Seguridad

Cuaderno Red de Cátedras Telefónica

Universidad de Salamanca

La privacidad en el espacio virtual (riesgos y cauces de protección)

Cátedra Telefónica de la Universidad de Salamanca

La creciente información de todo tipo de empresas y actividades, el acceso masivo a Internet y el uso abusivo de las Redes Sociales, están convirtiendo al hombre actual en el "ciudadano transparente", controlado y controlable, un ser "a la intemperie" en la Red, con su libertad individual, su privacidad y su dignidad seriamente comprometidas: otro grave riesgo, del que apenas somos conscientes, de la "era digital". A continuación se propone una reflexión sobre este riesgo y sobre sus cauces de protección.

Mariluz Gutiérrez Francés

Septiembre 2011

www.catedras.telefonica.es
http://catedraseguridad.usal.es

Telefónica

Mariluz Gutiérrez Francés

Es Profesora Titular de Derecho Penal de la Universidad de Salamanca, donde se licenció con Premio Extraordinario de Licenciatura y Premio D. Teodoro Andrés Marcos en 1985, y donde obtuvo en 1990, también con Premio Extraordinario, el título de Doctor, como discípula de Dr. D. Ignacio Berdugo Gómez de la Torre. Su actividad docente se ha desarrollado en la Facultad de Derecho de la Universidad de Salamanca (en la que se le otorgó por el alumnado, en el Curso Académico 2005-2006, el Premio a la mejor trayectoria docente) y, durante trece años, en el Centro de Formación de la Policía Nacional en Ávila (habiendo sido reconocida su labor con la concesión de la Medalla al Mérito Policial). Su tarea investigadora, parcialmente desarrollada en la Universidad de Houston y en la Universidad de Georgetown (EE.UU), se ha dirigido, básicamente, hacia las nuevas formas de la criminalidad defraudatoria, destacando su libro *Fraude informático y estafa* (1991), entre otras muchas publicaciones sobre otras dimensiones de la llamada *Criminalidad informática*. En relación con dicha materia, ha participado en diversos Proyectos de Investigación de carácter internacional y ha colaborado en la Comisión de Expertos para la armonización legislativa en el ámbito de la Unión Europea, participando asiduamente en numerosos Cursos de Doctorado y Postgrados en Colombia, Venezuela, Bolivia y Argentina, e impartiendo Conferencias dentro y fuera de nuestras fronteras.

Índice

Issn: 2174-7628

1. Introducción

> ***Nota de prensa: "Una pequeña compañía estadounidense ha creado el servicio gratuito para detectar los elementos "comprometedores" de Facebook –fotos, textos inapropiados, etc.- y limpiar perfiles en la Red. Se responde así a la demanda social creciente en el momento en que, cada vez más, las empresas rastrean en Internet, especialmente en las redes sociales, para investigar a los candidatos antes de ocupar un puesto de trabajo". A través del sitio Reppler.com, se puede obtener el propio perfil y, en cuestión de minutos, ofrece un informe con cuatro puntos: la impresión que se da con ese perfil, los contenidos aceptables, la información y los riesgos de seguridad y privacidad"***

Esta noticia, publicada hace sólo un mes en España, sorprendentemente, ha pasado casi inadvertida entre nosotros, inconscientes, una vez más, de la realidad que nos implica de modo incuestionable en el presente, sobre todo a nuestros jóvenes, y de cuyos efectos futuros no sabemos todavía suficiente: La realidad del *ciudadano transparente* del siglo XXI, el *ciudadano a la intemperie* en la Red. Lo vemos mejor desde un ejemplo:

> El joven A.A., de 27 años, licenciado en Derecho y Económicas, con un Máster en una Universidad de prestigio en los Estados Unidos, presenta su curriculum en la multinacional B.B para ocupar un cargo de cierta responsabilidad. Superadas por A.A sucesivas cribas, gracias a su brillante trayectoria académica, la multinacional procede a recabar de la empresa R.R el perfil del candidato en Internet.
>
> La empresa R.R., especializada en Seguridad informática, también, aunque de modo encubierto, desarrolla actividades de información y asesoramiento a los clientes. Recopila las "pistas" que los ciudadanos van dejando de sí mismos durante años en la Red: además de la información que aporta conscientemente en su perfil (datos personales, fotos familiares, gustos, fiestas, noches "locas", aficiones, viajes, opiniones sobre temas de toda índole, comentarios sobre jefes, profesores, políticos, compañeros de trabajo...), otros muchos datos que deja de modo inconsciente (la valiosa información que existe sobre él en su Colegio, su Universidad, los archivos informatizados de la Seguridad Social o Tráfico, y la que deja, por ejemplo, cuando se integra en un grupo, participa en chats, opina en foros, selecciona noticias o accede a periódicos digitales y páginas web, cuando se interesa por temas, actividades, negocios o mensajes publicitarios, efectúa consultas o compras, o cuando realiza una suscripción o selecciona una determinada emisora de radio...), sin olvidar las aportaciones que colegas, familiares y amigos hacen al conjunto. En suma, nuestro joven aspirante, a golpe de tecla, en unos instantes, sin saberlo, tiene actualizada ("activada") toda su

> historia, su trayectoria personal, familiar y profesional (sin derecho al olvido, a rectificar, a evolucionar), y se ha convertido en ese "ciudadano transparente", "a la intemperie", al que antes nos referíamos. La multinacional sabrá con exactitud la clase de persona que, en caso de hacerlo, incorpora a la empresa (más o menos sana, leal, sincera, impulsiva, con capacidad de liderazgo, generosa, crítica, conflictiva o resentida...) Conocerá, incluso antes que él, sus reacciones y forma de actuar ante cada eventualidad, propuesta, sugerencia u orden en el futuro, y, lo más grave, tendrá mayor y mejor capacidad para controlarlo y manipularlo. Todas esas posibilidades se las reporta ahora Internet.

Este ejemplo no es un caso de laboratorio, mera ciencia ficción, aunque en España se aprecia una falta absoluta de sensibilidad en torno al tema, especialmente en nuestros jóvenes. Con todo, nos parece un dato significativo que en el último Informe anual de la Agencia Española de Protección de Datos (AEPD) haya aumentado exponencialmente el número de denuncias vinculadas a lo que se conoce como *"derecho al olvido en Internet"*, porque es una prueba evidente de que los ciudadanos empiezan a sentir las consecuencias negativas de noticias, datos e informaciones que sobre ellos circulan en la Red. En otros países, como los Estados Unidos, existe una creciente inquietud por la percepción que el mundo pueda tener de uno mismo, actualmente y en el futuro. Y esa preocupación por la seguridad, la privacidad y el impacto futuro de los contenidos en la Red, está impulsando la adopción de medidas, unas veces preventivas, otras reparadoras, como la creación del servicio referido al principio: un servicio para limpiar perfiles en Internet.

En las próximas líneas nos proponemos traer algunas observaciones sobre los riesgos del uso masivo de Internet, especialmente, aunque no sólo, de las Redes sociales, en los derechos y libertades fundamentales del hombre moderno, con el objetivo de favorecer una toma de conciencia acerca de dichos riesgos, revisar las vías con que cuenta el ciudadano para protegerse frente a los mismos y, en último término, abrir cauces para la reflexión.

2. Un poco de historia: el "caso Publi-Gest"

Conviene remontarse hasta hace un par de décadas. Quizá todavía algunos recuerden un caso que a mediados de 1991 ocupó la primera plana de telediarios y demás medios de comunicación, provocando gran asombro y extraordinario impacto en nuestro país. Me refiero al llamado "caso PUBLI-GEST", el primer supuesto de tráfico de datos personales de que se tenemos noticia en España. Pese a la alarma creada, el asunto nuclear del tráfico de datos terminó con un Auto de sobreseimiento de la Audiencia Provincial de Madrid, de 14 de abril de 1993, Auto que ratificaba el emitido por el Juzgado de Móstoles el 1 de septiembre de 1992, donde se reconocía la inexistencia, en el Derecho español entonces vigente, de una normativa aplicable a un hecho de esas características. (Sólo quedó pendiente la eventual responsabilidad por delito de cohecho, por la captación de información, a cambio de dinero, de los funcionarios públicos encargados de su custodia).

Recordamos los aspectos esenciales de aquel supuesto: En 1991, tras las investigaciones oportunas, la Policía detuvo a J.G, por las actividades desarrolladas a través de la empresa PUBLIGEST S.L, de la que era dueño. Al parecer, la empresa se dedicaba a recopilar todo tipo de datos relativos, unas veces a personas físicas (v.gr: nombre, domicilio, número del documento nacional de identidad, empresa en la que trabajaban, ingresos, automóviles que figuraban a su nombre, datos de afiliación a la Seguridad Social), y otras veces a empresas-personas jurídicas (Código de Identificación Fiscal, número de trabajadores, etc.). Todos esos datos se integraban en ficheros automatizados, se trataban con los programas adecuados y se obtenían "perfiles de ciudadanos", que luego eran vendidos, según los intereses de cada cliente, a diversas empresas o particulares (para campañas de publicidad directa y otros fines). En ocasiones, sin embargo, se empleaban directamente por la propia Compañía implicada o se intercambiaban ficheros con otras empresas del sector.

Como queda reflejado en el Auto de sobreseimiento del Juzgado de Móstoles, la información se recababa por distintas vías: a) la compra o intercambio de ficheros con otras empresas del sector; b) la captura de los datos que figuran en los cupones de concursos de amplia difusión; c) la copia de los datos proporcionados por partidos políticos, sindicatos, Seguridad Social, Ayuntamientos, fundamentalmente referidos a datos obrantes en padrones o censo electoral, al encargar trabajos de informatización para la celebración de elecciones u otros fines públicos, que luego utilizaban con fines privados; d) mediante solicitud directa a los organismos o funcionarios públicos encargados de estos datos.

La explicación del sobreseimiento aparece con nitidez en el Auto: la mayor parte de los datos recopilados y tratados por PUBLI-GEST S.L. no eran secretos (en el sentido de afectar a la esfera íntima de la persona), sino públicos (figuraban inscritos en Registros y Archivos públicos), de amplia difusión (se entregaban sin restricciones a empresas de publicidad y a solicitantes particulares), y muchos, incluso, eran expuestos en ocasiones para el conocimiento general (vgr. las listas electorales, que entonces se exponían en los colegios electorales cuando se celebraban elecciones). En el momento en que se llevaron a cabo las actividades denunciadas, primero, no existía una regulación exhaustiva del contenido y los límites de la publicidad de aquellos datos; y, segundo, los tipos del Código Penal entonces vigente no contemplaban

dichos supuestos (salvo en caso de ofrecimiento o solicitud de dádivas, presentes, regalos o promesas a los encargados de la custodia de estos datos para su facilitación (artículos 386, 390 y 391 del Código Penal derogado), lo cual no constaba más que en un supuesto, que se remitió al Juzgado de Instrucción de Sevilla competente.

La secuencia de fechas y normas resulta esclarecedora: el caso se destapó en 1991 y en septiembre de 1992 el Auto de sobreseimiento del Juzgado de Móstoles pone sobre la mesa la laguna de nuestro ordenamiento jurídico para dar una respuesta idónea, adaptada a la demanda de la sociedad. Un mes después, precipitada por la alarma social que provocó la impunidad de los implicados, sale la Ley Orgánica Reguladora del Tratamiento Automatizado de Datos (LORTAD), precedente de la actual Ley Orgánica de Protección de Datos de Carácter Personal (LODP), si bien hay que esperar hasta el Código Penal de 1995 para que tal clase de supuestos pudieran tener relevancia penal. La última reforma de 2010 aún toca algunos aspectos con incidencia en la materia de la que aquí nos ocupamos.

El interés de este caso, a nuestro juicio, va más allá de una mera referencia histórica, y por eso lo traemos a estas páginas, porque, en torno al mismo, hallamos algunas de las claves para explicar la situación actual, situación que, lejos de haberse resuelto con la normativa vigente, se ha complicado ostensiblemente en el presente, con la dependencia masiva de Internet en el mundo globalizado moderno y, sobre todo, debido a la vertiginosa expansión de las Redes sociales a la que estamos asistiendo.

¿Por qué aún ofrece interés este caso?

1º Por lo que significó en términos de **sensibilización o concienciación social**: Para aquellas fechas, la sociedad española ya se había incorporado sin complejos a las múltiples ventajas y posibilidades que reportaban las Tecnologías de la Información y Comunicación Electrónica (TICs). Nadie, entre nosotros, cuestionaba que estábamos en plena "era tecnológica", y a un nivel bastante parejo al del resto de países de nuestro entorno en cuanto al grado de penetración social. De eso éramos bastante conscientes, las computadoras se habían instalado en la "normalidad" de nuestro quehacer cotidiano y de forma espectacular avanzábamos hacia la "era de Internet". Pero no éramos tan conscientes, sin embargo, de nuestra paralela incorporación a su dimensión pervertida y abusiva. Las advertencias sobre los riesgos, la parte vulnerable de la "revolución tecnológica", parecían más bien mera retórica, puro ejercicio intelectual de juristas y estudiosos, o, como mucho, predicable de otros países mucho más desarrollados, pero no del nuestro; en suma, sólo eso: pura advertencia abstracta de un riesgo potencial. El "caso PUBLI-GEST", en dichas coordenadas, de alguna forma sirvió para abrirnos los ojos sobre esa dimensión pervertida de la Informática en relación a un bien personalísimo, muy valioso, que nadie había considerado hasta entonces seriamente en peligro: la intimidad, o, para ser más precisos, la *nueva cara* de la intimidad.

Por lo demás, los ciudadanos empezamos a advertir la relevancia de ciertos actos aparentemente neutros e inocuos de nuestra vida cotidiana (vgr. rellenar un impreso para solicitar una muestra gratuita de un producto; o el cupón para participar en un sorteo; o el pago de un bien o servicio con una tarjeta electromagnética, o remitir un formulario para una suscripción...). Bajo la apariencia de "generosidad" de la empresa que regala una muestra, o sortea un televisor, o premia por el uso de su

tarjeta de cliente, en realidad se encubre un cauce para recabar de nosotros información de toda índole, de gran valor para quien la posee. Y esa información, que no es nada por sí misma, al unirse a otras, también neutras, con el tratamiento informático adecuado, permiten construir nuestro más íntimo retrato.

> En este estadio, hablar de intimidad ya queda estrecho, porque intimidad está unida a la idea de secreto, reservado; pero ahora el concepto se desborda, implicándose, además de la intimidad, otros bienes y valores personalísimos de rango constitucional, vinculados a la dignidad, la libertad personal y el libre desarrollo de la personalidad

2º En el **orden jurídico**, como antes avanzábamos, el caso PUBLI-GEST tuvo consecuencias inmediatas: aunque en 1978 la Carta Magna ya emplazaba al legislador para que limitara el uso de la Informática en orden a garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos (art. 18.4 CE), no se había considerado una materia prioritaria y el legislador ordinario se estaba "tomando su tiempo" para cumplir el mandato del constituyente. Este hecho precipitó el desarrollo legislativo del referido precepto y en octubre de 1992 se publica la LORTAD, acercándonos a la mayoría de los ordenamientos de nuestro entorno, especialmente en el ámbito europeo. Así se abre una nueva etapa, con el reconocimiento y tutela de la *privacidad*, primero en el orden administrativo, y luego, a partir de 1995, refrendado en el orden penal.

3. Rasgos diferenciadores de la situación actual: expansión de internet y las redes sociales (de la intimidad a la "Extimidad")

¿Cuál es la situación en estos momentos? ¿Hasta dónde llega el alcance de la normativa que se ha venido desarrollando desde 1992 hasta el presente? ¿Existen nuevos riesgos? ¿Están atendidos, en su caso, suficientemente en el marco jurídico actual? Los elementos, a nuestro entender, diferenciadores de la situación presente pueden reconducirse a estos puntos: En los últimos años, en los hábitos y pautas de comportamiento social de los ciudadanos se pueden apreciar cambios notables que inciden en la materia que nos ocupa:

1º En los últimos años, se han producido cambios notables en los hábitos y pautas de comportamiento social de los ciudadanos, con gran incidencia en la materia que nos ocupa, sobre todo por el extraordinario incremento del uso de Internet en nuestra vida cotidiana. Junto a la gran masa de ciudadanos que, por razones de edad, nos ha tocado adaptarnos a esa realidad, hasta incorporarla a nuestras actividades profesionales y personales usuales, las nuevas generaciones, las que empiezan a

incorporarse ahora al mercado laboral, ya han nacido y crecido en la "era de Internet". Internet forma parte de su cultura y hábitos.

2º Otro aspecto diferenciador, que a nadie pasa inadvertido del momento presente, está conectado al fenómeno relativamente reciente de las Redes Sociales, al uso masivo de las Redes Sociales, por precisar más. Los Sistemas de Redes Sociales (SRS) se han convertido, en poco más de seis años, en la punta de lanza de la llamada web 2.0, que implica un modo nuevo de utilizar la Red: de alguna forma, el usuario se ha apropiado de la Red; ya no es un mero observador, que recurre a Internet para buscar información y mirar lo que otros publican; ahora busca algo más, ser protagonista de todo lo que sucede, participa, interviene, opina, expone, crea. Y, en lo que aquí nos ocupa, el sujeto tiende a desinhibirse, exponiendo públicamente cuestiones de su vida personal, laboral, familiar...

> Esta nueva forma de relacionarse es la que ha llevado a acuñar la expresión "extimidad", por la exteriorización permanente, ante la comunidad virtual, de los aspectos de la vida privada que clásicamente pertenecían al terreno de lo íntimo y reservado.

(Los estudios sobre las características y dimensión de este tipo de aplicaciones ofrecen unos datos de lo más revelador: en noviembre de 2010, el 70% de los internautas en España era usuario o pertenecía a alguna Red Social, frente al 51% sólo un año antes. Como no podemos entrar con detalle en el análisis de la magnitud del fenómeno, para un resumen actualizado de estos estudios, recomendamos el libro, recientemente publicado, sobre *Menores y Redes Sociales*, de Xavier Bringué y Charo Sádaba).

3º A los anteriores elementos diferenciadores, vinculados al cambio de comportamiento del ciudadano, hay que sumar, como factor adicional y muy relevante de riesgo, el proceso generalizado de informatización que ha tenido lugar en empresas y servicios de toda índole, y en organismos y Administraciones Públicas a cualquier nivel. De esta suerte, resulta que cada individuo aparece retratado, lo quiera o no, desde los flancos más diversos. Y, no se olvide, es una información de muy fácil (casi ilimitado) almacenamiento, de muy fácil acceso (a tiempo real, desde los puntos más remotos), de fácil tratamiento y comunicación, desde cualquier punto del planeta hasta cualquier punto del planeta (las grandes ventajas que reportan las TICs).

4º No podemos obviar, por último, un factor de extraordinaria trascendencia en este escueto bosquejo de la situación actual, vinculado a los hechos terroristas de gran escala en distintos países. Como ha denunciado de forma reiterada la doctrina penal dentro y fuera de nuestras fronteras, tal sucesión de gravísimos atentados ha servido como detonante de todo un elenco de medidas contra el crimen en general y el terrorismo en particular, que ponen en crisis reconocidas garantías de raigambre constitucional, rompiéndose los límites a la injerencia estatal "legal" en el espacio más íntimo y privado de la vida del ciudadano.

Como quiera que sea, la conjunción de los factores anteriores marca la diferencia frente a lo que ocurría hace dos décadas, cuando salió a la luz el "caso PUBLIGEST":

1º La cantidad de información que existe en el espacio virtual sobre el ciudadano es muy superior.

2º El contenido de dicha información es mucho más completo y heterogéneo, comprendiendo ahora datos más sensibles y personalísimos: desde la más mínima incidencia concerniente a la salud (enfermedades, tratamientos, dietas, fármacos), hasta los detalles últimos de la trayectoria académica, vida laboral, movimientos bancarios y situación económica, sin excluir cualquier aspecto de las relaciones personales, comunicaciones, ocio, eventos familiares, ideología, preferencias, gustos, aficiones, opiniones, intereses...

3º Y esa información es vulnerable, de alguna forma está "a la intemperie", a veces, ante conductas ilegales (bien por parte de los que poseen o tratan la información ajena, que pueden hacer mal uso de ella, bien por parte de terceros que acceden subrepticiamente a la misma, como los *hackers*), pero, en ocasiones, ante actuaciones invasivas dentro del marco de la legalidad (ahora, por "razones de seguridad y prevención de la delincuencia", los Estados se han dotado del marco normativo idóneo para intervenir y controlar la información concerniente a sus ciudadanos, expresión del llamado "Derecho penal del enemigo").

4. Intereses en riesgo: la privacidad en la red

Está fuera de duda que el uso abusivo de las posibilidades que ofrecen las TICs en la sociedad moderna supera con creces el terreno del que nos ocupamos en estas líneas. El catálogo de bienes e intereses que cabría citar entre los seriamente comprometidos por la utilización pervertida de las tecnologías informáticas sería amplísimo (vgr. indemnidad sexual de menores, bienes de contenido patrimonial y socioeconómico, seguridad del Estado, etc.). Sin embargo, aquí concentramos nuestro examen en el ámbito personalísimo de la intimidad, sus nuevas perspectivas, (intimidad informática o *privacidad*, si se prefiere), en conexión con la información y los datos que obran en el *espacio virtual* sobre los ciudadanos.

Hecha esta advertencia, parece oportuno detenerse, siquiera brevemente, a examinar qué intereses resultan seriamente amenazados en dicho ámbito, sin perjuicio de que en otro apartado se analicen cuáles y en qué medida puedan recibir protección jurídica.

1º Como se recordará, el artículo 8.4 de nuestra Carta Magna emplazaba al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos. Ahora bien: cabe preguntarse si los intereses en peligro por el uso de las TICs se circunscriben a los derechos fundamentales aludidos por el legislador constitucional en el

referido precepto. A nuestro juicio, cerrar el tema con esta referencia es hoy manifiestamente insuficiente o, cuanto menos, superficial. Ya era insuficiente hace dos décadas, y ahora con mayor motivo.

2º Seguro que bastante influido por el "caso PUBLI-GEST" y muy relevantes aportaciones doctrinales (como la brillante monografía de MORALES PRATS sobre *La tutela penal de la intimidad: "privacy" e informática"*), el legislador de 1992, al redactar el Preámbulo de la LORTAD, afina con mayor precisión y da la pista certera (a nuestro entender) de lo que está en juego. Reproducimos tal referencia por su interés:

> "El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la **privacidad**, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: Aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en la que se desarrollan las facetas más singularmente reservadas de la vida de la persona –el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, ***la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.*** Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo". (Los subrayados son nuestros)

Se denomine privacidad o intimidad informática, el acierto del legislador en el párrafo trascrito reside en la intuición de que el uso de las TICs compromete algo más que la intimidad entendida en un sentido clásico: Sin los límites que antes representaban el espacio y el tiempo, como veremos con algunos ejemplos, hoy está amenazada la intimidad personal y familiar, el honor, pero también la propia imagen, la libertad individual, el derecho al libre desarrollo de la personalidad y, en último extremo, la dignidad misma del sujeto, gravemente comprometida cuando es "cosificado", manejado, clasificado, manipulado en sus decisiones, opciones, elecciones..., cuando es diseccionado, vigilado u ordenado desde fuera, y, en general, cuando de forma inconsciente pierde las riendas de su propia vida.

a) La intimidad personal y familiar se ***ve*** afectada, tanto en su dimensión negativa (como facultad del titular de excluir a terceros de determinados ámbitos propios, privados, personalísimos), como en su dimensión positiva (como facultades jurídicas de poder de control sobre determinados datos y aspectos relativos a la intimidad del sujeto). La intimidad es vulnerable, tanto ante actuaciones de otros ciudadanos y empresas privadas (que pueden introducir en nuestros ordenadores personales programas tipo *troyanos*, con los que seguir nuestra vida vigilando comunicaciones, actividades, correos), como ante actuaciones desde el propio aparato del Estado (que, so pretexto de prevenir y combatir la criminalidad,

puede barrer nuestras comunicaciones, entrar en el disco duro de nuestro ordenador y vigilar y controlar nuestros pasos, incluso con cobertura legal). Sirven como muestra algunos ejemplos:

- Un alumno de Postgrado de Perú, cuando busca en Internet bibliografía de un profesor español, se encuentra, de forma inesperada, las fotos del citado profesor en su vivienda durante la cena familiar de Nochevieja (colgadas en PICASA por su hermana), las de su viaje a Japón con su pareja, y sus aportaciones y comentarios en un foro virtual sobre anorexia, bulimia y trastornos alimentarios; vídeos de su hijo desde que nació, sus comentarios a las noticias de la prensa local...
- Un joven que ha superado las pruebas de conocimientos en las Oposiciones a la Policía Nacional, es eliminado en la entrevista final porque, entre los datos que de él se manejan en el CNP, constan aún los conflictos que tuvo en su Colegio cuando tenía trece años, en plena crisis preadolescente.

b) El honor del ciudadano, como su imagen y su buen nombre, también pueden resultar seriamente ***afectados*** por el efecto multiplicador, *sine die*, que tiene cualquier noticia que le concierna si se expande por la Red. Otro ejemplo:

- Un destacado personaje público se ve involucrado en las investigaciones por el delito de cohecho del que es presuntamente autor un conocido. El hecho aparece en los periódicos digitales de su localidad. Aunque posteriormente se comprueba que no tenía ninguna vinculación con el asunto, la noticia seguirá viva, más allá de las fronteras del país, para siempre; sin derecho a eliminarla, al olvido, a que se restablezca su nombre...
- Las imágenes poco afortunadas de una persona una noche de copas son grabadas y colgadas en youtube. A partir de ese momento, con cualquier buscador y desde cualquier lugar del mundo, se volverá a actualizar aquel momento, y la persona arrastrará ese peso de por vida.

c) La libertad individual y el derecho al libre desarrollo de la personalidad se ven, asimismo, cuestionadas en este ámbito como consecuencia del control que sobre el sujeto se ejerce desde distintas instancias. ¿Qué capacidad de libertad le queda a una persona que sabe que es controlada, por ejemplo, en sus gustos, costumbres, aficiones, relaciones, hábitos de consumo, opiniones, material que comparte o descarga de Internet...? Más ejemplos:

- Un sujeto, casado y padre de familia, con aspiraciones en la política, se ve obligado a cortar la relación con una persona amiga, consciente de que sus comunicaciones telefónicas y telemáticas son interceptadas y los datos sobre tal relación pueden perjudicarle notablemente en sus aspiraciones en caso de ser filtrados a los medios de comunicación.

d) La dignidad de la persona, en fin, se ve amenazada siempre que es tratada como un mero objeto (según apuntábamos antes, cuando se la clasifica, maneja, manipula, ya sea para que adquiera ciertos bienes, ya sea para que vote de determinada forma en un proceso electoral) y, en general, cuando se somete al individuo a control y vigilancia permanente, privándole de la condición de ciudadano.

5. Peculiaridades de los intereses afectados: la disposición del titular de la *privacidad*

En estas nuevas coordenadas, son muchos quienes se plantean que, por mor del impacto de las TICs, los bienes y derechos fundamentales amenazados, especialmente la intimidad, han dejado de presentar las características tradicionales y adquieren un contenido diverso. (Queremos entender que a esto se refería el Fiscal de delitos informáticos de Granada, Francisco Hernández, cuando en 2009 alertaba de una intimidad "debilitada" con el uso de comunidades virtuales y Redes Sociales, y de la necesaria "redefinición" del derecho a la intimidad). Seguramente es cierto, aunque conviene ahondar en los aspectos que determinan esa especial configuración:

De una parte, la intimidad (como el derecho al honor, a la propia imagen o la libertad) es un bien de carácter personal, individual y disponible. Este último rasgo, su disponibilidad, determina que el consentimiento de su titular adquiera una incuestionable trascendencia en la calificación jurídica de las actividades que puedan incidir sobre el mismo. Pues bien: aquí hallamos hoy una de las notas que lleva a muchos a afirmar que estamos ante un bien con nuevos perfiles. ¿Por qué?: Porque buena parte de la información y datos personales que circulan en la Red y se archivan electrónicamente se han suministrado (expuesto) voluntariamente por su titular. Para mayor precisión, cabría diferenciar varios niveles:

a) Datos que el sujeto, de modo absolutamente espontáneo y voluntario, deja en la Red en su perfil (en una Red Social, en un blog personal o una página web), o en su presentación en diversos foros o grupos.

b) Datos e informaciones que se requieren de forma obligatoria e inevitable en ciertos ámbitos, públicos o privados, y respecto a los cuales se tiene muy poca o ninguna capacidad de maniobra por parte del titular. Pensemos en una denuncia de tráfico, en una historia clínica, en la solicitud de un contrato de seguro o de una beca, en los formularios de Hacienda o de la Seguridad Social). Aquí, se consiente, se ofrecen los datos personales que se requieren con consentimiento (libre e informado, inequívoco, exige la LODP), pero, claro está, sólo para un fin específico.

c) Datos e informaciones nuestros que son suministrados, al margen de nuestra voluntad, frecuentemente por personas cercanas, sobre todo familiares y amigos (vgr. fotos de reuniones familiares o fiestas con amigos, incidencias de un viaje que hicimos juntos, vídeos de eventos del Colegio colgados en la página web del Centro, imágenes de una manifestación u otro acto público captadas y publicadas en un periódico digital, etc).

d) Datos e informaciones que recaban de nosotros cuando desarrollamos ciertas actividades, en las que nos servimos de las ventajas que reportan las TICs (por ejemplo, cuando navegamos por Internet y dejamos a los servidores valiosa información reflejada en el historial, o cuando abonamos bienes y servicios con tarjetas electromagnéticas, o cuando realizamos operaciones a través de la banca electrónica). Por lo general, el ciudadano en estos casos, o bien no es demasiado consciente de lo que

está exponiendo de sí mismo, o es consciente pero sólo tolera suministrar esa información como una especie de peaje inevitable de la agilidad, comodidad y ventajas de las modernas tecnologías (al final, prefiero que me puedan seguir la pista de mi viaje siguiendo los movimientos de mi tarjeta de crédito a tener que llevar dinero en efectivo, por ejemplo). En cualquier caso, la persona aquí nunca presta su consentimiento al uso, tratamiento y comunicación de esa información.

e) Datos e informaciones que el ciudadano procura conscientemente guardar a toda costa (ni tolera ni, menos aún, consiente) y, sin embargo, pese a todo, son intervenidos y controlados, unas veces por terceros que penetran a distancia en los ordenadores personales mediante la utilización de *malware*, programas espías, otras veces por actuaciones desde el propio aparato del Estado y diversos organismos incluso más allá de las fronteras. (vgr. el contenido de comunicaciones y mensajes electrónicos; el contenido en el disco duro o en el historial de Internet en el ordenador personal).

Como se puede observar, la peculiaridad más significativa es que algunas de las dimensiones de la privacidad se exponen voluntariamente en la Red, es decir, existe consentimiento del titular. En bienes de carácter personal, salvo que expresamente se prevea en la Ley (tal es el caso de la vida y la salud individual), el consentimiento del titular, su renuncia, la disposición voluntaria, convierte (o debiera convertir) en lícito cualquier comportamiento que incida en ellos. En los supuestos que ahora nos ocupan la cuestión no es tan sencilla:

1º En relación con los adultos, los mayores de edad: Por coherencia con los criterios que se mantienen en otros ámbitos, especialmente en la esfera penal, para que el consentimiento tenga eficacia, ha de ser expreso y libre (con conocimiento de aquello sobre lo que se consiente, de ahí que se hable de "consentimiento informado" en la esfera sanitaria, y voluntario, sin coacción, amenaza, engaño o recabado por precio). La LOPD, al referirse al consentimiento del afectado, preciso para el tratamiento de los datos, emplea el adjetivo "inequívoco" (art. 6 LOPD y arts. 12 ss. Reglamento), y en la Guía para el ciudadano de la AEPD se aclara: Ha de ser un consentimiento libre, previo e informado, específico (para un modo concreto de tratamiento sobre el que se ha informado) y revocable.

La exigencia de que sea "expreso" entendemos que no está cubierta a base de presunciones, es decir, interpretando que se consiente cuando no hay pronunciamiento expreso en contra (ejemplo: uno puede consentir a que le hagan unas fotos una noche de fiesta, pero de ahí no puede deducirse que consienta en cualquier uso público posterior con las mismas); como tampoco puede presumirse el consentimiento en los casos en los que el propio sujeto titular de la información privada interceptada, por desconocimiento, exceso de confianza o dejadez, no adopta suficientes medidas de seguridad para la protección de ordenadores y sistemas informáticos frente a ataques de terceros (por ejemplo, cortafuegos, antivirus actualizados, etc.). Frente a los que justifican conductas de hackers, crackers y *snniffers* en las escasas medidas de seguridad de las víctimas, entendemos que no puede confundirse la falta de diligencia, la dejadez o el exceso de confianza, con el consentimiento a las intromisiones en la intimidad. El consentimiento no se presume (ni debiera hacerse) en el delicado ámbito de la disposición de bienes jurídicos personalísimos. (Consecuencias de esa errónea presunción se han conocido en la esfera penal, especialmente en los delitos contra la libertad sexual, y con buen criterio hoy son rechazadas).

En la materia que nos ocupa, más allá de las páginas y contenidos en la Red que el adulto decide hacer públicos ante la generalidad, en el resto de los casos el consentimiento, o bien no existe en absoluto (ejemplo: en absoluto se consiente ante quien intercepta subrepticiamente las comunicaciones telemáticas o instala en nuestro ordenador personal un *troyano* o programa espía para controlar nuestras actividades en la Red), o bien carece de los requisitos para que posea relevancia (por ejemplo, el sujeto puede aceptar o tolerar que la gran superficie tenga conocimiento de sus hábitos de consumo cuando usa la tarjeta de cliente y quedan registradas todas sus compras por el sistema de códigos de barras, pero no consiente acerca de usos posteriores con esos datos; otro ejemplo: el sujeto consiente en que el público en general tenga conocimiento de su opinión expresada en una comunidad virtual, pero no presta su consentimiento a que se cruce esa opinión con otras que ha reflejado en otros ámbitos y se haga un perfil de él).

> En suma, en muchos casos el titular no es consciente de la información que concierne a su intimidad, luego difícilmente pueda hablarse aquí de consentimiento; y en otros supuestos en los que efectúa actos de disposición sobre dimensiones parciales de su esfera íntima, sin embargo, carece de una suficiente percepción de los riesgos, con lo cual más bien hablaríamos de un consentimiento viciado.

b) En relación con los menores de edad el tema es aún más delicado. En ellos confluyen una serie de circunstancias que agravan los riesgos en el ámbito que nos ocupa: De una parte, como veíamos inicialmente, son generaciones ya nacidas en la "era de Internet web.2" y su dependencia de las TICs es más acusada. La pertenencia a las Redes Sociales representa, en su entorno, un factor indispensable de integración social desde muy temprana edad, se comunican, expresan, interaccionan a través de ellas y determinan sus índices de popularidad y consideración. A través de las comunidades virtuales, se facilitan las relaciones y la falta de inmediatez propicia la desinhibición y la exposición pública. Por otro lado, en los jóvenes, por lo general, la percepción del riesgo es menos acusada que en el adulto, de tal suerte que difícilmente serán conscientes de lo que están poniendo en juego cuando cuelgan en la Red fotos, comentarios, opiniones, vídeos, críticas y datos muy íntimos, propios o ajenos. A diferencia de lo que ocurre en el mundo de los adultos, en la gente joven se observa una clara necesidad de "compartir", hacer públicos aspectos de su vida privada y, cuanto mayor es la difusión, mejor.

En este contexto, ¿qué relevancia tiene el consentimiento del menor? Si el menor ha consentido en las intromisiones en su privacidad, ¿debe considerarse lícita, sin más, cualquier agresión a este bien? Como es sabido, en nuestro ordenamiento jurídico no existe un criterio uniforme sobre el momento a partir del cual se estima válido el consentimiento de un menor. No deja de producir cierto estupor que, en algunos ámbitos jurídicos, el límite de edad esté en trece años -ej. en los delitos contra la libertad sexual-, en otros, los catorce –ej. para delimitar la responsabilidad penal-, en otros, el límite relevante sean los dieciséis –ej. para consentir en una intervención quirúrgica, según la Ley de 2009; o para someterse a un aborto-, y en otros ámbitos, en cambio, los dieciocho años constituyen la frontera –ej. para que tenga eficacia el consentimiento en las lesiones, para votar o para entrar en el ámbito del Derecho Penal de

adultos-. Con este panorama tan poco clarificador, al tiempo de pronunciarnos sobre la validez del consentimiento del menor para disponer de su privacidad, estimamos coherente (aunque no necesariamente razonable) fijar el límite en los catorce años: Coherente, porque es el límite fijado en la normativa vigente sobre protección de datos (art. 13 del Reglamento de la LOPD) para admitir la eficacia del consentimiento del menor; razonable, no parece tanto: si consideramos que la escasa percepción del riesgo es mucho más acusada en edades más bajas y si tenemos en cuenta las consecuencias que pueden arrastrar en el futuro los menores por conductas frívolas e inconscientes de exposición en la Red, acaso hubiera sido preferible un límite de edad algo superior.

Respecto a la relevancia del consentimiento de los menores en la exposición de parcelas de su privacidad, cabe hacer una última reflexión vinculada a ciertas pautas de conducta nada infrecuentes entre los progenitores: hasta ahora nos hemos referido a casos en que los propios menores comparten aspectos íntimos personales. Es un tema que preocupa a padres y educadores y que focaliza esfuerzos de la comunidad educativa para alertar a las nuevas generaciones de los riesgos que corren (se pretende proteger a los menores frente a conductas como el *bulling*, el *grommming* y otros abusos que favorece el anonimato de la Red). Sin restar importancia a estos esfuerzos, echamos en falta una paralela concienciación a padres y familiares sobre la eventual repercusión que pueden tener para sus menores "exponerlos" en la Red desde su más tierna infancia (¡se llegan a colgar, en ocasiones, hasta las ecografías antes de nacer!). Nos parece que con estas actuaciones inconscientes e imprudentes se está afectando muy seriamente, ya no sólo a la privacidad del menor, comprometiendo su futuro (nada desaparece del espacio virtual), sino también –lo que es más grave- su propia seguridad. En gran medida, el adulto está contribuyendo a hacer de su hijo ese *ciudadano transparente* del futuro que tanto nos alarma.

6. Vías para proteger la privacidad: marco normativo

Llegados a este punto, vamos a aproximarnos a las medidas que ofrece el Derecho positivo vigente para la protección de la privacidad o la intimidad informática, si se prefiere. El punto de referencia, evidentemente, lo fija la Carta Magna, que, como ya ha sido expuesto, conecta los riesgos del uso abusivo de la informática con los derechos fundamentales, especialmente honor e intimidad. A partir de este punto, el marco normativo de referencia es amplio, porque se conforma por las diversas Directivas comunitarias que inciden en el tema, las normas a través de las cuales el legislador español ha trasladado al Derecho interno las Directivas comunitarias (especialmente, la LSICE y Ley General de Telecomunicaciones), los Convenios internacionales ratificados por España (entre ellos, de modo destacado, el Convenio sobre Ciberdelincuencia del Consejo de Europa).

Aquí, de forma simplificada, vamos a circunscribirnos a los dos niveles del Derecho positivo vigente para la tutela de la *privacidad*, que reconducimos a los dos niveles: protección "extrapenal" y protección penal.

6.1. Protección en la esfera "extrapenal": la LOPD y el Reglamento que la desarrolla

Como se ha reflejado más arriba, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (vigente desde el 15 de enero de 2000), viene a sustituir a la LORTAD, de 1992, adaptándola a la Directiva comunitaria de 1995 (Directiva 95/46/CEE). Aunque conserva muchas de las aportaciones de su predecesora, y en tal sentido se establece que se mantiene la vigencia de la LORTAD en todo lo que no se oponga a la Ley, sin embargo, cubre algunas de sus carencias, entre las que cabe destacar su ámbito de aplicación: que ya no queda restringido a la protección de los *datos informatizados* de carácter personal sino que abarca los datos de carácter personal que se hallen en cualquier tipo de archivo o registro, informatizado o no.

Con carácter general, importa en esta sede destacar los siguientes aspectos:

1º Sólo atiende a la tutela de una de las facetas de la privacidad o intimidad informática, pues, como se ha indicado anteriormente, con las pautas de comportamiento actuales (uso masivo de Internet, exposición de aspectos personales en redes sociales y foros virtuales de distinta naturaleza), muchos otros aspectos de la privacy escapan hoy al ámbito de esta Ley.

2º La LOPD es una norma de naturaleza administrativa, no penal, cuyo objetivo prioritario es dispensar una protección *preventiva* (aunque establezca un cuadro de infracciones y sanciones para reforzar su eficacia y garantizar su cumplimento). Este carácter nos parece de extraordinario interés para el objeto del presente estudio, porque la fuerza de la norma radica justamente en la exigencia de adopción de una serie de medidas *previas* al daño, como veremos (a diferencia del Derecho penal que, aun cuando procure la protección preventiva de bienes jurídicos, opera *a posteriori*, cuando ya hay afección al bien jurídico). En estas coordenadas (actuación preventiva) han de interpretarse los límites establecidos para recabar datos personales, los límites al uso de los mismos, las medidas de seguridad impuestas a las personas físicas, empresas y organismos públicos titulares de ficheros, encargados de los mismos o responsables de su tratamiento; y, desde luego, en tales coordenadas adquiere el máximo sentido la Agencia Española de Protección de Datos (AEPD), con una trayectoria impecable desde su creación, no sólo velando por el cumplimiento de la Ley, sino también educando al ciudadano sobre las medidas de autoprotección (cfr. *El derecho fundamental a la protección de datos: Guía para el ciudadano, accesible en su página web*).

3º Aún cabe resaltar un último aspecto de carácter general: En esta norma se fijan los contornos del *derecho a la protección de datos* (para algunos, derecho a la autodeterminación informativa), elevado a la *categoría de derecho fundamental* en las célebres Sentencias constitucionales 290 y 292, ambas de 30 de noviembre de 2000 (no puede olvidarse, al efecto, el antecedente que remonta hasta la Sentencia del Tribunal Constitucional Federal Alemán, de 15 de diciembre de 1983, sobre la Ley del Censo de

población). En suma, la protección de datos de carácter personal constituye hoy un verdadero derecho fundamental, cuyo contenido persigue garantizar el poder de disposición y control de los individuos respecto de sus datos personales. Según la doctrina del Tribunal Constitucional (en las Sentencias citadas, entre otra muchas), este derecho "faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y (que) también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

> Esos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder de oponerse a esa posesión y usos." (Fundamento jurídico 7º de la STC 292/2000, de 30 de noviembre).

Resumimos, a continuación, cómo se concreta la protección que la LOPD y el Reglamento que la desarrolla dispensan al ciudadano:

A) Ámbito de aplicación de la Ley

La LOPD es de aplicación a los datos de carácter personal (cualquier información concerniente a personas físicas, identificadas o identificables), registrados y organizados en soporte físico que los haga susceptibles de tratamiento (soporte informatizado o no, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso) y a toda modalidad de uso posterior de esos datos por los sectores público y privado.

(Quedan excluidos datos de personas jurídicas, ficheros de carácter personal o doméstico, algunos referidos a materias reservadas, o relativos a la investigación del terrorismo y formas graves de delincuencia organizada. El Reglamento de la LODP, como se aclara en la Exposición de Motivos del Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba, tiene un ámbito más amplio, al ser posterior a la Ley de Servicios de la sociedad de la información y del comercio electrónico, de 2002, y a la Ley General de Telecomunicaciones, de 2003, a fin de armonizar su contenido, especialmente en lo que a las competencias de la AEPD concierne).

B) Principios de la protección de datos

Habida cuenta de que el derecho fundamental que nos ocupa opera en relación con el tratamiento por terceros de los datos personales, y a fin de que no se desvirtúe su contenido, el legislador configura una serie de principios que han de ser respetados:

1º **Derecho/deber de información**: Ampliamente configurado en el articulado de la Ley, abarca desde el momento en que son requeridos los datos de carácter personal al ciudadano, verbalmente o por escrito (información expresa, precisa e inequívoca, sobre la existencia del fichero, fines de la recogida de datos, destinatarios de los mismos, su carácter obligatorio o no, consecuencias de no suministrarlos) hasta cualquiera de las fases posteriores, pues no en vano la información es el presupuesto del consentimiento y, además, el soporte de los derechos de acceso, rectificación, consulta, cancelación, impugnaciones.

2º **Principio del consentimiento**: El artículo 6 LOPD consagra la necesidad del consentimiento *inequívoco* (y revocable) del afectado para el tratamiento de los datos de carácter personal, a menos la ley disponga otra cosa. (Sólo se exceptúan ciertos supuestos, como los datos de carácter personal que recojan las Administraciones públicas para el ejercicio de las funciones propias en el ámbito de sus competencias, o se trate de proteger un interés vital del interesado si el interesado está física o jurídicamente incapacitado para dar su consentimiento...).

3º **Principio de calidad de los datos**: Con este principio se hace referencia, no sólo a la exigencia de exactitud, veracidad, actualización de los datos personales recogidos, sino también a la exigencia de proporcionalidad (pertinencia y adecuación entre los datos requeridos a la finalidad perseguida) y al deber de cancelación cuando dejan de ser necesarios. Se regula de forma amplia, con el paralelo derecho del interesado de conocer esos datos, requerir su modificación o cancelación, y se completa con la prohibición de recoger datos por medios desleales, fraudulentos o ilícitos. (Vid. art. 4 LOPD).

4º **Principio de seguridad de los datos**: Se trata de uno de los puntos fuertes de la normativa vigente, que impone a los responsables de los ficheros y, en su caso, encargados del tratamiento de los mismos la adopción de las medidas técnicas y organizativas que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, naturaleza de los datos almacenados y los riesgos a que están expuestos (art. 9 LOPD). (Vía reglamentaria, se desarrollan de forma detallada estas exigencias, delimitando nivel de seguridad alto, medio y básico, según el contenido de los ficheros y tratamiento de la información, y ya son de aplicación tanto a ficheros y archivos automatizados como no automatizados. Se regulan distintos plazos para implementar estas medidas en caso de ficheros ya existentes, imponiéndose desde su creación cuando se trate de ficheros posteriores a la entrada en vigor de esta norma). La exigencia de guardar secreto por los responsables de ficheros, la obligación de notificar la existencia, creación y modificación de los mismos en el Registro General de Protección de Datos, y el disponer de políticas de seguridad, implica, en último extremo, garantizar la integridad, disponibilidad y confidencialidad de los datos; el incumplimiento de dichas exigencias legales se considera infracción grave, lleva aparejadas

sanciones pecuniarias elevadas y, en caso de las Administraciones públicas, cabría la apertura de un procedimiento disciplinario contra el responsable.

C) Derechos que asisten a los afectados

Si el derecho fundamental a la protección de datos se define como el derecho del ciudadano a ejercer el control sobre su información personal, es imprescindible otorgarle las herramientas para hacer efectivo ese control. En la definición de los derechos de consulta, acceso, rectificación, cancelación y oposición, la LOPD contempla un amplio elenco de facultades que sirven al sujeto, unas veces como mecanismo de protección previo de esa parcela de su privacidad (antes de que se haya producido el daño), y otras veces como vía de reparación (operan a posteriori.) Recogemos ahora en síntesis esos derechos:

1º Derecho de CONSULTA: Supone la facultad de conocer, recabando la información oportuna del Registro General de Protección de Datos, si se están tratando nuestros datos de carácter personal, con qué fin y quiénes son los responsables de ese tratamiento (art. 14 LOPD).

2º Derechos ARCO: Se viene conociendo de esta forma a los derechos de ACCESO, RECTIFICACIÓN, CANCELACIÓN y OPOSICIÓN, aunque son derechos independientes entre sí. Permiten al ciudadano, gratuitamente:

a) Conocer qué datos suyos de carácter personal se están tratando, por quién, cómo se han obtenido o de dónde proceden y las comunicaciones realizadas con los mismos (DERECHO DE ACCESO);

b) Solicitar del responsable del tratamiento la rectificación, corregir errores o modificar datos que resulten inexactos o incompletos para garantizar la certeza de la información sometida a tratamiento (DERECHO DE RECTIFICACIÓN);

c) Solicitar la cancelación de los datos que resulten inadecuados o excesivos, para que se bloqueen y no sean sometidos a tratamiento (DERECHO DE CANCELACIÓN);

d) Oponerse al tratamiento de datos que no precisan consentimiento del titular, cuando concurra algún motivo legítimo y fundado en el caso concreto que lo justifique, siempre que la ley no disponga lo contrario (DERECHO DE OPOSICIÓN) (ej. una persona que ha huido de su país por amenazas terroristas y requiere que se supriman sus datos de los registros de su empresa para evitar ser localizado).

3º Derecho de TUTELA: La normativa vigente prevé un procedimiento sencillo ante los responsables del tratamiento correspondientes para hacer valer los derechos que se acaban de mencionar, pero, en caso de no obtenerse respuesta o rectificación satisfactoria y, en general, para todos los casos de actuaciones contrarias a la Ley, se articula el mecanismo de reclamación ante la Agencia Española de Protección de Datos o de la Comunidad Autónoma competente (art. 18 LOPD), y la resolución puede recurrirse por vía contencioso-administrativa.

4º Derecho a INDEMNIZACIÓN: Cuando de las actuaciones contrarias a la Ley se derive daño o lesión para los bienes o derechos del lesionado, existe derecho al resarcimiento. Vías: a) Si son ficheros de titularidad pública, por la legislación reguladora del régimen de responsabilidad de las Administraciones públicas; b) Si los ficheros son de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

Desde un punto de vista práctico, la relevancia de estos derechos en la tutela efectiva de la privacidad, al menos en el momento actual, a nuestro entender, es relativa:

- Por una parte, en la mayoría de los casos, el ciudadano carece de perspectiva suficiente para conocer en qué archivos o ficheros constan datos suyos, su exactitud, proporcionalidad y uso que se esté dando a los mismos; igual que, salvo casos flagrantes y notorios, ignora las medidas de seguridad adoptadas por quienes están a cargo de los ficheros (por ejemplo, al ciudadano, por lo general, le pasa inadvertido el hecho de que, sólo conociendo el número del documento nacional de identidad de otro, puede encontrarse con todos sus datos registrados en los archivos de la Dirección General de Tráfico, cuestión que recientemente ha denunciado un experto en seguridad de datos ante la AEPD). Si esto ya es complicado en el ámbito de las Administraciones públicas, lo es aún más en el sector privado.
- Segundo, las medidas de seguridad exigen inversión económica, y en momentos de crisis, como el presente, cuando se está recortando de forma tan severa en otras partidas más notorias (ej. no renovación de contratos temporales en la sanidad pública, reducción de servicios, o de camas en los hospitales), ¿no cabe pensar que la seguridad en la protección de nuestros datos puede también resentirse?
- Tercero, los mecanismos que configura la LOPD tienen un ámbito limitado al territorio español, cuando, en la actualidad, buena parte de esos datos (especialmente los que quedan en los SRS (Servicios de Redes Sociales) se alojan en servidores fuera de nuestras fronteras (tal es el caso de facebook, por ejemplo, por citar una de las redes sociales más conocidas).

Pese a nuestras reticencias, no obstante, no dejamos de valorar su alcance, especialmente en lo que concierne a la labor que desarrolla la Agencia Española de Protección de Datos, de la que nos ocupamos a continuación.

D) La Agencia Española de Protección de Datos

Ya en el Derecho Comunitario y en los Derechos de los Estados miembros se había previsto, como pieza esencial de todo el sistema, la existencia de una autoridad independiente de control para garantizar de modo efectivo el derecho a la protección de datos. La Agencia Española de Protección de Datos, creada por la LORTAD, es, entre nosotros, esa autoridad independiente, y a ella se le atribuyen "diversas funciones y potestades, de información, inspección y sanción, para prevenir las violaciones de los derechos fundamentales antes mencionados" (STC 290/2000, de 30 de noviembre). Sus competencias han sido ampliadas por la Ley de Servicios de la sociedad de la información y del comercio electrónico y la Ley General de Telecomunicaciones. A la AEPD le corresponde velar por el cumplimiento de la legislación

en materia de protección de datos de carácter personal y controlar su aplicación, especialmente en lo relativo a los derechos de información, acceso, rectificación, cancelación y oposición.

1º Funciones en relación con el ciudadano

a) Atender a sus peticiones y reclamaciones
b) Información de los derechos reconocidos por la Ley
c) Tutelar los derechos en las comunicaciones electrónicas
d) Promover las campañas de difusión a través de los medios

2º Funciones en relación con quienes tratan datos

a) Inspección, corrección, exigencia cumplimiento de obligaciones
b) Emitir autorizaciones previstas en la Ley
c) Potestad sancionatoria
d) Autorizar transferencias internacionales de datos

3º Otras funciones asignadas

a) Cooperación internacional
b) Dictar recomendaciones e instrucciones en materia de seguridad
c) Velar por la publicidad en los tratamientos de datos

VALORACIÓN:

En orden a la función prioritaria de asegurar la tutela efectiva del derecho fundamental del ciudadano a la protección de sus datos de carácter personal, entendemos que la AEPD desarrolla un papel esencial en la sensibilización e información en materia de seguridad y vías de autoprotección. En el momento actual de absoluta dependencia de las TICs en nuestro quehacer cotidiano, consideramos absolutamente prioritario que cada persona adquiera una completa percepción de los riesgos que amenazan a su privacidad, a su dignidad y a sus derechos más íntimos y personalísimos. Por eso entendemos tan relevante:

- ***Que se dé máxima difusión a las Instrucciones y Recomendaciones dictadas por este organismo (para conocer los riesgos a que se expone, las pautas de conducta cuando opera en la Red, para que conozca las vías para protegerse y proteger a sus menores);***

- ***Que la Guía para el ciudadano, de reciente publicación, sea conocida por la generalidad de las personas, especialmente los internautas, sobre todo si son menores de edad (se está poniendo mucho énfasis en la protección de la indemnidad sexual de los menores, pero no existe una paralela preocupación por su privacidad) ;***

- *Que los ciudadanos accedamos con asiduidad a la página web de la Agencia, permanentemente actualizada en el marco de sus competencias y actividad.*

Terminamos este apartado con un extracto de la Memoria de la AEPD correspondiente a 2010, que ilustra sobre los aspectos más destacados de su actividad. De acuerdo con lo publicado en dicha Memoria:

- El número total de investigaciones por denuncias y de oficio, fue de 4302 (un 4% más que el año anterior), y se recibieron 1643 solicitudes de tutela de los derechos.
- Se resolvieron 767 procedimientos sancionadores, de los que 591 acabaron con sanción. (El sector de las telecomunicaciones aglutinó más del 50% del total de las sanciones).
- Durante el 2010, la AEPD inició de oficio investigaciones a grandes compañías del sector de Internet, como Google, Facebook y Myspace, por supuesta transmisión de datos de perfiles.
- La seguridad y la difusión de datos en Internet y el sector de la videovigilancia se consolidan como los ámbitos más destacados de la preocupación ciudadana.
- En el ámbito sanitario se iniciaron 114 actuaciones de investigación en 2010 vinculadas a casos de vulneración del deber de guardar secreto e insuficiente implantación de medidas de seguridad.
- Un último dato reseñable por su interés para la materia de la que nos ocupamos: Según se informa en la Memoria, en 2010 se incrementaron las consultas ciudadanas y las reclamaciones –en un 56%- para solicitar ante la AEPD *"el derecho al olvido"* en Internet. Se trata de solicitudes de ciudadanos pidiendo que se cancelen sus datos en Internet, u oponiéndose a que éstos sean recuperados por buscadores. (Sobre todo se refieren a datos personales en diarios oficiales, medios digitales de comunicación y sentencias, y su indexación por parte de buscadores). El 75% de las resoluciones estimaron las reclamaciones de los ciudadanos.

6.2. Protección de la privacidad en la esfera penal

Existen dos rasgos diferenciadores de la protección penal de un bien jurídico: Por una parte, aunque al Derecho Penal de un Estado social y democrático de Derecho se le asigne una función preventiva, lo cierto es que, en concreto, actúa (o debiera hacerlo) sólo cuando ya se ha apreciado una afección (lesión o puesta en peligro relevante) al bien jurídico; es decir: el Derecho Penal actúa (debería actuar) cuando ya hay lesión del bien jurídico o está muy próxima. Por otro lado, el Derecho Penal es (debiera ser) *ultima ratio*, y sólo debiera operar ante las agresiones más graves e intolerables a los bienes jurídicos más relevantes. En la materia que nos ocupa, eso significa:

- Que con el Derecho Penal sólo se debiera intervenir cuando ya está seriamente comprometida la privacidad en alguna de sus dimensiones;

- Que sólo debiéramos acudir a este instrumento tan grave si no existe otra vía menos agresiva y aflictiva; ha de reservarse para los supuestos de mayor entidad, y siempre respetando las exigencias del principio non bis in idem, garantía irrenunciable en un Estado de Derecho. (No cabe duplicidad de castigo por el mismo hecho y con el mismo fundamento en sede penal y administrativa; en caso de procederse por la vía penal, se paralizan las actuaciones en sede administrativa hasta tanto se resuelva en sede penal).

Hechas tales advertencias, repasamos las vías de tutela de la privacidad en el orden penal. Como se ha avanzado, hasta la reforma penal de 1995 no existía en materia penal más previsión que la protección de la privacidad circunscrita a la idea clásica de intimidad (conectada a la idea del "secreto", documentado, de comunicaciones telefónicas, de imágenes privadas). Desde la reforma de 1995, adquieren también relevancia penal otras conductas que no pivotan sobre el concepto tradicional de secreto. Exponemos ahora, en resumen, las principales previsiones para la tutela penal de la privacidad, incluyendo las novedades introducidas en la reforma de 2010:

Cuestiones de carácter general sobre la protección penal:

1º Estamos ante delitos de los llamados "semipúblicos", porque se requiere denuncia de la persona agraviada o su representante legal, salvo cuando el agraviado sea menor de edad, incapaz o persona desvalida, o el delitos afecte a los intereses generales o a una pluralidad de personas, o el autor sea autoridad o funcionario público que realizare los hechos abusando de su condición.

2º La vía penal es más complicada que la protección por vía administrativa, ya que hay que demostrar ante los Tribunales que se actuó de forma dolosa, cuestión que no siempre es fácil, y, en algunos supuestos, adicionalmente, ha de quedar claro un ánimo especial en el autor (vgr: ánimo de descubrir los secretos o vulnerar la intimidad; ánimo de perjudicar; ánimo de lucrarse, elementos subjetivos del injusto adicionales al dolo, que incorporan los tipos descritos en los artículos 197 y siguientes del Código Penal). Con lo cual, si no es posible dejar constancia de ello, puede ser más eficaz la protección extrapenal.

3º La tutela penal, por lo demás, no se circunscribe a las actuaciones ilícitas de encargados y responsables de ficheros, archivos, compañías o Administraciones públicas que recaban, utilizan, tratan o transmiten información concerniente al ciudadano (aunque este carácter determina la aplicación de modalidades agravadas), sino que se orienta a la protección frente a cualquier ataque a la privacidad, incluidos los que proceden de conductas de terceros ajenos al proceso de datos.

4º Con carácter general, las penas se agravan si el autor revela o difunde los datos, imágenes o informaciones de carácter personal de otro, si negocia o trafica con esa información para lucrarse con ella, o si el contenido de la información pertenece a lo que se conoce como el "núcleo duro" de la intimidad (datos que revelen ideología, religión, creencias, salud, origen racial o vida sexual), y si la víctima es menor de edad o incapaz.

Modalidades típicas:

1º Ataques a la intimidad "documentada" en cartas, papeles, mensajes de correo electrónico y efectos personales (art. 197.1, inciso 1º CP). Aunque desde el punto de vista objetivo parece necesario el "apoderamiento" (material) del soporte, entendemos que no es preciso: primero, por la inclusión de los

mensajes de correo electrónico en el enunciado; y, segundo, porque el propio legislador emplea el verbo "apoderarse" para casos en los que basta una simple captación mental (párrafo segundo del mismo artículo). En todo caso, se precisa la actuación dolosa y, además, que se pruebe el ánimo de descubrir los secretos o vulnerar la intimidad de otro. Podría aplicarse, por ejemplo, al empleado de los Servicios Informáticos de un centro que puede acceder a las direcciones de correo institucional de los empleados del mismo, pero también al tercero extraño que ha logrado instalar un programa troyano en el ordenador de otro y accede a toda la actividad desarrollada desde el mismo.

2º Ataques a la privacidad de las telecomunicaciones: el cauce lo hallamos en el mismo número del artículo citado, que incluye, además de la interceptación de las telecomunicaciones, la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación. En el plano subjetivo, deben probarse, como en el inciso anterior, el dolo y la intención de "descubrir los secretos o vulnerar la intimidad de otro". Nótese que la aplicación de esta figura no precisa la efectiva constatación de la lesión de la intimidad (es un *delito de peligro*). Bastaría con probar que se han utilizado dichos artilugios por el autor, aunque no se pueda demostrar que en el caso concreto se agredió el bien jurídico.

3º Ataques a la privacidad de los datos de carácter personal: En el párrafo segundo del artículo 197 del Código Penal hallamos la principal innovación, en esta materia, de la reforma de 1995. Se castiga a quien, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de terceros, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado, y, en general, al que acceda sin autorización a esos datos.

4º Ataques a la privacidad mediante el acceso, por cualquier medio o procedimiento y vulnerando las medidas de seguridad, a datos o programas contenidos en un sistema informático, o mantenimiento en el mismo sin autorización. Esta redundante previsión del párrafo tercero del artículo 197 del Código Penal, ha sido incluida en la reforma que entró en vigor el pasado mes de diciembre. Aunque no es ésta la sede para ahondar en su examen, coincidimos con quienes critican el nuevo precepto, que recoge supuestos ya tipificados en el número anterior y, sorprendentemente, los castiga con menos pena, pese a incorporar una exigencia típica adicional: la vulneración de medidas de seguridad (lo que es tanto como castigar, por ejemplo, con más pena el hurto que el robo con fuerza, a menos que así pretenda premiarse al más preparado desde el punto de vista técnico, al que cuenta con medios y conocimientos para vulnerar las medidas de seguridad de equipos y sistemas informáticos; o, desde la perspectiva de la víctima, como si "penalizáramos" al más diligente y se protege frente a amenazas externas. Un error incomprensible, en cualquier caso).

5º Ataques a la privacidad por los que tienen lícitamente conocimiento de datos e información de carácter personal de otros. Existen dos vías: Primera, para actuaciones ilícitas o abusivas de los encargados o responsables de los ficheros o archivos, soportes informáticos o telemáticos (art. 197.5º CP), y segunda, para los casos de revelación de secretos ajenos conocidos por razón del oficio, relaciones laborales o actividad profesional (art. 199 CP).

6º Ataques a la privacidad desde el aparato del Estado: Como ya se ha expuesto anteriormente, una de las más graves amenazas que hoy acechan a la privacidad del ciudadano procede de las actuaciones de control y vigilancia desarrolladas desde el propio Estado (cuando no desde otros Estados). Si por razones de seguridad y para luchar contra el crimen el Estado puede servirse de programas para

rastrear todas nuestras comunicaciones, si puede acceder al disco duro de nuestro ordenador personal para conocer qué clase de archivos y material almacenamos, y hasta introducir programas espía en las computadoras de los ciudadanos a fin de conocer toda su actividad en la Red, quedan pocas esperanzas de preservar los aspectos más íntimos y personalísimos de nuestra vida. En todo caso, al menos con carácter testimonial, el Código Penal conserva una serie de previsiones para reprimir los atentados contra la intimidad y contra sus garantías constitucionales. Resumidamente, ante actuaciones ilícitas o abusivas desde el propio aparato del Estado contra la privacidad, cabría:

a) Si no media causa por delito, recurrir a las figuras apuntadas anteriormente, agravadas cuando el autor es autoridad o funcionario público que abusa de su condición (art. 198 CP).

b) Si media causa por delito, pero no se respetan las garantías constitucionales o legales de los derechos aquí en conflicto (vgr: intimidad, honor, derecho a la reserva de datos personales, derecho a la propia imagen, derecho al honor y secreto de las comunicaciones), los cauces en sede penal se hallan en los artículos 534 y siguientes del Código Penal. Ejemplos: Sin autorización judicial o superando los límites de la autorización, registro de papeles y documentos (incluidos los electrónicos), intervención de comunicaciones o utilización de artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o cualquier otra señal de comunicación, divulgación o revelación de la información obtenida, etc.

7. Reflexiones finales

En marzo de 2010, con la colaboración de varias empresas de seguridad informática, el FBI, la Policía canadiense y la Guardia Civil española, se logra desmantelar la mayor red de *bots* jamás conocida, que tenía controlados (*zombis*) casi trece millones de ordenadores en todo el mundo. En la llamada "Operación Mariposa" fueron detenidos tres jóvenes de nacionalidad española, sin grandes conocimientos en Informática, que operaban sobre todo desde España. Al parecer, infectaban los ordenadores con esos pequeños programas que permiten el control remoto del equipo sin conocimiento ni consentimiento del usuario y, después, instalaban diferentes ejemplares de *malware* (*keyloggers*, troyanos bancarios avanzados, troyanos de acceso remoto, etc.), para poder realizar más acciones desde los ordenadores zombis: obtención de información de carácter personal y económica, fraudes, blanqueo de capitales..., aunque, especialmente, el negocio lo centraban en el alquiler de ordenadores "zombis" a otros ciberdelincuentes para todo tipo de ilícitos.

Llama la atención de este caso, no sólo las cifras, la dimensión de la "red Mariposa" y los sistemas informáticos comprometidos, sino, además, que se llegó a descubrir, tras meses de investigación, por un "despiste": en un momento, uno de los implicados se confió y no ocultó debidamente su dirección IP, como hacían siempre, con lo cual ya se le pudo rastrear.

Este caso, como la noticia conocida en estos días sobre el "robo de datos de carácter personal" de 20.000 usuarios de la plataforma de formación *online* del centro de seguridad del Instituto Nacional de Tecnologías de la Comunicación (Inteco), sirven para ilustrar estas últimas reflexiones:

1º Las TICs son un magnífico e imprescindible componente de las sociedades modernas, pero no podemos desconocer que los sistemas y equipos informáticos, aun los más sofisticados, preparados y

protegidos, son altamente vulnerables. No hay sistemas absolutamente seguros, ni sitios web ni ordenadores absolutamente protegidos.

2º El ciudadano del presente siglo, sin renunciar a las múltiples ventajas de la TICs, debiera tomar conciencia de los riesgos que derivan de la actual "dependencia informática", a fin de adoptar unas medidas mínimas de protección de sus bienes e intereses. Las leyes, por sí solas, tienen poca fuerza para otorgar tutela suficiente en este ámbito: uno de los rasgos comunes de la *ciberdelincuencia* es la dificultad de su detección, prueba y persecución. La mejor protección, en cualquier caso, es la prevención, la autoprotección.

3º La *privacidad*, como compendio de bienes personalísimos vinculados a la intimidad, al honor, a la propia imagen, a la libertad de autodeterminación y, en último extremo, a la dignidad misma del sujeto, es uno de esos bienes gravemente comprometido por el uso actual de las TICs, y aún desconocemos qué consecuencias puede tener en el futuro. Deberíamos sensibilizarnos, tomar cautelas y, sobre todo, deberíamos formar a nuestros jóvenes para que aprendan a controlar su exposición en la Red: No sólo han de defenderse de acosadores y pederastas; aquí hablamos de evitar la sociedad de *ciudadanos transparentes* del mañana.

Otra nota de prensa, para terminar: Al tiempo de cerrar estas líneas, nos sorprende esta noticia en la prensa digital:

"La red de activistas *Anonymus*, en respuesta a la detención de tres de sus miembros el pasado viernes, ha atacado durante la madrugada del domingo la página web de la Policía Nacional. También atacaron la web del INEM y la del Servicio Público de Empleo Estatal. La Policía Nacional había desarticulado en fechas recientes a la cúpula de esta red de *hackers*, que controlaba un importante elenco de sistemas informáticos de organismos gubernamentales, financieros y empresariales de todo el mundo".