalidas, donde puede suplir la denuncia la actuación del Ministerio Fiscal)[75]. No obstante, esta percepción inicial respecto a la titularidad del bien jurídico, desaparece cuando se analiza el art. 200, que hace referencia a los datos reservados de personas jurídicas[76].

---

[74] CARRASCO ANDRINO, "Descubrimiento y revelación de secretos", *Derecho Penal Español. Parte Especial (I)*, 2ª ed. aumentada y corregida conforme a la LO 5/2010, Dir. Álvarez García, Tirant lo Blanch, Valencia, 2011, pp. 755 ss.

[75] En el art. 201 también se incluyen como excepciones a la exigencia de denuncia por el agraviado, por una parte, cuando afecta a intereses generales o a una pluralidad de personas, y por último, cuando es el autor un funcionario fuera de los casos permitidos por la ley y sin mediar causa por delito, del art. 198.

[76] Sobre las diversas interpretaciones, vid, CARRASCO ANDRINO, ult. cit.

- Sin ahondar en críticas conocidas sobre el juego de agravaciones confusas y superpuestas que incluye el texto (en absoluto coordinadas con las previsiones y términos que emplea la LOPD), aún quisiéramos señalar la inquietante equiparación de penas para conductas que no son igualmente disvaliosas, poniendo en peligro el principio de proporcionalidad. No puede ser lo mismo lesionar la intimidad/privacidad que ponerla en peligro).

- En esta regulación, consecuencia del principio de *ultima ratio*, sólo se castigan conductas dolosas, restricción que no aparece en la LOPD.

La reforma de 2010 del CP, por su parte, al introducir el citado párrafo tercero, ha planteado más problemas de los que ha resuelto. En un afán por seguir lo previsto en el Convenio sobre Ciberdelincuencia, el legislador pretende castigar las conductas de "mero hacking". Sin embargo, es más que discutible que tales conductas no estuvieran ya comprendidas en el párrafo anterior, con lo cual resultaría redundante y, peor aún, castigado con pena inferior. Por lo demás, la configuración autónoma como delito del hacking o mero intrusismo, es una cuestión bastante polémica, por posible atentado contra los principios de lesividad y *ultima ratio*[77].

Estas breves pinceladas sobre las figuras específicas del Código Penal para la protección de la privacidad frente a las amenazas derivadas del uso abusivo de las TICs, aún debieran completarse con otros tipos penales con los que eventualmente pudieran entrar en concurso: nos referimos al art. 256 (que castiga a quien hiciere uso de un equipo terminal de telecomunicación sin consentimiento ocasionando un perjuicio superior a 400 euros) y el art. 264 (donde se castigan los daños informáticos, incluyendo borrado o destrucción de datos y programas, siempre que ocasione un resultado grave). No obstante, la incardinación sistemática de estos preceptos entre los delitos contra el patrimonio, impedirá su aplicación cuando no se produzca una disminución patrimonial constatable, lo cual no es fácil que se dé, o se pueda probar, en los atentados contra la privacidad.

[77] MATELLANES RODRÍGUEZ, "La tutela de la intimidad en el Código Penal" en *Revista Penal*, Nº 23, LA LEY, enero de 2009, p. 60.

3. Reflexiones sobre el alcance del fenómeno informático en el Derecho penal internacional.

Como ya afirmara GALÁN MUÑOZ[78], el fenómeno informático representa uno de los mayores retos a los que se enfrenta no sólo el Derecho Penal español, sino el de todos los países industrializados. Ningún país ni individuo escapa a los peligros que genera el uso amplio y masivo de los sistemas informáticos y ello muestra la necesidad que tiene el Derecho Penal de la colaboración internacional para hacer frente a los retos planteados por la "Sociedad de Riesgo Mundial," haciendo nuestras las palabras de BECK[79]. Esta colaboración ya se puso en marcha hace medio siglo y ha sido decisiva para que aquellos países industrializados, que se ven afectados por la problemática, hayan adaptado sus legislaciones y llevado a cabo reformas legislativas que den una respuesta y afronten de modo similar un problema global. Sin embargo, ni la colaboración internacional a través de propuestas referidas a la represión y persecución de la criminalidad informática, ni ninguna de las últimas reformas legislativas nacionales relativas a la materia, han conseguido acabar con la enorme inseguridad jurídica imperante en la investigación penal en Internet[80].

Uno de los motivos[81] que puede explicar este fracaso lo situaríamos en los organismos que impulsan la creación de los instrumentos internacionales, que tienden a adoptar una política de máximos en cuanto a la cesión de garantías del ciudadano frente a los poderes públicos, con la finalidad de exterminar cualquier laguna de punibilidad y también con el objetivo de contar con el apoyo y ratificación del mayor número posible de Estados para sus instrumentos. Sin embargo, tal y como afirma MORALES

---

[78] GALÁN MUÑOZ, "La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales" en *Revista Penal*, Nº 24, LA LEY, (julio 2009), p. 105.

[79] BECK, *¿Qué es la globalización?*, Paidós, Barcelona, 2008, pp. 87 y ss. y 190 y ss.

[80] En la actualidad, la prensa a nivel nacional e internacional se ve inundada de noticias referentes al "Derecho al olvido" en Internet y el pronunciamiento del Tribunal de Justicia de la Unión Europea en su sentencia de 13 de mayo de 2014 reconociendo este derecho.

[81] SILVA SÁNCHEZ, "Los principios inspiradores de las propuestas de un Derecho penal europeo. Una aproximación crítica" citado por GALÁN MUÑOZ, "La internacionalización de la represión…", ob., cit., p. 107.

GARCÍA[82], con respecto a la Convención europea sobre Cyber-crime del Consejo de Europa, a día de hoy no se puede discutir que en el ámbito del Derecho Penal internacional, el binomio prevención-represión está resultando vencedor en comparación al binomio garantías-libertades.

CONCLUSIONES

1º El desarrollo de las TICs, unido a su creciente masificación en el mundo actual, han generado un estado de "dependencia tecnológica" que nos reporta múltiples ventajas (acceso instantáneo a toda clase de información, comunicación ágil, fácil y barata con cualquier rincón del mundo, o la realización de toda clase de actividades y prestación de todo tipo de servicios. Sin embargo, no se ha logrado evitar el "lado oscuro" del desarrollo tecnológico, las actuaciones abusivas y maliciosas que aprovechan el alto grado de vulnerabilidad que los sistemas informáticos y la información almacenada, tratada y comunicada por ellos. Uno de los ámbitos más severamente afectados por esta actividad criminal es el que incide en los bienes y derechos más personalísimos del individuo, que en estas páginas hemos denominado "privacidad".

2º Tras constatar la existencia de este nuevo interés social valioso para los miembros de las sociedades modernas, hemos procurado delimitar su contenido, tomando con primera y esencial referencia la Carta Magna y la interpretación que doctrina y jurisprudencia hacen de ella (sin olvidar las normas de carácter internacional, especialmente emanadas de las instituciones europeas). En este punto, hemos concluido que el bien personalísimo privacidad, lejos de coincidir con el derecho clásico a la intimidad, supera y desborda el mismo, configurándose como un compendio de derechos y libertes derivadas de la dignidad de la persona, y que incluye la libertad, el derecho al libre desarrollo de la personalidad, la intimidad personal y familiar, el honor y la libertad informática.

3º Hemos procurado identificar los principales riesgos que amenazan la privacidad personal como consecuencia del uso abusivo de las posibilidades que ofrecen

---

[82] MORALES GARCÍA, "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la convención europea sobre Cyber-crime" en *Delincuencia informática. Problemas de responsabilidad, Cuadernos de Derecho Judicial IX*, 2002, pp. 18 y ss.

las TICs, llegando a la conclusión siguiente: como ha puesto de relieve recientemente el Tribunal Superior de Justicia de la Unión Europea, aunque los ciudadanos llegáramos a ser conscientes -en parte- de los datos que constan de nosotros en la Red, sin embargo, nunca podríamos imaginar hasta qué punto son empleados esos datos y menos aún con qué fines. Estamos expuestos, no sólo ante sujetos privados y empresas que almacenan, compran, venden, manipulan y tratan informáticamente todo tipo de datos de carácter personal, sino también ante instituciones y organismos nacionales e internacionales. Desde los mismos se controla, espía y manipula al ciudadano sin que pueda llegar a percatarse.

4º Tras un rápido recorrido por la medidas de prevención aconsejadas para minimizar –que no evitar- los atentados contra la privacidad personal, se han sometido a examen los mecanismos jurídicos de que dispone el ordenamiento español específicamente para la protección de los datos de carácter personal. A tal efecto, nos hemos centrado en la LOPD, primero, y en las previsiones del CP después. Nuestra percepción global es que este cuadro normativo adolece de cierta falta de coherencia, acaso por actuar el legislador con precipitación, "a impulsos" de las indicaciones que se realizan desde la esfera internacional. A la vista de las sucesivas reformas que han afectado a esta materia, también pudiera intuirse que ha preocupado más el dar una respuesta rápida para apaciguar las demandas de la población, que se siente indefensa frente a Internet. Valoramos, en cualquier caso, la labor que se está desarrollando desde la AEPD, especialmente por la agilidad de su actuación y por su incidencia en la concienciación de los ciudadanos.

5º Debemos poner fin a estas líneas valorando positivamente la modernización de nuestra legislación en este ámbito de la criminalidad, colocándonos en la línea de los países de nuestro entorno. Sin embargo, a continuación hemos de reflejar nuevamente nuestro escepticismo acerca de la eficacia de la misma. Las dificultades de detección, prueba y persecución de estos hechos, sobre todo cuando tienen lugar en el espacio virtual, hacen sospechar que las medidas jurídicas señaladas sólo van a ser de aplicación a un grupo muy reducido de supuestos, y ni siquiera a los más graves. Urge educar a la sociedad, jóvenes y no tan jóvenes, para quedar desnudo, "a la intemperie" en la Red.

BIBLIOGRAFÍA

ÁLVAREZ-CIENFUEGOS SOTO, "Informática y Derecho penal. Los delitos relativos a la informática" en *El Código Penal de 1995: Parte Especial*, 1ª ed., Consejo General del Poder Judicial, Catalunya, 1996.

AMÍN, *El capitalismo en la era de la globalización*, Paidós, Barcelona, 1999.

BECK, *¿Qué es la globalización?*, Paidós, Barcelona, 2008.

CARRASCO ANDRINO, "Descubrimiento y revelación de secretos", en *Derecho Penal Español. Parte Especial, (I)*, 2ª ed. Dir. Alvarez García, Tirant lo Blanch, Valencia, 2011.

CARRILLO, "Derecho a la información y veracidad informativa", en *Revista española de derecho constitucional*, Nº 23, 1988.

DAVARA RODRÍGUEZ, "El derecho al olvido en Internet", *Diario La Ley, Sección Tribuna*, Nº 8137, LA LEY, 30 de julio de 2013.

DOMINGO, *¿Conflictos entre derechos fundamentales?: un análisis desde las relaciones entre los derechos a la libre expresión e información y los derechos al honor y la intimidad*, Centro de Estudios Políticos y Constitucionales, Madrid, 2001.

GALÁN MUÑOZ, "La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales" en *Revista Penal*, Nº 24, LA LEY, julio de 2009.

GARCÍA-PABLOS DE MOLINA, "Reflexiones sobre el actual saber jurídico-penal y criminológico", en *Revista de Legislación y Jurisprudencia*, agosto de 1981.

GARCÍA RIVAS, *El poder punitivo en el Estado democrático*, Ediciones de la Universidad de Castilla-La Mancha, Cuenca, 1996.

GARRIGA DOMÍNGUEZ, *Tratamiento de datos personales y derechos fundamentales*, 2ª ed., Dykinson S.L., Madrid, 2009

GUTIÉRREZ FRANCÉS, *Fraude informático y estafa*, Ministerio de Justicia, Madrid, 1991.

GUTIÉRREZ FRANCÉS, "La privacidad en el espacio virtual (riesgos y cauces de protección)" en *Cuaderno Red de Cátedras Telefónica*, Septiembre, 2011.

HERNÁNDEZ RAMOS, "El derecho al olvido digital en la Web 2.0" en *Cuaderno Red de Cátedras Telefónica*, Mayo 2013.

HORMAZÁBAL MALARÉE, *Bien jurídico y Estado social y democrático de Derecho*, 1ª ed., PPU, Barcelona, 1991.

KÜSTER, -HERNÁNDEZ, "De la Web 2.0 a la Web 3.0: antecedentes y consecuencias de la actitud e intención de uso de las redes sociales en la web semántica" en *Universia Business Review*, Primer trimestre 2013.

LUCAS MURILLO DE LA CUEVA, "Las funciones de la Agencia de Protección de Datos" en *Jornadas sobre el Derecho Español de la Protección de Datos Personales*, Agencia de Protección de Datos, Madrid, 1996.

MATELLANES RODRÍGUEZ, "La criminalidad informática como manifestación del fenómeno de la globalización" en *Revista Penal*, Nº 22, LA LEY, julio de 2008.

MATELLANES RODRÍGUEZ, "La tutela de la intimidad en el Código Penal" en *Revista Penal*, Nº 23, LA LEY, enero de 2009.

MESTRE DELGADO, "Reformas legales contra el cibercrimen", *La Ley Penal, Sección Editorial*, Nº 105, LA LEY, 2013.

MIR PUIG, *Función de la pena y teoría del delito en el Estado Social y Democrático de Derecho*, BOSCH, Casa Editorial S.A., Barcelona, 1982.

MOISÉS BARRIO, "Los delitos cometidos en internet. Marco comparado, internacional y derecho español tras la reforma penal de 2010" *La Ley Penal, Sección Legislación aplicada a la práctica*, Nº 86, LA Ley, Octubre 2011.

MORALES GARCÍA, "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la convención europea sobre Cyber-crime" en *Delincuencia informática. Problemas de responsabilidad, Cuadernos de Derecho Judicial IX*, 2002.

MORALES PRATS, *La tutela penal de la intimidad: privacy e informática*, "Prólogo" de QUINTERO OLIVARES, 1ª ed., Ediciones Destino S.A., Barcelona, 1984.

MORILLAS CUEVA, *Curso de Derecho Penal Español. Parte General*, Madrid, 1996.

MUÑOZ CONDE, *Introducción al Derecho penal*, BdeF, Montevideo-Buenos Aires, 2001.

NAVARRO LÓPEZ, *Bienestar insuficiente, democracia incompleta: sobre lo que no se habla en nuestro país*, Anagrama, Barcelona, 2003.

PÉREZ LUÑO, "Las generaciones de derechos fundamentales" en *Revista del Centro de Estudios Constitucionales*, Nº 10 (Septiembre - Diciembre 1991).

PÉREZ LUÑO, *Nuevas tecnologías, sociedad y derecho. El impacto socio-jurídico de las N.T. de la información*, FUNDESCO, Madrid, 1987.

PÉREZ LUÑO, "Intimidad y protección de datos personales: del Habeas Corpus al Habeas Data", en GARCÍA SAN MIGUEL, *Estudios sobre el derecho a la intimidad*, Tecnos, Madrid, 1992.

PÉREZ LUÑO, *Derecho Humanos, Estado de Derecho y Constitución*, 8ª ed., Tecnos, Madrid, 2003.

ROMEO CASABONA, *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Comares, Granada, 2006.

SAINZ CANTERO, *Lecciones de Derecho penal, Parte general*, Barcelona, 1980, 1982 y 1985.

SANTOS GARCÍA, *Nociones generales de la Ley Orgánica de Protección de Datos y su Reglamento*, 2ª ed., Tecnos (Grupo Anaya, S.A.), Madrid, 2012.

SIEBER, "Criminalidad informática: Peligro y prevención", en *Delincuencia Informática*, Mir Puig (Comp.), PPU, Barcelona, 1992.

VON LISZT, *Tratado de Derecho penal*, trad. de la 20ªed. alemana por Luis Jiménez de Asúa, adicionado con el Derecho penal español por Quintilliano Saldaña, t. II, 4ª ed., Reno, Madrid, 1999.

ZAFFARONI, –ALAGIA–SLOKAR, *Derecho penal. Parte general*, 2ª ed., Ediar, Buenos Aires, 2002.

ENLACES WEB

Agencia Española de Protección de Datos: http://www.agpd.es/portalwebAGPD/index-ides-idphp.php

Inteco–LOPD:
http://www.inteco.es/Formacion/Legislacion/Ley_Organiza_de_Proteccion_de_Datos/

Parlamento Europeo – Protección de datos: http://www.europarl.europa.eu/news/es/top-stories/content/20130901TST18405/html/Protecci%C3%B3n-de-datos

RECURSOS WEB

http://sociedad.elpais.com/sociedad/2013/03/17/actualidad/1363555505_736818.html

http://europa.eu/legislation_summaries/information_society/data_protection/l14012_es.htm

http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2000-0000_Consentimiento-otorgado-por-menores-de-edad.pdf

http://www.rtve.es/noticias/20140401/70-usuarios-redes-sociales-se-conecto-traves-del-movil-2013/908881.shtml

http://www.eprivacidad.es/

JURISPRUDENCIA CITADA Y CONSULTADA

Sentencias del Tribunal Constitucional: 115/2000, de 5 de mayo; 6/1988, de 21 de enero; 240/1992, de 21 de diciembre; 47/2002, de 25 de febrero; 75/2002, de 8 de abril; 101/2003, de 2 de junio; 185/2002, de 14 de octubre.

Sentencias del Tribunal de Justicia de la Unión Europea:

- STJUE 6 de noviembre de 2003, as. C-101/01, *Petición de decisión prejudicial planteada por el Göta hovrätt): Bodil Lindqvist*.
- STJUE 13 de mayo de 2014, as. C-131/12, *Google Spain, S.L. y Google Inc. vs. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González*.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Resolución R/00397/2003, de 11 agosto. Procedimiento PS/27/2003. [Tratamiento de datos de salud sin consentimiento]

Resolución de 30-12-2009. Expediente E/01154/2009. [Cesión de datos de salud a Juzgado de Instrucción]