Tribuna

Ciberciudadanía y «nuevos» derechos: hacia la neo-privacidad

LA LEY 6501/2014

Ciberciudadanía y «nuevos» derechos: hacia la neo-privacidad

Josu OSÉS ABANDO
Letrado - Director de Gestión Parlamentaria
Parlamento Vasco

El advenimiento de la sociedad global/digital conlleva la progresiva mutación de nociones y realidades jurídicas y políticas firmemente asentadas. La salvaguarda de los datos personales, o privacy, se ve esencialmente afectada por la explosión comunicacional que, si bien está socializando el conocimiento en una escala exponencial, multiplica los riesgos de deslizamiento de nuestra identidad hacia escaparates virtuales de muy difícil control. Entre la manipulación, pública o privada, y la explotación mercantil de «lo que somos», ¿es posible activar nuevas líneas de defensa de nuestra neo-privacidad?

I. INTRODUCCIÓN

La confluencia de avances tecnológicos está revolucionando los paradigmas tradicionales de una manera tan radical que tan solo estamos avizorando los contornos preliminares de un nuevo estadio de la Humanidad. Sectores productivos enteros están intentando migrar al espacio digital o desapareciendo ante un marco competitivo cuya implacabilidad es pareja a su meteórica e incesante mutación.

Y esto afecta también a otros terrenos de la convivencia humana como la Política o el Derecho. Las ideologías dominantes, el mandato representativo clásico, las formaciones políticas, la Democracia, en suma, así como el Derecho como fuente primordial de la noción canónica de la Soberanía estatal, se observan incapaces de abarcar y regular la virtualidad de un espacio que escapa a las coordenadas que las han fundamentado en las últimas décadas.

En efecto, Democracia y Derecho experimentan una crisis simultánea (y en absoluto casual) que, en última instancia, impugna la concepción de perfecta localizabilidad y determinación del «Poder». Por contra, la globalizada realidad actual conlleva una relativización del Poder hacía multipolos que interactúan de forma muchas veces contradictoria e imprevisible tanto en el terreno económico como en el geopolítico.

Pero no quiere esto decir que Democracia y Derecho pertenezcan al pasado Precisamente el ideal democrático es la aspiración que ha conducido a que, como nunca en el pasado, sea mayor el número de países que disfrutan de regímenes razonablemente democráticos y que a se reivindique, al menos teóricamente, por la práctica totalidad de los movimientos políticos que luchan por transformar sus respectivos entornos. No obstante, es innegable que el imparable desarrollo de las TIC hace inevitable el surgimiento de una gobernanza multinivel fundamentada en parámetros harto distintos. En otras palabras, podemos hablar de la «agonía democrática» siempre que nos remitamos al origen etimológico del sustantivo, *ágonos,* es decir «lucha».

Sirvan estas consideraciones de sucinta aportación a un panorama que a todo jurista y, en general, a cualquier interesado en la calidad del estatuto democrático del ciudadano, le debe suscitar un interés preferente.

II. EL ESCENARIO CUANTITATIVO DE LA «NUEVA» PRIVACIDAD

Realizando un muy somero apunte histórico, estamos transitando desde lo que allá en los inicios (a nivel realmente operativo, hace unos 20 años más o menos) surgía como una nueva herramienta de puesta en conexión de (algunos) equipos informáticos por medio de un protocolo TCP-IP, hacia la masiva estructuración en red de una cantidad inimaginable de datos. Dicho de otro modo, a partir del derecho a la autodeterminación informativa «de lo que yo he colgado en la red», se asiste a la multiversalidad no ya de muchos datos sino del núcleo de la identidad del individuo.

Echemos un rápido vistazo a las previsiones que los observadores más solventes ofrecen como muy posible perspectiva evolutiva a corto/medio plazo.

— En cuanto al número de dispositivos imbricados en la Red, es un hecho cierto que ya en 2008 superó al número total de humanos y sigue creciendo a un ritmo mucho más rápido que nosotros. Había 13.000 millones en 2013 y habrá 15.000 millones en 2015 y 50.000 millones en 2020. Estas cifras incluyen teléfonos, chips, sensores, implantes, nuevos dispositivos *wearables,* y otros que ahora ni siquiera podemos concebir.

— No es tan fácil obtener una cuantificación sensata del volumen de información que intercirculará. De entre las múltiples profecías podemos atender a un informe de IDC (*International Data Corporation,* empresa líder en análisis de recursos y mercados digitales) (1) según el cual, de 2005 a 2020 el universo digital se multiplicará por 300 pasando de 130 a 40.000 exabytes (1 exabyte = 109 gigabytes) lo que supone una tasa per cápita de más de 5.200 gigabytes de información en 2020; de 2012 hasta 2020, el universo digital se está duplicando cada dos años. Y, por último, en 2015 en el seno de tan solo un par de domicilios particulares se generará el mismo tráfico de datos que todo el contenido en Internet en 1995 (http://vimeo.com/23903009).

La UIT (Unión Internacional de Telecomunicaciones) añadió, celebrando el día de Internet en 2013, que en el año 2016 habrá 81 «exabytes» de tráfico de contenidos en Internet cada mes, que corresponden a toda la información que podría almacenarse en unos 20.000 millones de DVDs y suponer un volumen de datos 54 veces superior al del año 2005 (2).

III. ¿TODOS Y TODO EN LA RED?: *BIG DATA*

Almacenamiento, obtención y explotación masivos de datos. Esta sería una telegráfica

aproximación definitoria del *Big Data.* ¿Es necesario poner de relieve que la enorme acumulación de información no pasaría de ser una simple mejora en la gestión y ahorro físico del almacenamiento si no estuviera íntimamente anudada a la posibilidad de analizar, correlacionar y explotar datos provenientes de múltiples fuentes?

A nuestros efectos, y coincidiendo con García Mexía, debemos hacer referencia específica a dos facetas claves del *Big Data:* el almacenamiento de datos «en la nube» o *Cloud computing* y el denominado «Internet de las cosas» como grandes vectores tecnológicos (3).

El *Cloud computing* no es, en esencia, otra cosa que la deslocalización de los datos desde la cercanía física a su propietario (persona física o jurídica) hacia macroemplazamientos más o menos ignotos situados a distancia (en «la nube») y a cargo de los prestadores del servicio.

La legislación actual pudiera ya tener una aplicación ordinaria y bastante literal en este caso. Como señala DOMAICA MAROTO (4), el art. 12.2 LOPD obliga al depositario como encargado del tratamiento del archivo a una instrumentalidad absoluta en el tratamiento de los datos que le ha confiado su propietario, es decir a no hacer una utilización indebida. Sin embargo, la aplicación de una legislación estatal adecuada choca en su efectividad con la lejana ubicación de la nube y su compartimentación en multitud de servidores con especificaciones muy variables y ubicuas.

Es evidente que, aunque necesaria, ni mucho menos será la solución una normativa europea por muy protectora que finalmente diseñe la Unión Europea si quedan nubes extraterritorialmente inmunes.

Respeto al Internet de las cosas (IdC), su concepto encuadra el conjunto de tecnologías que posibilitan una interconexión inteligente entre objetos para, en principio, facilitarnos aspectos cotidianos de nuestra vida.

Destacan los denominados dispositivos *wearables:* ropas y aparatos de uso personal permanente que, actualmente por medio del *smartphone,* tabletas o relojes-sensores, monitorizan nuestra actividad física, controlan parámetros de salud (programando, por ejemplo, la absorción programada de insulina o de una medicina, el control del colesterol, los hábitos de sueño o el control de ingestión calórica), etc. O los hogares (*Smart home)* equipados con electrodomésticos, controles de alarmas y otras posibilidades de domótica inteligente.

A nivel colectivo, *las smart cities* están ya informando de los niveles de sustancias alergizantes o los centros de salud más cercanos o la ubicación de los niños en una área de juegos (en Santander hay ya instalados 12.000 sensores).

Precisamente hace escasas fechas subrayaba *The Economist:* («*The internet of nothings»,* 28 de mayo de 2014) a la privacidad como un problema que puede aguar la fiesta a prematuras euforias, planteando varios casos que ejemplifican la falta de seguridad de esta nueva extensión tecnología. Así, la denuncia de la Comisión Federal de Comercio (CTC) de Estados Unidos contra TrendNet, por vender cámaras de seguridad controlables vía Internet que carecían de medidas de seguridad razonables, lo cual puso a los pies de los crackers la privacidad de 700 usuarios de la compañía. En resumen, «muchos terminarán decepcionados porque faltan demasiadas piezas en el rompecabezas» vaticinaba el semanario, aunque parece imparable una tendencia que podría alcanzar una media de 10 dispositivos permanentes por persona en 2020 (5).

IV. NEUTRALIDAD, MERCANTILIZACIÓN DE LA RED Y PROTECCIÓN DE DATOS

En 1993 el Centro Europeo de Física de Partículas (CERN) publicó una declaración en la que autorizaba la utilización gratuita y libre de la WWW, creada por Tim Berners-Lee cuatro años antes; el mismo inventor ha recalcado repetidamente la vocación universal que le motivó a abrir la www a todo el mundo. Y bien puede decirse que, históricamente, se trata del adelanto tecnológico que ha logrado una mayor expansión en menos tiempo.

También es cierto que en 2013 permanecía un grado de «brecha digital» que aqueja a los dos tercios de la población mundial que no tienen todavía acceso al mayor tráfico de información y de datos del mundo, oscilando entre un grado de conectividad de hasta más del 70 % en Europa (del 78 % de Suecia al 30 % de Hungría, Grecia y Portugal, pasando por el 65 % español (6) y de media de la UE) frente al 16 % en África.

Iniciativas como el Proyecto Loon de Google (para llevar la conexión a la red a aquellas zonas del planeta a las que todavía no ha llegado por medio de globos flotantes en la estratosfera que rebotan la señal de Internet) o Internet.org (Facebook, Samsung, Eriksson, Nokia, trabajando en proyectos conjuntos), hacen previsible el incesante incremento de zonas con cobertura. Otra iniciativa que parece más adelantada es O3B *(Other Three Billion),* consorcio impulsado por SES (dueño de Astra), HSBC, Google, etc., combinando el alcance de los satélites —ya han lanzado e instalado ocho— con la velocidad de la fibra (7).

Pero aun teniendo bien presentes estas diferencias, son enormemente menores si las cotejamos con los respectivos PIB o los índices de desigualdad social. Lo cual quiere decir que la Red es un formidable vehículo de progreso si, además, lo aunamos a su naturaleza descentralizada que hace ciertamente complicada, por lo menos, toda tentativa de censura y control ideológicos.

Pues bien, el universo digital conlleva una lucha por el control económico y la optimización de ingresos provenientes de las insospechadas posibilidades de negocio que se espera genere. La inevitable, pero todavía no mensurable, monetización de la Red acarreará sin duda nuevos interrogantes para lo que estamos denominando «nueva» privacidad. Además de la brecha digital a la que acabamos de referirnos, dos son los aspectos que merecen cierto detenimiento: la llamada neutralidad de Internet y la mercantilización de los datos.

En cuanto a la primera, se ha producido hace un mes una declaración que, sorpresivamente, no ha tenido excesivo eco mediático en Europa. Alcaldes de las grandes ciudades de EE.UU (entre los que se cuentan enclaves tecnológicos de primer nivel como San Francisco y Nueva York) han solicitado a la antes mencionada CFC que se preserven los principios de transparencia y de no discriminación y que defiende la neutralidad en la red en las próximas regulaciones que lleve a cabo en el sector. También han asumido el doble compromiso propio de defender la transparencia y el libre flujo de información a través de Internet y de orillar todo bloqueo e injustificada discriminación de tráfico legal en la red. Tal declaración carece de fuerza vinculante pero sí aporta un muy fuerte impulso político en un momento en el que se está originando un debate sobre la posibilidad de acceso a diferentes velocidades por parte de los proveedores de Internet, cobrando tarifas desiguales a los proveedores de contenidos en base a las velocidades de descarga que se esté dispuesto a abonar. Esto significaría que, en la práctica, el tráfico de datos dependería de la capacidad económica para poder pagar las tarifas impuestas por aquellos, dándose una Red discriminatoria.

No hacen falta excesivas dotes premonitorias para augurar una correlativa diferencia en la protección de datos, unos con salvaguarda de primer nivel y otros con mayor levedad de preservación. El debate surgió formalmente en enero a raíz de una sentencia del Tribunal Supremo y de una iniciativa de la propia CFC que lanzó una consulta-sondeo en pro de la «liberalización» de Internet que culminará en julio (8) y que también cuenta con la oposición frontal de Google, Facebook, Microsoft, Netflix y Amazon, etc.

En segundo lugar, por el lado de la rentabilización de los datos se puede pasar de la banalidad a la venalidad en expresión gráfica de Borja ADSUARA (9). La gran operadora ATT ha ofertado a los usuarios (por ahora circunscritos a la capital de Texas, Austin) la gratuidad de acceso con fibra óptica a cambio del uso de los datos generados en la navegación para su reventa con fines de marketing comercial.

V. SEGURIDAD Y PRIVACIDAD

El caso *Wikileaks* y las filtraciones difundidas por Edward Snowden sobre las actividades de la NSA constituyen el perfecto ejemplo de simbiosis entre opacidad, asalto a la esfera privada e irresponsabilidad. Por eso es pertinente comprobar la reacción de los agentes jurídicos competentes, en especial el poder judicial.

Con fecha 8 de abril emitió el Tribunal de Justicia de la Unión Europea un fallo declarando la invalidez de la Directiva 2006/24/CE que obligaba a los proveedores de comunicaciones a retener determinados datos y a ponerlos a disposición de la autoridades estatales, teniendo su origen en sendos casos suscitados en vía de decisión prejudicial en relación con las respectivas legislaciones de transposición de la directiva ante el Tribunal Supremo de Irlanda (a instancia de la ONG Digital Rights contra la Ley antiterrorista de 2005) y el Tribunal Constitucional austríaco (demanda del Gobierno del Land de Carintia contra la Ley federal de telecomunicaciones). Esta decisión del alto Tribunal comunitario manifiesta una relevancia especial no tanto porque innove radicalmente la doctrina jurisdiccional anterior, sino porque se produce en un momento de expectativa de próxima revisión de la legislación comunitaria. Podemos sintetizarla en tres grandes ideas-clave (10):

a) Las grandes posibilidades de cometer delitos y ampararse en la web implican que sea concebible una injerencia en la vida privada de las personas en aras, precisamente, de la lucha contra la criminalidad. La Carta Europea de Derechos Fundamentales posibilita en su art. 52.1 el establecimiento de limitaciones al ejercicio de los derechos fundamentales pero siempre que se guarde el principio de proporcionalidad, aún más si, como es el caso, se da un tratamiento automatizado de los datos.

b) Sin embargo, la directiva no respetaba las condiciones citadas desde una doble perspectiva. Por un lado se advierte una evidente falta de proporcionalidad dada la inconcreción de lo que se denomina «delito grave», que se deja al albur de las tipificaciones estatales; por la indeterminación procesal: no fijaba un régimen adecuado de autorizaciones (bien del juez, o de la autoridad competente); y, finalmente, por la indeterminación del período de conservación, de 6 a 24 meses, sin tener en cuenta a las personas afectadas o al ilícito perseguido.

c) Por otro lado, adolecía de un escaso sistema de garantías frente a abusos o accesos ilegítimos, ni tampoco marcaba una garantía clara de destrucción de los datos.

Esta transcendental decisión es el eslabón final de las críticas a la directiva, que ya se habían expresado en el informe de evaluación presentado por la Comisión en el Parlamento Europeo (COM-2011-225 final) y por el Controlador europeo para la protección de datos.

Visto este ejemplo alentador de cómo las instituciones europeas cumplen su labor garantizadora de la privacidad, y a la espera de cómo culmine tras la constitución de la nueva legislatura de la Eurocámara el proceso en marcha de modificación de la normativa comunitaria de protección de datos, no podemos sino lamentar un ejemplo diametralmente opuesto: la nueva Ley mexicana de telecomunicaciones.

Surgida de forma contradictoria de la reforma constitucional de 2013 derivada del Pacto por México suscrito por los tres principales partidos para la inclusión social en la Sociedad del Conocimiento, la Ley aprobada en julio obliga a los proveedores de telecomunicaciones a «proporcionar la localización geográfica en tiempo real, de cualquier tipo de dispositivo de comunicación a solicitud de los titulares de las instancias de seguridad o de los servidores públicos en quienes se delegue esta facultad» (art. 189); los arts. 190 y 191 les obligan a aceptar la intervención gubernamental de las comunicaciones privadas y, por último, con arreglo al art. 192, deben mantener el registro de los usuarios y las comunicaciones efectuadas durante dos años. Abierto el plazo para elevar recurso ¿modificará el Tribunal Supremo estas perniciosas novedades legislativas?

VI. CONCLUSIONES: RESPONSABILIDAD INDIVIDUAL, CONCIENCIA SOCIAL Y PROTECCIÓN INSTITUCIONAL PARA LA «*NUEVA*» *PRIVACY*

1. Los interrogantes que, como señalábamos al comienzo de estas reflexiones, se inscriben en cambio de paradigmas de la organización social en su conjunto, no han hecho sino darse por iniciados. La ciudadanía espera del Derecho y de las instituciones democráticas una urgente reacomodación para situar la privacidad en el globalizado caos digital.

Ahora bien, el protagonismo de la sociedad civil, tan creciente y extendidamente demandado en el contexto de la actual crisis sistémica, lleva ínsita la responsabilización de todos en el cuidado en la gestión de nuestros datos. Tampoco en este caso es defendible un inconsciente populismo que trasladara las soluciones —más provisionales y aproximativas que nunca— a las instituciones públicas ni, por contra, al supuesto libre juego del mercado.

Asistimos a un entrecruzamiento aparentemente contradictorio entre varios derechos, todos ellos vigorosamente reclamados: privacidad, libertad de expresión, transparencia, control parlamentario (11), y únicamente la promoción de una conciencia cívica podrá hacer efectivo el uso racional del libre y consciente consentimiento; todo ello en la medida en que tal consentimiento siga siendo una pieza necesaria,

de acuerdo con las directrices básicas de la vigente LOPD, para la cesión de datos. Porque no hay que engañarse: la evidencia es que «no somos nada celosos de nuestra identidad digital» a la vez que cada día más «hay quien sabe de nosotros más de lo que imaginamos» (12).

A modo de ejemplo estadístico, parece que en la sociedad vasca se da una preocupación ciudadana en torno al problema equiparable a los países con mayor penetración digital (aproximadamente un 66 % de personas preocupadas y un 59 % de sabedoras de la necesidad del consentimiento), reflejo de lo cual es que las reclamaciones ante la Agencia Vasca de Protección de Datos (AVPD) se están disparando en 2014 hasta en un 50 % (13).

Otra señal positiva radica en que, de acuerdo con los estudios más recientes, parece que los jóvenes están dejando de poder ser encuadrados en el tópico rótulo del «digifrikismo». Antes bien, son mucho más celosos de su privacidad online, según investigadores de Oxford (14), y esto va ya conllevando, por ejemplo, la migración desde las redes sociales tan en boga en el último quinquenio a vías más seguras y cerradas de mensajería instantánea.

2. Volviendo al consentimiento consciente me parece fuera de toda duda que el papel de las APD ha de insistir y responder a la pregunta ¿Cómo se puede proteger al usuario de sí mismo? Es evidente, en nuestra opinión, que tienen una encrucijada bastante similar a otros organismos controladores, parlamentos incluidos: reencontrar su misión en un contexto histórico bien diferente del que fueron creados. Para ello debe ponerse de relieve como atributo o línea de actuación de las APD una cierta *customización* de la actividad tuitiva, conjugable con la siempre necesaria generalización normativa de la ley. La complejidad exponencial del espacio digital obliga a segmentar las actividades de formación según tipos de datos y sobre todo en relación con las edades de la población.

Por último, pero no menos importante, las APD deben de mantener y, si es posible, intensificar la coordinación entre ellas como forma de contraatacar la desterritorialización de las novedades infractoras. Y aunque actualmente nuestra AVPD tiene por ley competencia únicamente sobre los ficheros de titularidad pública, ha logrado insertarse en los foros a nivel estatal (mediante la participación del director en el Consejo Consultivo de la AEPD, la integración en diversos grupos de trabajo y, a nivel operativo, con la remisión de los expedientes iniciados en la AVPD pero de competencia resolutiva de la AEPD) e internacional (Conferencia europea anual de autoridades de protección de datos; el denominado «Grupo de Berlín» de carácter más técnico; Conferencia internacional de autoridades de protección de datos).

A modo de resumen: asistimos ya a un inmenso ciberbazar en el que quizá pensemos aparecer tan íntimamente resguardados como cabalmente decidamos, pero estoy seguro de que, a la vez, seremos conscientes en nuestro fuero interno de que otros sabrán de nosotros lo que les interese para su poder comercial o para la supremacía política. Es la ruptura de la fronteriza nitidez entre «vida digital» y «vida real», el tránsito del recinto de la privacidad personal hacia el gran escaparate digital. Por eso debemos trabajar y formarnos para evitar el desistimiento o la renuncia al legítimo reducto personal. Para lo cual lo primero que tenemos que tener presente es, como señalábamos al comienzo, que debemos situarnos ante un ineluctable cambio de ciclo histórico con un desconocido empoderamiento de las potencialidades democráticas y, en paralelo, con nuevos peligros para los derechos que conforman nuestra autonomía. Entre otros, el derecho a la neo-privacidad. ■

NOTAS

(1) The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Grow th in the Far East (http://idcdocserv.com/1414).

(2) http://www.elmundo.es/elmundo/2013/05/17/navegante/1368766608.html.

(3) GARCÍA MEXÍA, P., Derechos y libertades, internet y tics, Tirant Lo Blanch, 2014, págs. 33 y ss.

(4) DOMAICA MAROTO, J. M., «Algunas cuestiones en torno al derecho fundamental a la protección de datos en la denominada "informática ubicua"», Revista de Derecho UNED, núm. 11, 2012.

(5) Para más datos sobre IdC y privacidad, es muy esclarecedor J. VIJAYAN en su estudio «6 ways the Internet of Things will transform enterprise security» (http://www.computerworld.com/s/article/9247485/6_ways_the_Internet_of_Things_will_transform_enterprise_security?).

(6) Es remarcable que el 71 % de los vascos entre 16 y 74 años utiliza de forma habitual Internet, según el informe «La Sociedad de la Información en España» de 2012 de la Fundación Telefónica. También debe tenerse en cuenta la plasmación normativa del principio de no exclusión digital en los estatutos autonómicos reformados: balear (2007, art. 29), andaluz (2007, art. 10.3.12), castellano-leonés (2007, art. 21), valenciano (2006, art. 19), aragonés (2007, art. 28.2), catalán (2006, art. 53), extremeño (2011, art. 7). Se puede consultar el buen análisis de NAVARRO MÉNDEZ, J. I., «El acceso ciudadano a las nuevas tecnologías de la información en los estatutos de autonomía reformados: ¿Un nuevo derecho social?», en Derechos sociales y principios rectores. Actas del IX Congreso de la Asociación de Constitucionalistas de España, Tirant Lo Blanch, 2012, págs. 834 a 847.

(7) http://www.o3bnetworks.com/homepage.aspx.

(8) El documento —paradójicamente titulado FCC Launches Broad Rulemaking to Protect and Promotethe Open Internet— está consultable en http://www.fcc.gov/document/fcc-launches-broad-rulemaking-protect-and-promote-open-internet; la carta-respuesta de 20 grandes firmas en http://cdn1.vox-cdn.com/assets/4422119/letter_to_FCC.pdf, y, finalmente, una útil referencia crítica EE.UU., hacia una red de dos velocidades: ¿una para ricos y otra para pobres? en http://www.elconfidencial.com/tecnologia/2014-05-16/eeuu-hacia-una-red-de-dos-velocidades-una-para-ricos-y-otra-para-pobres_131558/.

(9) ADSUARA, B., «De la protección a la prostitución de datos» (http://blogs.elconfidencial.com/tecnologia/menos-tecnologia-y-mas-pedagogia/2014-01-14/de-la-proteccion-de-datos-a-la-prostitucion-de-datos_75778/).

(10) No es baladí señalar que la génesis de esta directiva coincidió históricamente con los atentados terroristas en Madrid (11 de marzo de 2004) y Londres (7 de julio de 2005). Para un análisis más detenido de la STUE nos remitimos a CASTETS-RENARD, C., «L´invalidation de la directive 2006/24/CE par la CJUE: une onde de choc en faveur de la protection des données personnelles», Recueil Dalloz, de 26 de junio de 2014, y sobre su repercusión en la normativa española a RODRÍGUEZ LAINZ, J. L., «Sobre la incidencia de la Directiva 2006/24/CE en la ley española sobre conservación de datos relativos a las comunicaciones», Diario LA LEY, núm. 8308, de 12 de mayo de 2014. El estado actual de la cuestión es analizado por A. GALÁN MUÑOZ en «La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea (1)», Diario LA LEY, núm. 8356, de 17 de julio de 2014.

(11) Me remito sobre este tema de frecuente controversia en la práctica parlamentaria a mi segunda intervención en la Jornada del X aniversario de la Agencia Vasca de Protección de Datos, celebrada el 24 de febrero de 2014 en el Parlamento Vasco, y recogida en el libro de próxima publicación dedicado a dicha jornada.

(12) En sendas expresiones de los dos directores que ha tenido la AVPD, Iñaki VICUÑA (http://elpais.com/diario/2012/01/28/paisvasco/1327783210_850215.html(e Iñaki PARIENTE DE PRADA (http://www.diariovasco.com/20120602/local/quien-sabe-nosotros-imaginamos-201206022056.html).

(13) http://ccaa.elpais.com/ccaa/2014/02/23/paisvasco/1393178649_121262.html.

(14) A New Privacy Paradox: Young people and privacy on social network sites, en http://www.oxfordmartin.ox.ac.uk/downloads/A %20New %20Privacy %20Paradox %20April %202014.pdf.