DOCUMENTOS

10

Paloma Llaneza. Abogado y socio de Razona LegalTech.

La Generación Z: incógnitos y privados

La Generación Z está, en general, más preocupada por la privacidad que los Millennials, pero menos que la Generation X o los Baby Boomers. Sin embargo, esta preocupación no se traslada a los pagos con aplicaciones móviles o cuando usan las redes sociales. La Generación Z trabaja en la nube y desde la movilidad, y confiaría en sus teléfonos inteligentes y en las organizaciones que les facilitan, gratuitamente, servicios en nube y aplicaciones móviles sin limitación. Sin embargo, los proveedores de esos servicios acceden a la información sensible y a datos de sus usuarios que, tras ser tratados, pueden ser cedidos a otras organizaciones (bancos, compañías de seguros, farmacéuticas, empresas de publicidad, gobierno …) que toman decisiones basadas en esos datos con impacto en su vida, patrimonio, economía y perspectivas laborales de las que no son conscientes.

Los estudios demuestran que el actual sistema de protección de la privacidad mediante la recogida informada del consentimiento es virtualmente inútil y no protege a la juventud que las acepta sin tan siquiera clicar en el *link* en donde están disponibles.

Palabras clave: Privacidad, intimidad, protección de datos personales, datos personales, anonimización, consentimiento informado, Generación Z.

Incógnitos y privados

¿Es más consciente la Generación Z sobre los riesgos de la privacidad que sus hermanos mayores de la Generación Y? ¿Exigirán en el futuro un sistema legal que les proteja frente a la intromisión de los gobiernos y los OTT como Google o Facebook? ¿Cómo se compadece esa preocupación con el exhibicionismo constante en redes sociales? ¿Pasará la solución por entornos en los que se minimice la exposición y recogida de datos personales? ¿Es necesaria una política de concienciación sobre las serias consecuencias que tiene la recogida indiscriminada de datos personales?

El uso intensivo de aplicaciones como Snapchat, Secret y Whisper por parte de la Generación Z (Gen Z o iGen) se usa como ejemplo de que esta generación daría una mayor importancia a la privacidad, tras haber aprendido de los efectos que una exposición incontrolada habría tenido para sus hermanos mayores, los Millenials. Según esta apreciación, los riesgos e inconvenientes que implica compartir toda su información en internet habrían calado en ellos, pasando a usar plataformas que les permitan gestionar su información de manera efímera y segura.

Esta afirmación no está carente de aristas como veremos, ya que esas aplicaciones, si bien evitan la sobreexposición frente a terceros de la intimidad de sus usuarios, permiten a los proveedores de esos servicios acceder a información sensible y a datos de sus usuarios que, tras ser tratados, pueden ser cedidos a organizaciones que toman decisiones con base a esos datos, decisiones con un indudable impacto en su vida, patrimonio, economía y perspectivas laborales. Esto es especialmente

importante si se considera que la Gen Z es la primera generación que viven totalmente en la nube: allí guardan sus fotos, su información sensible, allí trabajan de manera colaborativa usando herramientas facilitadas por los OTTs. Esta actitud tiene un importante impacto en cómo la Gen Z percibe la privacidad, entendida como limitación del acceso de la información que publican en redes, pero con una total despreocupación de los efectos que tiene para su intimidad y desarrollo personal futuro el ceder toda su información a corporaciones que regalan servicios a cambio de datos.

Así se aprecia de los datos publicados por *The Center for Generational Kinetics*(1) que establece que la iGen Z está, en general, más preocupada por la privacidad que los Millennials, pero menos que la Generation X o los Baby Boomers. Así por ejemplo, a un 63% de la Generación Z le preocupa proteger su intimidad cuando realizan un pago con tarjeta, frente al 58% de los Millennials. La Generación Z también estaría más preocupada (un 38%) que los Millennials (29%) cuando se trata de proteger su identidad en la remisión y recepción de mensajes online. Sin embargo, **esta preocupación no se traslada cuando los miembros de la Generación Z pagan con aplicaciones móviles o cuando usan las redes sociales. Parece que esta confianza es tan nativa como el uso de las aplicaciones en esta generación**. Se fían de las aplicaciones móviles porque están en su vida desde el inicio. Se fían de las redes sociales que son para ellos tan naturales como jugar en el parque para los Baby boomers. Así pues, la Generación Z confía en sus teléfonos inteligentes y en las organizaciones que les facilitan, gratuitamente, servicios en nube y aplicaciones móviles.

Tampoco manifiestan la más mínima preocupación por proteger su privacidad en el trabajo, lo que se espera que impacte de modo negativo en la seguridad general de las empresas según se vayan incorporando al medio laboral y vayan escalando posiciones(2) dentro del mismo.

El estudio *The Center for Generational Kinetics* concluye que los miembros de la Generación Z:

- Están más preocupados de la privacidad pero esta preocupación se ve compensada con su tendencia innata a incorporar novedades tecnológicas.
- Esta preocupación disminuye cuando usan dispositivos móviles, pues confían en los prestadores de servicios en la nube, en las aplicaciones que instalan, y en los privilegios a los que éstas acceden sin ningún criterio de protección.
- No están preocupados por proteger su privacidad en el trabajo al que, por su edad, aún no se han incorporado.

Expresión pública v. privacidad

Como ya hemos destacado, la Generación Z es consciente de que la exposición en redes tiene un coste y, por ello, usan aplicaciones de contenidos efímeros y saben cómo configurar las preferencias de privacidad en los servicios que usan. En el caso de Facebook, por ejemplo, un 60% tienen configurados sus perfiles como privados, según un estudio de Pew Research Center(3) "*La Generación Z, Social Media, and Privacy*"(4).

Según este estudio, la Gen Z comparte una amplia gama de información sobre sí mismos en las redes sociales. Mientras no se protegen de los

(1)
iGen Tech Disruption: 2016 National Study on Technology and the Generation After Millennial. http://genhq.com/wp-content/uploads/2016/01/iGen-Gen-Z-Tech-Disruption-Research-White-Paper-c-2016-Center-for-Generational-Kinetics.pdf

(2)
Un 34% la Generación Z, un 35% los Millennials, 38%, un 37% la Generación X y un 37% los Boomers.

(3)
Richard Yao, Gen Z and Digital Privacy October 30, 2014 https://www.ipglab.com/2014/10/30/gen-z-and-digital-privacy/

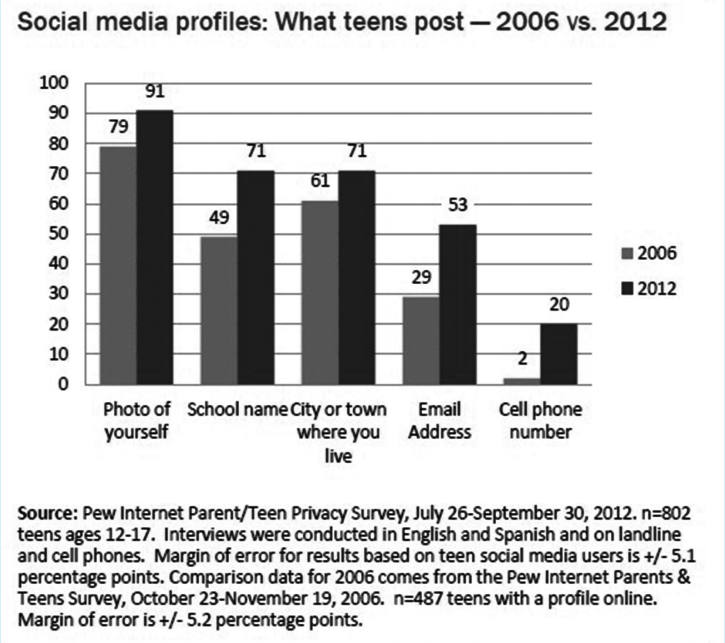
(4)
Teens, Social Media, and Privacy. Mary Madden, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, Aaron Smith and Meredith Beaton May 21, 2013. Pew Research Center. http://www.pewinternet.org/files/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/

prestadores, la Generación Z adopta medidas para restringir el acceso de terceros a sus perfiles, gestionando su reputación en las redes sociales.

Estas son algunas de las principales conclusiones de este estudio basado en una encuesta a 802 adolescentes que examina su gestión de la privacidad en las redes sociales.

1. **La Generación Z comparte más información acerca de sí mismos en redes sociales de lo que lo hicieron los Millenials (Figura 1)**
    - Un 91% publica selfies, frente al del 79% de los Millenials.
    - Un 71% publica el nombre de su universidad, frente al 49% de los Millenials.
    - Un 71% publica la ciudad o pueblo en el que viven, frente al 61% de los Millenials.
    - Un 53% publican su dirección de correo electrónico, frente al 29% de los Millenials.
    - Un 20% publicar su número de teléfono móvil, frente al 2% de los Millenials.
    - Un 92% publica su nombre real en su perfil.
    - Un 84% publica sus intereses reales, películas, música o libros que les gustan.
    - Un 82% facilita su fecha de nacimiento.
    - Un 62% publica su estado civil; y
    - Un 24% publica videos personales.

Figura 1



Source: Pew Internet Parent/Teen Privacy Survey, July 26-September 30, 2012. n=802 teens ages 12-17. Interviews were conducted in English and Spanish and on landline and cell phones. Margin of error for results based on teen social media users is +/- 5.1 percentage points. Comparison data for 2006 comes from the Pew Internet Parents & Teens Survey, October 23-November 19, 2006. n=487 teens with a profile online. Margin of error is +/- 5.2 percentage points.

2. Los miembros más mayores de la Generación Z es más probable que compartan determinados contenidos que los más jóvenes, si bien no se aprecia diferencia entre chicos y chicas, que tienden a publicar el mismo tipo de contenido.
3. Un 16% de los usuarios de redes sociales han configurado su perfil para incluir su ubicación por defecto en sus publicaciones.
4. La Generación Z usa más Twitter que los Millenials.
5. Las cuentas públicas en Twitter son la norma.
6. El usuario medio de Facebook tiene 300 amigos, mientras que el usuario medio de Twitter tiene 79 *followers*.
7. Los perfiles de la Generación Z en Facebook son un reflejo de su vida *offline*: siete de cada diez tienen a sus padres como amigos en Facebook.
8. Los más mayores de la Generación Z tienen una mayor variedad de amigos en Facebook, mientras que los más jóvenes tienden a ser más cautelosos con la gente que no conocen en la vida real.
9. Un 60% de los usuarios de Facebook configuran sus perfiles como privados y están convencidos de que saben cómo gestionar la herramienta de configuración de privacidad.
10. Las chicas suelen proteger más que los chicos sus perfiles.
11. La Generación Z es consciente de la importancia de la reputación *online* y adoptan medidas para protegerla.
12. La Generación Z revisa y borra contenidos de sus redes como parte de la gestión de su identidad *online*.
13. Un 74% han borrado alguna vez a un amigo de su perfil y un 58% ha bloqueado a alguien en una red social.
14. Un 26% ha publicado información falsa (nombre, edad o localización) para proteger su privacidad.
15. No manifiestan una especial preocupación por la cesión a terceros de sus datos personales. Sólo un 9% estarían muy preocupados.
16. La Generación Z no sería consciente del acceso de terceros a los datos que comparten en redes sociales.
17. Sin embargo, sus padres estarían muy preocupados sobre cuanta información obtienen las empresas de publicidad sobre el comportamiento de sus hijos *online*.
18. Aquellos de la Generación Z más preocupados por el acceso a sus datos por terceros es más probable que gestionen su reputación online.
19. Más de la mitad de los entrevistados han decidido no publicar un contenido preocupados por su reputación.

Vemos pues una mayor conciencia en la Gen Z sobre la reputación *online* y la gestión de su identidad digital pero una despreocupada ignorancia sobre la trascendencia del tratamiento de sus datos personales por las organizaciones y redes sociales que les prestan servicios de manera gratuita.

Para centrar el debate, conviene definir qué es la privacidad, la protección de datos, ver cómo se articula en nuestra legislación y, en fin, reflexionar si esta regulación es la más adecuada para proteger los intereses de la Gen Z.

¿Qué es la privacidad?

El concepto de privacidad no es unánime en todas las culturas legales si bien todos coinciden en señalar que se trataría de reclamar la protección frente a terceros de la vida privada, de aquellos aspectos personales que se preferiría no dar a conocer.

Según la RAE **Privacidad** es la cualidad de lo privado, es el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.

Visto así, la privacidad excluiría todo aquel conocimiento que fuera público o visible, o que hubiéramos expuesto voluntariamente en redes sociales o al aceptar unas condiciones generales al instalar una aplicación, empezar a usar un servicio o usar un objeto conectado.

De ahí que sea necesario establecer un concepto más concreto que proteja a los ciudadanos del impacto del uso de teléfonos inteligentes, aplicaciones y servicios en la nube y del tratamiento masivo de los datos con impacto a su intimidad. Ese concepto sería el de protección de datos, entendido como el derecho a la propiedad de los mismos, a retirar el consentimiento dado, a controlar su uso, en definitiva, allí donde los datos se encuentren. Así, los datos son siempre del titular de los mismos quien puede gestionarlos con total libertad y control.

Son datos protegibles aquellos que identifican o son aptos para identificar a una persona física, lo que supone incluir en el ámbito de dato personal cualquiera, desde los generados automáticamente por los dispositivos y aplicaciones, hasta los facilitados voluntaria o inconscientemente por parte del usuario: metadatos, una dirección postal, fotos, huellas digitales, vídeos, cualquier dato al que, aplicada la adecuada minería de datos, permita identificar a la persona que está tras ellos.

El derecho a la protección de datos

La primera actuación protectora de los datos personales tiene lugar en el marco del Consejo de Europa a través del Convenio Nº 108 del Consejo de Europa de 28 de Enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal(5), confiriéndole la consideración de derecho fundamental como viene siendo práctica común en la Unión Europea, frente a la protección de derecho del consumidor que otorga Estados Unidos.

En este sentido su artículo primero establece que

> *"el fin del presente Convenio es garantizar en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos")".*

En 1995 se aprueba 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(6), otorgando al derecho a la protección de datos el rango de derecho fundamental, tal y como se observa en su artículo primero al definir el objeto de la misma que no es otro que garantizar la

(5) https://www.boe.es/boe/dias/1985/11/15/pdfs/A36000-36004.pdf

(6) http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A31995L0046

protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

Amplía así el ámbito de protección con respecto al Convenio 108 puesto que este se aplica a tratamientos automatizados y la Directiva se aplica a tratamientos automatizados y no automatizados.

El compromiso de la Unión Europea en la protección de este derecho se consolida con la Carta de los Derechos Fundamentales de la Unión Europea del año 2000(7), al incluir en el artículo 8 la protección de datos de carácter personal:

> *"1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*
>
> *2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.*
>
> *3. El respeto de estas normas queda sujeto al control de una autoridad independiente".*

Por último en fechas recientes y tras más de cuatro años de tramitación legislativa, se ha aprobado el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos o RGPD)(8). El Reglamento nace ante la necesidad de adaptar la normativa a los avances tecnológicos salvando las lagunas existentes en la Directiva 95/46/CE. Su entrada en vigor se produce el 25 de mayo de 2016 pero su aplicación se pospone hasta el 25 de mayo de 2018, fecha en la que queda derogada la Directiva 95/46/CE, lo que provoca una situación de transitoriedad en el momento de redactar estas líneas.

El derecho a la protección de datos en España, como no podía ser de otra manera, ha corrido en paralelo al de la Unión Europea, considerando como derecho fundamental la protección de datos personales. La primera manifestación se produce tras la ratificación del Convenio 108 con la promulgación de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal(9).

Posteriormente, fue derogada por la actual Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal(10), constituyendo el marco jurídico general en materia de protección de datos personales junto con su reglamento de desarrollo, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal(11).

Por su parte el Tribunal Constitucional en sus Sentencias 290/2000(12) y 292/2000(13) vino a reconocer el carácter de derecho fundamental de la protección de datos personales definiéndolo como **un derecho de la autonomía de la voluntad del individuo sobre el control de sus propios datos manejados por terceros:**

(7) http://www.europarl.europa.eu/charter/pdf/text_es.pdf

(8) http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL% 3A2016%3A119%3ATOC

(9) https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189

(10) https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

(11) https://www.boe.es/buscar/act.php?id=BOE-A-2008-979 Téngase en cuenta que varios artículos han sido anulados por sendas Sentencias del Tribunal Supremo de 15 de julio de 2010 y 8 de febrero de 2012.

(12) http://www.boe.es/boe/dias/2001/01/04/pdfs/T00070-00093.pdf

(13) http://www.boe.es/boe/dias/2001/01/04/pdfs/T00104-00118.pdf

"un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'", lo que se ha dado en llamar "libertad informática" (FJ 6, reiterado luego en las SSTC 143/1994, FJ 7, 11/1998, FJ 4, 94/1998, FJ 6, 202/1999, FJ 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4).

Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran".

El problema del consentimiento

Todo el esquema protector de la legislación de datos de carácter personal se basa en la adecuada obtención del consentimiento del titular de los datos, lo que requiere una previa información de a qué tipo de tratamiento se facilita el consentimiento. Ello supone que esa información ha de ser clara, sin ambigüedades, en un lenguaje comprensible para el titular de los datos, de tal modo que el acto volitivo de consentir sea consciente.

En el mundo de las redes sociales, del uso de aplicaciones móviles o de objetos conectados, el consentimiento es simplemente ilusorio, bien porque no hay información previa ni vía de prestarlo, bien porque el tipo de información facilitada es tal larga e incomprensible, que el usuario no la lee. De hecho, los formularios de consentimiento están diseñados como un paso previo, necesario y sin cuya aceptación no se pueda alcanzar la pantalla siguiente y obtener el servicio o descargar la aplicación a la que pretendemos acceder.

En este sentido resulta revelador el trabajo realizado por la Universidad de Berkeley(14) en que plantean un ejercicio para determinar si la presencia de un link a una política legal de privacidad (protección de datos) en una web o en la descarga de una app tiene alguna influencia significativa en la voluntad de los usuarios para facilitar información personal.

(14)
Coen, Rena; King, Jennifer; and Wong, Richmond.. The Privacy Policy Paradox. UC Berkeley School of Information.

Hay múltiples estudios que exploran el contenido y eficacia de estas políticas de privacidad. Como hemos indicado, se presume que la elección sobre si facilitar o no datos personales, viene regido por el consentimiento informado que parte de la premisa de que los usuarios son seres racionales capaces de leer en profundidad documentos legales para evaluar las prácticas de privacidad y protección de datos de una web o una aplicación móvil. Múltiples estudios ya han confirmado que la mayoría de nosotros sabemos que estas condiciones legales se leen muy raramente(15), que leer las políticas de privacidad de cada web que se visita nos llevaría una cantidad de tiempo poco razonable(16); y que están a menudo escritas en un lenguaje tan complejo que están lejos de la compresión lectora de la mayor parte de los usuarios.

En definitiva, las políticas de privacidad y protección de datos son documentos legales escritos por abogados para abogados y no para usuarios finales y mucho menos para adolescentes.

Una encuesta de 2009 determinó que la mayoría de los participantes creían que las políticas de privacidad y protección de datos protegían sus derechos, cuando en realidad están orientadas a asegurarse la recogida de datos y cesión sin problemas. De hecho, muchas condiciones, aun cumpliendo la ley escrupulosamente, suponen de facto una invasión de la intimidad de sus usuarios(17). En el piloto previo a este estudio de la Universidad de Berkeley comprobaron que ninguno de los participantes hizo clic en el *link* que llevaba a las condiciones de privacidad.

El estudio parte de la base de que **los usuarios no son conscientes de la elección que realizan y de las consecuencias e implicaciones que para su vida privada puede tener. Una decisión sin pensar cómo facilitar información de salud a través de una app conectada con una pulsera de entrenamiento o un reloj inteligente, puede tener consecuencias negativas en el medio plazo si el desarrollador de la app cede (y sin duda lo hará) esos datos a una compañía de seguros que los puede utilizar para denegar un seguro de vida, de salud o para aumentar considerablemente la prima.**

Parece, por tanto, que tal vez un sistema basado en la recogida de consentimiento pueda no estar protegiendo los derechos fundamentales a la intimidad y a la protección de datos de los individuos y mucho menos de los adolescentes que conforman la Gen Z.

El consentimiento en la ley

Tanto el artículo 5 de la LOPD como los artículos 12 a 14 del Reglamento general de protección de datos obligan, con carácter previo a la recogida de datos personales, a facilitar información clara y permanente al interesado sobre una serie de aspectos como son los fines y usos previstos. Dicho deber de transparencia en la información plantea problemas de diversa índole ya mencionados, a saber:

- Uso de largas y farragosas políticas de protección de datos o privacidad que casi nadie entiende ni lee.
- En dispositivos de pantalla reducida el tamaño es un hándicap a la hora de facilitar esa información.
- Una vez que se ha informado sobre unos fines y/o comunicaciones previstas se plantean problemas de cómo informar y ser transparentes ante finalidades o comunicaciones no previstas en el momento inicial.

(15)
Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: self-reports versus observed behavior. International Journal of Human-Computer. Studies, 63(1), 212. Milne, G. R. and Culnan, M. J. (2004), Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. Journal of Interactive Marketing, 18(3), 15–29.

(16)
McDonald, A. M., & Cranor, L. F. (2008). The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society 2008 Privacy Year in Review Issue, 4, 543.

(17)
Turow, J., King, J., Hoofnagle, C. J., Bleakley, A., & Hennessy, M. (2009). Americans reject tailored advertising and three activities that enable it. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214,

- Intervención de diversos responsables de tratamiento como el fabricante del producto, el diseñador del sistema operativo, tiendas de aplicaciones, diseñadores de aplicaciones, terceros (publicidad, operadores de servicios de comunicaciones, mercantil que regala un servicio que se remunera con los datos, uso de dispositivo wearable, etc ...). Todos ellos deben de capaces de informar al interesado en los términos establecidos en la normativa de protección de datos.

En este sentido el artículo 12.7 del RGPD permite facilitar la información en combinación con iconos normalizados También se podrían establecer *links* permanentes a políticas de privacidad o facilitar la información en capas como ocurre con los avisos de *cookies*. En lo que respecta a los usos futuros, teniendo en cuenta que los dispositivos móviles podrían incluir de fábrica la posibilidad de informar al interesado a través de una advertencia en la pantalla con *link* a la nueva política de privacidad o a la versión modificada.

Salvo que el tratamiento pueda encuadrarse dentro de una de las excepciones al deber de obtener el consentimiento (ejecución de un contrato o precontrato en interés del afectado, interés legítimo del responsable de tratamiento o un tercero salvo que prevalezcan los derechos y libertades del interesado, etc) el consentimiento debe ser:

- Libre.
- Específico.
- Iinformado.
- Inequívoco.

Lo que equivale a que sea expreso requiriendo en el RGPD una "*declaración o una clara acción afirmativa*". De tratarse de categorías especiales de datos incluidos en el artículo 7 de la LOPD o del artículo 9 y 10 del RGPD, el consentimiento deberá prestarse de manera explícita. Al igual que ocurre con el derecho de información se plantean, entre otros, los siguientes problemas:

- Que el consentimiento sea explícito o inequívoco requiere poder probar por parte del responsable de tratamiento que se otorgó. Por su parte el artículo 7.1 del RGPD dispone que cuando el tratamiento se base en el consentimiento, el responsable debe estar en disposición de demostrar que se otorgó. Por ello no basta con incluir por ejemplo una casilla para marcar y un botón con la palabra "acepto", sino que debe quedar registrado de algún modo que esa acción se realizó.
- En relación con futuros tratamientos no previstos inicialmente, se deben diseñar procedimientos y métodos técnicos que hagan posible la obtención de nuevos consentimientos para nuevos tratamientos.
- Al ser revocable, se deben establecer procedimientos y métodos técnicos de fácil localización y acceso permanente por parte del afectado.
- En relación con 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), el artículo 5.3 establece la necesidad de obtención del consentimiento del abonado para captar información almacenada en el equipo terminal. No es necesario obtenerlo si esa captación se realiza con el único fin de "efectuar o facilitar la transmisión

de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o el abonado".

- En relación con el tratamiento basado en un interés legítimo de responsable, cabe traer a colación para las tecnologías IoT el Considerando 49 del RGPD que entiende que las medidas destinadas a garantizar la seguridad de una red constituyen un interés legítimo.
- Cuando se trata de **servicios** de la sociedad de la información **destinados a menores de 16 años o 13, en el supuesto que el Estado miembro rebaje la edad como máximo hasta los 13 años, el RGPD establece que el consentimiento sólo será lícito si lo otorga el titular de la patria potestad o tutela legal del menor, debiendo realizar el responsable esfuerzos razonables atendiendo a la tecnología disponible para verificar esa autorización. Por su parte el artículo 13 del Real Decreto 1720/2007 establece con carácter general la edad de 14 años como edad a partir de la cual no es necesario contar con el consentimiento de padres o tutores.**
- Los diferentes responsables de tratamiento también deben obtener el consentimiento del interesado antes de iniciarse el tratamiento. En relación con las aplicaciones preinstaladas en el dispositivo debería ser posible su desinstalación si no son necesarias para el funcionamiento del mismo y, con carácter general, cuando se desinstale cualquier aplicación se debe entender que se ha revocado el consentimiento que legitima el tratamiento, entrando en juego la supresión de los datos o en su defecto los plazos de mantenimiento de los mismos, así como la comunicación de la supresión a los cesionarios.

En lo que respecta a las comunicaciones de datos (cesión a terceros) volvemos a tener idéntica problemática. El artículo 11 de la LOPD dispone con carácter general el consentimiento previo del interesado o que se ampare en alguna de las excepciones legalmente previstas (amparada por norma con rango de Ley, en interés vital del afectado, etc). Por su parte el RGPD tanto en su artículo 13.1.e) como en el 14.1.e) establece el deber de informar sobre "*los destinatarios o las categorías de destinatarios de los datos personales, en su caso*" y que sobre ese deber de información previo se solicitará el posterior consentimiento, por lo que nos remitimos a lo reflejado en líneas anteriores.

La mitigación de la falta de consentimiento de facto: el derecho a cancelar o cambiar de opinión

Transparencia e información, consentimiento y comunicaciones de datos no pueden ofrecer un óptimo nivel de protección sin un adecuado sistema de ejercicio de derechos de acceso, rectificación, cancelación y oposición (Título III de la LOPD) o de acuerdo con el RGPD acceso, rectificación, supresión "derecho al olvido", oposición, decisiones individuales automatizadas, portabilidad y limitación en el tratamiento.

En relación con estos derechos se plantean las siguientes cuestiones:

- Se debe estar en disposición de informar sobre las comunicaciones de datos realizadas, tanto a otros responsables y partes relacionadas con ese dispositivo, como de las realizadas al interactuar con otros dispositivos.

- Que **se anonimicen lo datos no exime del deber de informar sobre la misma así como del riesgo de reidentificación existente y aceptable que se recoge en el análisis de riesgos realizado**. Con un riesgo aceptable de reidentificación no aplica la normativa de protección de datos pero, como indicamos, ello no exime del deber de responder a la solicitud del ejercicio del derecho por parte del afectado.
- Se debe apostar por **nuevos modelos que otorguen el control sobre sus datos a los interesados facilitándoles la portabilidad de los mismos y permitiéndoles en todo momento otorgar o revocar el consentimiento para el tratamiento, así como tener información permanente sobre los fines y usos, comunicaciones previstas o realizadas**, etc, como pueden ser los denominados *data personal spaces* (espacios de datos personales) o *data stores* (almacenes de datos), y por los que han apostado tanto la Comisión Europea, como el Supervisor Europeo de Protección de Datos y ENISA.

Por todo ello, estos son alguno de los puntos principales a tener en cuenta por todos los intervinientes en un tratamiento de datos personales obtenidos del uso de teléfonos inteligentes, aplicaciones y servicios en la nube:

- Cada responsable de tratamiento debe obtener los datos necesarios para la finalidad del tratamiento.
- Se deben establecer políticas de plazos de mantenimiento de la información.
- El usuario debe ser capaz de desconectar el dispositivo o alguna de sus aplicaciones y funcionalidades cuando no las esté utilizando.

El RGPD refuerza el principio de responsabilidad de responsables de tratamiento. Anteriormente al analizar los principios relativos del tratamiento, constatábamos como el apartado 2 del artículo 5 del RGPD introduce el principio de "responsabilidad proactiva" al establecer que el responsable del tratamiento tiene que cumplir las estipulaciones recogidas en el apartado 1 de ese mismo artículo y se capaz de demostrarlo.

Por su parte el artículo 24 del RGPD introduce un nuevo concepto denominado *accountability*, de difícil traducción al castellano (responsabilidad, compromiso,...). Queda reflejado en el artículo 24 del RGPD, en concreto en su apartado 1 al disponer:

> *"Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario".*

Se abre por tanto un escenario de responsabilidad que en algunos supuestos será objetiva y en otros supuestos será subjetiva.

En lo que respecta a la responsabilidad objetiva se producirá en la medida en la que el responsable de tratamiento no sea capaz de demostrar aspectos tales como:

- Que se informó previamente al interesado y que se obtuvo su consentimiento inequívoco o explicito según el caso, y si se facilita esa información de manera permanente y es de fácil localización.

- Que se ha atendido al ejercicio de un derecho formulado por un interesado respondiendo en plazo.
- Que la trasferencia internacional está amparada en alguno de los supuestos o excepciones que la legitiman.
- Que se ha notificado la violación de seguridad de datos a la autoridad de control y, en su caso, a los afectados.
- Que se ha realizado la preceptiva Evaluación de impacto en protección de datos.

Por otro lado tal y como comentábamos, existe también un ámbito de responsabilidad subjetiva debido al enfoque basado en el riesgo dispuesto a lo largo del articulado del RGPD como se puede comprobar en los artículos 24 (responsabilidad), 25 (privacidad por diseño) y 32 (seguridad). Nos podemos encontrar ante estos supuestos cuando:

- Se produce un ciberataque con éxito a los sistemas de información del responsable o encargado de tratamiento. Será responsable si se demuestra que no adoptó las medidas adecuadas atendiendo a la tecnología disponible, a los costes de implementación, a la naturaleza y fines de los tratamientos y a los riesgos de probabilidad y gravedad para los derechos y libertades de las personas físicas.
- Un empleado facilita información sobre horarios, itinerarios, aficiones, etc de clientes de la compañía a terceros. En base a los mismos criterios el punto anterior se deberá valorar si las medidas eran las adecuadas, máxime cuando el apartado 4 del artículo 32 del RGPD dispone que "*el responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros*".

El tratamiento masivo de datos y medidas de mitigación

El artículo 35.1 RGPD establece la necesidad de realizar una evaluación de impacto "*Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación de impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares*".

El uso de teléfonos inteligentes, aplicaciones y servicios en la nube permiten recoger datos que el artículo 9.1 del RGPD inserta en las categorías especiales de datos, entre ellos los relativos a la salud. Estos en el marco de la telemedicina se procesan por el responsable del tratamiento para monitorizar la salud de la persona física titular del Derecho a la Protección de Datos. Del mismo modo los dispositivos IoT también facilitan la confección de perfiles que pueden sustentar la toma de decisiones con efectos jurídicos.

El artículo 35.7 del RGPD describe el contenido mínimo que comprenderán las evaluaciones de impacto especificando que será:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas de seguridad previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Adquieren por ello especial relevancia todas las medidas tendentes a garantizar la minimización de los tratamientos, al igual que las medidas de seguridad aplicadas a los diferentes procesos.

El propio RGPD entiende como una medida apropiada aplicar la **seudonimización**(18) y por supuesto que la **anonimización** de datos excluiría a ese tratamiento del ámbito de aplicación de la normativa de protección de datos (LOPD y RGPD). **No obstante, se ha comprobado que uniendo información disociada de diversas fuentes se puede reidentificar a titulares de esos datos personales, por lo que el mero hecho de anonimizar per se, no sería suficiente**(19) sino que se deben utilizar técnicas o incluso combinaciones de técnicas de anonimización que permitan tras un análisis de riesgos, que el riesgo residual de reidentificación sea aceptable.

Debe tenerse en cuenta que la información anonimizada exime de realizar una Evaluación de impacto en protección de datos, pero no exime de realizar un análisis de riesgos de reidentificación y que anonimizar supone realizar un tratamiento de datos, con las consecuencias que ello conlleva.

El uso de **herramientas de cifrado en la transmisión de datos o en el alojamiento de los mismos tanto en servidores físicos como virtuales se revela como muy recomendable para estos tratamientos**.

Lamentablemente, como pone de manifiesto el Grupo de Trabajo del Artículo 29 en su Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos, estas herramientas no se están utilizando con carácter generalizado puesto que actualmente está primando la eficiencia ante la seguridad.

No obstante, y atendiendo a lo dispuesto en los apartados 1 y 2 del artículo 32 del RGPD(20), **el cifrado, seudonimización y anonimización van a tener que generalizarse para determinados tratamientos, sobre todo aquellos que supongan un riesgo para los derechos y libertades de los individuos, manejen a gran escala que categorías especiales de datos y tratamientos habituales y sistemáticos de aspectos personales de individuos.**

Conclusiones

La falta de virtualidad de las políticas de protección de datos y de las cláusulas de información previas al consentimiento, unido a los problemas técnicos de recogida del consentimiento en los objetos conectados, uso de

(18)
El artículo 4.5 la define como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

(19)
Dictamen 5/2014 sobre técnicas de anonimización del Grupo de Trabajo Articulo 29.

(20)
"1.Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.
2.Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".

teléfonos inteligentes, aplicaciones y servicios en la nube hace recomendable la adopción de medidas tendentes a obligar a que los dispositivos IoT sean Privacy conformance desde su diseño y por defecto que se basen en *Privacy-enhancing technologies* (PET) y que se trabaje en la concienciación de los adolescentes en cuanto al impacto futuro del uso intensivo de estos servicios orientados a financiarse con sus datos.

Resulta sin duda complicado protegerles en un entorno en el que facilitan un consentimiento a un tratamiento de sus datos de manera poco transparente y, en algunos casos, ilegal, al no contar con la edad mínima para emitirlo válidamente. Que los prestadores no se encuentren en la jurisdicción de la EU (prácticamente todos se encuentran en EEUU) no ayuda a un control efectivo por parte de las administraciones competentes, a pesar de su futuro sometimiento cuando el RGPD entre en vigor.

Los estudios analizados dejan sentada la ignorancia o despreocupación de la Generación Z en cuanto al tratamiento de sus datos por parte de los prestadores de los servicios y aplicaciones gratuitas que usan, lo que dificulta que se vean impactados por el tratamiento de sus datos en su perjuicio. No sólo ignoran que su modelo de negocio se basa en la recogida masiva de datos para su venta o cesión, sino que, aun sabiéndolo, la única opción para protegerse es simplemente no usar el servicio o no instalar la aplicación lo que, con su perfil, está fuera de toda cuestión.

Por tanto, corresponde a los poderes públicos asegurar el cumplimiento de la ley y proteger los derechos de los adolescentes de la Generación Z exigiendo la limitación de la recogida de datos y la limitación de su uso.

Referencias bibliográficas

Coen, Rena, King, Jennifer, y Wong, Richmond, (2016), *The Privacy Policy Paradox*. UC Berkeley School of Information.

iGen Tech Disruption, (2016), *iGen Tech Disruption: 2016 National Study on Technology and the Generation After Millennial*: http://genhq.com/wp-content/uploads/2016/01/iGen-Gen-Z-Tech-Disruption-Research-White-Paper-c-2016-Center-for-Generational-Kinetics.pdf.

Jensen, C., Potts, C., y Jensen, C., (2005), "Privacy practices of Internet users: self-reports versus observed behavior". *International Journal of Human-Computer*. Studies, 63(1), 212.

Madden, Mary, Lennart, Amanda, Cortesi, Sandra, Gasser, Urs, Maeve, Duggan, Smith, Aaron, y Beaton, Meredith, (2013), *Teens, Social Media, and Privacy*. Pew Research Center: http://www.pewinternet.org/files/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/.

McDonald, A. M., y Cranor, L. F., (2008), "The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society Privacy Year" en *Review Issue*, 4, 543.

Milne, G. R., y Culnan, M. J., (2004), Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. Journal of Interactive Marketing, 18(3), 15–29.

Turow, J., King, J., Hoofnagle, C. J., Bleakley, A., y Hennessy, M., (2009), *Americans reject tailored advertising and three activities that enable it*: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

Yao, Richard, (2014), *Gen Z and Digital Privacy*: https://www.ipglab.com/2014/10/30/gen-z-and-digital-privacy/.