EL IMPACTO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN EN EL DERECHO A LA VIDA PRIVADA

Las nuevas formas de ataque a la vida privada

Désirée Barinas Ubiñas

Doctora en Derecho. Universidad del País Vasco-UPV/EHU

BARINAS UBIÑAS, Désirée. El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada. Las nuevas formas de ataque a la vida privada. *Revista Electrónica de Ciencia Penal y Criminología* (en línea). 2013, núm. 15-09, p. 09:1-09:60. Disponible en internet: http://criminet.ugr.es/recpc/15/recpc15-09.pdf
ISSN 1695-0194 [RECPC 15-09 (2013), 17 sep]

RESUMEN: Vivimos en una época en la que cada día la sociedad incorpora nuevos desarrollos tecnológicos que van transformando las interacciones sociales, económicas, políticas y culturales y redefiniendo los campos de acción del individuo. La llegada del internet y de la era digital recontextualiza las interrelaciones humanas, creando un "nuevo mundo" en el que el sentido del tiempo y el espacio muta y las limitaciones físicas parecerían desaparecer. Nos enfrentamos así a herramientas capaces de extraer información del mundo físico y ponerla a disposición de forma masiva, permanente e interconectada en un espacio virtual, donde el ser humano se vuelve generador y consumidor de información. Cabe entonces preguntarse cuál es el impacto de dichas tecnologías en los derechos y libertades del hombre, y en particular de la vida privada, derecho que se ha visto innegablemente redefinido frente a las nuevas amenazas que presentan las tecnologías de la información y de la comunicación.

PALABRAS CLAVE: Datos personales. *Data mining*. Biometría. Ciberespacio. *E-goverment*. Geolocalización. Internet. Redes sociales. Seguridad. Tecnologías de la Información y la Comunicación (TIC´s). Vida privada. Video-vigilancia.

Fecha de publicación: 17 septiembre 2013

transmisión de comunicaciones en línea. 1.1.2.3. Trazabilidad de la utilización de Internet. 1.1.2.4. El data mining y la generación de perfiles en Internet. 1.2. Las redes sociales e interactivas: una exposición voluntaria. 2. Las personas: generadores de datos. 2.1. La comercialización de la personalidad. 2.1.1. La personalización y el derecho a la privacidad. 2.1.2. El flujo trasnacional de datos. 2.1.3. La comercialización de los derechos personales. 2.2. El control estatal: ¿transparencia total? 2.2.1. El e-goverment y la creación de perfiles digitales. 2.2.2. La vigilancia estatal: una lucha entre la seguridad y la libertad.

El impacto de las tecnologías de la información y de la comunicación (TICs) en el desarrollo de la sociedad actual es innegable, jugando un rol transcendental que se manifiesta de forma transversal no tan solo en los aspectos culturales y sociales de esta, sino también en sus aspectos económicos y políticos y, en lo que aquí más interesa, también jurídicos[1].

Las TICs se están convirtiendo en un elemento nodal de la estructura socio-económica y cultural de nuestros tiempos[2], donde la información se ha transformado en un valor primario, potencializándose la colecta y manipulación de datos y la comunicación e interconexión de los mismos. Vemos cómo se generan nuevos canales de interacción social, haciendo que surja junto al mundo "físico" un mundo "virtual", cuya regulación no puede quedar fuera del amparo del Derecho[3]. Un mundo en el que las personas son representadas a través de datos y donde la generación, digitalización, disponibilidad e interconexión de la información se encuentran a la base de su estructura. Dentro de este nuevo esquema de interacción cabe preguntarse cómo quedan protegidos los derechos y libertades fundamentales y muy particularmente la vida privada por las amenazas que esto puedo suponer para ella[4]

¿Pero qué es exactamente lo que ha cambiado? ¿Cuáles son estas tecnologías "intrusivas" y cuál su impacto en el derecho a la vida privada?

1. **Del mundo físico al mundo virtual**

1.1. ***Una infraestructura tecnológica de vigilancia y trazabilidad***

En la década de los setenta ya se anunciaba el fin de la vida privada[5] frente al

[1] A este respecto Antonio-Enríquez Pérez, que destaca los riesgos así como las posibles alternativas frente a esta revolución tecnológica, entre las que señala el acuñar un nuevo concepto de intimidad, en sentido amplio. PÉREZ LUÑO (Antonio-Enríquez). *Nuevas tecnologías, sociedad y derecho: el impacto socio-jurídico de las N.T. de la información*. Colección Impactos, 1ª Ed., Madrid, Fundesco, 1987, 154 pp.

[2] Ver a CASTILLO JIMÉNEZ (Cinta). "Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información." *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, Nº 1, 2001, pp. 35-48.

[3] Ver a este respecto CLIMENT BARBERÁ (Juan). Derecho y nuevas tecnologías. 1ª Ed., Valencia, Universidad Cardenal Herrera-CEU, 2001, 70 pp.

[4] POULLET (Yves). "Data protection legislation: What is at stake for our society and democracy?" *Computer Law & Security Review,* Vol. 25, Nº 3, 2009, pp. 211-226.

[5] En este sentido, ver a URABAYEN (Miguel). *Vida privada e información: un conflicto permanente*. 1era. Ed., Pamplona, Universidad de Navarra, 1977, pp. 27-28.

desarrollo de técnicas y herramientas que hicieron posible la comunicación masiva y la vigilancia de las personas a través de dispositivos que implican una intromisión directa en el desarrollo normal de sus vidas.

El Juez William Douglas decía ya en 1966 en su voto disidente de la sentencia dada por la Suprema Corte de los Estados Unidos en el caso de *Osborn v. United States*, que "*estamos entrando rápidamente en la era en que no habrá privacidad, en la que todos estarán sujetos a vigilancia todo el tiempo, en la que no existirán secretos para el gobierno. […] Las fichas de todos los ciudadanos aumentan en número y tamaño. Ahora las están pasando a ordenadores de forma tal que por el simple gesto de apretar un botón, todos los miserables, los enfermos, los no populares y las personas de la nación que se aparten de lo uniforme puedan ser instantáneamente identificados. Estos ejemplos demuestran que por todas partes la privacidad y dignidad de nuestros ciudadanos están siendo reducidas, a veces a través de pasos imperceptibles. De forma individual, cada paso puede ser de poca importancia. Pero cuando se ve como un todo, comienza a emerger una sociedad muy diferente a cualquiera que hemos visto - una sociedad en la cual el gobierno puede entrometerse en las regiones secretas de la vida del hombre a voluntad. […]*"[6].

Nos preguntamos qué diría hoy frente a técnicas más avanzadas que permiten un seguimiento y vigilancia continua y la posibilidad incluso de controlar a las personas a través de la utilización de dispositivos biométricos[7], disponibles no sólo para el gobierno sino también para los particulares.

En 1999 Scott McNealy, cofundador de Sun Microsystems (una importante compañía del sector de las nuevas tecnologías), sería más dramático aún al decir: "*Usted tiene cero privacidad. Supérelo*"[8], para ser parafraseado en el año 2006 por Steve Rambam, un experto en privacidad e investigador privado estadounidense, quien anunció la muerte de la vida privada en una Conferencia sobre Seguridad

[6] Traducción libre de la autora: "*We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government. (...)The dossiers on all citizens mount in number and increase in size. Now they are being put on computers, so that, by pressing one button, all the miserable, the sick, the suspect, the unpopular, the off-beat people of the Nation can be instantly identified. These examples and many others demonstrate an alarming trend whereby the privacy and dignity of our citizens is being whittled away by sometimes imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen -- a society in which government may intrude into the secret regions of man's life at will*". Voto disidente del juez William Douglas. Caso *Osborn v. United States*, *385 U. S. 323, 1966.*

[7] Según la Real Academia de la Lengua Española la biometría es el "*estudio mensurativo o estadístico de los fenómenos o procesos biológicos*." Página Web www.rae.es Responsable: Real Academia Española. Este término es comúnmente utilizado hoy en día, sin embargo, para referirse a la implementación de dispositivos automáticos que miden e identifican características biológicas e intransferibles propias de las personas que permiten reconocerlas, como, por ejemplo, las huellas dactilares, el iris del ojo, la palma de la mano o la voz, entre otras.

[8] Traducción libre de la autora: "*You have zero privacy. Get over it"*. Fue una respuesta dada por el empresario en una conferencia de prensa, tal y como lo cita FROOMKIN (A. Michael). "The Death of Privacy?" *Stanford Law Review*, Vol. 52, Mayo 2000, p. 1463.

Informática en San Diego, señalando los grandes cambios que ha sufrido el manejo de las bases de datos y la capacidad para investigar y relacionar información en los últimos 10 años[9]. Una recolección y manipulación de la información que muchas veces es ignorada por la persona objeto de la misma, que incluso ha motivado que se hable en la actualidad de los "tratamientos invisibles" de datos[10].

Para entender mejor la configuración de estas nuevas tecnologías y, al mismo tiempo, comprender el modo en que afectan al derecho a la vida privada hemos separado aquellas que permiten la colecta y manipulación de datos relativos a la persona extrayéndolos del mundo "físico" y aquellas que se desarrollan únicamente en el mundo "virtual", aunque finalmente se interrelacionen unas y otras.

Esto es necesario para comprender cómo van surgiendo la confección de perfiles y la determinación de patrones de comportamiento, que van horadando las barreras de lo que representa la idea de privacidad desde una reconfiguración de la identidad y personalidad del ser humano, ahora representada, dentro de este entorno digital, a través de datos que se interconectan. Las personas, sus deseos, sus preferencias, sus acciones, sus no acciones, su propio ser dentro del entorno digital se ven transformadas en datos: en ceros y unos que navegan por las autopistas de la información y que generan ambientes que se van moldeando y condicionando por las elecciones de cada individuo, a la vez que van cerrando y creando círculos de opciones, información que no pasa desapercibida para quien tiene la capacidad de acceder a ella y la posibilidad, así, de entrar en nuestra privacidad.

1.1.1. *Las tecnologías generadoras de la información: extracción de información del mundo "físico", que se traslada al mundo "virtual"*

Inicialmente las nuevas amenazas de la sociedad de masas se identificaban con los dispositivos de escucha de conversaciones cara a cara entre las personas (que hoy día vemos vendiendo en programas de televisión como la cosa más normal del mundo), los dispositivos de interceptación telefónica, la video-vigilancia, los aparatos fotográficos (que permiten incluso tomar fotos infrarrojas y a amplias distancias), para añadirse posteriormente luego los dispositivos de seguimiento no tan sólo colocados sobre objetos (un vehículo por ejemplo, para localizarlo), sino sobre personas[11], los cuales terminan convergiendo en la digitalización de la información generada para facilitar su uso e interconexión[12].

[9] Ver RAMBAM (Steve). "Privacy Is Dead - Get Over It". *Google vídeos*. Fuente: http://video.google.com/ videoplay?docid=-3837095373845286 24# Responsable: Google.

[10] Ver a MARTÍNEZ MARTÍNEZ (Ricard). "Vida Privada e Internet". *Revista Datos Personales.* Agencia de Protección de Datos de la Comunidad de Madrid, Nº 7, Enero 2004. Fuente: http://www.datospersonales.org Responsable: Agencia de Protección de Datos de la Comunidad de Madrid.

[11] Ver a LESSIG (Lawrence). *Code: and other laws of Cyberspace*. Versión 2.0.Basic Books, New York, 2006, pp. 202-209 y a URABAYEN (Miguel). *Vida privada e información: un conflicto permanente*. 1era. Ed., Pamplona, Universidad de Navarra, 1977, pp. 27-32.

[12] TAIPALE (Kim A.). "Why can't we all get along ? How techonologie, Security and Privacy can coex-

Hoy en día el desarrollo de la tecnología ha potenciado, por una parte, el desarrollo de herramientas que permiten la recolecta masiva de información y, por otra parte, la creación de registros y su manipulación en un entorno digital en el que su interconexión y disponibilidad se ven magnificados. Se alimenta así el mundo "virtual del mundo "físico" en el que convivimos, no siempre (o casi nunca) con las debidas garantías. Destacamos, sin ánimo de exhaustividad, las siguientes manifestaciones de esta realidad.

1.1.1.1. Video-vigilancia

La video-vigilancia de las ciudades y espacios públicos ha sido una medida implementada por varios gobiernos para prevenir y perseguir la criminalidad, fungiendo como una vía "no intrusiva" de control social, sobre todo en los espacios urbanos[13] y siendo utilizada también por las entidades privadas para garantizar la seguridad de sus instalaciones[14].

Un perfecto ejemplo de esto es Londres, conocida por ser, si no la ciudad más video-vigilada, una de ellas, con un millón de cámaras instaladas en sus calles, que filman, en promedio, unas 300 veces al día a un ciudadano[15]. Sin embargo, no ha sido probada la efectividad de una medida fuertemente criticada por su costo y el detrimento a la vida privada que representa[16].

A esta tendencia se han sumado no sólo países europeos, como España y Francia, al margen por supuesto de Estados Unidos, sino cada vez en mayor medida también países latinoamericanos[17].

ist in the Digital Age", *Cybercrime: digital cops in a networked environment*. 1ª Ed., New York, New York University Press, 2006, pp. 151-183.

[13] SADIN (Éric). *Surveillance globale.* 1ª Ed., Paris, Climats, 2009, pp. 62-63.

[14] La misma ha proliferado en los últimos años bajo el discurso de la seguridad. Un ejemplo de ello es Francia, donde la CNIL señala en su 29º informe que percibió una duplicación de estos dispositivos, que a su vez resultó en un aumento de las quejas por su uso de un 43%, suscitando inseguridad jurídica en los ciudadanos, sobre todo por aquellos colocados en los lugares de trabajo o por copropietarios y vecinos. Ver CNIL. *29e Rapport d'activité 2008,* pp. 23-26.

Fuente: http://lesrapports.ladocumentationfrancaise.fr/BRP/094000211/0000.pdf Responsable: CNIL.

[15] La densidad es la mayor de Reino Unido, que cuenta con unos 4 millones de cámaras instaladas. SAENZ (Aaron). "London's Surveillance Fails – Only 1 Crime Solved per 1000 Cameras". *Singularity hub*, 1ero Septiembre 2009. Fuente: http://singularityhub.com/2009/09/01/londons-surveillance-fails-only-1-crime-solved-per-1000-cameras/ Responsable: *Singularity hub.*

[16] Claude Marie Vadrot resalta la falta de pruebas sobre su efectividad. Ver VADROT (Claude-Marie). *La grande surveillance, caméras, ADN, portables, Internet…* 1ª Ed., Paris, Éditions du Seuil, 2007, pp. 30-39; 48-54. Ver a este respecto también BOWCOTT (Owen). "CCTV boom has failed to slash crime, say police ". *The Guardian*, 6 mayo 2008. Fuente: http://www.guardian.co.uk/uk/2008/may/06/ukcrime1 Responsable: The guardian y SAENZ (Aaron). "London's Surveillance Fails – Only 1 Crime Solved per 1000 Cameras". *Singularity hub*, 1ero Septiembre 2009.

Fuente: http://singularityhub.com/2009/09/01/londons-surveillance-fails-only-1-crime-solved-per-1000-cameras/. Responsable: Singularity hub.

[17] Así, por ejemplo, se anuncia en República Dominicana la instalación de 400 cámaras para mantener la vigilancia en zonas neurálgicas del casco urbano de la capital. Véase APOLINAR (Bethania). "Cámaras filmarán actos delictivos en la capital". *Listín Diario*, 28 Febrero 2011. Fuente: http://www.listin.com.do/la-republica/2011/2/28/179277/Camaras-filmaran-actos-delictivos-en-la-capital Responsable: Listín Diario.

Inicialmente analógica y ahora digital[18] la tecnología de la vigilancia ha dado pasos significativos que van desde la capacidad de observar a distancia y la reducción del tamaño de los aparatos, que se vuelven imperceptibles para las personas, hasta la incorporación de cámaras que hablan y permiten "llamar al orden a los ciudadanos". Un proyecto, instalado en Middlesbourgh desde 2007, ha incorporado esta última tecnología, apoyada por el gobierno británico, que busca extenderla a otras ciudades[19]. En el mismo se involucró a menores para que propusieran los mejores textos pregrabados: "[…] *el gobierno incentiva a los niños a enviar un mensaje a los adultos: si no actúa correctamente, será confrontado a la vergüenza de ser denunciado públicamente*"[20], se diría, en un estilo de tintes orwellianos.

La precognición de los actos, el "escaneo" permanente de todos los individuos y su reconocimiento facial están a la puerta de entrada. Caminamos hacia una tecnología que permite de forma automática que los sistemas de video-vigilancia denuncien comportamientos "sospechosos" y "caras" sospechosas, para llegar a anticipar incluso las reacciones "potencialmente peligrosas", desarrollándose también el video en tres dimensiones, que permitirá una mejor identificación de los individuos cuyas imágenes han sido capturadas[21]. Pero, falta por definir qué es un comportamiento y un rostro "sospechoso": ¿un extranjero?, ¿la persona friolera muy vestida para la estación del año?, ¿cualquier persona que no sea "normal"?, ¿normal para quién? La discriminación se encuentra latente en el principio mismo que la justifica: ¿somos ahora todos sospechosos?, ¿dónde quedó la presunción de inocencia?, ¿la intención dolosa queda reducida a un algoritmo informático?, ¿dónde quedó el derecho del acto y elemento material de la infracción? Pasamos así de una vigilancia reactiva a otra proactiva, en la que no sólo somos constantemente observados, sino, al mismo tiempo, comparados con un patrón "socialmente aceptable", en el que hay que encajar dentro de un grupo predefinido[22]. ¿Dónde quedó el libre desarrollo de la persona?, ¿el derecho a ser diferente?, ¿el derecho a la pluralidad?, ¿el derecho a la libertad? … ¿el derecho a la privacidad? No lo sabemos. El balance entre la seguridad y la privacidad como fundamento de la libertad individual se tambalea.

[18] Fanny Coudert señala la problemática que surge al digitalizar e interconectar las informaciones y cómo se diluyen el derecho a la transparencia y la finalidad con que fueron recolectadas. Ver COUDERT (Fanny). "Towards a new generation of CCTV networks: Erosion of data protection safeguards?" *Computer Law & Security Review*, Vol. 25, Nº 2, 2009, pp. 145-154.

[19] HOME OFFICE (UK). "Talking CCTV brings voice of authority to the street". *The National Archives*, 4 de abril 2007. Fuente: http://webarchive.nationalarchives.gov.uk/+/http://www.homeoffice.gov.uk/about-us/news/talking-cctv Responsable: Home Office. (*The Home Office* es, como se sabe, el Departamento del gobierno británico responsable de la inmigración y los pasaportes, de las políticas sobre drogas y de los crímenes, anti-terrorismo y la policía).

[20] Comentario del ministro de interior John Reid citado por VADROT (Claude-Marie). *Op. Cit.* p. 28.

[21] Ver a SADIN (Éric). *Op. Cit*. pp. 87-94 y a VADROT (Claude-Marie). *Op. Cit.* pp. 42-47.

[22] Ver a COUDERT (Fanny). "When video cameras watch and screen: Privacy implications of pattern recognition technologies". *Computer Law & Security Review,* Vol. 26, Nº 4, 2010, pp. 377-384.

Esto sin hablar del posible uso de estas tecnologías para la realización de estudios sobre el comportamiento humano, con los objetivos más diversos, y la identificación de las preferencias de las personas, tanto para fines gubernamentales como comerciales[23].

No se puede dejar tampoco fuera del debate la video-vigilancia privada en centros comerciales, escuelas, tiendas, empresas y espacios "privados" controlada por particulares, así como la posibilidad de ser grabado en cualquier momento por cualquier persona con una cámara de video integrada en su celular que facilita la captación de imágenes a escala masiva de los hechos de los cuales son testigos y que frecuentemente termina en el Internet[24]. Esta problemática se extiende al plano laboral, en el control habitual de los empleados[25].

Y junto a la posibilidad generalizada de adquisición de cámaras de video conectadas a la Web, nos enfrentamos también a la captación de imágenes por particulares de la vía pública[26] y de lugares incluso que debieran considerarse privados con las posibilidades de una amplia difusión, sin que necesariamente se legitimen su fin ni se tomen las medidas pertinentes para controlar su divulgación. Por eso se dice que ahora ya también al lado del "*Big brother*" se encuentran los "*Little brothers*"[27].

En relación con ello, el Grupo del Artículo 29[28] señaló las problemáticas que se plantean a todo este respecto en un documento de trabajo relativo al tratamiento de datos personales mediante vigilancia por videocámara, destacando que "*si bien la vigilancia por videocámara parece estar en cierto modo justificada en determinadas circunstancias, también se dan casos en los que se recurre a la protección mediante videocámaras de manera impulsiva, sin considerar adecuadamente los*

[23] Ver a este respecto a FROOMKIN (A. Michael). *Op. Cit.* pp. 1477-1479.

[24] También se propugna que la video-vigilancia lleva a la "auto vigilancia" o "*sousvelliance*". Ver a GLOVER (Barbara), OWEN (Eric) y STORM (Paula). "15th Conference on Computers, Freedom and Privacy: Panopticon". *Library Hi Tech News* , Vol. 22, Nº 8, pp. 4-8.

[25] Ver a MARTÍNEZ MARTÍNEZ (Ricard). "Vida privada en Internet (II). La monitorización informática". *Revista Datos Personales*. Agencia de Protección de Datos de la Comunidad de Madrid, Nº 8, Marzo 2004. Fuente: http://www.datospersonales.org Responsable: Agencia de Protección de Datos de la Comunidad de Madrid.

[26] Esta problemática fue trata por el Agencia de Protección de Datos Española e incluso por la CNIL quienes sostienen posiciones similares al establecer que la vigilancia de las áreas públicas debe limitarse al Estado. Ver AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Inspección Sectorial de Oficio-Videocámaras en Internet*. Junio 2009, 30 pp. Fuente:
https://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/dfs/plan_sectorial_camaras_internet_2009.pdf Responsable: Agencia Española de Protección de Datos y CNIL.

[27] Como es conocido, la alusión al "*Big brother"* es la metáfora utilizada, haciendo referencia al libro 1984 de Orwell, a la vigilancia absoluta de los gobiernos, que elimina toda privacidad, característica de sistemas totalitarios y represivos; la expresión *"Little brothers"* haría referencia entonces a la amenaza a la privacidad que representan las bases de datos del sector privado. Ver a este respecto a SOLOVE (Daniel). *The digital person.* 1era. Ed., New York, New York University Press, 2004, p. 32.

[28] El Grupo del Artículo 29 sobre la protección de datos personales fue creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995. Es un órgano comunitario independiente y de carácter consultivo sobre la protección de los datos y la intimidad.

requisitos y medidas pertinentes" [29].

1.1.1.2. Geo-localización

Inicialmente diseñado con fines militares para luego ser abierto a la sociedad civil el GPS (*Global Positioning System*)[30] resulta hoy en día una herramienta de navegación y localización masivamente implementada en áreas que van desde la aeronáutica, las telecomunicaciones, la explotación minera y los sistema de respuesta a emergencias, hasta el transporte ferroviario, marítimo y automovilístico, siendo utilizado para fines cuyos creadores nunca imaginaron[31].

Este sistema, si bien no es perfecto[32], permite localizar a una persona u objeto con una margen de error de entre 30 y 50 metros (para fines civiles) [33], en cualquier parte del mundo, y seguir y registrar todos sus desplazamientos. Las fronteras físicas desaparecen en el posicionamiento global de un "objetivo".

El GPS ha encontrado su contrapartida rusa en el GLONASS[34] y europea en GALILEO, que todavía no está en uso y que ha sido diseñado, como alternativa al sistema estadounidense, para ofrecer servicios civiles[35].

Si bien puede resultar extremadamente efectivo y recomendable a fin de facilitar la búsqueda en casos de emergencia, los usos comerciales que se plantean no siempre son los más sanos para la vida privada. Así, las empresas lo colocan en los vehículos asignados a sus empleados para tener un control total sobre sus desplazamientos y se ha propuesto la utilización de los datos colectados por las compañías de seguros para monitorear la conducta de sus clientes[36].

Otro punto a resaltar es el de la telefonía móvil, que tiene la capacidad de ubicar en todo momento los celulares que operan bajo su servicio, comenzando a abrirse

[29] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *WP 67 Documento de trabajo relativo al tratamiento de datos personales mediante vigilancia por videocámara*. Bruselas, Adoptado el día 25 de noviembre de 2002, p. 3.

[30] Este no es el único medio de geo-localizar un objeto (y a la persona que lo utiliza), pero sí el más conocido. Existen, no obstante tecnologías paralelas e igualmente efectivas. John Lever señala, citando a Hoshen y a Koshima, la existencia de localizadores basados en 6 tipos diferentes de tecnología: sistemas de señales de direccionamiento, señales de tiempo de llegada, GPS, Servidores que se asisten del GPS, intensificadores de señales y ubicación de huellas. Ver LEVER (John A.). "Unintended consequences of the Global Positioning System*". Systems Engineering*, Vol. 7, Nº 3, 2004. pp. 219-220. Asimismo, Paul Schwartz señala los chips portables, en especial el wOzNet que utiliza la información del GPS. SCHWARTZ (Paul M.). "Property, Privacy, and Personal Data". *Harvard Law Review*, Vol.117, Nº 7, 2004, pp. 2062-2064.

[31] LEVER (John A.). *Op. Cit.* pp. 217-228.

[32] Ver a este respecto SADIN (Éric). *Op. Cit.* pp. 39-60.

[33] *Ibídem,* p. 219.

[34] Para mayor información ver la página oficial del GLONASS: www.glonass-ianc.rsa.ru

[35] Para más información sobre éste sistema de navegación satelital ver la página web de la Agencia Espacial Europea sobre Galileo y de la Comisión Europea sobre Galileo, www.esa.int/esaNA/galileo.html y http://ec.europa.eu/enterprise/policies/satnav/galileo/index_en.htm

[36] La CNIL, en Francia, ha exteriorizado una especial preocupación sobre la utilización de geo-localizadores en los vehículos de particulares proponiendo una desconexión voluntaria en todo momento y restricciones para la transmisión de los datos. Ver CNIL. *30e Rapport d'activité, 2009*. pp. 80-81. Fuente: http://www.cnil.fr/fileadmin/documents/ La_CNIL/publications/CNIL-30erapport_2009.pdf Responsable: Commission Nationale de l'Informatique et des Libertés.

todo un mercado para los servicios de telecomunicaciones basados en la localización[37]. Los celulares comunican constantemente su ubicación a fin de poder dar continuidad a la señal y poder conectarse, lo que genera una trazabilidad constante del individuo que lo lleva. Una vez almacenada esta data se potencializa el daño que puede producir a la vida privada, al poderse reconstruir cada movimiento realizado.

1.1.1.3. Biometría

La biometría permite identificar y autentificar de manera inequívoca a una persona a través de sus características corporales y fisiológicas, que lo hacen único, creciendo exponencialmente su utilización para controlar la entrada en zonas físicas y virtuales.

Encontramos así tecnologías que miden aspectos físicos y fisiológicos de una persona como el reconocimiento del iris, la retina, las huellas dactilares, el ADN, la voz, el olor corporal, las manos, las venas, el rostro y otros, que permiten utilizar el cuerpo como un "pasaporte"[38].

Asimismo, se ha desarrollado también la biometría del comportamiento, que consiste en analizar y reconocer gestos, como la dinámica de la firma o de digitar en un teclado o la forma de caminar[39], para la autentificación de una persona[40].

Actualmente, los dispositivos biométricos diseñados permiten la identificación y autentificación de la persona, sea a través del análisis directo de una parte del cuerpo o de características que se comparan contra una base de datos, sea a través de un dispositivo que contiene las características de la persona (una tarjeta por ejemplo) que las compara con una base de datos centralizada o descentralizada[41]. Este último es el caso de los documentos de identificación biométricos, como el pasaporte o la cédula de identidad, recientemente implementados y cuya imposición es progresiva[42].

Los datos así generados se encuentran ligados a la persona de forma permanente: al formar parte de ella no pueden nunca ser cambiados, a la vez que proveen, sobre todos los relacionados con el ADN, información sobre el sujeto referida a su raza, sexo,

[37] MCGILLIGAN (Robin) y ROWE (Heather). "Location technology and data protection". *Computer Law & Security Report*, Vol. 17, Nº 5, 2001, pp. 333-335.

[38] Sobre los diferentes tipos de tecnologías biométricas, ver GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *WP 80 Documento de trabajo sobre biometría.* Bruselas, Adoptado 1 Agosto 2003. pp. 3-4.

[39] *Ibídem.*

[40] SADIN (Éric). *Op. Cit*, pp. 170-171.

[41] Ver a GRIJPINK (Jan). "Privacy Law: Biometrics and privacy". *Computer Law & Security Report*, Vol. 17, Nº 3, 1 2001, pp. 154-160 y a SADIN (Éric). *Op. Cit*, pp. p. 69.

[42] El Grupo del Artículo 29 señala el riesgo de la creación de una base de datos centralizada nacional y europea de todos los ciudadanos que habitan en Europa, frente a la generalización de su uso. Ver GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. "Dictamen 3/2005, sobre la aplicación del Reglamento (CE) Nº 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros". *Diario Oficial* L 385, 29 de diciembre 2004, pp. 1 -6.

propensión a enfermedades, etnia e incluso estados anímicos[43], revelando aspectos sensibles que, en su caso, pueden generar discriminación. Los datos biométricos son universales (pues todos los generamos), permanentes (al medir características inherentes de nuestro cuerpo que no podemos cambiar) y únicos de cada persona[44] y el planteamiento de cambios de identidad que algunos sugieren como medida para proteger la privacidad se ve disminuido frente a los dispositivos biométricos.

En muchos países la autoridad pública colecta ya hoy el ADN de forma compulsiva como parte de su sistema de control social, dentro de sus políticas para la prevención del crimen, generando bases de datos irrefutables[45].

Y si hasta ahora la recolección y manipulación de datos biométricos se limitaba a fines legales (investigaciones criminales[46]), hoy en día se generaliza su uso implementándose dispositivos biométricos a fin de controlar la entrada en el trabajo e incluso en la cantina escolar[47], las bibliotecas o para acceder a un ordenador, siendo ya comunes las *laptops* que integran un reconocimiento dactilar[48].

El Grupo del Artículo 29 plantea una interesante reflexión sobre la insensibilización generalizada que la introducción de la biometría en la vida

[43] FROOMKIN (A. Michael). *Op. Cit.* pp. 1494-1496.

[44] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *WP 80 Documento de trabajo sobre biometría.*Bruselas, Adoptado 1 Agosto 2003, p. 3.

[45] Ver a este respecto a FROOMKIN (A. Michael). *Op. Cit.* pp. 1494-1496 y a VADROT (Claude-Marie).*Op. Cit.* pp. 55-58.

[46] Considerada como una prueba pericial, las pruebas biométricas se incorporan en investigaciones criminales a fin de determinar los perfiles genéticos de los posibles involucrados, hablándose incluso de una "criminalística biológica". Es bueno destacar que en el plano civil la prueba de ADN es utilizada con un 99,9% de certeza en procesos de paternidad. Si bien tradicionalmente no se considera la toma compulsiva del ADN como un atentado a la intimidad corporal, si se considera una injerencia a la intimidad personal. Ver a este respecto FERNÁNDEZ ÁLVAREZ (Belén María). "El ADN desde una perspectiva penal". *Noticias Jurídicas,* Diciembre 2006. Fuente: http://noticias.juridicas.com/articulos/55-Derecho%20Penal/200612-11156578461200.html Responsable: Noticias Jurídicas, y LÓPEZ-FRAGOSO ÁLVAREX (Tomás). "Las pruebas biológicas en el proceso penal. Consideraciones sobre la identificación por el ADN". *Derecho y Salud*, Vol. 3, Enero-Diciembre 1995, pp. 225-234. Ver también, sobre la protección particular del genoma humano el Convenio Europeo sobre los Derechos Humanos y la Biomedicina, de Oviedo (Asturias), de 4 de abril de 1997 y la Declaración Universal sobre el Genoma Humano y los Derechos Humanos, aprobada el día 11 de noviembre de 1997 en la 29ª Conferencia General de la UNESCO.

[47] A este respecto, algunas autoridades europeas han rechazado la utilización de la tecnología biométrica por no considerarla proporcionada. Es el caso de la CNIL francesa para las cantinas escolares y la AEPD para el uso de la huella dactilar para prestar un servicio comercial a los clientes. Ver CNL. *La CNIL dit non aux empreintes digitales pour la biométrie dans les écoles.* Article, 25 septiembre 2008. Fuente: http://www.cnil.fr/la-cnil/actu-cnil/article/article/la-cnil-dit-non-aux-empreintes-digitales-pour-la-biometrie-dans-les-ecoles/ Responsable: Commission Nationale de l'Informatique et des Libertés, así como AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Informe 0082/2010*. Fuente:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2010-0082_Creaci-oo-n-de-una-base-de-datos-a-trav-ee-s-de-la-huella-dactilar-queda-sometido-a-la-LOPD-y-es-desproporcionado.pdf Responsable: Agencia Española de Protección de Datos.

[48] En un estudio sobre la biometría y la privacidad de Australia, Yue Liu expuso el peligro de la utilización para fines secundarios de la biometría recolectando datos privados relativos a las propensiones y salud del individuo que muchas veces el mismo desconoce, así como sobre la utilización innecesaria de la misma, problemáticas comunes al uso de esta tecnología. Ver LIU (Yue). "Privacy regulations on biometrics in Australia". *Computer Law & Security Review*, Vol. 26, Nº 4, 2010, pp. 355-367.

cotidiana puede tener en la actual y en futuras generaciones, así como sobre el hecho de que es muy fácil colectar estas informaciones sin el consentimiento de la persona, pues son datos que "generamos" y "exponemos" constantemente[49].

Hay quien defiende la utilización "anónima" de estos datos, que serían revelados sólo a la autoridad competente en cada momento[50]. Pero, ¿qué de anónima tiene la recolección de datos únicos y permanentes de una persona? Si lo que se busca es anonimidad ¿no existe una forma más proporcionada y menos intrusiva de garantizar la misma?, ¿no es la identificación y autentificación o verificación inequívoca lo que se busca con la recolección de datos biométricos?

1.1.1.4. Traspasando las barreras de los sentidos

A diferencia de otras tecnologías, en principio, hay algunas que no buscan ser utilizadas en la vida diaria de una persona, sino obtener información puntual de una forma no "intrusiva". Hablamos aquí del monitoreo a través de imágenes satelitales, de visores que permiten ver a través de las paredes, de escáneres corporales y del llamado "polvo inteligente" que integra en partículas potentes sensores tan pequeños que los hacen capaces de volar con el viento y transmitir información[51]. Evidentemente, algo que las caracteriza es el desconocimiento de la persona sobre los datos que se recolectan, al poderse sentir aparentemente protegida en su privacidad por barreras "físicas".

Un gran debate se ha suscitado con la idea de integrar los escáneres corporales como medida de seguridad rutinaria en los aeropuertos[52], lo que llevó al Grupo del Artículo 29 a responder una consulta sobre el tema, que no dejó de ser vaga, condicionando su "aceptabilidad" a su "necesidad"[53]. Siendo el respeto de la integridad física de una persona un componente indiscutible de la dignidad humana y la exposición de su cuerpo uno de los valores más específicos de su privacidad, nos queda por ver qué se entenderá por "necesario" o "proporcionado". Aceptamos ya el escaneo y la revisión de nuestros objetos personales como medida rutinaria de seguridad, pero ¿aceptaremos ahora la exposición de nuestros cuerpos?

1.1.1.5. Monitoreando las cosas y las personas: la RFID y la nanotecnología

[49] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *WP 80 Documento de trabajo sobre biometría*. *Op. Cit*.

[50] GRIJPINK (Jan). *Op. Cit.*

[51] FROOMKIN (A. Michael). *Op. Cit.* pp. 1496-1501.

[52] El mismo se encuentra a prueba en algunos aeropuertos, como los de Hamburgo y Manchester, en los que no es "obligatorio" en este periodo de "prueba". Ver AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID. "El aeropuerto de Hamburgo instala un escáner de cuerpo entero". *Revista Datos Personales*. Agencia de Protección de Datos de la Comunidad de Madrid, Nº 48, Noviembre 2010. Fuente: http://www.datospersonales.org Responsable: Agencia de Protección de Datos de la Comunidad de Madrid.

[53] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *Consultation: The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection.* Adoptado 11 Febrero 2009, 15 pp.

La tecnología llamada RFID (*Radio Frequency Identification*) consiste básicamente en un *tag* (etiqueta) que emite datos a requerimiento de un lector a distancia[54] con la finalidad de conectarlos con lo que se ha denominado "el Internet de las cosas", es decir la creación de una red de información que controle el intercambio de productos, las condiciones de almacenamiento y preservación de los mismos[55] y su reutilización[56], permitiendo la gestión del inventario, así como la trazabilidad de su "vida útil". Lo que se propone en la actualidad es la utilización de estas "etiquetas" en el control del transporte, en la identificación de los equipajes y tarjetas de embarque a fin de localizar a los pasajeros que estén retrasados, así como para el monitoreo de medicamentos (que pueden ser relacionados con los pacientes), el suministro de información médica o el control de acceso y la gestión de cualquier tipo de producto[57].

Esta tecnología es, por otra parte, utilizada desde hace años en los animales domésticos (etiquetas inyectadas e incorporadas a las mascotas)[58]. Y lo que plantea ahora este "*Verichip*", inicialmente implantado sobre animales, es su posibilidad como medio de identificación de las personas para suministrar información sobre ellas y gestionar su interacción con el mundo externo[59], promocionándose como un medio de guardar y suministrar datos médicos, como un medio de localizar a las personas en cualquier parte de un inmueble (no sólo como control de acceso) e incluso como un sustituto de las tarjetas de crédito[60]. Así, pasamos del Internet de

[54]El análisis del G29 identifica *tag* activos y pasivos, teniendo los primeros energía propia y pudiendo emitir información a requerimiento o no de un lector (lo que disminuye su vida útil) mientras los segundos no poseen energía propia y se activan únicamente a requerimiento de un lector. Un trabajo interesante que explica y describe esta tecnología es la Guía sobre seguridad y privacidad de la tecnología RFID de la AEPD que agrega a esta clasificación los *tag* o etiquetas "semi-pasivas", explicando su uso y aplicaciones. Ver GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. WP 105 *Document de travail sur les questions de protection des données liées à la technologie RFID* (radio-identification). Adoptado 19 enero 2005, pp. 3-4 y AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Guía sobre seguridad y privacidad de la tecnología RFID, Mayo 2010, 49 pp. Fuente:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/julio/Guia_RFID.pdf Responsable: Agencia Española de Protección de Datos.

[55]Se plantea, por ejemplo, que cuando un producto se encuentre en el límite de inventario establecido automáticamente se generen órdenes de compra del mismo o que cuando se compre en el supermercado, automáticamente los productos que hayan sido seleccionados se carguen a la cuenta de usuario del cliente (lo que a su vez es controlado a fines de inventario) e incluso que la ropa se "comunique" con la lavadora para indicarle las condiciones de lavado. Ver a este respecto a SADIN (Éric). *Op. Cit*, pp. 187-194.

[56] WEBER (Rolf H.). "Internet of Things – New security and privacy challenges". *Computer Law & Security Review*, Vol. 26, Nº 1, 2010, pp. 23-30.

[57] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *WP 105 Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification). Op. Cit.* pp. 4-6.

[58] VADROT (Claude-Marie). *Op. Cit.* pp. 15-17.

[59] SADIN (Éric). *Op. Cit.* pp. 194-200.

[60] Las medidas del *Verichip* son 1 cm de largo por 2 mm de diámetro y se inserta en el cuerpo humano. En la página Ciberhabitat del gobierno mexicano se ofrece información del Director Comercial del Grupo SOLUSAT, sobre esta tectología, quien indica que a futuro se propone para sustituir documentos oficiales como "*la visa, pasaportes, credenciales de acceso, credenciales de seguros médicos, etc., ya que en un mismo dispositivo se pueden manejar diferentes bases de datos, inclusive con imágenes y fotografías del*

las cosas al "Internet de las personas".

Estos *tag* pueden contener informaciones esenciales sobre un objeto, animal o persona y colectar información sobre ellos, permitiendo su monitoreo[61]. Y aunque, como bien señala Éric Sadin, pronto nuestra vida privada se transformará en un derecho a la "desconexión"[62], ésta es algo no contemplado por esta tecnología, en la que los *tag* suministran información a requerimiento de un lector y cuyo tamaño y ubicación en el interior del cuerpo humano y de cualquier otro objeto no hace posible su fácil manipulación.

El Grupo del Artículo 29 exterioriza su preocupación en la interconexión de los datos colectados, de las cosas y las personas, que permite la creación de perfiles de consumo, hábitos y comportamientos, así como el acceso a información privada y sensible (por ejemplo datos de salud), prácticamente accesibles a cualquier establecimiento que posea un lector adecuado[63].

Más que una visión orwelliana de la sociedad, estamos enfrentándonos a una panóptica[64] donde desaparecen las barreras entre los espacios públicos y privados, ante la posibilidad de ser observados de forma permanente, y dónde el anonimato difícilmente es posible.

No podemos continuar sin destacar que las evoluciones tecnológicas avanzan a pasos agigantados y en direcciones no imaginadas que parecerían obtenidas de novelas de ciencia ficción. Si hoy en día ya es posible que un ser humano controle un robot a través un dispositivo instalado en el cerebro[65], ¿quién nos dice que el próximo paso no será controlar al cerebro humano, máxime cuando ya hablamos de cerebros bio-digitales y de interfaces computarizadas del cerebro (*Brain-computer interface*)[66]? Habremos entonces cruzado una nueva frontera y ya no se tratará del control sobre nuestra información y la forma en que ella puede ser utilizada para clasificarnos, discriminarnos, manipularnos o controlarnos, sino del de la libertad

portador" especificándose que "*la próxima generación de Verichip, podrá funcionar como biosensor, al medir la temperatura o pulso de una persona y registrar sus variaciones*". GALVAN ALCANTARA (Sergio). *VeriChip, Tecnología para la identificación de personas*. Marzo 2006. Fuente: http://www.ciberhabitat.gob.mx/hospital/verichip/ Responsable: Instituto Nacional de Estadística y Geografía (México).

[61] Ver sobre las problemáticas particulares de los RFID frente a la protección de la privacidad a DE HERT (Paul), GUTWIRTH (Serge), MOSCIBRODA (Anna), *et-al*. "Legal safeguards for privacy and data protection in ambient intelligence". *Personal and Ubiquitous Computing*, Vol. 13, Nº 6, 2009, pp. 435-444.

[62] SADIN (Éric). *Op. Cit*. p. 192.

[63] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *WP 105 Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification). Op. Cit*. 24 pp.

[64] En el concepto desarrollado por Jeremy Bentham en 1971, la casa de inspección o panóptico responde a una arquitectura que permite una vigilancia constante de sus residentes sin que éstos sepan si están siendo observados o no, permaneciendo los vigilantes ocultos. Ver a este respecto a CAS (Johann). "Computación ubicua, privacidad y protección de datos: opciones y limitaciones para reconciliar contradicciones sin precedentes". *Revista Española de Protección de Datos*. Agencia de Protección de Datos de la Comunidad de Madrid-Thomson Civitas, Nº 6, Enero-Junio 2009, pp. 80-81.

[65] VADROT (Claude-Marie).*Op. Cit.* pp. 120-121.

[66] Ver sobre este tema a BIRBAUMER (Niels). "Breaking the silence: Brain–computer interfaces (BCI) for communication and motor control". *Psychophysiology*, Nº 43, 2006, pp. 517–532.

de nuestros pensamientos y decisiones en lo más interno de nuestro ser.

1.1.1.6. "Carnetización" y registro: ¿todos fichados?

Si bien es cierto que estas tecnologías de gran impacto dan un salto cuántico en la capacidad de personalizar y recolectar información sensible sobre un individuo, también es cierto que muchas de las informaciones y registros que se colectan hoy en día y alimentan las grandes bases de datos estatales y privadas no necesitan un componente tecnológico muy sofisticado[67]. Por ejemplo, una base de datos de una pizzería donde se almacenan, no sólo las preferencias en la comida, la cantidad y la frecuencia con que consume, sino también la dirección, teléfono y número de tarjeta de crédito (si paga con ella, lo cual es común) de los clientes, como mínimo. Datos que deben ser confiables, ya que aquellos quieren que les llegue la pizza. Y lo mismo ocurre con todos los productos y servicios propuestos a domicilio en general (farmacias, restaurantes, supermercados, entre otros) así como aquellos que implican una "afiliación", como los centros de alquiler de vídeos o clubes de cualquier tipo. De hecho, en la actualidad es común que cuando se acude por primera vez a una tienda y se compra algo le pidan a la persona "su nombre y apellido, número de teléfono y zona donde habita" para "incluirla en nuestra lista de clientes frecuentes" y recibir un trato "VIP", solicitándose incluso en ocasiones el número de identificación (carnet de identidad, pasaporte, etc.) "porque hay que reportar los impuestos con su número de comprobante fiscal y la factura lo requiere".

Para todo ello no se necesita más que un ordenador y un manejador de base de datos, tan básico como cualquier propuesta estándar del mercado, o un *software* propietario a fin de llenar las necesidades de la entidad y manejar las características particulares de los servicios y/o productos ofrecidos.

Esto sin contar que cada movimiento realizado con nuestra tarjeta de crédito y débito es registrado, generándose un "perfil" de uso del usuario que "algunos" agradecen al recibir una llamada a media noche preguntando si retiró una "x" cantidad de dinero de un cajero nunca usado por el cliente o por haberse realizado consumos que no encajan en el "comportamiento habitual" y que podrían ser un fraude. Hay toda una dimensión que no ve el cliente y es la construcción de un perfil y de una etiqueta para la persona, que puede ser la razón por la que nunca le den un crédito, un préstamo o un trabajo o por la que, desde otra óptica, reciba nuevas ofertas de productos y servicios[68].

Asimismo, hoy día asistimos a la "carnetización" del individuo, sobre todo en los países desarrollados, donde se generan tarjetas capaces identificarnos y trazar nuestros movimientos: como las de transporte personal, transporte de vehículos

[67] FROOMKIN (A. Michael). *Op. Cit.* p. 1472.
[68] *Ibídem*, pp. 1474-1476.

(dispositivos incorporados a los vehículos que transitan por vías de pago), de salud, para entrar a la empresa (si es que no hay incluso que poner la huella digital), para acceder a las bibliotecas, para acceder al parqueo del trabajo o de la universidad, para almorzar, para comprar en determinados centros comerciales, sin hablar, por supuesto, de los documentos de identidad y pasaportes biométricos[69], transparentando el círculo de interacción y preferencias humanas.

La información termina siendo digitalizada e incorporada a las autopistas de la información. Y, al final, todo se transforma en datos: ¡ceros y unos!

1.1.2. *La infraestructura del ciberespacio: una gran base de datos interconectados*

La llegada de la era digital revoluciona la forma en que es manejada la información frente a la posibilidad ilimitada que nos dan tanto su manipulación electrónica como Internet, que lo que agrega el componente de un acceso sin fronteras y permanente en el que se pierde la noción de espacio y tiempo[70]. Esto permite una mayor recolección de datos, su conservación automática y su interconexión, así como la posibilidad de convergencia de todas las informaciones recolectadas, de fácil manipulación.

Internet[71] constituye en sí mismo una gran base de datos disponible en línea y el canal por excelencia de la comunicación electrónica[72]. El mismo tiene su origen, como es sabido, en el ARPANET (*Advanced Reasearch Project Agency*), creado por el Departamento de Defensa de los Estados Unidos, que tenía por finalidad inicial establecer un nuevo medio de comunicación descentralizado capaz de funcionar incluso cuando uno de los canales fuera destruido. Inicialmente fue creada para transmitir correos electrónicos, siendo revolucionada al crearse en 1973 un protocolo capaz de transmitir paquetes de información que permiten

[69] Sobre la identificación y autentificación de las personas ver a CLARKE (Roger) y SMITH (Anita). "Privacy in electronic media: identification, authentication and anonymity in a legal context". *Computer Law & Security Review*, Vol. 16, Nº 2, 2000, pp. 95-100.

[70] Justamente uno de los mayores retos que presenta la regulación de Internet es su carácter trasnacional. Ver BAZURO (Andrea) y SAGARRA (Eduard). "Internet: la necesidad de soluciones transnacionales y de una regulación específica. La inadecuación de una visión parcial de los problemas." *Revista de la contratación electrónica,* Nº 21, 2001, pp. 107-116.

[71] El FNC (*Federal Networking Council*) de los Estados Unidos mediante la resolución de 24 de octubre de 1995 lo definió como sigue: "*Entendemos por Internet un sistema global de información que: está relacionado lógicamente por un único espacio global de direcciones basado en el protocolo IP o en sus extensiones; es capaz de soportar comunicaciones usando el conjunto de protocolos TCP/IP o sus extensiones y/o otros protocolos compatibles con IP; proporciona, usa o hace accesible, de manera pública o privada, servicios de alto nivel en capas de comunicaciones y otras infraestructuras relacionadas*". Citado por DE ANDRÉS BLASCO (Javier) "¿Qué es Internet?". *Principios de derecho de internet*. 1ª Ed., Valencia, Tirant lo Blanch, 2005, pp. 30-98.

[72] La misma es considerada como un medio de comunicación. Ahora bien, no todo a lo que se puede acceder a través de ella tiene un carácter "público" y por tanto manipulable. De ser así todos los datos que se trasmiten a través de ella serían como peces en el mar, esperando ser atrapados por las redes del pescador. Ver a este respecto a LALANA (Ángel Daniel Oliver). "Internet como fuente de información accesible al público: pensando el derecho de protección de datos en su contexto social y jurídico". *Revista de Contratación Electrónica*, Nº 77, Diciembre 2006, pp. 3-33.

interconectar diversas redes entre sí[73]. Se trata del TCP/IP (*Transmission Protocol, Internet Protocol*), base del espectacular desarrollo de Internet. La ruta que siguen los paquetes en Internet no es controlable por el usuario, sino dinámica y guiada por la lógica de seguir la vía más rápida.

Y si bien el sistema nace propiamente en los años ochenta como consecuencia de un proyecto de interconexión entre las redes de la NSF (*National Science Foundation*) llamado CSNET (*Computer Science Network*) y el ARPANET, con un nombre que se debe al hecho de constituir la interconexión una *inter-networking*, no fue sino hasta los noventa cuando su utilización generalizada se materializó con la creación de la Web (o *World Wide Web*).

La Web consiste en la representación gráfica de Internet, pudiendo ser considerada como un sistema de documentación interactiva conectada: hablamos de los llamados hipertextos[74], que permiten pasar de una página a otra de forma automática permitiendo "navegar" al internauta, uno de los recursos más utilizados en Internet[75]. Hoy día hablamos ya de la Web 2, con la incorporación de las redes sociales y demás servicios interactivos[76] e incluso de la Web 3, con la introducción de la inteligencia artificial en la búsqueda y manejo de datos y contenidos en la misma[77].

Para tener una idea de la dimensión de este medio, es bueno saber que en 2011 alrededor de dos mil doscientos setenta y cinco millones de personas se encontraba conectadas a Internet, representando alrededor del 32,5% de la población mundial (un 70% de población está conectada en los países desarrollados y un 24% en los países en vías de desarrollo)[78]. Pero, estamos ante un crecimiento exponencial en el que entre 2000 y 2010 el uso de Internet ha tenido un crecimiento del 444,8%, quintuplicándose el número de usuarios. En Latinoamérica Internet ha penetrado en un 39,5%, mientras en Europa lo ha hecho en un 61,3% y en Estados Unidos y Norteamérica en un 78,6%[79].

[73] Para más información ver a DE ANDRÉS BLASCO (Javier). *Op. Cit.*

[74] Hipertexto : "*Tecnología que permite la navegación sobre la Web autorizando desplazamientos gracias a vínculos integrados en documentos interactivas*". Traducción libre de la autora. JEZ (Emmanuel) y PANSIER (Frédéric-Jêrome). *Initiation à l'internet juridique*. Collection Découvrir Droit@Litec. 2ª. Ed., Paris, Litec, 2000, p. 114.

[75] Ver a este respecto a JEZ (Emmanuel) y PANSIER (Frédéric-Jêrome). *Op. Cit.* pp. 1-8.

[76] Ver a O'REILLY (Tim). "Qué es Web 2.0. Patrones del diseño y modelos del negocio para la siguiente generación del software." *Tribuna*, 23 febrero 2006. Fuente:
http://sociedadinformacion.fundacion.telefonica.com/DYC/SHI/seccion=1188&idioma=es_ES&id=2009100116300061&activo=4.do?elem=2146 Responsable: Fundación Telefónica.

[77] Ver a ZELDMAN (Jeffrey). "Web 3.0". *A List Apart*, Nº 210, 16 enero 2006. Fuente: http://www.alistapart.com/ articles/web3point0. Responsable: A List Apart.

[78] . Estadísticas de INTERNATIONAL TELECOMMUNICATIONS UNION. *The World in 2010: ICT Facts and Figures*. Fuente: http://www.itu.int/ITU-D/ict/statistics/. Responsable: International Telecommunications Union.

[79] La concentración de usuarios de Internet se encuentra en Asia, que representa el 44.8% de los usuarios mundiales, frente a un 22.1% de Europa, 12 % de Norteamérica, 10.4 % de Latinoamérica y el Caribe, 6.2% de África, 3.4% de Medio Oriente y 1.1% de Oceanía. Fuente Internet World Stats, www.internetworldstats.com/stats4.htm al 31 diciembre 2011, derechos de autor de Miniwatt Marketing

Si bien, como algunos claman, en la arquitectura inicial del ciberespacio se propiciaba el anonimato y la libertad, hablándose incluso de que era imposible ser regulado[80] y se seguía el axioma liberal "*laissez faire laissez passer*"[81], esto ha evolucionado hacia una arquitectura que ha hecho extremadamente eficiente y eficaz la posibilidad de control[82], lo que autores como Lawrence Lessig atribuyen a las manos invisibles del mercado y del gobierno[83].

La tecnología de la información en el ciberespacio afecta la privacidad en una forma nunca antes vista. Anteriormente era necesario que la persona interactuara con el mundo exterior y en la sociedad de una forma tangible para plantearse la cuestión de la protección de la vida privada. Hoy en día esta puede ser violentada desde el propio seno del hogar por la recolección automática de los datos y huellas dejados en línea[84], así como por la posibilidad que existe de acceder a los archivos de un ordenador una vez que se está conectado[85]. La interacción en el "mundo virtual" o "ciberespacio" resulta mucho más peligrosa que en el "mundo real".

En este sentido Ricard Martínez Martínez señala que: "*En las autopistas de la información es donde probablemente se manifiesta con mayor claridad la dimensión informacional de la vida privada ya que su funcionamiento se basa esencialmente en el intercambio, transferencia y acumulación de información. La posibilidad de procesar informaciones a partir de datos personales más o menos voluntariamente cedidos, en el Internet, permite que el usuario revele de modo inconsciente hábitos, gustos, preferencias, ideología, etc. […]*"[86].

Paul Schwartz plantea como primer paso para dimensionar la problemática el de definir qué es ciberespacio y qué se entiende por datos personales[87].

Group.

[80] Ver a BORSOOK (Paulina). *How anarchy works*. Referenciada por LESSIG (Lawrence). *Op. Cit.* p. 2.

[81] Ver a este respecto a GARCÍA MEXÍA (Pablo). "El derecho de Internet". *Principios de derecho de internet*. 1ª Ed., Valencia, Tirant lo Blanch, 2005, pp. 99-131 y a GUERRERO PICO (María del Carmen). *El Impacto del Internet en el Derecho Fundamental a la Explotación de Datos de Carácter Personal. Estudios de Protección de Datos*. 1ª Ed., Madrid, Agencia de Protección de Datos de la Comunidad de Madrid, Thomson Civitas, 2006, pp. 330-335.

[82] Hoy en día es comúnmente aceptado que Internet no escapa al imperio de la ley. Sin embargo, sus características conllevan proyecciones singulares en el plano jurídico. Ver en este sentido a CHILLÓN MEDINA (José María). *Derecho de las Telecomunicaciones y de las Tecnologías de la Información*. 1ª Ed., Santo Domingo, Escuela Nacional de la Judicatura, 2004, pp. 464-469.

[83] LESSIG (Lawrence). *Op. Cit.* pp. 4-5.

[84] La CNL ha clasificado estas " huellas" en *cookies*, el histórico de navegación (que se encuentra en el computador, en el explorador y en el histórico del sitio visitado), los datos generados por la configuración técnica del ordenador (IP, *hostname*, el explorador de la máquina, la pagina que conduce al sitio), los motores de búsqueda (como Google, que guardan preferencias, acciones y localización), el intercambio de información y el histórico de conexión, que rastrea cada página visitada. Ver página CNIL, Fuente: http://www.cnil.fr/vos-libertes/vos-traces/ Responsable: Commission Nationale de l'Informatique et des Libertés.

[85] Ver a este respecto, sin buscar ser exhaustivos, GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *WP 37 Documento de trabajo Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea.* Bruselas, Adoptado 21 de noviembre de 2000, 110 pp.

[86] MARTÍNEZ MARTÍNEZ (Ricard). "Vida Privada e Internet". *Op. Cit.*

[87] SCHWARTZ (Paul M.). "Privacy and Democracy in Cyberspace". *Vanderbilt Law Review*. Vol. 62,

Pues bien, tomando la definición dada por Nathan J. Muller, puede entenderse por ciberespacio el "*espacio creado para la comunicación y otras actividades a través de la interconexión de computadoras*"[88]. La Real Academia de la Lengua Española lo define como el "*ámbito artificial creado por medios informáticos*"[89]. En cuanto a los datos personales, existe una definición consensuada: son los datos relativos a una persona identificada o identificable, de forma directa o indirecta[90].

Y es así como va surgiendo la preocupación por proteger los denominados "datos personales" como elemento del derecho a la vida privada de los individuos. Ello porque la infraestructura tecnológica en que se fundamenta Internet, y la tecnología digital en general, que garantiza la interoperabilidad, interconexión y funcionamiento de este medio convergente, permite una vigilancia total de las actividades realizadas en el ciberespacio, así como el establecer una interconexión entre ellas[91]. Como dijo Lawrence Lessig, en Internet "*el código es la ley*"[92].

Cabe destacar que, frente a los avances tecnológicos y la capacidad de interconexión masiva de la información, nos encaminamos a un espacio en que datos que inicialmente podían considerarse como irrelevantes pueden transformarse en datos personales, concepto que con el tiempo deberemos replantearnos, asumiendo que prácticamente cualquier dato puede transformarse en un dato personal dependiendo del uso y manipulación a que esté sujeto.

1.1.2.1. Acceso a las computadoras (ordenadores) personales sin el consentimiento del individuo

Una vez que una computadora se conecta a Internet hace posible el acceso a los archivos y datos guardados y gestionados por ella[93]. Estos archivos revelan en

1999, p. 1610.

[88] MULLER (Nathan). *Desktop Encyclopedia of the Internet.* Citado por SCHWARTZ (Paul M.). "Privacy and Democracy in Cyberspace". *Op. Cit*. p. 1617.

[89] Página Web www.rae.es Responsable: Real Academia Española.

[90] Ver en este sentido OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, recomendación adoptada el día 23 de septiembre de 1980; el Convenio 108 del Consejo de Europa de 28 de enero de 1981, para la protección de los datos personales con respecto al tratamiento automatizado de los datos personales, entre otros textos; o el Art. 2 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 dato. En el mismo sentido *The Privacy Act* de 1974 de Estados Unidos define los registros de datos personales como el grupo de informaciones sobre una persona que es mantenido por una agencia, especificando que estos están conformados por toda información que constituya una identificación particular asignada a un individuo.

[91] De ahí que siempre que sea posible el Grupo del Artículo 29 recomienda el anonimato en Internet (mientras otros expertos dicen simplemente "mientan"). En sus propias palabras, "*Con todo, la amenaza a nuestra intimidad no se deriva únicamente de la existencia de gran cantidad de datos personales en Internet, sino también del desarrollo de soportes lógicos capaces de buscar en la red y recopilar todos los datos disponibles sobre una persona determinada*". GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *WP 6 Recomendación 3/97 Anonimato en Internet*. Bruselas, Adoptada 3 de diciembre de 1997, 14 pp.

[92] LESSIG (Lawrence). *Op. Cit.* p. 1.

[93] En una encuesta realizada en Santo Domingo (República Dominicana) en 2010 a un 11% de los encuestados le había sido sustraída información de su computadora y un 32% conocían a alguien a quien le había pasado esto.

innumerables formas aspectos confidenciales de sus usuarios[94].

En este sentido podemos puntualizar las siguientes amenazas a la privacidad, que a veces están entrelazadas:

- La entrada sin consentimiento al disco duro de la computadora, a través de "troyanos" o "gusanos"[95]. Esto representa uno de los mayores problemas, pues deja a merced de un intruso la integridad de la información y la confidencialidad de su contenido. Por otra parte, puede accederse incluso a informaciones consideradas borradas[96], al no existir una forma segura de eliminar un archivo de un disco duro, pues lo que hace la computadora en realidad es suprimirlo del directorio del manejador del disco para que aparezca como un espacio disponible y pueda reescribirse sobre éste. Pero, existen técnicas que permiten recuperar estos archivos, incluso una vez sobre-escritos. La única forma de borrar la información es destruyendo físicamente el soporte que la contenía.
- Al conectarnos a Internet se generan registros de datos en la memoria "caché" de la computadora. La memoria caché de la computadora es la que permite almacenar una serie de datos para su rápido acceso. Una vez conectados, un internauta genera registros tanto en su propia computadora como en la red[97]. Existen muchas memorias caché (de disco, de sistema, de programas)[98]. Por ejemplo, *Internet Explorer* prevé una memoria caché, lo que significa que este programa registra los sitios que visitamos para facilitar su posterior acceso, constituyendo normalmente el 10% del disco duro. Asimismo, los proveedores de Internet utilizan el mismo concepto con los servidores *proxy*[99]. Y a estos datos se accede desde las computadoras, por la interfaz de la red[100].
- Los programas espías o "*spywares*" que se instalan secretamente en las

[94]Ver a este respecto a SCHWARTZ (Paul M.). "Privacy and Democracy in Cyberspace". *Op. Cit*. pp. 1621-1626.

[95] Ver sobre el tema a FERNÁNDEZ RODRÍGUEZ (José Julio). "En torno a la Interacción entre Privacidad e Internet". *Revista Datos Personales.* Agencia de Protección de Datos de la Comunidad de Madrid. Nº. 7, Enero 2004. Fuente: http://www.datospersonales.org Responsable: Agencia de Protección de Datos de la Comunidad de Madrid.

[96] *Ibídem*.

[97] En este sentido, Paul Schwartz pone el ejemplo del caso de Mónica Lewinsky en el que los investigadores recuperaron algunos documentos desde su propia computadora y otros desde la computadora de destino del mensaje enviado. Ver SCHWARTZ (Paul M.). " Internet Privacy and the State". *Connecticut Law Review*. Vol. 32, 2000, p. 818.

[98] La memoria caché se caracteriza por ser una memoria volátil de una gran velocidad, intercalándose normalmente entre un medio de almacenamiento lento y un centro de tratamiento rápido.

[99] El *Proxy* se define como el "*Servidor de Internet sobre el cual se almacenan temporalmente los datos de los sitios más consultados. Su utilización permite aumentar radicalmente la rapidez de la transferencia de las informaciones relativa a los sitios más visitados*". Traducción libre de la autora. JEZ (Emmanuel) y PANSIER (Frédéric-Jêrome). *Op. Cit* p. 116.

[100] Ver CNIL. *La mémoire cache.* Fuente: http://w3.scola.ac-paris.fr/juniors/traces/cache.htm Responsable: Commission Nationale de l'Informatique et des Libertés.

computadoras para vigilar las actividades realizadas por el usuario[101]. Un análisis de Earthlink realizado entre enero y septiembre de 2004, sobre unos tres millones de sistemas, reveló la existencia de unos 83 millones de programas espías y un promedio de 26 programas espías por ordenador[102]. En este sentido el gobierno norteamericano tuvo una iniciativa en enero de 2005 (que no encontró eco en el Congreso), para crear el *Securely Protect Yourself Against Cyber Trespass Act,* también conocido como *Spy Act,* con la finalidad de proteger a los usuarios de Internet de las transmisiones desconocidas de sus datos personales a través de los programas espías[103]. Hoy en día continuamos a merced de estos programas espías que presentan como mayor problemática su carácter de "secretos" y el desconocimiento que se tiene sobre las informaciones que transmiten real y efectivamente. Junto a estos algunos colocan los *adware* que, a diferencia de los *spyware*, sí notifican su instalación[104].

- Las "*cookies*" son uno de los programas espías más conocidos, permitiendo, según explica el *Microsoft Computing Dictionary*, identificar a los usuarios, identificar al servidor para enviar versiones personalizadas de las páginas web y obtener información de las cuentas de los usuarios, entre otros propósitos, según se dice, "administrativos"[105]. Se habla ahora ya también de "super *cookies*"[106]. Si bien en principio estas están diseñadas para "reportar" al sitio web que las coloca, no es menos cierto que si alguien tiene acceso a las informaciones recolectadas por ellas puede acceder a datos personales de los internautas[107]. Y, así, el internauta no tiene control sobre la información recopilada y el uso que se le da a la misma[108].

[101] Para más información sobre programas espías ver BURGUEÑO ZARZA (José Antonio), CARRASCO SAN MARTÍN (Mª del Carmen) y GARVIA POLO (Teodoro). "Los spyware". *Revista de Contratación Electrónica*, Nº 80, Marzo 2007, pp. 3-70.

[102] Ver a CNET NEWS STAFF. "EarthLink finds spyware running amok". *CNET News*, 5 Octubre 2004. Fuente: http://news.cnet.com/EarthLink-finds-spyware-running-amok/2100-1032_3-5397333.html Responsable CNET y a CABALLÉ (Xavier). "Un promedio de 28 programas espías en cada ordenador que accede a Internet". *HISPASEC Sistemas*, 18 abril 2004. Fuente: http://www.hispasec.com/unaaldia/2002 Responsable HISPASEC SISTEMAS.

[103] Ver Página web: http://www.govtrack.us/congress/bill.xpd?bill=h109-29 Responsable: GovTrack.us.

[104] SCHWARTZ (Paul M.). "Property, Privacy, and Personal Data". *Op. Cit.* pp. 2064-2066.

[105] Referenciado por SCHWARTZ (Paul M.). "Privacy and Democracy in Cyberspace". *Op. Cit*. p. 1/624.

[106] Ver también a MENDOZA LUNA (Amílcar). "Los Cookies: ¿amenaza a la privacidad de información en la internet?". *Alfa-Redi: Revista de Derecho Informático*, Nº 30, Enero 2001, Fuente: http://www.alfa-redi.org/rdi-articulo.shtml?x=612 Responsable: Alfa-Redi.

[107] *Ibídem,* pp. 1624-1626.

[108] Ver a KIERKEGAARD (Sylvia). "Lobbyism and the 'opt in'/'opt out' cookie controversy. How the cookies (almost) crumbled: Privacy & lobbyism". *Computer Law & Security Report*, Vol. 21, Nº. 4, 2005, pp. 310-322. Y, sin embargo, no siempre los usuarios conocen las implicaciones de permitir o no la instalación de estos programas ni de su utilización. Tenemos así que en un estudio realizado en Santo Domingo (República Dominicana) en 2010, un 42% de los encuestados desconocía qué eran las *cookies*, frente a un 56% que si lo sabía.

- Y una realidad a la que también nos enfrentamos es la de la recolección y comercialización de los datos personales por el sector privado, que se sirve de la tecnología e infraestructura existente para crear un mercado de la información[109], realmente peligrosa en el caso de la utilización de Internet por criminales que obtienen datos de sus futuras víctimas, como ha sido destacado ya en México[110].

1.1.2.2. Interceptación y transmisión de comunicaciones en línea

La propia estructura de Internet hace posible que la información sea interceptada en cualquiera de las etapas de la trayectoria por la que pasa un paquete de información, ya que el mismo circula por diversos sitios hasta llegar a su destino final[111], lo que plantea la cuestión de determinar quién es el responsable de salvaguardar estas informaciones "en tránsito".

Ello es así por la interdependencia de los servidores y redes pertenecientes a diversas empresas, cuyo intercambio de información puede implicar una cesión de informaciones sin la autorización de los usuarios[112]. Esta situación se presenta independientemente de que los soportes utilizados sean en parte privados, como es el caso del correo electrónico. En este contexto se habla de los *sniffers*, programas que se utilizan para interceptar información en la red y de los *rootkits*, que permiten borrar las huellas dejadas después de una intrusión, así como del *superzapping*, especie de llave maestra cibernética y del "pinchado" de líneas[113].

Desde el punto de vista de la intromisión de la autoridad pública, el sistema ECHELON de interceptación de comunicaciones (se maneja por Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda) se presenta como el rey en la materia y es considerado la red planetaria de espionaje por excelencia, incluyendo no sólo las comunicaciones vía Internet, sino también telefónicas, por radio, satélite y fax[114]. No se trata de interceptaciones puntuales y justificadas por investigaciones criminales en curso, sino de un sistema que trabaja de forma continua y proactiva[115]. Junto a él se encuentra el CARNIVORE, específico para Internet[116].

[109] Ver SCHWARTZ (Paul M.)." Internet Privacy and the State". *Op. Cit*. pp. 818-819.

[110] A este respecto ver PRODIARIO. "Los narcos en México usan Facebook y otras redes sociales para secuestrar jóvenes". *Prodiario*, Santa Fé, 30 Mayo 2009. Fuente: http://www.prodiario.com.ar/despachos.asp?cod_des=60940 Resp: CMS de Noticias Web Grandi y Asoc.

[111] Ver a JEZ (Emmanuel) y PANSIER (Frédéric-Jêrome). *Op. Cit.* 73-76.

[112] ABERASTURI GORRIÑO (Unai) y CUBERO MARCOS (José Ignacio). "Reflexiones en torno a la Protección de los datos personales en las comunicaciones electrónicas". *Revista Vasca de Administración Pública.* Herri-Arduralaritzako Euskal Aldizkaria, Nº. 78, 2007, pp. 83-113.

[113] Para más información ver a FÍGOLI PACHECO (Andrés). "El Acceso No Autorizado a Sistemas Informáticos." *Alfa-Redi: Revista de Derecho Informático*, Nº. 17, Enero 1999, Fuente: http://www.alfa-redi.org/rdi-articulos.html?x=381 Responsable: Alfa-Redi.

[114] SADIN (Éric). *Op. Cit*, pp. 179-181.

[115] Ver, sobre sus riesgos, a GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *WP 18 Recomendación 2/99 Sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones.* Bruselas, Adoptada 3 Mayo 1999, 9 pp.

Por otra parte, en el ámbito laboral, el control del correo electrónico y del uso de los recursos de la Web, se plantea como una cuestión sobre la que todavía hay que debatir[117].

En este campo, podemos referir diferentes ejemplos de la jurisprudencia francesa, como el del denominado "caso Nikon"[118], en el cual la Cámara Social de la Corte de Casación en fecha 2 de octubre de 2001 afirmó el derecho de los empleados al respeto de su vida privada dentro de lo que sería la utilización del correo electrónico, no pudiendo tener acceso a éste los empleadores a menos que esté preestablecido en el reglamento interior y con el conocimiento previo de los empleados. Sin embargo, la propia Corte de Casación el día 17 de mayo de 2005[119] estableció que un acceso a los ficheros personales[120] de los asalariados sería posible bajo ciertas condiciones[121]. Más recientemente ha señalado que los empleados tienen derecho, aun en su lugar de trabajo, al respeto de su vida privada[122] y si bien en este caso el Alto tribunal aceptó que el empleador podía abrir los mensajes no identificados como personales que llegan al correo profesional de su empleado, no podía utilizarlos como motivo de despido si estos revelaban aspectos de su vida privada.

Tampoco la jurisprudencia española ha sido ajena a los casos de despido disciplinario por el mal uso de los recursos informáticos de la empresa, en particular del correo electrónico. Merece destacarse a este respecto la Sentencia del Tribunal Supremo de 26 de septiembre de 2007[123], que viene a unificar la doctrina sobre la posibilidad de controlar el uso personal de los recursos puestos a disposición del empleado (debiendo previamente haber sido informado por la empresa de los controles y prohibiciones existentes), pero sin dejar de proteger el derecho a la privacidad de los mismos, respetando la no interceptación de las comunicaciones, y de sus archivos personales. Sin embargo, la misma no delimita

[116] Para ampliar sobre el tema ver a GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *WP 37 Documento de trabajo Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea. Op. Cit*. pp. 36-38.

[117] KIERKEGAARD (Sylvia). "Privacy in electronic communication: Watch your e-mail: Your boss is snooping!". *Computer Law & Security Report*, Vol. 21, Nº. 3, 2005, pp. 226-236.

[118] Corte de Casación. (Francia). *Chambre sociale, 2 octobre 2001, 99-42.942.*

[119] Corte de Casación. (Francia). *Chambre sociale, 17 mai 2005, 03-40.017.*

[120] Se plantea así que el derecho a la vida privada no es absoluto. Sobre esta posición se critica la afirmación a la que llegan muchos autores de que la vigilancia se legitima por el hecho de "comunicarla"; sin embargo faltaría que la misma sea proporcionada. El empleado se encuentra en una situación de desventaja. El empleador "comunica" sus políticas de privacidad, las socializa, ¿pero es acaso el empleado libre de aceptarlas? Ver a AMEGEE (Maximilien). " La vie privée du salarié au sein de l'entreprise 6 ans après l'arrêt Nikon, Redéfinition ou juste confirmation? ". *Expertises des systèmes d´information*. Paris, Editora CELOG, Nº 319, Noviembre 2007. pp. 384-387.

[121] Ver también a VIGNEAU (Christophe). "El control judicial de la utilización del correo electrónico y del acceso a internet en las empresas en Francia". *Relaciones laborales: Revista crítica de teoría y práctica*, Nº 1, 2009, pp. 173-184.

[122] Corte de Casación (Francia). *Chambre sociale, 5 juillet 2011, Nº 10-17284.*

[123] STS 6128/2007, de 26 de septiembre.

claramente la legitimidad de los controles implementados por la empresa de forma abierta frente al posible conflicto con el derecho a la vida privada[124]. Así, ¿cualquier medida sería aceptable por el simple hecho de haberla comunicado?, ¿nos olvidamos de que el empleado es un elemento vulnerable en la relación laboral, merecedor de una protección particular frente al empleador?, ¿nos olvidamos de que los empleados no dejan de ser personas? Necesariamente debe exigirse un criterio de proporcionalidad a la hora de definir los controles a implementar, así como la delimitación del espacio privado y laboral del individuo, que no debe perder el derecho a su privacidad por el hecho de llegar a ser, además de persona, "empleado".

La protección particular del correo electrónico puede ser asimilada a la del internacionalmente reconocido derecho al secreto de las comunicaciones[125], lo que lleva a replantearse lo que justificaría una interceptación legítima del mismo y si dicha protección engloba tanto el contenido del correo como los datos relativos a su transmisión.

Con la llegada del Internet inalámbrico se abrió el debate sobre el acceso a través de redes públicas no securizadas[126], dentro de las cuales, justamente, se potencializa la recolección de los datos[127].

Indudablemente el tratamiento de estas cuestiones pone de relieve la necesidad de fortalecer la seguridad informática[128]. Así, la industria ha establecido estrategias para garantizar su defensa (*Defense in depth*), dividida en varias capas, que se inicia con la existencia de políticas, procedimientos y conciencia de lo que implica la idea de seguridad, continúa con la garantía de lo que es la seguridad física y va progresivamente cubriendo la protección del perímetro, del Internet *network*, de los *host* y de los programas hasta culminar con la de los propios datos[129].

[124] Ver a este respecto a AGUSTINA SANLLEHÍ (José R.). "Expectativa de privacidad en el correo electrónico laboral y prevención del delito (Reflexiones en torno a la Sentencia del Tribunal Supremo de 26 de septiembre de 2007)". *Revista La Ley Penal*, Nº 69, 2009, pp. 77-99.

[125] Ver en este sentido a FERNÁNDEZ RODRÍGUEZ (José Julio). *Op. Cit.,* a GARCÍA GONZÁLEZ (Javier). "Intervenciones de terceros en el correo electrónico. Especial referencia al ámbito laboral y policial". *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales,* Estudios de Derecho Penal y Criminología, Granada, Editoral Comares, 2006, pp. 297-323 y a JEZ (Emmanuel) y PANSIER (Frédéric-Jêrome). *Op. Cit.* p. 20.

[126] AURA (Tuomas) y ZUGENMAIER (Alf). "Privacy, Control and Internet Mobility". *Lecture Notes in Computer Science,* Security Protocols, Vol. 3957, 2006, pp. 133-145.

[127] Ver a este respecto MOLIST (Mercè). "La seguridad, talón de Aquiles del 'wireless'". *El País,* 26 de Diciembre de 2002. Fuente:

http://www.elpais.com/articulo/tecnologia/seguridad/talon/Aquiles/wireless/elpeputeccib/20021226elpcibtec_4/Tes Responsable: El País y El MUNDO. "Google tenía intención de almacenar los datos no encriptados de las redes WiFi". Y *El Mundo* (edición on-line), 10 de junio 2010. Fuente: http://www.elmundo.es/elmundo/2010/06/10/navegante/1276170691.html Responsable: El Mundo.

[128] Ver DAYARATHNA (Rasika). "The principle of security safeguards: Unauthorized activities". *Computer Law & Security Review*, Nº 25, 2005, pp. 165-172.

[129] Empresas como Microsoft trabajan en ofrecer mecanismos de protección, pero cuya aplicación dependerá de la configuración y nivel de seguridad requerido por el usuario. De ahí que el primer paso, como algo fundamental y primario, sea el conocer las amenazas y como defenderse. Entrevista a Silverio Saladin,

1.1.2.3. Trazabilidad de la utilización de Internet

La estructura de Internet permite que cada "clic" que hacemos quede registrado para poder relacionar las páginas web y medir el nivel de congestión de la red y así determinar las mejores rutas de acceso y transferencia de información, lo que, al mismo tiempo, hace posible el establecer una intensiva cibervigilancia sobre los usuarios[130]. Se generan así historiales de navegación y de conexión tanto en nuestro ordenador como en los servidores y en los sitios que visitamos.

Para que un individuo pueda acceder a Internet debe utilizar, como es conocido, un ISP *(Internet Service Provider*), proveedores de acceso a Internet, que actúan a modo de puerta de entrada a la red. Justamente esta condición los pone en una posición ventajosa, ya que tienen acceso a información sensible relativa al comportamiento de sus usuarios en Internet y les facilita con ello la posibilidad de relacionar la información existente de cualquier internauta. Así lo ilustra Paul Schwartz con el caso de *McVeigh v. Cohen*[131] en el que AOL, la compañía proveedora de Internet, reveló datos a terceros que permitieron la identificación de uno de sus usuarios, lo que pudo ser la causa de que fuera juzgado en un tribunal[132].

Por otra parte, como es igualmente sabido, para poder acceder a Internet se debe contar no tan sólo con una conexión, sino también con la dirección IP (*Internet Protocol*)[133] que proporciona el organismo denominado NIC (*Network Information Center*). Cada vez que nos conectamos para poder interactuar con otras páginas y servidores enviamos nuestra dirección IP, a fin de poder intercambiar información, lo que implica que nos identificamos con cada conexión que hacemos con un

Estratega de Tecnología de Microsoft Dominicana, República Dominicana, 7 Enero 2011. Ver a este respecto NATIONAL SECURITY AGENCY. *Defense in Depth*. Fuente:

http://www.nsa.gov/ia/_files/support/defenseindepth.pdf Responsable National Security Agency - Security Center.

[130] Ver a SCHWARTZ (Paul M.). "Privacy and Democracy in Cyberspace". *Op. Cit*. pp. 1618-1621.

[131] "*Ciertamente, el público tiene un interés en la preservación del derecho a la privacidad como defiende el demandante en este caso. Con literalmente todo el mundo en la world-wide web, la aplicación del ECPA es de suma importancia para aquellos que exponen la información más personal sobre sus vidas en cuentas privadas a través de Internet […] Es discutido en el registro exactamente como la Marina de Guerra presentó su persona a AOL cuando requirió información sobre el demandante. Los demandados alegan que Legalman Kaiser simplemente solicitó la confirmación de una hoja de fax que contenía la cuenta del demandante. El demandante sostiene, y AOL confirma, sin embargo, que el oficial naval 'engaño' al representante de AOL por "no revelar su identidad y propósito [de su solicitud] y por presentarse como un amigo o conocido del Oficial Mayor Chief McVeigh's (...)"* .Traducción libre de la autora. *McVeigh v. Cohen. 983 F. Supp. 215 (D.D.C. 1998).*

[132] Ver a SCHWARTZ (Paul M.). "Privacy and Democracy in Cyberspace". *Op. Cit*. pp. 1626-1628.

[133] La dirección del Protocolo Internet (IP) contiene el nombre del dominio y el nombre y localización de la organización que registró el nombre del dominio. Ver ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA). *Derecho de la Información: Acceso y Protección de la Información y Datos Personales en Formato Electrónico*. (Actualización realizada al informe presentado por el doctor Jonathan T. Fried en el 57º período ordinario de sesiones del Comité Jurídico Interamericano, CJI/doc.25/00 rev.1). 70º PERÍODO ORDINARIO DE SESIONES OEA/Ser.Q, 26 de febrero al 9 de marzo de 2007 CJI/doc.25/00 rev.2, San Salvador, El Salvador, 7 febrero 2007. p. 6.

servidor[134].

María del Carmen Guerrero Pico señala que el Grupo del Artículo 29 indica ciertas características del protocolo TCP/IP que pueden constituir una violación a la privacidad: así, el hecho de que la información se divide en paquetes que toman la ruta más corta, haciendo posible que la misma pase por un país donde no exista una protección adecuada de datos[135]; el hecho de que los servidores tengan IP fijas que permiten rastrear al internauta y con qué servidor ha intentado conectarse; y el hecho de la existencia de la orden "*ping*", disponible en los sistemas operativos, que permite saber a cualquier persona en Internet si un computador esta encendido y conectado a la red[136].

En todo caso, los usuarios, al navegar en Internet, dejan un flujo de datos al "pulsar" que permite recolectar información sobre las páginas visitadas, el tiempo empleado en ello y la información enviada y recibida. Esto sin hablar de la identificación de la dirección IP, la hora y fecha de la conexión y el *Uniform Resource Locator* (URL), que permite visualizar la página web anterior[137].

Conjuntamente con la interceptación y transmisión de las comunicaciones y la trazabilidad de las acciones en el ciberespacio, la llamada "nube" presenta también grandes problemas. Esta crea un espacio donde los servicios son ofertados a través de una red de telecomunicación y algunos de los recursos son "virtualizados"[138], conllevando la tercerización [139] del soporte tecnológico requerido para su

[134] En este sentido el Grupo del Artículo 29 señaló: "*La traducción entre el nombre de dominio y la dirección IP numérica se realiza a través de un servidor DNS que recibe y puede rastrear todos los nombres de los servidores de Internet con los que el usuario haya intentado contactar. En la práctica, quienes mantienen esos servidores de nombres de dominio suelen ser los proveedores de acceso a Internet, que disponen de capacidad técnica para conocer mucho más que eso"*. GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *WP 37 Documento de trabajo Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea. Op. Cit.* p. 16.

[135] Los *International Safe Harbor Privacy Principles* intentaron establecer un marco normativo común entre Estados Unidos y la Unión Europea a fin de asegurar un nivel de protección adecuado, fundamentándose en siete principios: aviso, elección, transferencia segura, seguridad, integridad de la data, acceso y exigibilidad, siendo de adopción voluntaria.

[136] GUERRERO PICO (María del Carmen). *Op. Cit*. pp. 411-412.

[137] Ver ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA). *Op. Cit.* pp. 5-7.

[138] La complejidad de la problemática dependerá de si la nube creada es doméstica o trasfronteriza, maximizándose el riesgo sobre la protección de los datos, ya que su visión es la de que todo se encuentre en esta "nube", que se mueve a través de todas las autopistas de la información y no necesariamente controladas por el proveedor del servicio. Ver al respecto CLARKE (Roger) y SVANTESSON (Dan). "Privacy and consumer risks in cloud computing". *Computer Law & Security Review*, Vol. 26, Nº. 4, 2010, pp. 391-397-. Así, empresas como Microsoft ofrecen modelos híbridos que permiten conservar "en casa" los datos sensibles de la empresa, a la vez que ofrece diferentes niveles para interactuar en la "nube": infraestructura, *software* y plataforma, sin descuidar la posibilidad de crear túneles encriptados para proteger el flujo de la información (Entrevista a Silverio Saladin, Estratega de Tecnología de Microsoft Dominicana, República Dominicana, 7 Enero 2011).

[139] Dar acceso a los datos personales a terceras partes presenta sus inconvenientes; es evidente; un ejemplo de ello es el caso del Hospital de Stanford, en el cual se dio acceso en línea por más de un año a los registros de 20.000 pacientes, con informaciones que van desde su nombre, apellidos e historial clínico hasta sus números de cuenta. El Departamento de Salud y Servicios Humanos de Estados Unidos resaltó que en los últimos dos años los datos de más de 11 millones de pacientes han sido violentados. SACK (Kevin).

funcionamiento y una libre circulación de los datos que no siempre va acorde con los niveles de protección requeridos por la legislación de cada país[140]. Se habla así de los proveedores de servicios web como distribuidores de "electricidad informática"[141].

Asimismo, ya somos testigos de cómo los procesadores Intel Pentium III tienen un número de serie IPSN (*Information Processing in Sensor Networks*) que permite identificar al usuario del mismo que haga transacciones en Internet[142], lo que deja claro que los fabricantes facilitan la vigilancia del uso de los equipos en la red; ello, por no hablar de la creación de Microsoft del *Globally Unique ID's* (GUIDS), para documentos individuales[143].

Y, en relación con todo ello, algo que no podemos dejar de considerar son los llamados "datos de conexión" que ahora las Directivas europeas obligan a conservar[144], a fin de garantizar la seguridad jurídica de los operadores, que permiten localizar la terminal empleada por los usuarios para transmitir cualquier información por vía electrónica. Surge aquí la disyuntiva entre libertad y seguridad[145].

Los sitos web[146] y los motores de búsqueda[147], por último, constituyen a su vez un punto focal de recolección de información en el ciberespacio, al utilizar desde *cookies* hasta formas de registro, lo que les permite manipular información y disponer de ella para fines diferentes de aquellos para los cuales fueron suministradas e incluso sin el conocimiento de los usuarios.

El manejo y recolección de la data y la omnipresencia en la Web resultan, en definitiva, cada día más preocupantes, sobre todo porque, además, las grandes empresas no tan sólo ofrecen los buscadores en la red, sino correos electrónicos y servicios interactivos, lo que posibilita un cruce entre los datos recolectados por

"Patient Data Posted Online in Major Breach of Privacy". *The New York Times,* 8 Septiembre 2011. Fuente: http://www.nytimes.com/2011/09/09/us/09breach.html?_r=1 Responsable: The New York Times.

[140] AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID. "'Cloud computing' choca con la legislación europea de privacidad". *Revista Datos Personales*. Agencia de Protección de Datos de la Comunidad de Madrid, Nºo. 48, Noviembre 2010. Fuente: http://www.datospersonales.org Responsable: Agencia de Protección de Datos de la Comunidad de Madrid.

[141] Ver a GABADOU (Hervé). "Le droit dans les nuages". *Expertises des systèmes d´information*, Paris, CELOG, Nº. 338, Julio 2009, p. 251.

[142] Ver a este respecto FERNÁNDEZ RODRÍGUEZ (José Julio). *Op. Cit.*

[143] Ver a SCHWARTZ (Paul M.). "Internet Privacy and the State". *Op. Cit*. p. 819.

[144] Ver Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE del Parlamento Europeo y Del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

[145] ABERASTURI GORRIÑO (Unai) y CUBERO MARCOS (José Ignacio). *Op. Cit.*

[146] Ver HSU (Chiung-wen-Julia). "Privacy concerns, privacy practices and web site categories: Toward a situational paradigm". *Online Information Review*, Vol. 30, Nº. 5, 2006, pp. 569-586.

[147] Ver a este respecto *Resolution on Privacy Protection and Search Engines*. *28th International Data Protection and Privacy Commissioners' Conference ,* London, United Kingdom, 2- 3 Noviembre 2006.

diferentes medios[148]. Es el caso de Google[149], una de las más utilizadas y que al unirse a la empresa DoubleClick, conocida por recolectar datos en Internet con fines publicitarios (y no siempre hacer el mejor uso de ellos[150]), crea un monopolio en este mercado[151].

1.1.2.4. El *data mining* y la generación de perfiles en Internet

Dentro de este contexto, tampoco podemos dejar de hablar del "*data mining*", que no busca más que, una vez almacenada la información, darle significado, automatizando la extracción de datos bajo determinados parámetros predefinidos, los cuales siguen patrones de enlace que permite clasificarlos y darles un sentido. De esta forma se puede generar información útil de donde parecía no haberla[152].

Esta técnica es utilizada tanto por las autoridades públicas como por las entidades privadas para fines diversos[153]. Así, los Estados pueden utilizarla para intentar prever ataques terroristas y garantizar la seguridad nacional -pero no sólo-, mientras el sector privado con fines mercadológicos, lo que no deja de plantear un problema de discriminación a largo plazo.

Esa asignación de significado permite tomar decisiones fundamentadas en una base de datos de "intenciones"[154]. Y esto es particularmente sensible cuando se hace por parte de un gobierno: no es lo mismo no recibir un anuncio promocional o descuentos de reducción para una determinada tienda que terminar en la cárcel de

[148] Nos señala así Pablo Andrés Palazzi que "*No sólo las búsquedas en Internet quedan almacenadas en Google, sino también las búsquedas realizadas en la barra de Google y dentro de la cuenta de Gmail, incluido también el correo electrónico allí recibido y borrado […] Como han señalado recientemente dos especialistas 'hoy en día las políticas y actividades de compañías como IBM o Microsoft tienen mucho más impacto que las acciones de una determinada Nación, ambas pueden amenazar o proteger la privacidad en el contexto de sus transacciones comerciales […] La información sobre las búsquedas en Internet parece no tener límites. Es decir, parece no haber un derecho al olvido en el mundo digital"*. PALAZZI (Pablo Andrés). "Google y el derecho a la privacidad sobre las búsquedas realizadas en internet". *Revista de Contratación Electrónica,* Nº. 74, Septiembre 2006, pp. 31-44.

[149] Ver a CHURCH (Peter) y KON (Georgina). "Google at the heart of a data protection storm". *Computer Law & Security Report,* Vol. 23, Nº. 5, 2007, pp. 461-465 y a DE CÓZAR (Álvaro). "Google sabe demasiado". *El País,* 11 de septiembre 2007. Fuente:
http://www.elpais.com/articulo/sociedad/Google/sabe/demasiado/elpeputec/ 20070911elpepisoc_2/es. Responsable: El País.

[150] En enero de 2000 DoubleClick fue perseguida ante una corte de California por no dar cumplimiento a sus propias políticas de privacidad. Ver a este respecto a TABATONI (Pierre), (Director). *La protection de la vie privée dans la société d'information.* Cahier des sciences morales et politiques, Tomo 1, 1era. Ed., Paris, Presses Universitaires de France, 2000, p. 32.

[151] APPEL (Marco). "Privacidad Virtual". *Proceso*, Nº 1638, 23 de Marzo de 2008, pp. 43-45 y PALAZZI (Pablo Andrés). *Op. Cit.*

[152] Ver a este respecto OLIVER LALANA (Angel Daniel). "El derecho fundamental 'virtual' a la protección de datos: tecnología transparente y normas privadas". *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía*, Nº. 5, 2002, pp. 1539-1546.

[153] Ver en este sentido a LEE (Ronald D.), RUBINSTEIN (Ira S.) y SCHWARTZ (Paul M.). "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches". *University of Chicago Law Review*, Nº 75, 2008, pp. 261-285.

[154] *Ibídem*, pp. 271.

Guantánamo. El costo para el individuo es muy diferente[155].

Utilizada esta técnica por la autoridad estatal como estrategia de defensa, pasamos del principio de que toda búsqueda debe estar fundamentada en una sospecha razonable e individual a estar bajo un control constante de nuestras actividades y a que un ordenador y los patrones predefinidos y asumidos "predigan" un posible comportamiento sospechoso. Esto sin hablar de la quiebra del principio de presunción de inocencia, frente a una medida cuya efectividad se desconoce[156].

Todos estamos bajo investigación ya que "las personas honestas no tienen nada que ocultar"[157].

Tenemos así una infraestructura tecnológica que potencia y facilita no sólo la recolección de información sino un constante seguimiento y trazabilidad de lo que ocurre en el mundo virtual, maximizando la accesibilidad y manipulación de la información en línea. Datos que tal vez considerados de forma aislada no conllevarían un atentado contra la vida privada de una persona, recolectados, tratados y manipulados de manera conjunta permiten conformar perfiles de comportamientos y preferencias personales, normalmente tratados sin el conocimiento ni consentimiento del internauta[158]. Así, si bien Internet es una ventana abierta hacia el mundo, es también una ventana abierta hacia todo aquel que accede a él[159].

Todo esto genera lo que Paul Schwartz denomina "*el espectáculo de horror de la privacidad*"[160], que posibilita las acciones que José Julio Fernández Rodríguez señala[161]:

- la creación de perfiles de los internautas (construidos en torno a su vida privada);
- la simple acumulación o registro de datos sin consentimiento;
- la transferencia de datos sin consentimiento;
- el empleo de una dirección IP asignada a otro ordenador;
- la interceptación de mensajes de correo electrónico;

[155] Ver a este respecto a SOLOVE (Daniel). "Data Mining and the Security-Liberty Debate". *University of Chicago Law Review*, Nº 74, 2008, pp. 352-353.

[156] *Ibídem*, p. 362.

[157] Ver a SOLOVE (Daniel). "Nothing to hide: the false tradeoff between privacy and security". *San Diego Law Review*, Vol. 44, 2007, pp. 745-772.

[158] Frente a posibilidades ilimitadas de control no todo lo que se "puede" hacer "debe" hacerse, arguyendo algunos autores que de la mano de la protección legal debe nacer una deontología profesional que vaya más allá de la técnica. Ver a BARROSO (Porfirio). *Ética y deontología informática*. 1ª Ed., Madrid, Fragua, 2007, pp. 63-66.

[159] Ver a este respecto el análisis sobre las nuevas amenazas y necesidad de adaptación al entorno virtual de GUERRERO PICO (María del Carmen). *Op. Cit*. pp. 229-370.

[160] Traducción libre de la autora: *"The privacy horror show"*. SCHWARTZ (Paul M.). "Privacy and Democracy in Cyberspace". *Op. Cit*. p. 1621.

[161] FERNÁNDEZ RODRÍGUEZ (José Julio). *Op. Cit.*

- la suplantación de personalidad;
- el hostigamiento electrónico;
- el uso indebido de directorios de correo electrónico o listas de usuarios.

Y esto no es todo porque con la llamada Web 2 y el boom de los espacios de diálogo surgen nuevos problemas al introducirse un nuevo paradigma en la interacción con la red: se combina la infraestructura de control existente con la sed de participación de los internautas. Veamos qué puede implicar este nuevo marco.

1.2. *Las redes sociales e interactivas: una exposición voluntaria*

De la utilización pasiva de los servicios ofertados en Internet hemos pasado en la última década a una generación de servicios interactivos, en los que el usuario es el gran protagonista, entrando en la llamada por O'Reilly, en 2004, Web 2[162]. Bajo esta nueva concepción de la Web los usuarios transitan de ser sujetos pasivos a ser sujetos activos, creándose una verdadera sociedad virtual unida por intereses comunes, en la cual desaparecen las fronteras físicas y que se comunica por un mismo lenguaje: el digital. Estos nuevos espacios promueven la creación del conocimiento y la interacción colectiva[163] frente a una convergencia de medios[164].

El Grupo Orange elaboró un estudio sobre las servicios ofertados en la Web 2, elaborando un mapa visual de la misma[165], en el que destaca la incorporación de weblogs, videoblogs, lectores de canales RSS (*Really Simple Syndication*), noticias y comentarios votados por usuarios, recomendaciones de contenido, buscadores especializados, plataformas para compartir fotos, videos y música, páginas de inicio personalizadas, redes sociales personales (de ocio), redes sociales profesionales, aplicaciones en línea y marcadores sociales, entre otros, dentro de los cuales los internautas son llamados a interactuar, comunicarse y "compartir".

Lo que cambia, más que la tecnología, es el paradigma de su utilización, convirtiéndose el sistema en un medio por excelencia para interrelacionarse con otros y generándose así una revolución social en la cual la llamada a la libre expresión y la retroalimentación son la regla. Todo el mundo busca estar "conectado" y al día de los acontecimientos de su grupo social, donde los intereses compartidos rebasan las fronteras físicas. Y, a su vez, el internauta se vuelve parte de esos eventos de actualidad y puede expresar su "ser" a una escala "mundial". Somos con ello testigos de una búsqueda sin precedentes de ser "vistos" y de "ver", en la que los *bulletin boards* personales quedan atrás y la conexión a través de espacios interactivos donde se facilita el acceso a otros se pone a la orden del día.

[162] O'REILLY (Tim). *Op. Cit.*

[163] CASTELLS OLIVÁN (Manuel). "Creatividad, innovación y cultura digital. Un mapa de sus interacciones". *Telos: Cuadernos de comunicación e innovación*, Nº 77, 2008, pp. 50-52.

[164] CASTELLS OLIVÁN (Manuel). "Un nuevo medio de comunicación: internet". *Treballs de comunicació,* Nº 17, 2002, pp. 5-22.

[165] ORANGE. *Mapa visual de la Web 2*. Ver http://internality.com/web20/ Responsable: Internality.

Indudablemente esta exposición voluntaria de los usuarios a través de los medios y servicios interactivos pone sobre el tapete un nuevo tipo de problemas en relación con la protección de los datos personales. Ello porque con esta forma de comunicación se revelan detalles sobre preferencias, deseos, gustos e ideologías no tan sólo propias, sino también de personas cercanas. De este modo se pasa a ser tanto sujeto de los datos posteados como generador de la información publicada, muchas veces sin tener una verdadera comprensión de sus implicaciones, dentro de una memoria digital que todo lo recuerda, lo guarda y lo pone a disposición[166].

Las redes sociales se revelan como un fenómeno que merece especial atención. Para 2011 aproximadamente el 65% de los usuarios de Internet registrados participaban activamente en ellas[167], frente al 27,3% de 2006[168]. Es hoy el medio por excelencia para compartir fotos, opiniones, videos, música, unirse a grupos, organizar eventos, escribir blogs, conocer nuevos amigos, establecer relaciones laborales o profesionales e incluso promocionar negocios.

Estas redes[169] *on line* surgen a finales de los años noventa con la creación del sitio web "clasemates.com" de Randy Conrads, creciendo exponencialmente a partir de 2003 con la aparición de las conocidas MySpace, Hi5, Xing, Facebook y Tuenti[170], y rápidamente han tenido una aceptación positiva de los usuarios, que las ven como un medio de conocer nuevas personas, permanecer en contacto con amigos, intercambiar ideas, promoverse a sí mismo, compartir conocimiento y experiencias o buscar la opinión de otros, reforzando un sentimiento de pertenencia a un grupo y poder de expresión[171].

Si bien en el mundo cibernético no existe una definición oficial[172] de las redes sociales, algunos autores las han definido como "*servicios prestados a través del Internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo disponiendo de herramientas que*

[166]Ver a POULLET (Yves). *Op.Cit.,* p. 216.

[167] Ver UNIVERSAL MCCANN. *The business of social, Wave 6*, Universal Mccann, 2012.

[168] UNIVERSAL MCCANN. *3era Oleada del Estudio Power to the people social media, Wave 4 de Universal Mccann,* 2009.

[169] Es bueno aclarar que el concepto de redes sociales en sí mismo no es nada nuevo y se fundamenta en la teoría de los seis grados de separación, inicialmente propuesta por Frigyes Karinthy y recogida por Duncan Watts, consistente en que todos estamos interconectados a través de una cadena de conocidos con no más de cinco intermediarios. Ver a este respecto AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID e INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACIÓN. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. 1ª Ed., Madrid, APDP 2009, pp. 38-39.

[170] VELA SÁNCHEZ MERLO (Cayetana)."La privacidad de los datos en las redes sociales". *Revista Española de Protección de datos*. Agencia de Protección de Datos de la Comunidad de Madrid-Thomson Civitas, Nº 5, Julio-Diciembre 2008, pp. 231-238.

[171] UNIVERSAL MCCANN. *Socialisation of Brands, social media tracker, Wave 5*, Universal Mccann, 2010 y UNIVERSAL MCCANN. *The business of social, Wave 6*, Universal Mccann, 2012.

[172] VELA SÁNCHEZ MERLO (Cayetana). "Atrapados en la red social". *Datos Personales*, Nº 43, Enero 2010. Fuente: http://www.datospersonales.org/ Responsable: Agencia de Protección de Datos de la Comunidad de Madrid.

permiten interactuar con el resto de usuarios afines o no al perfil publicado, ya sea publicando imágenes, vídeos o compartiendo otro tipo de información"[173]. El Grupo del Artículo 29 optó por una definición más sencilla al decir que podrían "*definirse generalmente como plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes. En sentido jurídico, las redes sociales son servicios de la sociedad de la información*"[174].

En la definición misma ya comienza a plantearse un debate que no tiene aún una respuesta jurídica clara, pero que es clave en lo que a la tutela de la privacidad se refiere: ¿las redes sociales son espacios públicos o privados? En la medida que el internauta controla los parámetros de privacidad y las personas con los que interactúa podría afirmarse que son espacios privados. Sin embargo, una vez publicada una información, el usuario no siempre controla la exposición de la misma frente a la "comunidad" que tiene acceso al perfil de sus propios contactos.

La integración en estas plataformas implica la creación de perfiles en línea que normalmente requieren registrar un mínimo de información personal[175], como el nombre y apellido, una dirección de correo electrónico y una fecha de nacimiento, y aceptar las condiciones de uso del servicio, en un contrato de "tómalo o déjalo", que la mayoría de las personas ni siquiera lee. Generalmente estas plataformas requieren que las informaciones dadas sean reales, aunque no realizan mayores esfuerzos para la verificación de la identidad, limitándole a la confirmación del correo electrónico dado. Esto implica que debajo del perfil proyectado cualquiera puede ser cualquier persona, interactuando menores, jóvenes, adultos, empresas, entidades u organizaciones dentro de un mismo universo, sea presentando su identidad real, un pseudónimo o creando un personaje.

Se inicia así una interacción en la que se plasman libremente datos personales y noticias de toda índole dentro de esta comunidad "virtual", fomentándose por los gestores del servicio que se suministre la mayor cantidad de información posible a fin de poder personalizar y genera un perfil "completo" del usuario, incluyendo renglones que van desde el nivel académico, profesión, lugar de trabajo, lugar de residencia, ideologías religiosas y políticas, hasta los libros y series de televisión favoritas. Pero esta información muchas veces involucra no sólo a la persona que la

[173] ARENAS RAMIRO (Mónica). "Redes sociales, ¿un virus sin cura?: las ventajas y los problemas para sus usuarios". *Datos Personales*, Nº 43, Enero 2010. Fuente: http://www.datospersonales.org/ Responsable: Agencia de Protección de Datos de la Comunidad de Madrid.

[174] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *WP 163 Dictamen 5/2009 sobre las redes sociales en línea.* Adoptado 12 de junio de 2009, p. 5.

[175] La mayoría de estas plataformas requieren que las informaciones dadas sean reales, aunque no realicen mayores esfuerzos para la verificación de la identidad. Ver a BARRIGAS (Jennifer). *Social Network Site Privacy: a comparative analysis of six sites.* The Office of the Privacy Commissioner of Canada, Febrero 2009, 55 pp.

pública, como antes se decía, sino a sus familiares y allegados[176], expuestos en esta red social "virtual" sin su conocimiento y, mucho menos, consentimiento[177].

Normalmente se diferencian dos tipos de redes sociales: las genéricas o de ocio y las profesionales; destaca entre las primeras Facebook con unos 955 millones de usuarios al mes[178] y entre las segundas LinkedIn con unos 175 millones de miembros, en datos de mediados de 2012[179]. Sin embargo, ambas comparten características comunes, teniendo por finalidad principal la de interrelacionar para una posible interacción a todos sus usuarios y de forma ilimitada, fomentando que se puedan establecer contactos "reales"[180].

Actualmente, incluso, las redes se promueven como un medio por excelencia de interacción social, no sólo por celebridades o por la industria del entretenimiento o a nivel empresarial, sino por las propias universidades[181] o por la propia Administración gubernamental[182], de un revolucionario modo en el que la interacción entre las personas, la participación ciudadana y el desarrollo profesional cobran nuevos matices.

Ahora bien, en esta interacción el usuario deja datos, de forma consciente y voluntaria, al convertirse en generador de información, o de forma inconsciente, a través de los métodos de extracción secundaria (pues su perfil de usuario se puede relacionar con los sitios en los cuales navega en Internet), ya sea de sí mismo ya sea de sus elaciones desplegadas en su lista de contactos, a través del uso de etiquetas, metadatos e incluso de recomendaciones a no usuarios de la red[183].

Justamente, el modelo de negocio de las redes sociales, que permite su sostenibilidad, no es otro que el de la publicidad en línea. Por ello el principal

[176] Como muestra de ello, en un estudio realizado en Santo Domingo (República Dominicana) en 2010 las estadísticas arrojan que un 30% de los encuestados habían visto publicadas fotos suyas en Internet sin su consentimiento y un 48% conocían a personas que les había pasado esto, reduciéndose considerablemente cuando se trata de informaciones privadas donde un 6% habían visto expuestas las mismas sin su consentimiento y un 25% conocían a alguien a quien le hubiese ocurrido.

[177] Ver a este respecto VILASAU SOLANA (Mónica). "¿Hasta dónde deben regularse las redes sociales?" *Revista Española de Protección de Datos*. Agencia de Protección de Datos de la Comunidad de Madrid-Thomson Civitas, Nº 6, Enero-Junio 2009, pp. 105-138.

[178] Estadísticas de facebook. Ver http://www.facebook.com/press/info.php?statistics

[179] . Estadísticas de linkedIn. Ver http://press.linkedin.com/

[180] AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID e INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACIÓN. *Op. Cit.* 185 pp.

[181] Ver a DUVEN (Carolyn J.) y TIMM (Dianne M). "Privacy and social networking sites:" *New Directions for Student Services,* Vol. 2008, Nº 124, 2008, pp. 89-102.

[182] Sólo hay que ver los sitios del gobierno de Estados Unidos que proponen enlaces a facebook, twiter, youtube y rss como formas de contactarlo (http://www.usa.gov/gobiernousa/) o del Francés, que propone sus propias aplicaciones "web" (http://www.gouvernement.fr/), siendo más común ofrecer un seguimiento a través de facebook y twiter (incluyendo unos pocos Estados youtube), como en los portables del Reino Unido, Brasil, Chile, México o República Dominicana, entre otros muchos (http://www.direct.gov.uk/en/index.htm, http://www.brasil.gov.br/, http://www.gobiernodechile.cl/sitios-del-gobierno/, http://www.gob.mx/wb/SFP/SFPInicio, http://www. presidencia.gob.do/app/frontpage.aspx).

[183] VILASAU SOLANA (Mónica). *Op. Cit.*

objetivo es recolectar datos personales para poder crear perfiles, determinar las preferencias y gustos de los usuarios y ofrecer un marketing personalizado (con suscripción a servicios, pagos por uso, venta de productos, etc.)[184], que lleva a cuestionar el carácter gratuito de estos servicios. Así, Microsoft pagó 170 millones de euros para aliarse con Facebook, a fin de consolidar su posición en el mercado publicitario, valorándose aproximadamente cada usuario único de esta red en unos 300 dólares[185].

Por ello, como bien señala Ricard Martínez Martínez, "*la llave de acceso a Internet, la moneda para la recepción de servicios aparentemente gratuitos no es otra que la información personal que asociada a la información global y al conocimiento acumulado constituyen la fuente de riqueza por excelencia de lo que Castells denomina muy gráficamente como 'Galaxia Internet'*"[186].

La gestión de los datos personales expuestos en las redes sociales y su protección es en gran medida responsabilidad de los prestadores de servicios que ofrecen la interrelación. Inicialmente definida en declaraciones dadas a conocer a los usuarios antes de integrarles en ellas, no siempre queda claro, sin embargo, quién es el responsable del tratamiento de los datos que se vayan ofreciendo. Los usuarios deben expresar su aceptación a dicho tratamiento y lo más que proclaman los prestadores de servicios, en la mayoría de los casos, es su "respeto por la privacidad", conscientes, eso sí, de que el principal elemento para ganar a los navegantes *on line* es el nivel de confianza que inspiren.

Con todo, nos vemos frente a la llamada trampa de la autonomía, que bien señala Paul Schwartz[187], al tener que lidiar con unos prestadores de servicios que normalmente se reservan la potestad de modificar sus políticas de privacidad o con otros que establecen políticas que permiten prácticamente hacer cualquier cosa con la información recolectada. Y como antes se decía, el usuario no deja de enfrentarse a acuerdos de "acéptalo o déjalo" imponiéndose de algún modo la idea de que el hecho de decidir participar en línea se considera en sí mismo como la decisión de aceptar cualquier uso de la información personal generada.

Al lado de los proveedores del servicio están los proveedores de aplicaciones, que para que puedan funcionar requieren la utilización de nuestros datos personales y que muchas personas confunden con el responsable de la red social.

Rápidamente desaparecen nuestros sueños de privacidad cuando verificamos la imposibilidad en la mayoría de las redes de borrar nuestra cuenta (la inactivan pero no la borran), cuando leemos las políticas de acceso y transferencia de

[184] AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID e INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACIÓN. *Op. Cit.* pp. 54-66.

[185] FOREST (David). "Le trou noir juridique des réseaux sociaux". *Expertises des systèmes d´information*, Paris, CELOG, Nº 340, Octubre 2010, pp. 343-344.

[186] MARTÍNEZ MARTÍNEZ (Ricard). "Vida Privada e Internet". *Op. Cit.*

[187] SCHWARTZ (Paul M.). "Internet Privacy and the State". *Op.Cit.*, pp. 815-859.

nuestros datos a terceros de los que ellos no se hacen responsables y la facultad de modificar previa "comunicación"[188] las políticas de privacidad previamente definidas sin que exista una posibilidad de debate[189]. Más delicado es el caso de las personas que sin ser usuarios de los servicios se ven expuestos en ellos y que no tienen, en la mayoría de los supuestos, mecanismo alguno para acceder, rectificar, cancelar o "inhabilitar" la información publicada y utilizada sobre ellos.

Ahora bien, también parte de la responsabilidad por esta injerencia en la vida privada corresponde a los usuarios: al ser quienes configuran los parámetros de privacidad deseados y quienes publican uno u otro nivel de información. De hecho, uno de los mayores problemas que en ésta se plantea es el de la falta de conciencia social y, con ella, el hecho de la exposición voluntaria de datos personales sensibles, sobre todo en las redes de ocio, donde fácilmente se muestran no sólo la película favorita, el grupo de amigos y familiares y lo que se cenó el domingo, sino la ideología, pertenencia racial, preferencias religiosas, políticas y otras. Datos que pueden ser fácilmente "descontextualizados", al decir de Dumortier, utilizándose en un contexto distinto a aquel en que fueron emitidos[190].

Muchas veces los usuarios desconocen el nivel de difusión de la información publicada, siendo un elemento fundamental de la gestión de las redes sociales, como se ha indicado, la utilización comercial de los datos recolectados (incluyendo la cesión de los mismos) y el permitir el acceso a los proveedores de aplicaciones, incluso desde la indexación de los datos en los motores de búsqueda. Y, claro, expuestos "voluntariamente", son los usuarios de la red los "responsables" de los datos publicados.

Es un hecho. La mayoría de las personas interactúan en estas redes con los parámetros definidos por defecto por los prestadores del servicio, que tienden a fomentar la mayor exposición de datos, conformando la recolección de los mismos el motor económico de su actividad. Esto a pesar de que consistentemente las recomendaciones han sido las de configurar parámetros por defecto respetuosos con la vida privada[191]. Pero, el matrimonio entre las redes sociales y la privacidad resulta complejo.

Fijémonos en que las redes sociales se utilizan incluso por las empresas de reclutamiento de personal para conocer gustos y preferencias, por las agencias de detectives privados como un recurso natural de información[192] o, más allá de todo

[188] Ver a BARRIGAS (Jennifer). *Op. Cit.*

[189] Ver a BARRIGAS (Jennifer). *Op. Cit.* y POULLET (Yves). *Op. Cit.,* pp. 211-226.

[190] VILASAU SOLANA (Mónica). *Op. Cit.* pp. 112-114.

[191] Ver GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *WP 163 Dictamen 5/2009 sobre las redes sociales en línea. Op. Cit.* pp. 6-7; BARRIGAS (Jennifer). *Op. Cit.* y Resolución sobre Protección de la Privacidad en los Servicios de Redes Sociales. 30ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Estrasburgo, 15-17 de octubre de 2008.

[192] De hecho agradecen les faciliten el trabajo. RAMBAM (Steve). *Op. Cit.*

lo imaginable, por criminales para seleccionar a sus víctimas[193]. Esto es sólo una muestra de cómo puede ser usada la información que se pone a disposición "allá afuera".

La situación se hace más compleja aún cuando entra en la ecuación la protección de los menores, que son partícipes habituales de esta sociedad "*on line*" y cuyas características de vulnerabilidad les hacen blancos fáciles. En un estudio realizado en Reino Unido ya en 2007 se señala que un 83% de los adolescentes interactúan en línea[194], siendo este solo hecho una preocupación latente en toda Europa, así señalada en el estudio sobre la privacidad de las redes sociales realizado en conjunto por INTECO y la Agencia Española de Protección de Datos[195], que no deja de estar presente también en Latinoamérica y en el resto del mundo[196].

No existen restricciones particulares de edad para la utilización de las redes sociales, aunque bien es cierto que la mayoría de las plataformas prohíben el registro de menores de 13 años, recomendando solicitar el permiso de los padres para quienes tienen entre 14 y 18 años[197]. Pero cabe plantearse obviamente cómo puede tenerse la certeza de ello si no existen medios para identificar de forma fehaciente a la persona que suscribe el servicio.

Los menores se ven expuestos a interactuar con personas adultas y, en su caso, malintencionadas, que pueden manipularlos, haciéndose pasar incluso por otros menores en un mundo donde "cualquiera puede ser un perro" y en donde es fácil fingir y construir una personalidad. Ejemplo claro de esto es el *child grooming* o

[193] A este respecto ver PRODIARIO. "Los narcos en México usan Facebook y otras redes sociales para secuestrar jóvenes". *Prodiario*, Santa Fé, 30 Mayo 2009. Fuente: http://www.prodiario.com.ar/despachos.asp?cod_des=60940 Responsable: CMS de Noticias Web Grandi y Asociados.

[194] ATKINSON (Shirley), JOHNSON (Chris) y PHIPPEN (Andy). "Improving protection mechanisms by understanding online risk". *Information Management & Computer Security*, Vol. 15 , Nº 5, 2007, pp. 382-393. La situación no es muy diferente en Australia, donde estudios han revelado que en 2007 el 55% de los menores entre 12 y 17 años tiene un perfil en línea y en Estados Unidos, donde el 70% de todos los adolescentes visitan redes sociales. Ver a RAYMOND CHOO (Kim-Kwang). "Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences". *AIC Reports*. Research and Public Policy Series 103, Australian Institute of Criminology, 2009, p. X.

[195] AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID e INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACIÓN. *Op. Cit.*

[196] Así lo demuestra la Red Iberoamericana de Protección de Datos que tuvo entre sus temas centrales en 2007 y 2009 la protección de los menores en la sociedad de la información. Ver http://www.redipd.org/documentacion/ Documentos/Menores/index-ides-idphp.php A este respecto se han realizado diversos estudios focalizados sobre todo en los adolescentes. Sobre ello, ver a BALARDINI (Sergio). "Hacia un entendimiento de la interacción de los adolescentes con los dispositivos de la Web 2.0. El caso de Facebook". *Datos personales y libertad de expresión en las redes sociales digitales: Memorándum de Montevideo*. 1ª Ed., Buenos Aires, Ad-Hoc, 2010, pp. 71-117 y a LEÓN KANASHIRO (Laura). "Adolescentes y Web 2.0: privacidad y riesgos". *Datos personales y libertad de expresión en las redes sociales digitales: Memorándum de Montevideo.* 1ª Ed., Buenos Aires, Ad-Hoc, 2010, pp. 21-69.

[197] Ver a este respecto el análisis de PANIZA FULLANA (Antonia). "Cuestiones jurídicas en torno a las redes sociales: uso de datos personales para fines publicitarios y protección de datos de menores". *Revista Española de Protección de Datos.* Agencia de Protección de Datos de la Comunidad de Madrid-Thomson Civitas, Nº 6, Enero-Junio 2009, pp. 60-68.

acoso de menores por Internet en el que las redes sociales juegan un papel básico en su comisión[198].

Pero el problema también se presenta con menores de entre 14 y 18 años, cuya información se recolecta a partir de la capacidad que, en el mundo virtual, tienen para "permitir" la utilización de sus datos personales con fines comerciales. Menores que se ven expuestos a la configuración de una red que busca, como antes se señalaba, la mayor extracción de información posible sobre sus miembros y que por eso son objeto de campañas publicitarias personalizadas que fomentan el consumismo. Menores que pueden acceder a informaciones no necesariamente aptas para su edad y que se exponen a entrar en un mundo cuyas consecuencias desconocen, seducidos por la inmediatez y rapidez de un ciberespacio en el que "pertenecen" a grupos sin fronteras físicas.

Y, cómo no, con mayores proclives a ignorar y/o menospreciar los riesgos de las redes.

Haciéndonos eco de los principales peligros identificados por la Agencia Española de Protección de Datos e INTECO en el estudio realizado sobre las redes sociales[199], señalamos los siguientes:

- la exposición de datos que pueden considerarse como sensibles.
- la falta de conciencia de los usuarios de que sus datos pueden ser accesibles a cualquier persona y de su valor en el mercado;
- la manipulación de los datos por terceros malintencionados;
- la publicación de información sin autorización de la persona, que puede serle perjudicial, tanto de personas usuarias como no usuarias del servicio;
- las condiciones de registro que permiten una recolección y explotación comercial, prácticamente ilimitada, por parte de los proveedores del servicio.

A ello cabe agregar la recolección secundaria de datos, muchas veces desconocida por los usuarios, que permite personalizar aún más los perfiles; la cesión a terceros desconocidos de datos personales cuyo tratamiento y protección escapan al conocimiento y control de los internautas; la suplantación de identidad[200]; y, en particular para los menores, la exposición descontextualizada de

[198] Ver a CHILDNET INTERNATIONAL. *Online grooming and UK law*. Fuente: http://www.childnet-int.org/downloads/online-grooming.pdf Responsable: Childnet International. También a DURÁN ALEMÁN (Jeanette), ESQUIVEL GUTIÉRREZ (Walter) y GRILLO RIVERA (Milena). "Expresiones de violencia interpersonal y social en el ciberespacio desde la vivencia adolescente: estado del arte de la investigación". Datos personales y libertad de expresión en las redes sociales digitales: Memorándum de Montevideo. 1ª Ed., Buenos Aires, Ad-Hoc, 2010, pp. 179-219.

[199] AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID e INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACIÓN. *Op. Cit.* pp. 67-71.

[200] Una muestra simple de la problemática de la suplantación de identidad digital es el robo de los correos electrónicos, donde la persona puede tener acceso no sólo a información privada sino a la lista de contacto de la persona usurpada y hacerse pasar por ella. En una encuesta realizada en Santo Domingo (República Dominicana) a un 21% de los encuestados les había sido robado su correo electrónico y un 57%

su imagen y datos personales[201].

Por ello se recomienda desde la utilización de pseudónimos y "mentir" en línea[202], la educación y formación de los usuarios, la transparencia en la utilización de los datos, la configuración de parámetros respetuosos de la privacidad, el respeto al derecho de acceso, rectificación y cancelación de los usuarios, la incorporación de medidas técnicas de protección de la vida privada e, incluso, hasta repensar la interacción en las redes sociales[203].

Bajo un esquema de gratuidad (correo electrónico, buscadores de contenido, manejadores de blogs, descargadores de aplicaciones, redes sociales, páginas interactivas, entre otros), hay realmente un precio que pagar: el de la privacidad, en un mundo virtual donde las personas se vuelven por excelencia "generadoras" de datos.

2. **Las personas: generadores de datos**

2.1. ***La comercialización de la personalidad***

El valor de los datos personales como un activo dentro de la llamada Sociedad de la Información es innegable y somos testigos de una mercantilización de los mismos que representa una verdadera "riqueza" para aquellos que poseen dicha información. Así, las empresas en línea son valoradas en gran medida por la carpeta de usuarios que poseen y, en consecuencia, por la masa informacional a la que tienen acceso y pueden interrelacionar. Google, por ejemplo, compró Dobleclick por 3,1 billones de dólares[204], estando ella misma valorada a principios de 2011 en aproximadamente 200 billones de dólares; casi tanto como Microsoft, que con sus 242 billones compite con Apple y sus 310 billones y está muy por encima de los 83 billones en que se estima Amazon, los 37 billones de Ebay, Yahoo y sus 21 billones y otras compañías *on line*[205]. Las redes sociales también aumentan progresivamente su valor, con Facebook a la cabeza con unos 85 billones, seguida de Twitter con 3,8 billones y LinkedIn con 2,4 billones[206].

conocían a alguien que le había ocurrido esto.

[201] AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID e INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACIÓN. *Op. Cit.* p. 87.

[202] Lo que en parte contradice la razón de las redes sociales de establecer interacciones "reales". Ver a este respecto VILASAU SOLANA (Mónica). *Op. Cit.* pp. 116-117.

[203] Ver GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *WP 163 Dictamen 5/2009 sobre las redes sociales en línea. Op. Cit.* También la Resolución sobre Protección de la Privacidad en los Servicios de Redes Sociales. 30a. Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Estrasburgo, 15-17 de octubre de 2008 y el Memorandum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes. (Memorándum de Montevideo), Montevideo, 27-28 de julio de 2009.

[204] NOTIMEX. "Aprueba UE fusión de Google y DoubleClick". *El Siglo de Torreón*, 12 marzo 2008. Fuente: http://www.elsiglodetorreon.com.mx/noticia/337345.html Responsable: El Siglo de Torreón.

[205] Ver a este respecto www.finance.yahoo.com

[206] Ver a este respecto www.sharespost.com/companies

Explican Charles Jenning y Lori Fena, fundadores de Truste, que las compañías que se desarrollan en Internet se cotizan hasta en dos mil dólares por cliente[207], aunque existeen muy diversas formas de cotizar la información, como se muestra con los vendedores de registros y la comercialización que hacen de listas de ficheros y datos de forma aislada[208].

Lo queramos o no el mercado ha puesto un precio a nuestra información, lo que para muchos replantea la naturaleza de este derecho sobre los datos personales, en una tendencia hacia su consideración no como un derecho personal sino como un derecho de propiedad o, al menos, un híbrido, que en todo caso aproxima su protección a la de los bienes intelectuales.

Todo esto genera una fracción entre la clásica visión de la vida privada como un derecho fundamental y personal y la demanda de la cibereconomía, donde el flujo y manipulación de los datos es uno de sus elementos principales y donde la tradicional idea de la *privacy* se contempla como un freno al desarrollo del comercio electrónico y de los negocios "en línea"[209]. Sin embargo, esta visión económica de la naturaleza de los datos personales, en cuanto al contenido de su protección se refiere, no deja de suscitar problemas que rebasan el aspecto jurídico al recontextualizar la concepción misma que coloca al ser humano como un fin y no como un medio en la sociedad de consumo.

En este contexto, uno de los principales problemas a que se enfrenta la protección misma del derecho a la vida privada es el propio modo en que es ejercido por sus titulares, que muchas veces exponen de forma alegre sus datos personales. En un estudio referenciado por Richard A. Hamilton y Lisa D. Spiller se señala que si bien el 69% de la población se mostraba en desacuerdo con la recolección de sus datos para fines comerciales, esta proporción se reducía a un 31% al explicarles las ventajas existentes para ellos como consumidores. Asimismo, otros estudios demuestran que las personas son más reticentes al uso comercial de ciertas informaciones, como la médica y la financiera[210].

Y así van surgiendo aspectos que necesariamente hay que considerar dentro de esta visión mercantilista del uso de la información personal: el de la personalización del mercadeo y la discriminación, el de la cesión de la información y la problemática del flujo trasnacional de datos, el de la comercialización de bienes personales o el del surgimiento de un nuevo "derecho de propiedad sobre los

[207] Citado por BELLEIL (Arnaud). *E-Privacy*. 1era. Ed., París, Dunod, 2001, p. 36.

[208] Resulta ilustrativo encontrar en línea empresas que venden "más de mil registros de jóvenes entre 18-25 años", "de personas mayores", "mujeres", locatarios", etc., "en cumplimiento" de las normas protectoras de los datos personales (según aclaran). Ver por ejemplo http://www.easyfichiers.com/

[209] Ver a PORTO MACEDO (Ronaldo). "Privacidad, mercado e información". *Cuestiones constitucionales: revista mexicana de derecho constitucional,* Nº 6, 2002, pp. 135-151.

[210] Ver referencias a diversos estudios sobre el mercado y la privacidad en HAMILTON (Richard A.) y SPILLER (Lisa D.). "Opinions about privacy: does the type of information used for marketing purposes make a difference?" *International Journal of Nonprofit and Voluntary Sector Marketing*, Vol. 4, Nº 3, Septiembre 1999, pp. 251-264.

datos personales".

2.1.1. *La personalización y el derecho a la privacidad*

Internet conllevó el nacimiento de una "nueva" economía en la que se intensifica la competencia sin fronteras frente a ofertantes que ni siquiera necesitan existir "físicamente" y en la que el consumidor, se dice, es el "rey". Sin embargo, no es menos cierto que con ella viene una infraestructura de vigilancia y trazabilidad y el desarrollo de un modelo de negocio en el que no siempre se paga con dinero, sino con datos, todo ello para brindar un servicio mejor ya que "el cliente así lo quiere"[211].

Del estudio estadístico de las tendencias del mercado, los *spam*, la publicidad en masas y la creación de perfiles genéricos de consumo se pasa a la creación de perfiles individuales, al marketing "*one to one*" y a la publicidad personalizada, a través del perfeccionamiento de métodos para monitorear y trazar e interconectar los comportamientos en línea. Así, observamos cómo se utilizan programas que interrelacionan y dan un "valor inteligente" a los datos erráticamente suministrados, a lo que sigue el "Internet de las cosas" pero también el "Internet de las personas", al mismo tiempo que se promueve la "fidelización" de los usuarios.

Todo ello enmarca una economía de la predictibilidad de la "intención" en busca de satisfacer al "cliente", que en unos años podría conducir incluso a la "creación" de la intención frente a generaciones completamente expuestas a medios de comunicación social "personalizados" y a una tecnología de monitoreo y trazabilidad.

Así, en el estudio realizado por Universal Mccann sobre la socialización de las marcas, buscando comprender la naturaleza de la demanda social de cada consumidor, categoría y mercado para asegurar el éxito de un producto, la agencia publicitaria visualiza una nueva evolución en la interacción con los consumidores destacando que el 47% de los usuarios de redes sociales en línea son miembros de una marca y ven de forma positiva la publicidad recibida a través de ellas[212], a diferencia de los correos no solicitados (*spam*), cuya recepción ha sido mayormente valorada de forma negativa.

Con ello se deja de lado la consideración de las personas como seres humanos transformándolas en consumidores potenciales o activos, objeto de observación constante a fin de satisfacer y prever sus "necesidades".

Por ello, no sólo somos vigilados, sino que la información que se ha obtenido de nosotros es utilizada para que nos lleguen solicitudes, ofertas y anuncios que nunca pedimos, fomentándose el consumo en un mundo de "predictibilidad". Y surge así

[211] BELLEIL (Arnaud). *Op. Cit.* pp. 7-40.

[212] UNIVERSAL MCCANN. *Socialisation of Brands, social media tracker, Wave 5*, Universal Mccann, 2010.

la famosa problemática del "*opt in*" y el "*opt out*", resaltando la mayoría de los defensores de la privacidad que el requerimiento del consentimiento previo para la recepción de publicidad debe ser necesario, aunque esto no esté tan claro en todos los países[213], por lo que, aunque la primera opción consiste en entender que sólo se debería poder recibir aquello que se demanda -sobre todo con la difusión del uso del *spam* o correos no solicitados-, la segunda aceptaría que se permita la recepción del mensaje siempre que el destinatario pueda solicitar ser retirado de la lista de difusión.

Estas comunicaciones comerciales no solicitadas presentan un doble atentado a la privacidad: por una parte, el derivado de la utilización de un dato de carácter personal (como es la dirección de correo electrónica de una persona) para un uso no autorizado y, por otra, la intromisión generada a la "paz" del individuo al recibir masivamente información no deseada.

Esto lleva a reflexionar sobre la interacción de las leyes de protección del consumidor y de tutela de los datos personales, siendo internacionalmente reconocido que estas tienen por finalidad el afrontar un desequilibrio en la "*capacidad económica, nivel de educación y poder de negociación*"[214] del público en general frente a los proveedores, ofreciendo una protección contra las cláusulas abusivas y la manipulación de la información ofrecida por los suplidores y sus necesidades. Pesa así sobre el Estado[215] la responsabilidad de garantizar el

[213] Mientras Estados Unidos, en su *CAN-Spam Act* de 2003, plantea el "*opt out"* como medio por excelencia, el Parlamento Europeo prefirió dejar un cierto margen de decisión a los legisladores nacionales (ver las Directivas 2000/31/CE del Comercio Electrónico, la 97/66/CE y 2002/58/CE, sobre privacidad y telecomunicaciones y la Directiva 2009/136/CE, que se refiere a los mensajes publicitarios que se remiten utilizando las nuevas tecnologías de los servicios de comunicaciones avanzadas, como el correo electrónico, los mensajes de telefonía móvil -mensajes SMS o MMS-, los llamadores automáticos, los mensajes de fax o las llamadas de telefonía vocal), aunque da claramente preferencia en el caso de particulares al "*opt in*" frente al envío masivo y automatizado de correos, siendo necesario el consentimiento previo en estos casos. Tenemos así que algunos países, si bien instituyen el "*opt in*" (sobre todo para la protección de particulares), conciben el "*opt out*" como una opción en ciertos casos, como por ejemplo, la existencia de una relación comercial previa o la calidad del receptor, diferenciándose entre particulares y profesionales. Ver por ejemplo la Ley francesa *Nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* y la *Nº 2011-302 du 22 mars 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques*. Ver a este respecto DROUARD (Etienne) y GAUTHRONET (Serge). *Communications Commerciales Non-Sollicitées et Protection des Données. Internal Market DG – Contract n°* ETD/99/B5-3000/E/96), *Commission des Communautés européennes*, Enero 2001, pp. 77-85.

[214] Resolución A/RES/39/248 de las Naciones Unidas, de 16 de abril de 1985, Directrices para la protección del consumidor.

[215] Se ha desarrollada así toda una legislación pro-consumidor tanto en Europa, como en Estados Unidos y Latinoamérica, siendo un tópico recurrente en los tratados de libre comercio y en la legislación nacional. Por ejemplo: Estados Unidos cuenta con el *Consumer Credit Protection Act of 1968, Codified to 15 U.S.C. 1601 note y el Fair Credit Reporting Act* (*FCRA), 15 U.S.C. 1681 et seq*., entre otros. La Unión Europea ha dictado diversas directivas relacionadas con la materia, así como un reglamento -*Règlement (CE) Nº 2006/2004 du Parlement Européen et du Conseil, 27 octobre 2004, relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs ("Règlement relatif à la coopération en matière de protection des consommateurs"*)-. Y, a nivel nacional, Inglaterra cuenta con *Unfair Contract Terms Act 1977, (1977, c. 50), Consumer Credit Act 1974,*

equilibrio entre los consumidores de bienes y usuarios de servicios y los proveedores, buscando promover un desarrollo económico y social justo, equitativo y sostenido.

No en vano el Acuerdo General sobre el Comercio en Servicios o *General Agreement on Trade in Services* (GATS), que forma parte de los tratados de la Organización Mundial del Comercio (OMC), en su artículo XIV letra c inciso ii, dispone dentro de los aspectos a considerar por los países miembros el establecimiento de leyes y regulaciones relativas al comercio de servicios que tomen en cuenta la protección de la privacidad de los particulares en relación con el tratamiento y la difusión de sus datos personales y la protección del carácter confidencial de los registros y cuentas individuales[216].

Incluso bajo el enfoque consumista se hace evidente dentro de este mundo "virtual" un doble desbalance:

- El de los internautas como potenciales consumidores de bienes y servicios y, por tanto, objeto del mercado publicitario, frente a la violación de sus derechos personales.
- El de los internautas como consumidores de un nuevo servicio: Internet y los medios sociales de interacción *on line,* en una época en la que ya se habla de que se provean servicios en la "nube"[217]. En este contexto, se evidencia un desequilibrio frente a la infraestructura de la red, las políticas de privacidad predefinidas y el poder real de negociación en la Web. En cuanto Internet es hoy, más que un lujo, una necesidad.

Se hace necesario, por tanto, plantear el problema del consentimiento como legitimador del uso de los datos personales cuando estamos en la mayoría de los casos ante a contratos de adhesión -problemática que se agrava cuando entra en juego el tratamiento de información de menores y de personas a las cuales la ley no les reconoce la posibilidad de dar un consentimiento válido-, así como el hecho de que la finalidad de la llamada "computación ubicua" [218] es, justamente, la recolección de datos con un propósito no siempre previsible y predefinido, siendo común, además, la cesión de los mismos.

(1974,c. 39), el The Unfair Terms in Consumer Contracts Regulations 1999 (SI 1999/2083), entre otros; en España existe la Ley 26/1984, de 19 julio, Ley de defensa de los consumidores y usuarios en España, Boletín Oficial del Estado Nº 176, de 24 julio 1984; en Francia existe incluso un Código que agrupa las leyes relativas al consumidor; y en Latinoamérica, por ejemplo, México cuenta con una Ley Federal de Protección al Consumidor publicada en el Diario Oficial de la Federación de 24 de diciembre de 1992, Última reforma publicada DOF 19-08-2010, en Chile la Ley Nº 19.496 establece Normas Sobre Protección de los Derechos de los Consumidores, Brasil cuenta con la *Lei Nº 8.078, de 11 de setembro de 1990, Código de Defesa do Consumidor* (L8078 - CDC) y la República Dominicana cuenta con la Ley 358-05, General de Protección de los Derechos del Consumidor o Usuario, 19 de septiembre de 2005, G. O. Nº 10337.

[216] Acuerdo General sobre el Comercio en Servicios de la Organización Mundial del Comercio. Anexo IB. Marrakech, Abril de 1994.

[217] Ver a GABADOU (Hervé). *Op. Cit.*

[218] Ver a CAS (Johann). *Op. Cit.* pp. 86-87.

Aun en los países donde existe una regulación legalmente instituida es usual aceptar el tratamiento no consentido de datos personales "necesarios para el servicio", que implica muchas veces la recolección y manipulación de información incluso no especificada al usuario y su posible transferencia a terceros no identificados.

Y de este modo el "sueño" del marketing puede traducirse en la "pesadilla" de los individuos ante estos llamados "*little brothers*" que todo lo observan en un mercado en el que la discriminación se pone a la orden del día. Desde el punto de vista de los comerciantes esta actividad sólo tiene por fin el poder vender más y de ninguna forma se pondría en riesgo esa confianza[219], pues los negocios se fundamentan en ella[220], pero ¿es esto suficiente para dejar de garantizar la privacidad?

De hecho, y ya de entrada, esta creación de perfiles particulares puede llevar a la discriminación de las personas[221]. Los datos obtenidos pueden utilizarse tanto para el diseño de estrategias comerciales, como para la adopción de decisiones individuales automatizadas que llevan a una clasificación de los usuarios de Internet, generándose una estratificación socioeconómica en la que se excluye a los clientes "no rentables", sea por no gastar lo suficiente, por no responder a ciertos anuncios o porque desean proteger su privacidad[222].

Esta tecnología permite incluso personalizar los precios de los productos ofertados, sea por el historial de consumo[223] (lo que ya ocurre en Amazon), sea por la elasticidad de las demandas, acuñándose el término "*privacy discrimination price*" con el que se explica que según los comportamientos y exigencias se generan "automáticamente" ciertas negociaciones a fin de realizar una oferta personalizada sin que ello siquiera sea de conocimiento del usuario[224].

Esto, obviamente, puede llevar a que determinadas personas reciban un peor servicio por entrar dentro de una lista de clientes "no deseados" al no ser

[219] BELLEIL (Arnaud). *Op. Cit.* p. 20.

[220] No en vano la Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), resalta la importancia de salvaguardar la confianza del consumidor, (ver el 7º considerando), siendo señalada la necesidad de consolidar "la confianza del comercio electrónico".

[221] Esto sin alludir a la llamada brecha digital, que se agudiza frente a las personas e incluso países que no tienen un efectivo acceso a las TIC's frente a los que sí. Aunque focalizado a los Estados Unidos, resulta interesante el informe NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (Estados Unidos de Norteamérica). *Falling Through the Net: Defining the Digital Divide*. Julio 1998. Fuente: http://www.ntia.doc.gov/ntiahome/fttn99/ Responsable: National Telecommunications and Information Administration.

[222] Ver a este respecto a OLIVER LALANA (Angel Daniel). *Op. Cit.*

[223] Ver en este sentido a ODLYZKO (Andrew). "The Unsolvable Privacy Problem and Its Implications for Security Technologies. *Lecture Notes in Computer Science*, Information Security and Privacy, Vol. 2727, Nº 219, 2003, pp. 51-54.

[224] Ver a este respecto a SCHWARTZ (Paul M.). "Property, Privacy, and Personal Data". *Op. Cit.* pp. 2077-2078.

suficientemente rentables, recomendando ciertos consultores, incluso, la creación de registros a tal efecto[225]. Y este peligro está latente no sólo para servicios y productos ofertados en línea, sino también para los que se ofertan en las tiendas "físicas" ante el mercado de la información que trae el Internet de las cosas y las personas.

La creación de "listas negras" está así a la orden del día -muy difundida, desde luego, en el sector crediticio-, alegándose en su favor el interés de las empresas de prevenirse contra ciertos clientes y su generación cuasi-automática como parte de la gestión del negocio. En su contra, hay que señalar, sin embargo, la dificultad de garantizar un buen manejo de ellas en términos de calidad de la información, seguridad y restricción de acceso a las mismas (confidencialidad) y la posibilidad de su utilización para fines distintos a aquellos por los que fueron generadas. Como bien señala Cédric Burton, estas listas generan el riesgo de "estigmatizar" una categoría de la población frente a dificultades que pueden ser pasajeras (incluso erróneamente), excluirla de ciertos servicios y afectar potencialmente los intereses de un grupo para proteger los de otro[226].

En este mismo orden de ideas se plantea también la problemática del tratamiento de datos sensibles[227] que normalmente hacen referencia a aspectos vinculados al origen étnico, religión, ideologías filosóficas o políticas, preferencias sexuales, pertenencia a grupos, así como a los que tienen que ver con la salud y a los registros criminales[228], que podrían llevar a una clara discriminación y a colocar a la persona en un cierto nivel de vulnerabilidad[229].

Y más allá de ello, sobre este tópico nos hacemos eco de Jean Michel Gruguière cuando señala que más que "datos sensibles" existen "tratamientos sensibles"[230], es decir tratamientos que deben implicar un mayor nivel de regulación y vigilancia debido a las consecuencias que el mal uso de la información podría generar[231]. En

[225] *Ibídem*.

[226] BURTON (Cédric). "A propos de l'avis de la Commission de protection de la vie privée du 15 juin 2005 sur l'encadrement des listes noires". *Défis du droit á la protection de la vie privée,* Cahiers du Centre de Recherches Informatique et Droit*,* Nº 31, 1ª Ed., Bruxelles, Bruylant-Facultés Universitaires Notre-Dame de la Paix de Namur, 2008, p. 148.

[227] En este sentido, ver el documento del G29 que resalta la particular problemática de generar "listas negras" basadas en la recogida y difusión de datos especialmente protegidos. Ver GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *WP 65, Documento de trabajo sobre las listas negras*, Adoptado 3 de octubre de 2002, 15 pp.

[228] Es interesante destacar que en su definición la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de julio 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 datos, no incluye entre los datos sensibles los registros criminales, por estar fuera de su alcance, al no afectar al tratamiento de datos relacionado con las actividades del Estado en materia penal (Ver Art. 3(2), 8).

[229] BING (Jon). "Introduction. Notions of sensitive personal data". *Défis du droit á la protection de la vie privée,* Cahiers du Centre de Recherches Informatique et Droit, Nº 31, 1ª Ed., Bruxelles, Bruylant-Facultés Universitaires Notre-Dame de la Paix de Namur, 2008, p. 194.

[230] BRUGUIÈRE (Jean-Michel). *Les données publiques et le droit.* 1ª Ed., Paris, Litec, 2002, pp. 55-56.

[231] Ver a este respecto a COY (Kevin L.). "The current privacy environment: Implications for third-party

este mismo orden de ideas, las Directrices de la Organización para la Cooperación y el Desarrollo Económico (OCDE) sobre protección de la privacidad y flujos transfronterizos de datos personales puntualizan que si bien algunos países han consensuado la existencia de datos particularmente sensibles, como es el caso de Europa, asimismo "*se puede afirmar que ningún dato es intrínsecamente 'privado' o 'sensible' pero puede llegar a serlo por su contexto y uso* […]"[232], posición de la legislación estadounidense. Datos que pueden ser considerados "triviales", almacenados y tratados de forma conjunta, pueden necesitar especial atención y protección.

Resulta así compleja la posición de los usuarios de la Web y de los servicios y productos en ella ofrecidos frente a la ilusión de un "consensualismo" y la predefinición de políticas de privacidad no negociables, la percepción generalizada de los datos personales como una mercancía intercambiable[233] y la dependencia dentro de la infraestructura actual de manejo de los negocios desde las nuevas tecnologías de la información y de la comunicación y el consecuente tratamiento de datos personales que lo motoriza[234].

La utilización comercial de los datos personales es una realidad que se impone y con ella viene, en un mundo "sin fronteras", la problemática del flujo trasnacional de los mismos.

2.1.2. *El flujo trasnacional de datos.*

La facilidad de transmisión de datos a través de la Web sin importar las fronteras plantea la problemática de su circulación a países donde no exista un nivel de protección adecuado en relación con el del país en el que su tratamiento y utilización fueron originalmente permitidos. Esto conlleva que haya que cuestionar quién es el responsable de asegurar el nivel mínimo de protección y cuál el marco legal aplicable[235].

Las organizaciones internacionales no han sido ajenas a esta cuestión, ya que los conflictos de seguridad, privacidad y falta de confianza pueden representar una barrera para el comercio, al ser el flujo de información parte de la nueva economía.

Así, por ejemplo, la Organización para la Cooperación y el Desarrollo Económico (OCDE)[236] y la Comisión de las Naciones Unidas para el Derecho

research". Journal of Continuing Education in the Health Professions, Vol. 21, Nº 4, 2001, pp. 203-214.

[232] Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales, 23 de septiembre de 1980. Apartado 7, párrafo 50.

[233] Ver en este sentido a TABATONI (Pierre), (Director). *Op. Cit. p.* 27.

[234] Ver con referencia a esto a TABATONI (Pierre), (Director). *La protection de la vie privée dans la société d'information*. Cahier des sciences morales et politiques, Tomo 2, 1ª Ed., Paris, Presses Universitaires de France, 2000, pp. 31-33.

[235] Ver a este respecto a PÉREZ ASINARI (María Verónica). "International aspects of personal data protection quoi vadis eu?" *Défis du droit á la protection de la vie privée,* Cahiers du Centre de Recherches Informatique et Droit, Nº 31, 1ª Ed., Bruxelles, Bruylant-Facultés Universitaires Notre-Dame de la Paix de Namur, 2008, pp. 381-413.

[236] La OCDE ha incluso emitido directrices y recomendaciones puntuales sobre el tema, llamando la

Mercantil Internacional (CNUDMI)[237] tienen dentro de su agenda de discusión ya este tema, sumándose a otros grupos de expertos también preocupados por la materia, como el Grupo del Artículo 29[238].

En este contexto, es indudable que 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, recontextualizó la problemática al exigir que la transferencia de datos sea posible sólo si el país tercero de que se trate garantiza un nivel de protección "adecuado" (Art. 25 de la Directiva), exigencia, sin embargo, insuficiente para muchos autores[239]. Por otra parte, se plantea con ello el reto de definir qué se entiende por un nivel "adecuado" de protección[240] y al mismo tiempo se genera un debate internacional a fin de que esta condición no represente una traba[241] para el comercio, lo que obliga a ir desarrollando principios internacionales básicos para la protección de los datos.

De esta necesidad surge la elaboración de los denominados "*Save Harbor Privacy Principles*" o principios de "Puerto Seguro" entre Europa y Estados Unidos en 1999[242]. Estos recogen básicamente las llamadas "*Fair Information Practices*",

atención sobre la importancia de solucionar esta problemática, estando sobre el tapete su discusión desde los años 80 y la conformación de un grupo de trabajo sobre la seguridad de la información y la vida privada. Ver las Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales, 23 de septiembre de 1980.

[237] La CNUDMI también dedica todo un grupo de trabajo (el IV) a discutir sobre estso, punto central de discusión desde los 90 y sobre el que ha elaborado diversos documentos, destacando en alguno de ellos que la solución más que legal debe ser tecnológica. Ver COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL. A/CN.9/WG.IV/WP 69 Electronic Data Interchange, 30a sesión, Viena, 26 Febrero - 8 Marzo 1996 y ver:

http://www.uncitral.org/uncitral/es/commission/working_groups/ 4Data_Interchange.html

[238] Entre los documentos más importantes emitidos por el G29 en la materia están el WP12 sobre Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de julio 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 datos; el WP 32, Dictamen 4/2000 sobre el nivel de protección que proporcionan los "principios de puerto seguro"; el WP 74 sobre la trasferencia de datos a terceros países y el WP107 sobre la cooperación para el establecimiento de una opinión común que garantice una salvaguardia adecuada como resultado de las reglas corporativas.

[239] Ver a este respecto a POULLET (Yves). "Flujo de datos Transfronterizos y extraterritorialidad: la postura europea". *Revista Española de Protección de Datos*. Agencia de Protección de Datos de la Comunidad de Madrid-Thomson Civitas, Nº 1, Julio-Diciembre 2006, pp. 93-113.

[240] Ver a ese respecto a GREENFIELD (Jo) y PEARCE (Graham). "Managing personal data flows to third countries". *Computer Law & Security Report*, Vol. 14, Nº 3, 1998, pp. 185-189; así como las recomendaciones del G29, WP 12, Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de julio 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 datos.

[241] Ver a este respecto a GARCÍA DEL POYO (Rafael) y GARI (Francisco). "Régimen jurídico aplicable a las transferencias internacionales y sus implicaciones en la actividad mercantil de las empresas multinacionales". *Revista Española de Protección de Datos.* Agencia de Protección de Datos de la Comunidad de Madrid-Thomson Civitas, Nº 2, Enero-Junio 2007, pp. 239-266.

[242] Ver en este sentido a KUNER (Christopher). "An international legal framework for data protection: Issues and prospects". *Computer Law & Security Review,* Vol. 25, Nº 4, 2009, pp. 307-317.

que incluyen los principios de información, elección, seguridad, integridad de la data, acceso y obligatoriedad [243] y las condiciones mínimas de protección ponderadas por las Naciones Unidas[244] en 1990, que resaltan el principio de respeto de la finalidad del tratamiento y de su legitimidad. Pero, el verdadero reto que ahora se plantea es el de cómo garantizar su cumplimiento, al no tener carácter coercitivo -lo que puede generar su falta de efectividad- y el que sean las empresas las que, voluntariamente, hayan de subscribir su cumplimiento.

Desde esta idea de voluntariedad van surgiendo también las llamadas "políticas de privacidad" que las empresas definen a fin de asegurar el mercado (pero cuyo contenido no es regulado en todos los países) e "informar" a sus usuarios a fin de obtenerse el consentimiento informado de los mismos en el tratamiento de sus datos personales. Aunque, como ya antes se señalaba, no dejan de ser acuerdos de adhesión, en los que las opciones se reducen a aceptarlos y tener acceso a un determinado bien o servicio o no aceptarlos y autoexcluirse del mismo.

La Web, en todo caso, replantea lo que entendemos por "flujo transnacional de información"[245]. La OCDE nos ofrece una definición sencilla de este concepto al decir que se entiende por flujo transfronterizo [246] de datos personales "*los movimientos de datos personales a través de fronteras nacionales*"[247]. Junto a ésta puede destacarse también la que encontramos en el Art. 12 del Convenio 108 del Consejo de Europa: "*transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento*"[248].

Cabría creer que todo aquello que circula por Internet entra dentro de esta definición, pero no siempre queda claro si la regulación desarrollada en las directivas europeas sobre la protección del flujo trasnacional de datos y en las normas generales desarrolladas para garantizar esos "niveles de protección adecuados" son aplicables a la Web.

[243] Ver a este respecto a NIMMER (Raymond T.) "Internationally interactive law: perspective on trans-border data control from the U.S ." *Défis du droit á la protection de la vie privée,* Cahiers du Centre de Recherches Informatique et Droit, Nº 31, 1ª Ed., Bruxelles, Bruylant-Facultés Universitaires Notre-Dame de la Paix de Namur, 2008, pp. 415-437.

[244]Directrices de las Naciones Unidas para la regulación de los archivos de datos personales informatizados, adoptadas mediante resolución 45/95 de la Asamblea General, 14 de diciembre de 1990.

[245] Ver a este respecto BARCELÓ (Rosa). "Introduction. Applying the provision on international data transfer to a wired world". *Défis du droit á la protection de la vie privée,* Cahiers du Centre de Recherches Informatique et Droit, Nº 31, 1ª Ed., Bruxelles, Bruylant-Facultés Universitaires Notre-Dame de la Paix de Namur, 2008, pp. 369-379.

[246] Ver a este respecto a DAVARA RODRÍGUEZ (Miguel Ángel). "La transferencia internacional de datos". *Revista Española de Protección de Datos.* Agencia de Protección de Datos de la Comunidad de Madrid-Thomson Civitas, Nº 1, Julio-Diciembre 2006, pp. 17-60.

[247] Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales, 23 de septiembre de 1980. Párrafo 1, c.

[248] Convenio 108 del Consejo de Europa para la protección de los datos personales con respecto al tratamiento automatizado de los datos personales, 28 de enero de 1981.

Si bien es cierto que la problemática originalmente se planteó en relación con la transferencia de datos dentro de grupos de filiales de un país a otro o a un tercero con el que se mantienen relaciones comerciales (vinculándose muchas veces la solución del problema con la suscripción de acuerdos contractuales y el establecimiento de procedimientos y políticas corporativas que garanticen un nivel de protección adecuado)[249], no es menos cierto que la circulación de datos toma otros matices cuando estos se colocan en la red, al ponerse a disposición, con ello, "trasnacionalmente".

El Tribunal de Justicia de las Comunidades Europeas ha negado ya que quepa aplicar a los contenidos colocados y accesibles en Internet la protección del Art. 25 de la Directiva 95/46/CE sobre protección de datos, por no haber habido "movimiento" que implicara la adopción de una posición activa del emisor en la transferencia de los mismos, estableciendo que no puede considerarse como tal el hecho de que desde un tercer Estado (desde una posición pasiva) se acceda a unos datos en la red[250].

Pero ¿no es una posición activa la de colocar datos en Internet a sabiendas de que los mismos serán accesibles en cualquier "tercer país"? ¿No es una ironía que se proteja la transmisión "cerrada" de los datos personales y no la disposición a nivel mundial a través de redes abiertas? ¿Qué es lo que buscamos garantizar?: ¿no es acaso un nivel mínimo de protección de los datos personales cuando circulan fuera de las fronteras nacionales? Rosa Barceló no lo pudo decir mejor: "*la imposibilidad de aplicar provisiones no significa que las metas perseguidas por estas se hayan vuelto, de alguna manera, irrelevantes*"[251].

Por otra parte, otra cuestión que cabe plantearse es la necesaria transmisión de datos que se genera de forma aleatoria en el recorrido que surge cada vez que un paquete de información se envía a través de la Web: diseñada para encontrar el camino más fácil nada nos garantiza que en esta ruta la data no pase por países que no cuenten con una nivel de protección "adecuado". Pues bien, tratada la misma como un problema de interceptación de telecomunicaciones, no deja de conformar una problemática que hoy día rebasa los contornos de lo nacional. Y así se inicia, a nivel tecnológico, el binomio conformado por la seguridad y la privacidad.

Definitivamente las nuevas tecnologías plantean un reto para el Derecho internacional y la definición de reglas estándares de protección de los datos personales y de la privacidad, en tanto que derecho fundamental cuyo respeto se

[249] Ver en este sentido los análisis planteados por SCHWARTZ (Paul). *Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment*. Privacy Projects, 2009, 73 pp.

[250] ORTEGA GIMÉNEZ (Alfonso). "Internet, publicación de datos personales y transferencias internacionales de datos: la sentencia del TJCE "Lindqvist", de 6 de noviembre de 2003." *Actualidad Jurídica Aranzadi*, Nº 790/2009 (Comentario), Pamplona, Ed. Aranzadi SA, 2009. Fuente: Base de datos Westlaw. BIB 2009\1907 Responsable: Westlaw.

[251] Traducción libre de la autora *"(...) the impossibility to apply a provision does not in itself mean that the goals intended by such provision have somehow become irrelevant*". BARCELÓ (Rosa). *Op. Cit.* p. 378.

impone sin importar las fronteras. Cómo se configure esta protección y cómo se garantice su cumplimiento son las piezas claves que definirán si después de todo la Era de la "informática" ha minado derechos y echado a la basura más de dos siglos de conquistas políticas, sociales y jurídicas o si, por el contrario, finalmente aprenderemos a contextualizar su uso y sus implicaciones para poder garantizar una "conexión" con los principios que definen un verdadero Estado de Derecho democrático.

2.1.3. *La comercialización de los derechos personales.*

Desde otra óptica, puede también señalarse que normalmente conceptualizados como derechos extrapatrimoniales, la comercialización de los llamados derechos personales presenta un reto para la lógica del Derecho occidental. La explotación económica de los atributos de la personalidad lleva a reflexionar sobre la verdadera naturaleza de estos derechos, la medida en que dicha mercantilización es posible y la posible existencia de un derecho de propiedad sobre los mismos.

Si bien es cierto que hoy en día se acepta el consentimiento como la base legitimadora de la utilización comercial de ciertos atributos de la personalidad, como la imagen y los datos personales, asimismo se resalta que la revocación de dicho consentimiento puede tener lugar en cualquier momento, debido a la naturaleza del bien negociado, al margen de que pueda también debatirse sobre su exclusión total del comercio o la plena aceptación de su concepción patrimonial[252]. Es bueno resaltar, en todo caso, que una de las características esenciales de la negociación de estos atributos es la de que en verdad no puede disponerse de ellos y transferirlos "definitivamente", pues al ser inherentes a la persona no pueden separase de ella. Si bien se pueden ceder o permitir ciertos usos de los mismos de una forma delimitada y concreta, siempre pertenecerán al individuo de quien emanan al ser inseparables de él y siempre existirán libertades que no puedan ser negociables[253].

Algunos autores señalan que una visión patrimonial de estos derechos beneficia en realidad sólo a aquellos que tienen mayor poder en el mercado de la privacidad, que no son otros que aquellos que colectan, procesan y transfieren los datos personales, establecen las reglas del juego y marcan el desarrollo de las tecnologías[254], quienes justamente son los que han provocado que los datos personales sean la moneda de cambio de los bienes y servicios del mundo virtual.

Como antes se indicaba, hay quien plantea también que no puede hablarse de un derecho de propiedad sobre el derecho a la vida privada, pues éste no beneficia

[252] Ver en este sentido a CABEZUELO ARENAS (Ana Laura). *Derecho a la Intimidad*. 1era. Ed., Valencia, Tirant lo Blanch, 1998, pp. 139-378 y a DOCQUIR (Benjamin). *Le droit de la vie privée*. 1era. Ed., Bruxelles, Groupe de Boeck, Larcier, 2008, pp. 111-150.

[253] Ver a este respecto a BRUGUIÈRE (Jean-Michel). *Op. Cit.* pp. 54-58.

[254] Ver a SCHWARTZ (Paul M.). "Property, Privacy, and Personal Data". *Op. Cit*. p. 2081.

solamente a un individuo, sino que es un interés (un bien jurídico) que también tiene una función social, lo que le convierte en un bien público que ha de ser protegido con independencia de la existencia del consentimiento individual que renuncie a ello. Enfoque de cierto tenor paternalista, frente a la idea de la libertad concedida a los individuos de "hacer lo que quieran", pero íntimamente relacionado a la concepción de un Estado entre cuyas finalidades está la de garantizar los derechos fundamentales. Si el favorecer el desarrollo del individuo, su plena autorrealización, se fija como objetivo fundamental de su misma existencia y si las personas son un fin en sí mismo, no puede negarse que garantizar una infraestructura en la que la privacidad pueda ser "realmente" ejercida es parte inexcusable del deber estatal.

Pero, hay también quien destaca la idea del nacimiento de un "nuevo derecho de propiedad", que descansa en la soberanía individual sobre los datos personales y en una concepción de la propiedad como suma de intereses a ser conciliados, proponiéndose una "inalienabilidad híbrida" que permita a los individuos compartir y colocar limitantes en el uso actual y futuro de su información personal. Desde esta perspectiva, hay que plantear el concepto de inalienabilidad, de derechos de salida, indemnizaciones y daños, de las garantías mínimas predefinidas[255] y, por supuesto, del derecho de propiedad y el de los derechos personales en sí mismos. Sí pareciera, en todo caso, que al hablar desde esta óptica de "cesión" de datos se hace más bien referencia a la comunicación de los mismos, lo que la diferencia de lo que es la concepción civilista tradicional de la cesión de bienes o créditos[256]. Pero también cabe afirmar que prohibir toda utilización de los datos personales resulta hoy imposible e inoperativo en una sociedad basada en el flujo de información: el uso comercial de los mismos es una realidad[257].

A modo de ejemplo, puede recordarse cómo se suscitó uno de los más grandes escándalos a nivel de protección de datos personales, cuando Toysmart.com[258], compañía propiedad de Disney, al caer en bancarrota anunció la venta de la información personal de sus clientes, incluyendo su nombre, dirección, información bancaria y familiar, sin que las personas cuyos datos se negociaban tuvieran derecho alguno a oponerse a la venta o a ser informados. Esto provocó un maremoto de reacciones en pro de proteger la privacidad, al ser una de las condiciones implícita del tratamiento de los datos originariamente obtenidos el uso

[255] Ver en este sentido a SCHWARTZ (Paul M.). "Property, Privacy, and Personal Data". *Op. Cit.* pp. 2094-2116.

[256] Ver a MESSIA DE LA CERDA BALLESTEROS (Jesús Alberto). *Cesión o comunicación de datos de carácter personal.* Estudios de Protección de datos, 1ª Ed., Madrid, Agencia de Protección de Datos de la Comunidad de Madrid, Thomson Civitas, 2003, 323 pp.

[257] LLACER MATACAS (María Rosa). "Comercialización de servicios y tutela de datos personales: el sector bancarios y asegurador". *Revista Española de Protección de Datos*. Agencia de Protección de Datos de la Comunidad de Madrid-Thomson Civitas, Nº 3, Julio-Diciembre 2007, pp. 171-220.

[258] Corte de los Estados Unidos del Distrito de Massachusetts. *Federal Trade Commission v. Toysmart.com et al*, 2000 *WL 34016434, D. Mass. July 21, 2000.*

confidencial de la información (más viéndose involucrados menores). Y condujo a que muchas empresas virtuales modificaran sus políticas de privacidad, a fin de evitar futuros conflictos legales, entre ellas Amazon y eBay (pese a las protestas de muchos de sus usuarios) que incluyeron la posibilidad de divulgación y cesión de los datos personales que se les facilitaran[259]. Con lo que se ve que la modificación operada en las políticas de privacidad y condiciones de uso de las sociedades virtuales no fueron precisamente las más protectoras de dicha privacidad en un marco local que lleva a la autorregulación y en el que siempre se impone la ley del más fuerte.

Es una realidad que uno de los mayores problemas que han surgido en este contexto es el del uso no consentido de los datos personales, en la medida en que la generación de los mismos, más que en una elección se transforma en una necesidad dentro de una sociedad que ha visto transformada la forma en que interactuamos diariamente y que lleva a la creación de perfiles digitales e incluso de una identidad digital de las personas. Esto genera expedientes que agrupan comportamientos, gustos y decisiones tomadas en un mundo virtual cada vez más estrechamente vinculado y condicionante del mundo "físico" e incluso el surgimiento de una nueva rama de empresas que se dedican precisamente a la recolección y tratamiento de datos personales con la única finalidad que la de su comercialización, con lo que desaparece ahora ya sí claramente el defendido principio de la finalidad que legitima un consentimiento "informado"[260].

De ahí van surgiendo las reivindicaciones que exigen configurar junto al mismo derecho a la vida privada un derecho al olvido digital[261], al anonimato[262] y a la desconexión. Derechos que deben ser viables jurídica y técnicamente.

2.2. ***El control estatal: ¿transparencia total?***

Si bien es cierto que los grandes emporios económicos han fomentado el desarrollo de una tecnología invasiva y ubicua, no es menos cierto que el gobierno también ha contribuido a la misma con su sed de control al ciudadano, justificando dicha intromisión, por regla general, con la explicación de una lucha contra el crimen organizado y el terrorismo y llegando a extremos nunca imaginados a partir

[259] CARROLL (Brian). "Price of privacy: Selling consumer databases in bankruptcy". *Journal of Interactive Marketing,* Vol. 16, Nº 3, 2002, pp. 47-58.

[260] Empresas como Aristotle International, Catalina Marketing Corporation y Donnelly Marketing Information Services se dedican a compilar bases de datos, por poner algunos ejemplos en el mercado norteamericano. Ver en este sentido a SOLOVE (Daniel). "The digital person and the future of privacy". *Défis du droit á la protection de la vie privée,* Cahiers du Centre de Recherches Informatique et Droit, Nº 31, 1ª Ed., Bruxelles, Bruylant-Facultés Universitaires Notre-Dame de la Paix de Namur, 2008, pp. 355-365.

[261] Ver a este respecto BERGUIC (Matthieu) y THIERACHE (Corinne). "L'oubli numérique est-il de droit face à une mémoire numérique illimitée". *Revue Lamy Droit de l'Immatériel*, Nº 62, Julio 2010, pp. 34-38 y a DESGENS-PASANAU (Guillaume). "Le droit à l'oubli existe-t-il sur internet?". *Expertises des systèmes d'information*, Paris, CELOG, Nº 343, Enero 2010, pp. 11-12.

[262] Ver a este respecto GRITZALIS (Stefanos). "Enhancing Web privacy and anonymity in the digital era". *Information Management & Computer Security*, Vol. 12, Nº 3, 2004, pp. 255-288.

del día 11 de septiembre de 2001[263] con el acceso a las mismas herramientas tecnológicas que el sector privado.

El Estado no es ajeno, por otra parte, a la utilización de las nuevas tecnologías en la prestación de los servicios públicos, como forma de agilizar y hacer más eficiente y transparente los mismos, lo que implícitamente conlleva la generación de expedientes digitales de los ciudadanos.

Así, el Estado y los ciudadanos interactúan con las TIC's desde dos perspectivas:

- como usuarios de los servicios públicos en el llamado "*e-goverment*" o administración electrónica;
- como entes sujetos a la vigilancia estatal.

2.2.1. *El e-goverment y la creación de perfiles digitales*

El mayor poseedor de datos personales no es otro que el Estado, que gestiona en el ejercicio de su función pública informaciones que van desde nuestro nacimiento y muerte, hasta nuestro nombre, estado civil, salario y afiliaciones; esto sin hablar de las generadas en la administración misma de los servicios públicos y como parte del control estatal (pruebas nacionales a los estudiantes, servicios sanitarios, transporte, licitaciones públicas, censos, registros civiles, registros de matrículas, registros de compañías, registros de patentes, de obras, seguimiento de expedientes administrativos y judiciales, naturalizaciones, registros policiales, registros criminales, pago de impuestos, etc.).

Pero, además, cuando se habla del gobierno electrónico o de la administración en línea no hay que pensar solamente en la utilización de las TIC's en la prestación diaria de servicios, sino en la interacción generada entre los ciudadanos y el Estado a través de la red[264] en diversos niveles:

- En un primer nivel, en el que se ofrece información actualizada y oportuna a los ciudadanos a través de las páginas web de las entidades públicas.
- En un segundo nivel, en el cual se posibilita el acceso a servicios electrónicos en línea y se facilita la realización de transacciones a través de la red, cuya

[263] MARTÍNEZ MARTÍNEZ (Ricard). *Una aproximación crítica a la autodeterminación informativa.* Estudios de Protección de Datos, APDCM, 1era. Ed., Madrid, Civitas, 2004, pp. 143-148.

[264] Tal como señalan France Belanger y Janine S. Hiller, hay que comprender que el Estado gerencia informaciones a las que tiene acceso o genera a través de diversas relaciones e interacciones, entre las que destacan: la relación entre el Estado y los ciudadanos para la prestación del servicio público; la relación entre el Estado y los ciudadanos para el fomento de la participación política (voto en línea, participación en línea de los procesos deliberativos, entre otros); la relación entre el Estado y los negocios, en tanto que actividad ciudadana (pago de impuestos electrónicamente, aplicación de su conformación a través de los portales, entre otros); la relación entre el Estado y los negocios como parte de un mercado -el Estado es también un consumidor de bienes y servicios, lo que implica la regulación de las relaciones comerciales del Estado con el sector privado, de la mano con la regulación de las compras y contrataciones de la administración pública-; la relación del Estado con sus empleados y la relación del Estado con otros Estados. Ver BELANGER (France) y HILLER (Janine S.). "A framework for e-government: privacy implications". *Business Process Management Journal,* Vol. 12, Nº 1, 2006, pp. 48-60.

carpeta de prestaciones tiende a aumentar y refinarse con los avances tecnológicos.

- En un tercer nivel, en el que se fomenta una participación política de la ciudadanía a través de portales interactivos y de la utilización de las herramientas de la Web 2[265].

El aparato estatal ha integrado la utilización de las nuevas tecnologías llevando como abanderadas la eficacia y la transparencia[266]. Pero, esto conduce a que la digitalización de la información y su integración en la red plantee las problemáticas propias de estos medios, agudizándose particularmente las mismas cuando hablamos de interconexión de bases de datos estatales, de transferencias interadministrativas y del subsecuente incremento de la publicidad de datos personales, sin mencionar la cantidad y calidad de la información colectada[267].

Curiosamente, la Administración pública fue inicialmente concebida como conjunto de entidades independientes, con competencias diferentes y con un manejo separado de las informaciones manipuladas, donde raramente se daban comunicaciones interinstitucionales. Estos intercambios dentro de la Administración eran severamente reglamentados, por lo que la interconexión de los datos de un ciudadano no era un problema[268]. Pero, esta realidad ha sido transformada por las facilidades que ofrece la Era digital para el tráfico y tratamiento de toda la información recopilada desde los diferentes sectores.

Fue justamente como una reacción a esta posible interconexión de datos, que de forma directa o indirecta desembocaría en un mayor control ciudadano y en una marcada invasión de la privacidad, por lo que surgieron las primeras leyes de protección de datos. Nos parece oportuno recordar el proyecto SAFARI (*Systéme Automatisé pour les Fichiers Administratifs et le Répertoire des Individus*) y la creación de la ley francesa "informática y libertad" de 1978 en la cual se buscaba la protección de los datos personales de los ciudadanos frente al Estado y la

[265] A ellos, entendidos como diversas etapas de evolución del *e-goverment*, France Belanger y Janine S. Hiller agregan aquél que tiende a unificar los servicios públicos a través de un portal que asegura la integración de los mismos frente a la ciudadanía. BELANGER (France) y HILLER (Janine S.). *Op. Cit*. pp. 50-52. Por su parte, Lorenzo Cotino Hueso diferencia entre una interacción básica y una avanzada, donde primero el ciudadano puede comunicarse con la administración y luego puede generase un diálogo. COTINO HUESO (Lorenzo). "La reciente cobertura jurídica para la interactuación de la Administración electrónica de los administrados: firma, registro y notificaciones electrónicas*". XVIII Encuentro sobre Informática y Derecho*. 1ªEd., Madrid, Universidad Pontifica Comillas, 2004, pp. 179-200.

[266] Ver a GUILLÉN CARAMÉS (Javier). "La administración electrónica*". Principios de derecho de internet*. 1ª Ed., Valencia, Tirant lo Blanch, 2005, pp. 247-292.

[267] Ver en este sentido a FERNÁNDEZ SALMERON (Manuel) y VALERO TORRIJOS (Julián). "Protección de Datos Personales y Administración Pública". *Revista Española de Protección de Datos*. Agencia de Protección de Datos de la Comunidad de Madrid-Thomson Civitas, Nº 1, Julio-Diciembre 2006, pp. 115-141.

[268] Ver a POULLET (Yves). "Administration électronique: le cas belge". *Défis du droit á la protection de la vie privée,* Cahiers du Centre de Recherches Informatique et Droit, Nº 31, 1ª Ed., Bruxelles, Bruylant-Facultés Universitaires Notre-Dame de la Paix de Namur, 2008, pp. 513-530.

posibilidad de ser "codificados"[269].

Hoy no estamos muy lejos de lograr esta "codificación ciudadana", cuando el número de seguridad social se usa como medio de identificación de una persona y permite dar acceso a la mayoría de los datos personales en Estados Unidos, se cuenta ya con un documento de identidad digital en países como España o en Italia se trabaja con la creación de una "red de la administración pública unificada", esto es, una red electrónica que conecte a todas las autoridades administrativas del país, y la mayoría de los países europeos cuentan con tarjetas de identificación sectoriales o unificadas[270], realidad a la que no es ajena tampoco Latinoamérica donde los documentos de identidad y electoral buscan o, al menos, consiguen codificar a sus ciudadanos.

En todos los Estados surge el problema de equilibrar la eficacia de la administración pública y la protección de los datos personales, ante tratamientos que en la mayoría de los casos pueden permanecer ocultos al ciudadano, por justificarse en una "cooperación interinstitucional". Todos los datos gestionados por la Administración pública parecerían formar parte del "aparato estatal", lo que puede llevar al abuso del acceso a la información[271].

Algunos Estados alegan que la simplificación administrativa conlleva la pérdida del control de la información personal, mientras otros arguyen que se deben aplicar los mismos principios que para el sector privado y respetar los principios del consentimiento y la finalidad en la utilización de los mismos[272], pero los expertos discuten si se debe permitir al Estado, con carácter general, la utilización de todas las tecnologías de trazabilidad que se encuentran a su disposición actualmente, resaltando sobre todo la problemática de los datos de transferencia y de la instalación de *cookies* o programas que permiten la creación de perfiles ciudadanos a fin de "personalizar" los servicios públicos, pero que a la vez recabarían un gran número de informaciones personales[273]. Habitualmente se alega que su utilización debería ser consensuada por el ciudadano, práctica seguida en principio tanto en Estados Unidos como en Europa. Sin embargo, no puede dejar de señalarse la brecha en el sistema, por una parte por la posibilidad de que el gobierno obtenga esa información al adquirirla de entidades privadas, por otra parte por la posibilidad

[269] Ver a este respecto la historia del CNIL: http://www.cnil.fr/vos-libertes/histoire/

[270] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS.*WP 73 Documento de trabajo sobre la administración en línea*, Adoptado 8 Mayo 2003, pp. 3-4.

[271] Ver a este respecto CASTRO MORENO (Abraham) y OTERO GONZÁLEZ (María del Pilar). *El abuso de información privilegiada en la función pública*. 1ª Ed., Valencia, Tirant lo Blanch, 2006, 164 pp.

[272] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS.*WP 73 Documento de trabajo sobre la administración en línea*, *Op. Cit*. pp. 16-18.

[273] Ver a este respecto a SÁNCHEZ NAVARRO (Álvaro). "La articulación del derecho a la protección de datos de carácter personal en la gestión electrónica de los procedimientos administrativos." *Revista Española de Protección de Datos*. Agencia de Protección de Datos de la Comunidad de Madrid-Thomson Civitas, Nº 3, Julio-Diciembre 2007, pp. 95-169; y a BELANGER (France) y HILLER (Janine S.). *Op. Cit.* pp. 53-56.

latente de que dicha recolección tenga lugar sin que la persona lo sepa[274].

El Estado se enfrenta así al reto de garantizar la utilización de los datos personales con fines legítimos[275] y gestionar correctamente los mismos frente a las exigencias de acceso a la información pública y su deber de rendir cuentas a la ciudanía[276].

Pero, la dimensión que toma la difusión de registros que se consideran normalmente públicos en la Era digital, hace que se presenten problemas antes ni siquiera planteados frente a las personas involucradas.

Es el caso, por ejemplo, de las sentencias judiciales y las resoluciones administrativas de cualquier índole o de la información fiscal[277].

Y si bien es cierto que la generación de muchos de estos registros se justifican por la modernización del Estado y el mejoramiento en la prestación de los servicios públicos, no es menos cierto que la rapidez y la facilidad con que los datos personales pueden ser recolectados e interrelacionados busca establecer un control de los ciudadanos que entraña la semilla de una vigilancia estatal ubicua.

2.2.2. *La vigilancia estatal: una lucha entre la seguridad y la libertad*

Originalmente los derechos fundamentales se erigen como límites al poder estatal a fin de garantizar el respeto de prerrogativas mínimas que garanticen el desarrollo de una vida digna. Sin embargo, en los últimos años somos testigos de cómo el concepto de "seguridad" rebasa todos los valores predefinidos y se convierte en la razón primaria del Estado que parece olvidar dichos límites al menos en lo que concierne a las ideas de libertad y dignidad humana.

[274] Ver este respecto a LÓPEZ LOMA (Luis). "El registro oculto *on line* y su conflicto con los derechos fundamentales según la doctrina alemana tras la sentencia del Tribunal Constitucional Federal de 27 de febrero de 2008". *Revista Española de Protección de Datos*. Agencia de Protección de Datos de la Comunidad de Madrid-Thomson Civitas, Nº 5, Julio-Diciembre 2008, pp. 223-228 y a LORENZ (Dieter). "El registro oculto de ordenadores como desafío en la dogmática de los derechos fundamentales y la reciente respuesta por la Constitución alemana". *Revista Española de Protección de Datos*. Agencia de Protección de Datos de la Comunidad de Madrid-Thomson Civitas, Nº 5, Julio-Diciembre 2008, pp. 9-24.

[275] Ver a este respecto PÉREZ VELASCO (María del Mar). "Los ficheros públicos". *Revista Datos Personales.* Agencia de Protección de Datos de la Comunidad de Madrid, Nº 16, Julio 2005. Fuente: http://www.datospersonales.org Responsable: Agencia de Protección de Datos de la Comunidad de Madrid.

[276] Ver en este sentido a Pierre Trudel, que llama a una redefinición del espacio donde circulan las informaciones y establece la necesidad de crear un marco regulador que permita efectivamente garantizar la correcta utilización de los datos personales dentro de una administración electrónica interconectada. Esto posibilitaría un flujo de las informaciones que permita un mejor servicio ciudadano, sin vulnerar sus derechos. TRUDEL (Pierre). "Hypothèses sur l'évolution des concepts du droit de la protection des données personnelles dans l'état en réseau". *Défis du droit á la protection de la vie privée,* Cahiers du Centre de Recherches Informatique et Droit, Nº 31, 1ª Ed., Bruxelles, Bruylant-Facultés Universitaires Notre-Dame de la Paix de Namur, 2008, pp. 531-558.

[277] Sobre ello, y en relación a la discusión en Estados Unidos, donde se reconoce como una excepción al derecho de acceso a la información pública el respeto a la privacidad, incluso de archivos considerados públicos pero estrechamente relacionados con un individuo, como los registros judiciales, ver a DAVIS (Charles)."Reconciling Privacy and Access Interests in E-Government". *International Journal of Public Administration*, Vol. 28, Nº 7, 2005, pp. 567-580.

A la metáfora del "Gran hermano" de Orwell que todo lo ve, se suma la de Kafka, en su libro "El juicio", en el cual el protagonista es juzgado sin conocer los cargos, en base a informaciones obtenidas de él que desconoce y cuyo uso le es ajeno[278].

Si bien es cierto que no se puede hablar dentro de Estados democráticos de una sed de dominio y represión totalitarista, las tecnologías actuales se caracterizan por el desconocimiento de la intromisión que permiten y su carácter no intrusivo o imperceptible (a pesar de su ubicuidad), con la consecuente generación de expedientes digitales que pueden marcar las decisiones que se toman sobre una persona.

Es llamativo a este respecto que los *Big Brother Awards*[279] premien las prácticas de creación de registros que conlleven una discriminación implícita de las personas que lo conforman y que se justifican en el control del riesgo y en la necesidad de identificación ciudadana.

Por ejemplo[280], en Francia han sido premiadas las compañías bancarias que ayudan al Estado a conformar registros sobre las personas no documentadas, denunciando a sus clientes. Cabe referir también aquí el caso de Christian Estrosi, alcalde de Niza, que instaló un denso y caro sistema de video vigilancia (600 cámaras con un costo de 7,6 millones de euros) que incluye el análisis automatizado de las imágenes, sin diferenciar menores ni adultos; igualmente, la creación de registros de educación escolar que genera expedientes de los niños a partir de los 3 años para llevar un control de su comportamiento escolar. Se han denunciado asimismo las tecnologías intrusivas permitidas por la Ley francesa, que obligaría a instalar programas espías y de monitoreo a todos los internautas franceses, así como el programa que pretendía imponer el gobierno Chino para conocer y filtrar las conexiones a Internet tanto de navegación por la Web como de otro tipo de servicios. Estados Unidos no se queda atrás con el proyecto de *US-Visit*, que recolecta de forma masiv los datos biométricos de todos sus visitantes, propone la implementación de un pasaporte estadounidense con RFID, gestiona la puesta en marcha de un sistema que compara a todos los viajeros con las listas de terroristas y persiste en el etiquetado con RFID de estudiantes de escuelas elementales.

Y si bien es cierto que muchos registros se justifican en la seguridad nacional y el control del riesgo ciudadano ¿qué peligro hay en que un niño de 3 años haga una

[278] Ver en este sentido a SOLOVE (Daniel). "The digital person and the future of privacy". *Défis du droit á la protection de la vie privée,* Cahiers du Centre de Recherches Informatique et Droit, Nº 31, 1ª Ed., Bruxelles, Bruylant-Facultés Universitaires Notre-Dame de la Paix de Namur, 2008, pp. 359-362.

[279] Es un premio que se concede a las instituciones privadas y estatales que amenazan la vida privada de las personas y existe en diversos países del mundo, tales como Alemania, Bélgica, España, Francia, Reino Unido, Estados Unidos, Australia, Japón, entre otros. Fue promovido por los fundadores de *Privacy International* en el Reino Unido en 1998.

[280] Ver http://www.bigbrotherawards.org/

rabieta o tenga problemas de conducta en un año escolar?, ¿debe quedar marcado por ello de por vida?, ¿qué peligro hay en que la gente viaje?, ¿eso justifica la implementación de dispositivos biométricos?

¿Es que no existen formas menos intrusivas de control?, ¿o todos los internautas somos presuntos culpables para ser monitoreados por el Estado? Entonces, ¿dónde queda la proporcionalidad de la intervención estatal?, ¿y dónde, en definitiva, una auténtica privacidad?

Todo ello sin mencionar los registros que se llevan como parte de un proceso penal, entre los que se encuentran las listas de presuntos culpables[281], lo que destruye la presunción de inocencia al incluir en la misma al menos en los registros policiales- a personas que pueden terminar siendo liberadas de toda responsabilidad; es llamativo en este contexto el sistema francés ARDOISE, que registra en una misma base de datos información de testigos, victimas y sospechosos. La problemática de la calidad de la información y la actualización de la misma se agudiza sin duda frente a la generación de "listas negras" del aparato estatal.

La lucha contra el crimen organizado y el terrorismo ha llevado a una política de protección estatal que sobrepasa la tradicional tutela preventiva, utilitarista o represiva a través del Derecho penal y de la actividad policial incorporando[282] nuevas tecnologías que posibilitan una vigilancia continua y oculta, buscando penetrar el "estado de la mente" de sus ciudadanos.

Y pasamos de presumir la inocencia de todo ciudadano a presumir la necesidad de una vigilancia de todos a fin de poder detectar una conducta "anormal", dentro de una configuración de la seguridad estatal en la que todos somos "sospechosos". El modelo penal garantista, resocializador, en busca de una justicia reparadora pasa a ser así reemplazado por el modelo penal de la "seguridad ciudadana"[283], acercándonos a un "Derecho penal del enemigo" en el que al parecer estamos en un perenne estado de guerra que todo lo justifica[284].

[281] Los Estado generan y conservan estas listas, incluyendo dentro de ellas incluso datos tan sensibles como el ADN. Recientemente un Tribunal estadounidense declaró ilegal el retener los datos genéticos de las personas que voluntariamente habían cooperado en la solución de un caso, cuando el Estado se negó a eliminar su perfil una vez declaradas inocentes. Ver ELLEMENT (John R.). "Court says state can't hold DNA". *Boston and Beyond. Now, Metro Desk*, 26 Agosto 2011. Fuente: http://www.boston.com/Boston/metrodesk/2011/08/appeals-court-says-cape-prosecutors-must-show-they-need-dna-profiles-worthington-witnesses/VDFsHvpTgMJTJLks6UGCuN/index.html Responsable: Boston and Beyond. Now, Metro Desk.

[282] Ver a LORENZ (Dieter). *Op. Cit.* pp. 9-24.

[283] Ver a DÍEZ RIPOLLÉS (José Luis). "De la sociedad del riesgo a la seguridad ciudadana: un debate desenfocado". Revista electrónica de ciencia penal y criminología, Nº 7, 2005. Fuente: http://criminet.ugr.es/recpc/07/recpc07-01.pdf Responsable: Revista Electrónica de Ciencia Penal y Criminología.

[284] Sobre el derecho penal del enemigo ver a GRACIA MARTÍN (Luis). "Consideraciones críticas sobre el actualmente denominado 'derecho penal del enemigo'". *Revista electrónica de ciencia penal y criminología*, Nº 7, 2005. Fuente: http://criminet.ugr.es/recpc/07/recpc07-02.pdf Responsable: Revista Electrónica de Ciencia Penal y Criminología, PÉREZ DEL VALLE (Carlos). "La fundamentación iusfilosófica del derecho

Sin embargo, la vigilancia y la intromisión en la vida privada de las personas, de ser la excepción justificada en los casos de delitos graves y por un tiempo limitado pasa a ser la norma, combinándose las bases de datos públicas con las conformadas por el sector privado y recopilándose información que va desde el monitoreo de las actividades financieras hasta el de las telefónicas[285]. Los servicios de inteligencia[286] ven así expandido su rango de acción y el manejo de mucha y muy diferente información[287].

La admisibilidad de las pruebas obtenidas a través de los registros ocultos se viene discutiendo, como es conocido, desde hace tiempo. Interesa destacar aquí la sentencia del Tribunal Federal Alemán de 31 de enero de 2007[288] que los declaró inadmisibles por falta de fundamento a estos efectos y que fue apoyada por el Tribunal Constitucional Alemán cuando que en una sentencia de 27 de febrero de 2008 declaró inconstitucional la norma que posibilita los registros *on line* de sistemas informáticos y justificó las interferencias secretas solo si *"existe una amenaza concreta para un interés jurídico preponderantemente importante"*[289].

Este modelo de vigilancia estatal ha traspasado las fronteras nacionales y ha llamado a la cooperación internacional[290], desde la que se legitima la utilización de sistemas como Echelon o Carnivore. Un Ejemplo de ello es la transmisión de datos de los pasajeros de aerolíneas a las autoridades norteamericanas y las transferencias internacionales dinerarias interbancarias SWIFT. Se ha discutido la validez de los acuerdos iniciales[291] realizados entre el gobierno estadounidense y la Unión Euro-

penal del enemigo. Precisiones sobre la interpretación de Kant". *Revista electrónica de ciencia penal y criminología*, Nº 10, 2008. Fuente: http://criminet.ugr.es/recpc/10/recpc10-03.pdf Responsable: Revista Electrónica de Ciencia Penal y Criminología y PORTILLA CONTRERAS (Guillermo). "Fundamentos teóricos del Derecho Penal y Procesal Penal del enemigo". *Jueces para la democracia*, Nº 49, 2004, pp. 43-50.

[285] Ver a GAYTON (Cynthia M.). "Beyond terrorism: data collection and responsibility for privacy". *VINE,* Vol. 36, Nº 4, 2006, pp. 377-394.

[286] REVENGA SÁNCHEZ (Miguel). "Servicios de Inteligencia y derecho a la intimidad*"*. *Revista española de derecho constitucional*, Año Nº 21, Nº 61, 2001, pp. 59-80.

[287] Ver sobre la vigilancia y el control del crimen a YAR (Majid). *Cybercrime and society*. 1ª Ed., London, Sage Publications Ltd., 2006, 200 pp.

[288] Ver a LORENZ (Dieter). *Op. Cit.* pp. 13-14.

[289] Tribunal Constitucional Federal Alemán. Sentencia BVerfGE 370, 595/07, de 25 de febrero de 2008. Revista Española de Protección de Datos. Agencia de Protección de Datos de la Comunidad de Madrid-Thomson Civitas, Nº 5, Julio-Diciembre 2008, pp. 317-396.

[290] Ver a RALLO LOMBARTI (Artemi). "El terrorismo internacional y sus conflictos: Seguridad versus privacidad - International terrorism and its conflicts: Security versus privacy". *Inteligencia y seguridad. Revista de análisis y prospectiva,* Nº 3, Diciembre 2007, Fuente: vLex, Id. vLex: VLEX-70306363. Responsable: vLex.

[291] Ver la Decisión 2004/496/CE del Consejo de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, oficina de aduanas y protección de fronteras de los Estados Unidos, y la Decisión 2004/535/CE de la Comisión de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al servicio de aduanas y protección de fronteras de los Estados Unidos.

pea[292] a este respecto, desde un prisma que, citando a Phillipe Walter, Encargado federal suplente de datos personales y transparencia de Berna (Suiza), permite afirmar "*[...] 'PNR'[293], 'Swift', 'pasaporte biométrico', 'ADN', 'control de fronteras', 'Eurosur'[294], 'refuerzo de los intercambios de datos con fines de cooperación policial y judicial', 'principio de disponibilidad', 'desarrollo del SIS'[295], 'Prüm'[296], 'interconexión', 'puesta en red', 'tecnologías de vigilancia ubicuas' [...] tantos vocablos vinculados a las políticas de seguridad en pleno auge desde el 11 de septiembre de 2001 y que nos recuerdan, por si fuera necesario, que vivimos en una sociedad de vigilancia. Capa tras capa, asistimos a la construcción sistemática de una línea Maginot tecnológica contra un enemigo huidizo e indeterminado y cuyas consecuencias en lo que respecta a las libertades individuales y al respeto de la intimidad podrían ser dramáticas (...)"*[297]. Medidas extremas, por otra parte, cuya efectividad no ha sido probada[298].

Justamente los acontecimientos del día 11 de septiembre de 2001 se alegan para justificar y de alguna manera "legitimar" estas medidas e iniciativas legislativas,

[292] Ver Corte de Justicia de la Unión Europea. Asuntos acumulados C-317/04 y C-318/04, Sentencia del Tribunal de Justicia (Gran Sala), Parlamento Europeo/Consejo de la Unión Europea, Luxemburgo, 30 de mayo de 2006. Para un análisis de la resolución del Tribunal Europeo que anula las decisiones sobre el intercambio de PNR ver a IRUJO AMEZAGA (Mikel). "Seguridad nacional versus derechos fundamentales." *Actualidad Jurídica Aranzadi* Nº 710/2006, Pamplona, Aranzadi SA, 2006. Fuente: Base de datos Westlaw. BIB 2006\948.Responsable: Westlaw.

[293] Ver la Propuesta de Decisión marco del Consejo de la Unión Europea de 6 de noviembre de 2007 sobre utilización de datos del registro de nombres de los pasajeros (*Passenger Name Record* - PNR) con fines represivos.

[294] Ver la Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones, sobre el examen de la creación de un sistema europeo de vigilancia de fronteras (EUROSUR), Bruselas, 13 febrero 2008, COM (2008) 68, final.

[295] Europa pasa del "SIS I" al "SIS II". El Sistema de Información de Schengen de segunda generación (SIS II) constituirá un sistema de información a gran escala con descripciones de personas y objetos. Ver Reglamento (CE) Nº 1104/2008 del Consejo de 24 de octubre de 2008 sobre la migración del Sistema de Información de Schengen (SIS 1+) al Sistema de Información de Schengen de segunda generación (SIS II) y Decisión Nº 2008/839/JAI del Consejo de 24 de octubre de 2008 sobre la migración del Sistema de Información de Schengen (SIS 1+) al Sistema de Información de Schengen de segunda generación (SIS II).

[296] El Tratado Prüm es un acuerdo de cooperación penal y policial e intercambio de información entre diversos países de Europa (Alemania, Austria Bélgica, España, Francia, Luxemburgo y Países Bajos), en relación a perfiles dactilares, ADN o registros de matriculas, para profundizar en la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, delincuencia transfronteriza y migración ilegal. No deja de sorprender que se coloque el problema migratorio junto al terrorismo. Ver Tratado entre el Reino de Bélgica, La República Federal de Alemania, El Reino de España, La República Francesa, El Gran Ducado de Luxemburgo, El Reino de los Países Bajos y la República de Austria, relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal (Tratado de Prüm), Prüm , 27 de mayo de 2005.

[297] WALTER (Jean-Philippe). "Perspectivas para la intimidad y la seguridad". *Revista Datos Personales*. Agencia de Protección de Datos de la Comunidad de Madrid, Nº 34, Julio 2008. Fuente: http://www.datospersonales.org

Responsable: Agencia de Protección de Datos de la Comunidad de Madrid.

[298] En un estudio sobre la interceptación de los correos por el FBI frente al terrorismo, Stephen Coleman cuestiona las posibilidades de detectar real y efectivamente comunicaciones entre terroristas con un escaneo masivo de los mismos. COLEMAN (Stephen). "E-mail, terrorism, and the right to privacy". *Ethics and Information Technology*, Vol. 8, Nº 1, 2006, pp. 17-27.

dentro de las que se destaca el llamado *Patriot Act* de Estados Unidos[299], que es la que, en cierta forma, inicia una bola de de nieve en el marco normativo a nivel internacional con su introducción de disposiciones que, entre otras consecuencias, restringen de modo importante lo que debe poder entenderse por auténtica privacidad.

En nuestro contexto, podemos destacar los cambios que la misma supone para la *Foreign Intelligence Surveillance Act* de 1978, modificada a fin de permitir el flujo de información entre agencias de inteligencia[300]. Especialmente controvertida es la nueva sección 215, titulada "Acceso a registros y otras cosas bajo el *Foreign Intelligence Surveillance Act"*, que extiende la clase de registros que se pueden realizar así como los objetos que el gobierno puede requisar, eximiendo a las autoridades públicas de demostrar una sospecha individual y requiriéndoles únicamente que indiquen que la información a obtener se considera "relevante" para una investigación llevada a cabo contra el terrorismo o para actividades de inteligencia clandestinas[301]. Siendo el término "relevante" ciertamente difuso y peligroso.

Cabe referir también aquí el problema de la conservación de los datos de transferencia[302], fomentada dentro de las políticas europeas de lucha contra el terrorismo, así como para la prevención, investigación, descubrimiento y represión de la delincuencia y de las infracciones penales en general. Es por ello por lo que surge la Directiva 2006/24/CE sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica, por la que se modifica la Directiva 2002/58/CE, que exige su conservación dentro de un periodo de 6 meses a 2 años (no ya 90 días), haciendo recaer dicha obligación en los proveedores de servicios de comunicaciones electrónicas de acceso público y en los proveedores de redes públicas de comunicaciones[303], que deberán almacenar los datos que permitan rastrear e identificar el origen de una comunicación así como su destino, identificar la fecha, hora y duración de la comunicación, identificar el tipo de comunicación y el equipo utilizado para la misma, así como su localización.

En este sentido, Luis Ramón Ruiz Rodríguez señala que esta directiva marca la

[299] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107-56.*

[300] Con anterioridad a la Reforma era necesario que se dieran ciertos requisitos para permitir dicho flujo, habiéndose construido por la jurisprudencia de la *Foreign Intelligence Surveillance Court* la teoría denominada "*wall requirements*". Ver a este respecto a ALLEN (Anita L.). *Privacy Law and Society*. American Casebook Series, 1era. Ed., St. Paul, Thomson West, 2007, pp. 816-830. La autora cita a este respecto el precedente *In re all matter submitted to the Foreign Intelligence Surveillance Court. 218 F. Supp.2d.11 (Foreign Intel. Surv. Crt. 2002).*

[301] Ver *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107-56. Sec. 215.* Ver también en este sentido a ALLEN (Anita L.). *Op. Cit.* pp. 520-523, 778 y 782-789.

[302] Ver a FATTA (Chiara). "La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo". *Il Diritto Dell'Informazione e Dell'Informatica.* Milano, Editora A.Giuffré, Año XXIV, Nº 3, Mayo-Junio 2008, pp. 395-414.

[303] Ver a RALLO LOMBARTI (Artemi). *Op. Cit.*

muerte de la vida privada frente al control estatal, al romper los esquemas inicialmente instituidos por la Convención de la Cibercriminalidad de 2001 y por la propia Directiva 2002/58/CE; textos en los cuales la preservación de los datos era la excepción y no la regla, siempre desde la idea de proporcionalidad estatal y en casos concretos, exigiéndose condiciones de preservación ciertas y seguras y recayendo sobre el responsable de la misma un deber de protección y confidencialidad de los datos manejados[304].

La seguridad pública se transforma en el objetivo esencial del Estado, que busca transparentar las acciones de los ciudadanos, hasta llegar a "prever" sus comportamientos, siendo la recolección, tratamiento y análisis de datos personales la fuente primaria de este nuevo esquema de control que las nuevas tecnologías perfeccionan y hacen posible. Los Estados parecen olvidar que dentro de ese mismo concepto de "seguridad pública" se encuentra, de la mano de la protección de la seguridad nacional, la garantía de la infraestructura económica y la prevención del crimen y los delitos, la necesidad de tutela de los derechos y libertades de todos[305] como elemento esencial de un Estado de Derecho democrático.

Es absolutamente necesario proteger los llamados datos personales, cuya recolección, conservación, manipulación y transmisión indebida atenta sin duda contra el derecho a la vida privada.

¿Cómo hay que configurar esta protección desde el nuevo marco que ofrecen las actuales tecnologías de la información y comunicación? y ¿cómo va a impactar la misma en lo que es la delimitación del derecho a la vida privada?

A ello habrá que dar sin duda respuesta desde las diferentes ramas del ordenamiento jurídico y esperemos se dé en favor decididamente de una idea de privacidad "real" muy vulnerable con los avances tecnológicos.

[304] RUIZ RODRÍGUEZ (Luis Ramón). *Respuestas internacionales a los retos de la seguridad.* Edición Social, serie mayor, 1ª Ed., Valencia, Tirant lo Blanch, 2009, pp. 215-228.

[305] Ver a AQUILINA (Kevin). "Public security versus privacy in technology law: A balancing act?". *Computer law & security review,* Vol. 26, Nº 2, 2010, pp. 130–143.