ano 13 - n. 52 | abril/junho - 2013
Belo Horizonte | p. 1-256 | ISSN 1516-3210
A&C – R. de Dir. Administrativo & Constitucional

Revista de Direito ADMINISTRATIVO & CONSTITUCIONAL

A&C

EDITORA Fórum

A&C – REVISTA DE DIREITO ADMINISTRATIVO & CONSTITUCIONAL

IPDA
Instituto Paranaense
de Direito Administrativo

INSTITUTO DE DIREITO
ROMEU FELIPE
BACELLAR

EDITORA Fórum

Luís Cláudio Rodrigues Ferreira
Presidente e Editor

Av. Afonso Pena, 2770 - 16º andar - Funcionários
CEP 30130-007 - Belo Horizonte/MG - Brasil
Tel.: 0800 704 3737
www.editoraforum.com.br
E-mail: editoraforum@editoraforum.com.br

Impressa no Brasil / Printed in Brazil
Distribuída em todo o Território Nacional

Os conceitos e opiniões expressas nos trabalhos assinados são de responsabilidade exclusiva de seus autores.

Supervisão editorial: Marcelo Belico
Revisão: Cristhiane Maurício
Leonardo Eustáquio Siqueira Araújo
Lucieni B. Santos
Marilane Casorla
Bibliotecário: Ricardo Neto - CRB 2752 - 6ª Região
Capa: Igor Jamur
Projeto gráfico e diagramação: Walter Santos

A246 A&C : Revista de Direito Administrativo & Constitucional. – ano 3, n. 11, (jan./mar. 2003)- . – Belo Horizonte: Fórum, 2003-

Trimestral
ISSN: 1516-3210

Ano 1, n. 1, 1999 até ano 2, n. 10, 2002 publicada pela Editora Juruá em Curitiba

1. Direito administrativo. 2. Direito constitucional. I. Fórum.

CDD: 342
CDU: 342.9

Periódico classificado no Estrato B1 do Sistema Qualis da CAPES - Área: Direito.

Revista do Programa de Pós-graduação do Instituto de Direito Romeu Felipe Bacellar (Instituição de Pesquisa e Pós-Graduação), em convênio com o Instituto Paranaense de Direito Administrativo (entidade associativa de âmbito regional filiada ao Instituto Brasileiro de Direito Administrativo).

A linha editorial da A&C – Revista de Direito Administrativo & Constitucional segue as diretrizes do Programa de Pós-Graduação do Instituto de Direito Romeu Felipe Bacellar em convênio com o Instituto Paranaense de Direito Administrativo. Procura divulgar as pesquisas desenvolvidas na área de Direito Constitucional e de Direito Administrativo, com foco na questão da efetividade dos seus institutos não só no Brasil como no direito comparado, com ênfase na questão da interação e efetividade dos seus institutos, notadamente América Latina e países europeus de cultura latina.

A publicação é decidida com base em pareceres, respeitando-se o anonimato tanto do autor quanto dos pareceristas (sistema double-blind peer review).

Desde o primeiro número da Revista, 75% dos artigos publicados (por volume anual) são de autores vinculados a pelo menos cinco instituições distintas do Instituto de Direito Romeu Felipe Bacellar.

A partir do volume referente ao ano de 2008, pelo menos 15% dos artigos publicados são de autores filiados a instituições estrangeiras.

Esta publicação está catalogada em:
• Ulrich's Periodicals Directory
• RVBI (Rede Virtual de Bibliotecas – Congresso Nacional)
• Library of Congress (Biblioteca do Congresso dos EUA)

A&C – Revista de Direito Administrativo & Constitucional realiza permuta com as seguintes publicações:
• Revista da Faculdade de Direito, Universidade de São Paulo (USP), ISSN 0303-9838
• Rivista Diritto Pubblico Comparato ed Europeo, ISBN/EAN 978-88-348-9934-2

La protección de los datos personales en las redes sociales

Pablo Schiavi

Doctor en Derecho y Ciencias Sociales por la Universidad Mayor de la República Oriental del Uruguay. Master en Derecho Administrativo Económico por la Universidad de Montevideo de la República Oriental del Uruguay. Profesor de la materia "Recursos Administrativos"; del Taller Teórico-Práctico sobre el Acceso a la Información Pública y la Protección de Datos Personales y del Taller Teórico-Práctico sobre la Protección de Datos Personales en Salud "E-Salud" del Máster de Derecho Administrativo Económico de la Universidad de Montevideo. Aspirante a Profesor Adscripto en Derecho Público de la Facultad de Derecho de la Universidad de la República. Aspirante de la Cátedra de Derecho Administrativo de la Facultad de Derecho de la Universidad de Montevideo. Secretario de Redacción de La Justicia Uruguaya, Revista Jurídica. Certificado en Prevención del Lavado de Dinero y Financiamiento del Terrorismo por el Isede y la Facultad de Derecho de la Universidad Católica del Uruguay "Dámaso Antonio Larrañaga". Diplomado Internacional en Dirección y Gestión de Cooperativas de Ahorro y Crédito por el Instituto de Desarrollo Cooperativo (I.D.C.) y la Confederación Alemana de Cooperativas (D.G.R.V.). Miembro del Instituto de Derecho Administrativo de la Facultad de Derecho de la Universidad de la República. Ex-Asesor del Auditor Interno de la Nación, Auditoría Interna de la Nación (A.I.N). Asesor del Contador General de la Nación, Contaduría General de la Nación (C.G.N.) del Ministerio de Economía y Finanzas de la República Oriental del Uruguay. Autor de libros y artículos sobre temas de su especialidad. *E-mail*: <pablo.schiavi@cgn.gub.uy>. Twitter: <@PabloSchiavi>.

Resumen: A lo largo del presente trabajo abordaremos los principales lineamientos de la protección de datos personales en las redes sociales digitales. Haremos referencia al impacto de la llamada "Web 2.0" conocida como la "Web de las redes sociales" en la concepción tradicional de la protección de datos personales tanto en sus aspectos normativos como en sus sustentos doctrinarios. Nuestro recorrido se inicia en la situación actual de la problemática en la Unión Europea y en el mundo, teniendo presente que el modelo de crecimiento de estas plataformas se basa fundamentalmente en un proceso viral, con posibilidades de crecimiento de tipo exponencial y quizás desconocidas en cuanto a sus impactos. De ahí que la eventual vulneración de datos personales de los usuarios de las redes sociales se transforma en el objeto central de nuestro trabajo, destacando conceptos claves como el acceso seguro, la identidad digital, la neutralidad tecnológica

y la autorregulación con los códigos de conducta. El mayor desafío será cómo responder a las interrogantes que se plantean a millones de personas en el mundo en cuanto a los impactos y riesgos cada vez más sensibles a quienes se exponen al ser parte de del "ciberespacio" en estos días.

Palabras-clave: Protección de datos personales. Redes sociales. Web 2.0. Acceso seguro, identidad digital. Neutralidad tecnológica. Autorregulación. Códigos de conducta.

> [...] *Habrá que hacer conciencia que el ciberespacio no es un espacio virtual, sino que forma parte de nuestro espacio real* [...] (Jacqueline Peschard Mariscal)

1 Introducción

El reconocimiento a las dimensiones internacionales de la protección de los datos personales en la era digital, la importancia de los desafíos a la protección de los datos personales de los más jóvenes en internet y la urgencia de elaborar marcos normativos que puedan orientar a los Estados y a las empresas en sus esfuerzos para responder a esos desafíos,[1] es, hoy en día, objeto de múltiples debates, conferencias y seminarios en todo el mundo.

Es un lugar común afirmar que hoy en día vivimos la era digital, en donde gracias al avance de las tecnologías de la información, el Internet se ha convertido en un medio de comunicación plenamente socorrido, al punto que forma parte ya del desarrollo de nuestras actividades cotidianas. Asimismo las redes sociales en Internet han devenido herramientas de comunicación multifuncionales, que

[1] BERNIER, Chantal – *El Memorándum de Montevideo: un marco de referencia para la protección de los datos personales de los jóvenes en Internet en la región Iberoamericana*; Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes; Memorándum de Montevideo; Carlos G. Gregorio – Lina Ornelas, Compiladores; IIJusticia – Instituto de Investigación para la Justicia, IFAI – Instituto Federal de Acceso a la Información y Protección de Datos; México, 2011, p. 16.

nos permiten entrar en contacto con personas de todo el mundo y compartir experiencias de muy variado tipo en esta nueva aldea global: permiten obtener, almacenar y transmitir un sin número de datos, documentos, fotografías, videos, música, —entre otros—, y el acceso a éstos es tan sencillo con simplemente un clic.[2]

El desarrollo de las tecnologías de la información y las comunicaciones (TIC) en la segunda mitad del siglo pasado ha traído consigo el surgimiento de nuevas posibilidades para la sociedad. El nacimiento de las redes determina nuevos modos de hacer, cambios en las relaciones sociales o el inicio de comunidades humanas que eran totalmente impensables hasta hoy. Aunque las nuevas tecnologías comportan, como regla general, numerosas ventajas para el público potencialmente destinatario de las mismas, en ocasionen, todo hay que decirlo, se plantean ciertos problemas como consecuencia del uso indebido que de las mismas se hacen. Un ejemplo que al respecto puede apuntarse es el de las redes sociales y los potenciales problemas de privacidad que pueden suscitarse.

La irrupción de las nuevas tecnologías de marcado carácter social —*blogs*, *wikis*, *podcast*, redes sociales, etc.— ha determinado un alto grado de interconectividad entre los usuarios de Internet lo que, dicho sea de paso, les permite intercambiar todo tipo de opiniones sobre diferentes productos y experiencias con otras personas.[3]

En tal sentido, la llegada de la "*Web* 2.0" ha supuesto una verdadera revolución, pues el potencial usuario adquiere un nuevo papel dentro del soporte, ya que deja de ser un mero espectador de contenidos para ser el que elige, el que participa e, incluso, el que crea esos contenidos. En suma, la *Web* 2.0 es una *Web* más colaborativa que permite a sus usuarios acceder y participar en la creación de un conocimiento ilimitado y, como consecuencia de esta interacción, se generan nuevas oportunidades de negocio para las empresas.

La sociedad de la información y la comunicación necesariamente debe tener como su centro de atención a las personas; esto es, la aproximación a la sociedad

[2] PESCHARD MARISCAL, Jacqueline – *Protección de las niñas, niños y adolescentes en el ámbito digital: responsabilidad democrática de las instituciones de gobierno y de las agencias de protección de datos*; Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes; Memorándum de Montevideo; Carlos G. Gregorio – Lina Ornelas, Compiladores; IIJusticia – Instituto de Investigación para la Justicia, IFAI – Instituto Federal de Acceso a la Información y Protección de Datos; México, 2011, p. 22.

[3] LÓPEZ JIMÉNEZ, David – *La protección de datos de carácter personal en el ámbito de las redes sociales electrónicas: el valor de la autorregulación*; Universidad de Alcalá de Henares. Servicio de Publicaciones, 2009.

de la información y la comunicación desde una perspectiva basada en "derechos" implica colocar la dignidad humana, el desarrollo humano y los derechos como ciudadanos globales y digitales por encima de las consideraciones tecnológicas o la relación comercial productor-consumidor. Más aún, implica educar en la ciberciudadanía y proteger en este ámbito a las niñas, niños y adolescentes para garantizar una navegación segura.[4]

A lo largo del presente trabajo abordaremos los principales lineamientos de la protección de datos personales en las redes sociales digitales. Haremos referencia al impacto de la llamada "Web 2.0" conocida como la "Web de las redes sociales" en la concepción tradicional de la protección de datos personales tanto en sus aspectos normativos como en sus sustentos doctrinarios.

Nuestro recorrido se inicia en la situación actual de la problemática en la Unión Europea y en el mundo, teniendo presente que el modelo de crecimiento de estas plataformas se basa fundamentalmente en un proceso viral, con posibilidades de crecimiento de tipo exponencial y quizás desconocidas en cuanto a sus impactos.

De ahí que la eventual vulneración de datos personales de los usuarios de las redes sociales se transforma en el objeto central de nuestro trabajo, destacando conceptos claves como el acceso seguro, la identidad digital, la neutralidad tecnológica y la autorregulación con los códigos de conducta.

El mayor desafío será cómo responder a las interrogantes que se plantean a millones de personas en el mundo en cuanto a los impactos y riesgos cada vez más sensibles a quienes se exponen al ser parte de del "ciberespacio" en estos días.

2 El impacto de la "Web 2.0" en el derecho a la protección de datos personales

2.1 La Web 2.0 – La Web de las redes sociales[5]

Internet ha creado un nuevo escenario en el que las relaciones personales cobran protagonismo. Las nuevas plataformas y herramientas colaborativas han producido un cambio desde una Web 1.0 basada en páginas estáticas, meramente

[4] PESCHARD MARISCAL, Jacqueline – *Protección de las niñas, niños y adolescentes en el ámbito digital: responsabilidad democrática de las instituciones de gobierno y de las agencias de protección de datos*; Ob. Cit; p. 22 y siguientes.

[5] OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN (INTECO). *Guía de introducción a la Web 2.0: aspectos de privacidad y seguridad en las plataformas colaborativas*. España, Febrero 2011. Disponible en internet: <http://observatorio.inteco.es>.

informativas, sin capacidad de generar una participación del usuario, hacia una Web dinámica donde se produce una interrelación que genera una suma de conocimientos y/o experiencias.

Es decir, la Web 2.0 o *Web Social* son personas colaborando, compartiendo y participando en un canal multidireccional abierto que permite lograr la máxima interacción entre los usuarios y les ofrece nuevas posibilidades de colaboración, expresión y participación.

Mientras, la evolución de la Red no se detiene, la aparición de nuevas tecnologías asociadas a los términos Web 3.0, Web 4.0 y Web 5.0 permitirán la integración de la *Red de los objetos*, el desarrollo de redes sensoriales y emotivas o la integración de la Web semántica dando acceso a información más relevante y personalizada que cambiará su estructura tal y como se conoce.

Las posibilidades de la Web 2.0 son casi ilimitadas. Entre la diversidad de herramientas que surgen diariamente en la Web 2.0, las redes sociales, los blogs, las wikis o las herramientas de sindicación son las que mayor peso tienen entre los internautas.[6]

a) Redes sociales

Las redes sociales son espacios virtuales en los que cada usuario cuenta con un perfil público, que refleja datos personales, estado e información de uno mismo. A su vez dispone de herramientas que permiten interactuar y conocer al resto de usuarios, por ejemplo mediante la creación de grupos de interés.

b) Blogs

Un blog es un sitio Web en el que el autor publica entradas o post, sobre temas de interés o como bitácora personal, y estos se almacenan cronológicamente. A su vez permite la inserción de comentarios (post) por parte de los lectores, convirtiéndose en una herramienta interactiva que constituye verdaderos foros de opinión.

Los post generalmente contienen texto, pero gracias al podcasting (incorporación de archivos multimedia a los posts), también incluyen imágenes, sonido y vídeos. En la actualidad existen variantes del concepto original de blog, entre los que se encuentran el fotolog o el videolog. La evolución de este modelo da paso al *microblogging*. El máximo exponente de dicho fenómeno es *Twitter*,

[6] OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN (INTECO). *Guía de introducción a la Web 2.0: aspectos de privacidad y seguridad en las plataformas colaborativas*. España, Febrero 2011. Disponible en internet: <http://observatorio.inteco.es>.

creado en 2006 y que en 2010 ha superado a *Myspace* en número de visitas. Responder a la pregunta "Qué sucede" utilizando menos de 140 caracteres se ha convertido en el nuevo fenómeno de la Web social.

c) Wikis

Una wiki es una página web que permite a sus participantes cambiar o editar sus contenidos, haciendo de la propia página una plataforma fácil y accesible para que los diversos usuarios puedan aportar contenidos bajo un mismo documento online. Así, el portal crece gracias al trabajo de una comunidad de individuos con un interés en común.

El primer wiki fue creado en 1995 por Ward Cunningham. El máximo exponente de este modelo de comunicación en la Red es la *Wikipedia*, un compendio del conocimiento humano en permanente proceso de construcción, con ediciones en 271 idiomas y en el que participan a diario cientos de miles de usuarios.

d) Foros

Dentro de las herramientas colaborativas se incluyen los foros. Suelen existir como complemento a un sitio web permitiendo a los usuarios discutir y compartir información relevante respecto de la temática del sitio, de modo libre e informal, generando una comunidad con un interés común.

e) Sindicación de contenidos

El formato RSS (*Really Simple Sindication*) es un formato que permite reunir de forma automatizada las noticias u otros contenidos de las webs y blogs por los que se tiene un especial interés (y que se denominan *feeds*) en un programa al que se llama agregador o lector de RSS y consultarlas de manera rápida.

f) Bookmarking

El *bookmarking* también permite organizar las webs favoritas etiquetando los portales o noticias mediante palabras clave relevantes, denominadas etiquetas (*tags*). Los usuarios pueden ver cuántas personas han usado una etiqueta y buscar todos los recursos a los que se ha asignado. También pueden conocer quién creó cada referencia y acceder a otras referencias del creador.

g) Herramientas

Además de las principales plataformas descritas, existen multitud de herramientas centradas en la generación de contenidos. Dos de los ejemplos más

representativos son YouTube y Flickr, con los que los usuarios pueden subir, compartir y ver vídeos y fotos, y aplicaciones ofimáticas (Google docs, Office live) o transmisiones en vivo (Justin.tv).

2.2 Sobre el derecho a la protección de datos personales

En la era electrónica existe una considerable preocupación por el impacto de internet en el derecho fundamental a la protección de datos personales.

Augusto Durán Martínez[7] define el derecho a la protección de datos personales "como la facultad o el poder que tienen las personas para actuar per se y para exigir la actuación del Estado o de quien tenga competencia para ello a fin de tutelar los derechos que pudieran verse afectados por virtud del acceso, registro o trasmisión a terceros de los datos que atañen a su personalidad".

"En general se dice que el derecho a la protección de datos personales es un derecho nuevo", agrega Durán Martínez, citando a Carlos E. Delpiazzo, que lo llama "novel derecho", razón por la cual, se le ha considerado un derecho de la tercera generación, subrayando que "si bien el derecho a la protección de datos es considerado hoy en día un derecho autónomo, es un derecho instrumental".

Sobre el punto destaca Carlos E. Delpiazzo[8] que "la mayoría de la doctrina continental utiliza la expresión 'derecho a la protección de datos personales' para designar el derecho bajo examen cuyo objeto es la tutela frente a la posible utilización no autorizada de los datos de la persona para confeccionar una información que, identificable con él, afecte a su entorno personal, familiar, profesional o social".

José Luis Piñar Mañas,[9] Director de la Agencia Española de Protección de Datos, señala que "el derecho fundamental a la protección de datos personales deriva directamente de la Constitución y atribuye a los ciudadanos un poder de disposición sobre sus datos, de modo que, en base a su consentimiento, puedan disponer de los mismos. El derecho fundamental a la protección de

[7] DURÁN MARTÍNEZ, Augusto. –*"Derecho a la protección de datos personales y al acceso a la información pública. Hábeas Data. Leyes Nº 18.331 de 11 de agosto de 2008 y Nº 18.381 de 17 de octubre de 2008"*, 2º Edición ampliada y actualizada. AMF. Montevideo, 2012, p. 12 y siguientes.

[8] DELPIAZZO, Carlos E. – "*A la búsqueda del equilibrio entre privacidad y acceso"*, Instituto de Derecho Informático. Facultad de Derecho. Universidad de la República. Protección de Datos Personales y Acceso a la Información Pública. FCU/AGESIC, Montevideo, 2009, p. 9.

[9] PIÑAR MAÑAS, José Luis. –*"Guía del Derecho Fundamental a la protección de datos de carácter personal"*, (Agencia Española de Protección de Datos, 2004). La información de esta Guía puede ser ampliada en Servicio de Atención al Ciudadano. Disponible en internet: <http://www.agpd.es>.

datos reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos. Ello supone que el desarrollo y la aplicación de las nuevas tecnologías ha introducido comodidad y rapidez en el intercambio de datos, lo que ha contribuido también al incremento del número de tratamientos de datos que se realizan cotidianamente. La bondad que aportan estas técnicas es indudable respecto del progreso de las sociedades modernas y de la calidad de vida de los ciudadanos, pero se hace necesario garantizar el equilibrio entre modernización y garantía de los derechos de los ciudadanos. Esta ponderación entre derecho del ciudadano a preservar el control sobre sus datos personales y la aplicación de las nuevas tecnologías de la Información, es el contexto en el que el Legislador consagra el derecho fundamental a la protección de datos de carácter personal".

El régimen de protección de los datos personales permite que los ciudadanos ejerzan su legítimo poder de disposición y control sobre los datos de carácter personal referidos a su persona que se encuentran registrados en bases de datos de titularidad de terceros. Es indudable que con el correr de los años la posibilidad de disponer información sobre las personas ha ido paulatinamente en aumento. Si a ello se le suma el importante papel que las bases de datos desempeñan en el mundo tecnificado y globalizado de hoy, surge con pocos cuestionamientos el derecho de las personas a protegerse frente a la intromisión de los demás. A tal fin, la legislación vigente faculta a los ciudadanos a decidir cuáles de esos datos quieren proporcionar a terceros, sea el Estado o un particular, o qué datos pueden esos terceros recabar, permitiendo asimismo que sepan quién posee sus datos personales y para qué, pudiendo inclusive oponerse a esa posesión o uso.[10]

La Ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.[11]

Con acierto señala Cristina Vázquez Pedrouzo[12] que "así como la transparencia se encuentra en el origen de las regulaciones sobre acceso a la información

[10] SCHIAVI, Pablo. –*"El control del acceso a la información pública y de la protección de datos personales en el Uruguay"*, Universidad de Montevideo. Facultad de Derecho. Montevideo, 2012, p. 75 y siguientes.

[11] Disponible en internet: <http://www.protecciondedatos.com.ar>.

[12] VÁZQUEZ PEDROUZO, Cristina. – *"El régimen jurídico del acceso a la información pública y la protección de datos personales"* ob. cit., p. 65.

pública, el desarrollo de la informática y su aptitud abarcadora de grandes volúmenes de información en tiempos reducidos ha creado la necesidad de tutelar los datos personales".

Analizando el panorama general de los datos personales, sostiene Héctor M. Delpiano[13] que "el régimen de los datos personales basa su razón de ser en algunos pilares fundamentales, de los cuales, probablemente el más importante de ellos es el de su pertenencia. Efectivamente, los datos de las personas hacen relación intrínseca e inseparable con el sujeto de derecho —persona física o jurídica— generadora de los mismos. La información conformadora del concepto de datos personales, en muchos casos nace con la propia personas y en otra se va creando a medida que transcurre su vida".

Jacqueline Peschard Mariscal,[14] en su carácter de Comisionada Presidenta del Instituto Federal de Acceso a la Información y Protección de Datos (México), señala con acierto que Internet es un espacio lleno de oportunidades, especialmente para los jóvenes, y en consecuencia, debe existir un balance entre el despliegue de la libertad de expresión y la protección de su dignidad como personas, ya que ellos tienen una expectativa razonable de privacidad al compartir su información con otros en los ambientes digitales. Sin embargo, habrá que hacer conciencia que el ciberespacio no es un espacio virtual, sino que forma parte de nuestro espacio "real".

Algunos de los riesgos asociados al Internet que se han identificado, al decir de Farith Simón Campaña,[15] son: uso abusivo y adicción, vulneración de derechos de propiedad industrial o intelectual, acceso a contenidos inapropiados, interacción y acechos por otras personas y *ciberbullying, grooming* y acoso sexual, amenazas a la privacidad, riesgo económico y fraude, riesgos técnicos y *malware*.

Agrega el citado autor que la Web 2.0, en particular las redes sociales, es una inestimable oportunidad para las personas accedan a información, expresen e intercambien opiniones, se asocien con otros con intereses similares.

---

[13] DELPIANO, Héctor M. – "*Protección de datos personales y acción de habeas data. La Ley Nº 18.831"*, Anuario de Derecho Administrativo, Tomo XV (F.C.U, Montevideo 2008), p. 169-170.

[14] PESCHARD MARISCAL, Jacqueline – *Protección de las niñas, niños y adolescentes en el ámbito digital: responsabilidad democrática de las instituciones de gobierno y de las agencias de protección de datos*; ob. cit., p. 65, p. 22.

[15] CAMPAÑA, Farith Simon – *El enfoque de derechos en el "Memorándum de Montevideo"*; Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes; Memorándum de Montevideo; Carlos G. Gregorio – Lina Ornelas, Compiladores; IIJusticia – Instituto de Investigación para la Justicia, IFAI – Instituto Federal de Acceso a la Información y Protección de Datos; México, 2011, p. 27.

Cita a Lina Ornelas Nuñez, que define a las redes sociales como "plataformas de comunicación en línea que facilitan al individuo crear o unirse a grupos conformados por más usuarios. A través de ellas, el individuo intercambia información con personas de ideología, gustos, necesidades y problemáticas afines. Son una forma de romper el aislamiento de la mayoría. Dan popularidad al anónimo, integración al discriminado.

2.3 Soluciones en la Carta de los Derechos Fundamentales de la Unión Europea[16]

El Consejo de Europa primero y el ordenamiento jurídico comunitario posteriormente han desarrollado un completo acervo normativo que incorpora un conjunto de reglas dirigidas a garantizar los derechos individuales en el ámbito de la protección de datos.

Tales normas, que contribuyen a la creación de un verdadero mercado europeo que facilite el libre intercambio de personas, mercancías, servicios y capitales, no sólo se encuentran en Directivas comunitarias de notable relevancia, ya que fueron incluidas en el artículo II-68 del Tratado por el que se establecía una Constitución para Europa que, como es sabido, fue sustituido por el Tratado de Lisboa de 13 de diciembre de 2007.

España ha incorporado esta área del acervo comunitario a través de la LOPD así como por el Reglamento de desarrollo —aprobado por Real Decreto 1.720/2007 de 21 de diciembre. En nuestro Ordenamiento la protección de datos ostenta la naturaleza de derecho fundamental. Así, como es sabido, el Tribunal Constitucional estableció la existencia de un derecho fundamental a la protección de datos personales en sentencias dictadas a lo largo de un decenio —desde la STC 254/1993 a la STC 292/200025— fundamentándolo en el art. 18.4 de la Constitución Española.

La Carta de los Derechos Fundamentales de la Unión Europea, de 07 de diciembre de 2000, ha recogido expresamente el derecho fundamental a la protección de datos en dos ocasiones, en la Parte I, Título VI (De la vida democrática de la Unión), el artículo I-51 (Protección de datos de carácter personal) establece en el epígrafe primero que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan" y en la Parte II (Carta de los Derechos

[16] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Disponible en internet: <http://www.agpd.es>.

Fundamentales de la Unión), Título II (Libertades), se introduce en el artículo II-68 la segunda referencia al derecho a la protección de datos, señalando de nuevo que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan", y añadiendo que "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", y que "toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación".

La Carta de los Derechos Fundamentales de la Unión Europea exige que en todos los Estados miembros exista una autoridad independiente que controle y garantice el Derecho Fundamental a la protección de datos.[17]

3 Las redes sociales

3.1 Origen y evolución de las redes sociales[18]

El origen de las redes sociales en Internet se remonta, al menos, al año 1995, cuando Randy Conrads crea el sitio web "classmates.com". Con esta red social se pretendía que los usuarios pudiesen recuperar o mantener el contacto con antiguos compañeros del colegio, instituto, universidad, etc.

En el año 2002 comienzan a aparecer sitios web que promocionan las redes de círculos de amigos en línea, adquiriendo popularidad en el año 2003 con la llegada de portales web como *MySpace* o Xing.

La popularidad de estas plataformas creció exponencialmente. Grandes empresas y multinacionales de Internet emprendieron entonces nuevos proyectos en el entorno de las redes sociales. Así, cabe señalar como claros ejemplos el lanzamiento de Orkut por Google o Yahoo! 360º por parte de Yahoo!

La expansión de este fenómeno es tal que las últimas estadísticas a nivel mundial cifran el número de usuarios de redes sociales en 272 millones, un 58% de los usuarios de Internet registrados en todo el mundo, lo que supone un incremento del 21% respecto de los datos registrados en junio de 2007.[19]

[17] PIÑAR MAÑAS, José Luis. –"Guía del Derecho Fundamental a la protección de datos de carácter personal", ob. cit.

[18] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Disponible en internet: <http://www.agpd.es>.

[19] Por ejemplo en el caso de España, las fuentes son diversas, pero todas coinciden que en 2008 el número de usuarios españoles de Internet que utiliza habitualmente redes sociales se sitúa

3.2 Concepto de red social

Las redes sociales online son servicios prestados a través de 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 permiten interactuar con el resto de usuarios afines o no al perfil publicado.[20]

El modelo de crecimiento de estas plataformas se basa fundamentalmente en un proceso viral, en el que un número inicial de participantes, mediante el envío de invitaciones a través de correos a sus conocidos, ofrece la posibilidad de unirse al sitio web.

Aunque estamos ante un fenómeno relativamente reciente su avance es sencillamente imparable. En este sentido, existen redes sociales, como *Facebook*, en las que ya existen más de 200 millones de usuarios y con su *chat* supera la barrera de los 1000 millones de mensajes electrónicos diarios. Otro dato que, a este respecto, podemos poner de relieve, a tenor de ciertos estudios de carácter empírico, es que dentro de las primeras veinte posiciones de los 500 sitios *Web* más visitados a nivel internacional existen cuatro redes sociales cuales son *Facebook*, *MySpace*, *Hi5* y *Orkut*.[21]

En cuanto a la fundamentación teórica, cabe señalar que cuando se habla de redes sociales, se hace referencia a las plataformas online desde las que los usuarios registrados pueden interactuar mediante mensajes, compartir información, imágenes o vídeos, permitiendo que estas publicaciones sean accesibles de forma inmediata por todos los usuarios de su grupo. Al centrarse en las relaciones de los individuos (o grupos de individuos) y no en las características de los mismos (raza, edad, ingresos, educación) se han utilizado para el estudio de hábitos, gustos y formas de relacionarse de los grupos sociales.[22]

entre el 40% y el 50%. En concreto, siguiendo con el estudio de Universal McCann el 44,6% de los internautas españoles utiliza estos servicios (Gráfico 1), porcentaje que aplicado a los datos de la Oleada XX de Red.es, en la que se señala que: "entre enero y marzo de 2008 unos 17,6 millones de personas han usado Internet en el último mes"; se cifra en 7.850.000 los usuarios habituales de Internet —mayores de 15 años y con conexión en el último mes que utilizan redes sociales.

[20] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Disponible en internet: <http://www.agpd.es>.

[21] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Disponible en internet: <http://www.agpd.es>.

[22] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Disponible en internet: <http://www.agpd.es>.

Toda red social se fundamenta en la teoría de los seis grados de separación, en virtud de la cual, cualquier individuo puede estar conectado a cualquier otra persona en el planeta, a través de una cadena de conocidos con no más de cinco intermediarios (con un total de seis conexiones). La cifra de conocidos aumenta a medida que lo hacen los eslabones de la cadena. Los individuos de primer grado serán los más próximos y, según se avanza en el grado de separación, disminuye la relación y la confianza.

El concepto de red social ha sido ampliamente analizado por profesionales de diferentes sectores, no existiendo en la actualidad un concepto absolutamente cerrado y aceptado por todos ellos.

Antes de analizar el concepto de red social, se debe tener en cuenta el tipo de red que se va a definir, por lo que es necesario diferenciar en un primer momento si se trata de una red social tradicional o de una red social online.

A pesar de que el concepto de red social es utilizado indistintamente para las redes sociales online y las tradicionales, este hecho supone incurrir en un error que puede provocar que el análisis posterior de los elementos que la componen y caracterizan se vea desvirtuado. En este sentido, se puede afirmar que las redes sociales online son "servicios de la Sociedad de la Información, consistentes en la creación de comunidades online de personas que comparten intereses, actividades, o que están interesados en explorar y conocer los intereses de los demás.[23]

Conviene señalar que una red social es, ante todo, una forma de interacción entre miembros y/o espacios sociales. A partir de esta premisa, se recogen a continuación algunas definiciones de redes sociales:

Marta Rizo García define a las redes sociales[24] como "Formas de interacción social, que se definen fundamentalmente por los intercambios dinámicos entre los sujetos que las forman. Las redes son sistemas abiertos y horizontales y aglutinan a conjuntos de personas que se identifican con las mismas necesidades y problemáticas. Las redes, por tanto, se erigen como una forma de organización social que permite a un grupo de personas potenciar sus recursos y contribuir a la resolución de problemas".

[23] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Disponible en internet: <http://www.agpd.es>.

[24] RIZO GARCÍA, Marta – "*Redes. Una aproximación al concepto*". Universidad Autónoma de la Ciudad de México. Disponible en internet: <http://sic.conaculta.gob.mx/centrodoc_documentos/62.pdf>.

Asimismo se han definido las redes sociales en Estudio "Castilla y León 2.0. Hacia la Sociedad de la Colaboración" (Edición 2008) como "Las Redes son formas de interacción social, definidas como un intercambio dinámico entre personas, grupos e instituciones en contextos de complejidad. Un sistema abierto y en construcción permanente que involucra a conjuntos que se identifican en las mismas necesidades y problemáticas y que se organizan para potenciar sus recursos".

3.3 Tipología de las redes sociales

Las redes sociales se pueden categorizar atendiendo al público objetivo al que se dirigen, o al tipo de contenido que albergan. De esta forma, se distinguen al menos, dos grandes grupos de redes sociales: generalistas o de ocio y profesionales.[25]

A pesar de que cada tipo presenta una serie de aspectos particulares, ambos grupos cuentan con una serie de características básicas y estructurales comunes: a) Tienen como finalidad principal poner en contacto e interrelacionar a personas. La plataforma facilita la conexión de forma sencilla y rápida; b) Permiten la interacción entre todos los usuarios de la plataforma, ya sea compartiendo información, permitiendo el contacto directo o facilitando nuevos contactos de interés; c) Permiten y fomentan la posibilidad de que los usuarios inicialmente contactados a través del medio online, acaben entablando un contacto real; d) Permiten que el contacto entre usuarios sea ilimitado, en la medida en la que el concepto espacio y tiempo se convierte en relativo, al poder comunicar desde y hacia cualquier lugar, así como en cualquier momento, con la única condición de que ambas partes acepten relacionarse entre sí; y, e) Fomentan la difusión viral de la red social, a través de cada uno de los usuarios que la componen, empleando este método como principal forma de crecimiento del número de usuarios.

a) Redes sociales generalistas o de ocio

Este tipo de redes se caracteriza porque su objetivo principal radica en el hecho de facilitar y potenciar las relaciones personales entre los usuarios que la componen. El grado de crecimiento de estas redes ha sido muy elevado en

[25] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Disponible en internet: <http://www.agpd.es>.

los últimos años, llegando a constituirse plataformas como *Facebook* en las que en diciembre de 2008 se produce la entrada diaria de más de 120 millones de usuarios activos que crean el contenido que define su sitio web.[26]

Los aspectos que caracterizan a las redes sociales generalistas o de ocio son: a) Ofrecen gran variedad de aplicaciones y/o funcionalidades que permiten a los usuarios prescindir de herramientas de comunicación externas, poniendo a su disposición una plataforma que integra todas las aplicaciones necesarias en una misma pantalla; b) Ofrecen y fomentan que los usuarios no se centren únicamente en operar de forma online, sino que este medio sirva de plataforma a través de la que poder convocar y organizar aspectos de su vida cotidiana; y, c) Ponen a disposición de la comunidad de usuarios parte del código usado para programar la plataforma, de modo que los usuarios puedan desarrollar aplicaciones propias, que sean ejecutadas dentro de la red social, o aplicaciones externas que se interconecten con la plataforma, logrando así el aumento de la utilidad y con ello de la difusión.

b) Redes sociales de contenido profesional

Se configuran como nuevas herramientas de ayuda para establecer contactos profesionales con otros usuarios. Entre ellas se encuentran webs como Xing o Linkedin y constituyen el segundo gran bloque de redes sociales.[27] Están creadas y diseñadas con la finalidad de poner en contacto y mantener la relación a nivel profesional con diferentes sujetos que tengan interés para el usuario.

Así, entre las principales utilidades cabe citar: a) Desde el lado del trabajador: la búsqueda de nuevas oportunidades de empleo, el establecimiento de nuevos contactos profesionales o la promoción laboral. Permiten a los usuarios entrar en contacto con otros profesionales de su sector a través de conocidos comunes de confianza, ayudando a mejorar las conexiones con otras personas que en circunstancias habituales serían inaccesibles debido a su cargo o responsabilidad; b) Desde el lado del empleador: la presencia en este tipo de redes sociales resulta cada vez más importante, ya que con mayor frecuencia, las empresas utilizan este nuevo recurso para identificar posibles candidatos participantes en sus

[26] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Disponible en internet: <http://www.agpd.es>.

[27] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Disponible en internet: <http://www.agpd.es>.

procesos de selección o profundizar en la información disponible del perfil de los candidatos seleccionados en un proceso de contratación determinado.

Este tipo de redes está en auge. Los beneficios que este tipo de redes sociales de carácter profesional pueden suponer y reportar al entorno empresarial no radican exclusivamente en servir como herramienta complementaria en un proceso de selección de personal, ni se quedan en las posibilidades que evidencian los datos indicados, sino que además resultan especialmente atractivas como alternativa de negocio, ya que además permiten: la realización de acciones de marketing personalizado; la creación de servicios premium de suscripción; la publicación de contenidos destacados y la promoción de contenidos propios, y la venta de bonos de "aumento de confianza del usuario".

3.4 Análisis de los aspectos más relevantes y problemática específica de las redes sociales

La tendencia actual de los servicios que la Red pone al alcance del usuario —foros, blogs, wikis o redes sociales— se construye a partir de un nexo común que tiene en su base la actividad colaborativa, a la vez que los cambios tecnológicos y sociales han contribuido a la implantación y crecimiento popular de esta nueva forma de creación, colaboración y acceso a la información.[28]

Pero la notoriedad de estos espacios sociales no queda exenta de riesgos o posibles ataques malintencionados. En este sentido, debe subrayarse el carácter pionero y la importancia del artículo 18.4 de la Constitución Española al prever la necesidad de que el legislador regule aquellos usos de la informática susceptibles de repercutir en los derechos fundamentales.

Asimismo, la aprobación del Convenio 108 de 1981 del Consejo de Europa, el conjunto de normas dictadas por las Comunidades Europeas en materia de protección de datos, sociedad de la información o propiedad intelectual, y las normas españolas que las desarrollan definen un horizonte normativo cuya proyección sobre la Web. 2.0 y las redes sociales son de carácter fundamental.

[28] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Disponible en internet: <http://www.agpd.es>.

4 Principales riesgos de vulneración de datos personales de los usuarios de las redes sociales

4.1 La importancia del acceso seguro y de la identidad digital

La notoriedad de estos espacios sociales online no queda exenta de riesgos o posibles ataques malintencionados. Es una preocupación de las organizaciones nacionales, europeas e internacionales con competencias en las materias afectadas por el uso de estas redes, que han impulsado la elaboración de normas y recomendaciones dirigidas a garantizar el acceso seguro de los usuarios — con especial atención a colectivos de menores e incapaces— a estas nuevas posibilidades online.[29]

Dada la gran cantidad de datos personales que los usuarios publican en sus perfiles, éstos se convierten en auténticas "identidades digitales" que facilitan un rápido conocimiento de datos de contacto, preferencias y hábitos del usuario.

Es en materia de protección de datos donde acontece el mayor número de situaciones desfavorables para la protección de los derechos de los usuarios, ya que las redes sociales fundamentan todos sus contenidos en los perfiles que los propios usuarios dan de alta y actualizan con asiduidad.

Así, entre las posibles situaciones de riesgo para la protección de datos de carácter personal, se encuentran: a) Casos de "phishing" y "pharming". Ambos fenómenos, muy explotados por los ciberdelincuentes para lograr la obtención de datos personales de los usuarios de Internet, así como de datos de carácter sensible o relativos a aspectos económicos (tarjetas de crédito, PIN de usuarios, etcétera); b) Social "Spammer" y "spam". El uso de las redes sociales como plataformas para el envío de correos electrónicos no deseados; c) Suplantación de identidad. Cada vez es más frecuente que usuarios que nunca se habían registrado en redes sociales online, comprueben como en el momento en el que intentan acceder, su "identidad digital", ya está siendo utilizada; d) La instalación y uso de "cookies" sin conocimiento del usuario. Otro posible riesgo relacionado con la participación del usuario en la red social radica en la posibilidad de que el sitio web utilice cookies que permitan a la plataforma conocer cuál es la actividad del usuario dentro de la misma. Mediante estas herramientas, las redes sociales pueden conocer el lugar desde el que el usuario accede, el tiempo de conexión,

[29] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Disponible en internet: <http://www.agpd.es>.

el dispositivo desde el que accede (fijo o móvil), el sistema operativo utilizado, los sitios más visitados dentro de una página web, el número de clicks realizados, e infinidad de datos respecto al desarrollo de la vida del usuario dentro de la red.

4.2 Las condiciones de uso y políticas de privacidad en las redes sociales

El conjunto de riesgos que se identifican a continuación no comporta necesariamente la comisión de ilícitos por el proveedor de servicios, sin perjuicio, de que los hechos demuestren que generalmente la configuración por defecto de sus servicios suele ofrecer una estándar bajo de privacidad.[30]

El consentimiento que presta el usuario es válido en el momento en que decide aceptar, la política de privacidad y condiciones de uso de la plataforma que constan en el formulario de registro. Por ello, debe estar muy atento a su contenido y consecuencias.

Evidentemente, esto no obsta a que resulte exigible que las políticas de privacidad deban ser transparentes, accesibles y claras. Del mismo modo, los usuarios deben valorar siempre, qué tipo de datos proporcionan a la plataforma y publican en su perfil, ya que no tiene la misma trascendencia el tratamiento por parte de la plataforma de los datos de carácter personal de nivel básico (nombre, dirección, teléfono, etc.), que otras información de contenido más sensible (nivel de renta, solvencia, recibos, afiliación sindical o política, salud, vida sexual, etc.), donde el nivel de protección y concienciación por parte del usuario deberá ser mucho mayor, dado que se trata de derechos pertenecientes a la esfera más íntima de su vida.

Como criterio general, cabe señalar que las redes sociales y plataformas colaborativas disponen de avisos legales, condiciones de uso y políticas de privacidad, aunque en ocasiones, redactadas en un lenguaje de difícil comprensión para el usuario. De esta forma, y a pesar de encontrarse recogidas en el sitio web, no alcanzan su finalidad última: que el usuario comprenda el objeto, la finalidad y el plazo para el que son recabados y tratados sus datos personales.

Así, el primer momento crítico para la protección de datos personales se encuentra en la fase inicial de registro del usuario, cuando este proporciona la información personal necesaria para poder operar en la red social. En este

[30] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Disponible en internet: <http://www.agpd.es>.

momento, los datos se pueden ver sometidos a varios riesgos: a) que el tipo de datos solicitados en el formulario de registro, aunque no obligatorios, sean excesivos. En este sentido, debe tenerse en cuenta que, con frecuencia, las redes sociales solicitan a los nuevos usuarios datos relativos a su ideología política, orientación sexual y preferencia religiosa. Si bien es cierto que estos datos tienen carácter voluntario y todo usuario es libre de publicar el contenido que deseé respecto a sí mismo, debe considerar las implicaciones que ello puede conllevar para su vida y las personas de su entorno, ya que estos datos serán visibles por todos sus contactos y, dependiendo de la configuración del perfil, por todos los usuarios de la red; b) la exigencia del consentimiento expreso y por escrito en lo que se refiere a datos relativos a ideología, religión o creencias, y expreso en el ámbito de la salud, origen racial y vida sexual; c) que el grado de publicidad del perfil de usuario sea demasiado elevado; d) que la finalidad de los datos no esté correctamente determinada.

El segundo momento considerado crítico para la protección de datos personales se sitúa en la fase intermedia, es decir, en la que el usuario desarrolla su actividad en la plataforma y utiliza los servicios y herramientas que ésta le ofrece. En este momento los aspectos que pueden poner en riesgo la seguridad y protección de datos personales de los usuarios son: a) la publicación excesiva de información personal (propia o de terceros). En esta fase se mantiene el posible riesgo que conlleva la publicación excesiva de información personal por parte de los usuarios; y, b) la posibilidad de que los usuarios publiquen también datos respecto de terceros, lo que puede conllevar el tratamiento y la cesión pública de datos de personas que no han prestado el consentimiento para ello.

4.3 De la política de privacidad a la política de utilización de datos – *Facebook*

La red social *Facebook* volverá a revisar de nuevo su polémica gestión de datos y cambiará el nombre actual por el de "Política de Utilización de Datos".

Una de las estrategias desplegadas por *Facebook*[31] es el cambio de nombre, a partir de ahora dejará de llamarla "Política de Privacidad" para nombrarla como "Política de Utilización de Datos".[32]

[31] Disponible en internet: <http://www.idg.es/pcworld/Facebook-cambia-las-politicas-de-privacidad-otra-v/doc120164-actualidad.htm>.

[32] Facebook/Política de uso de datos (al 08 de junio de 2012): *Información que recibimos sobre ti*
Recibimos diferentes tipos de información sobre ti, como:
Tu información

Se trata de la información necesaria para registrarte en el sitio, así como la que decides compartir.

- Información de registro: Cuando te registras en *Facebook*, te pedimos que introduzcas tu nombre, dirección de correo electrónico, fecha de nacimiento y sexo.

- Información que decides compartir: Tu información también incluye todo aquello que compartes en *Facebook*, como tus actualizaciones de estado, las fotos que subes o los comentarios que haces en la historia de un amigo. También incluye la información que decides compartir al realizar una acción, por ejemplo, cuando añades un amigo, indicas que te gusta una página o sitio web, añades un lugar a tu historia, usas nuestra herramienta de importación de contactos o bien, registras que tienes una relación con alguien. Tu nombre, fotos de perfil, fotos de portada, sexo, redes, nombre de usuario e identificador de usuario se tratan del mismo modo que la información que decides hacer pública. Tu fecha de nacimiento nos permite hacer cosas como mostrarte anuncios y contenido adecuado para tu edad.

- Información que otras personas comparten sobre ti: Recibimos información sobre ti de tus amigos y de otras personas, por ejemplo, cuando suben tu información de contacto, publican una foto tuya, te etiquetan en una foto o en una actualización de estado, en un lugar o cuando te añaden a un grupo.

Cuando la gente usa *Facebook*, puede almacenar y compartir información sobre ti y otras personas que tienen como amigos, como cuando suben y gestionan sus invitaciones y contactos.

Otra información que recibimos sobre ti. También recibimos otros tipos de información sobre ti: Recibimos información sobre ti cada vez que interactúas con *Facebook*, por ejemplo, cuando consultas la biografía de otra persona, envías o recibes un mensaje, buscas un amigo o una página, haces clic, consultas o interactúas de otro modo con cosas, utilizas una aplicación para móviles de *Facebook*, compras créditos de *Facebook* o compras otras cosas a través de *Facebook*. Cuando publicas cosas como fotos o vídeos en *Facebook* podemos recibir información adicional (o metadatos) como la hora, la fecha y el lugar en el que tomaste la foto o el vídeo. Recibimos la información del ordenador, teléfono móvil o dispositivo que utilizas para acceder a *Facebook*, incluso si varios usuarios inician sesión desde el mismo dispositivo. Esta información puede incluir tu dirección IP y otra información relativa, por ejemplo, a tu servicio de internet, tu ubicación, el tipo de navegador que utilizas (incluidos los identificadores) o las páginas que visitas. Por ejemplo, podemos obtener tus coordenadas GPS u otros datos de ubicación de modo que podamos decirte si tienes cerca a alguno de tus amigos.

Algunas veces obtenemos datos de nuestros socios publicitarios, clientes u otras terceras partes que nos ayudan (a nosotros o a ellos) a ofrecerte anuncios mejores, a interpretar la actividad que se desarrolla en línea y, en general, a mejorar *Facebook*. Por ejemplo, un anunciante podría facilitarnos información sobre ti (como cuál ha sido tu respuesta ante un anuncio publicado en *Facebook* o en otro sitio) para medir la eficacia de los anuncios y mejorar su calidad.

Nosotros recopilamos datos a partir de la información que ya tenemos sobre ti y sobre tus amigos. Por ejemplo, podemos recopilar datos sobre ti para saber qué amistades te deberíamos mostrar en tu sección de noticias o qué amistades podemos sugerirte que etiquetes en las fotos que publicas. Podríamos unir la ciudad donde te encuentras con información de GPS u otro tipo de información de ubicación que tengamos sobre ti, por ejemplo, para contarte, a ti y a tus amigos, cosas sobre otras personas o eventos que se estén celebrando cerca, o para presentarte ofertas que podrían interesarte. También podemos recopilar datos sobre ti para mostrarte anuncios que puedan interesarte.

Cuando obtenemos tus coordenadas de GPS, las combinamos con otra información de ubicación (como tu ciudad actual) que tenemos sobre ti, pero solo las conservamos durante el tiempo necesario para ofrecerte nuestros servicios, por ejemplo, los casos en los que conservamos tus últimas coordenadas de GPS para enviarte notificaciones relevantes. Solamente proporcionamos datos a nuestros socios publicitarios o a nuestros clientes después de haber eliminado tu nombre u otros datos que puedan identificarte, o bien después de haber combinado tus datos con los de otras personas de manera que dejen de estar asociados contigo.

El cambio de término es meramente representativo porque *Facebook* siempre ha tratado los datos de sus usuarios. Ésta iniciativa podría estar promovida por el acuerdo al que llegó *Facebook* con la Comisión Federal de Comercio con el fin de resolver las reclamaciones sobre el tratamiento de la privacidad que han reclamado numerosos usuarios en contra de la red social.

Facebook ha anunciado que pronto actualizará sus políticas de privacidad, luego que la Oficina del Comisionado de Protección de Datos de Irlanda le solicitara modificar y clarificar la forma en que se exponen las cláusulas de privacidad de esta red. *Facebook* afirmó que explicará de forma más transparente a los usuarios sobre cómo utiliza los datos que recopila.[33]

La idea es aclarar las políticas que ya existen de manera más amena, o agregando ejemplos. Es así como ahora veremos cambios en la nomenclatura, como por ejemplo la palabra "perfil" se reemplazará por "biografía", "publicación"

Información pública

Cuando usamos el término "información pública" (al que en ocasiones nos referimos como "información que se comparte con todos"), estamos hablando de la información que decides hacer pública, así como la información que está siempre disponible públicamente. Información que decides hacer pública Decidir hacer pública tu información significa exactamente eso: que todos podrán verla, incluidas las personas que no pertenecen a *Facebook*.

Decidir hacer pública tu información significa también que esta información:

- puede asociarse contigo (es decir, tu nombre, fotos del perfil, fotos de portada, biografía, identificador de usuario, nombre de usuario, etc.), incluso fuera de *Facebook*; puede mostrarse cuando alguien hace una búsqueda en *Facebook* o en un motor de búsqueda público; estará accesible para los sitios web, aplicaciones y juegos integrados en *Facebook* que utilizáis tú y tus amigos, y será accesible para cualquiera que utilice nuestras API, como la API de la gráfica social (Graph API). En ocasiones, cuando publiques algo (como cuando escribas en el muro de una página o comentes un artículo periodístico que incluye nuestro plug-in de comentarios) no podrás elegir un público concreto. Esto se debe a que algunas historias son siempre públicas. En general, se entiende que si no hay un icono para compartir, la información será pública.

Cuando otras personas comparten información sobre ti, también pueden optar por hacerla pública. Información que siempre es pública: **Los tipos de información que se enumeran a continuación son siempre públicos y se tratan como la información que hayas decidido hacer pública.:** Nombre: Ayuda a tus amigos y familiares a encontrarte. Si no te gusta compartir tu nombre real, siempre puedes eliminar tu cuenta.; Fotos del perfil y fotos de portada: Esto ayuda a tus amigos y familiares a reconocerte. Si no te gusta publicar ninguna de estas fotos, siempre puedes borrarlas. A menos que las elimines, cuando añadas una nueva foto de perfil o foto de portada, la foto anterior continuará siendo pública y permanecerá en el álbum de fotos de perfil o de fotos de portada.; Redes: Te ayuda a ver con quién compartirás la información antes de seleccionar "Amigos y redes" como opción personalizada. Si no quieres hacer pública tu red, puedes abandonar la red.; Sexo: Esto nos permite referirnos a ti correctamente en el sitio web.; Nombre de usuario e identificador de usuario.

[33] Disponible en internet: <http://america.infobae.com/notas/52691-Cmo-mejorar-la-privacidad-en-redes-sociales>

por "historia", entre otras. Asimismo se incluirán referencias a funciones, como las fotografías que elijamos de portada vinculadas a la biografía.

Además en la sección "Información" se indica qué datos del usuario son públicos y la información que *Facebook* obtiene cada vez que un usuario utiliza su aplicación móvil a través de sus smartphones, tablets, entre otros.

También se explica cómo *Facebook* usa tus datos para entregar avisos en otros sitios, cómo se usan las cookies y cómo *Facebook* puede "retener tus datos el tiempo necesario para proveerte servicios". Es así como cuando desactivas o eliminas una cuenta, de todos modos aparecerás en la lista de tus amigos, a pesar que hace mucho tiempo ya te hayas desactivado.

La configuración de la privacidad y las condiciones de uso de una de las redes sociales, sino la más representativa y masiva que existe en la actualidad, como *Facebook* ha despertado sucesivas controversias entre los millones de usuarios en el mundo.

Quizás y más allá de consejos esenciales para proteger nuestros datos en Internet,[34] debemos tener presente que todo lo que se publica en *Facebook* como

[34] *Infobae América* brinda cuatro consejos esenciales para **proteger sus datos en Internet:**

1. Compartir poca información con las aplicaciones

Al aceptar una **aplicación en** *Facebook*, antes se puede configurar qué tipo de información se quiere compartir, desde el cumpleaños hasta las interacciones en el muro. De todas formas, el programa tomará todos aquellos datos que sean públicos, como el género. Por eso, es importante no sólo **restringir lo que se autoriza a la aplicación** antes de comenzar a usarla, sino **configurar la privacidad del perfil** desde la opción que aparece en la flecha del margen superior derecho de la pantalla. Allí se elige la etiqueta **Aplicaciones, juegos y sitios web**. En *Twitter*, las aplicaciones que ya no se usan y que disponen de la información del usuario pueden eliminarse al ingresar en Configuración, y luego en la opción Aplicaciones. Desde allí, se les puede revocar el permiso.

2. Cuidado con la geolocalización

Es importante controlar con quiénes se comparte la ubicación en un determinado momento. Esta función en *Facebook* se desactiva —o se activa— antes de publicar en el muro, al hacer clic en el logo de *Facebook* Places. Esto debe hacerse manualmente dado que la red social no ofrece, actualmente, la opción de suspenderlo de manera permanente. En *Twitter*, está la opción, dentro de Configuración, Tweet Location, que se puede quitar con destildar la caja. Una consideración aparte merecen los dispositivos como iPhone, iPad y Blackberry, que pueden geolocalizar al usuario. En los **productos de Apple**, esto se modifica ingresando al menú Ajustes y seleccionando la opción General. Para **Blackberry**, se entra a Opciones, luego a Opciones avanzadas y, por último, a GPS. Al bloquear los móviles de esta manera, ninguna aplicación que se use en ellos podrá localizar al usuario. **3. Controlar si la agenda del móvil es tomada por las aplicaciones.** Muchas personas eligen sincronizar su agenda de contactos con la que tienen en *Facebook*, ya sea la del correo electrónico o la de su smartphone. Sin embargo, esta opción puede estar activada sin que el usuario tenga conocimiento. En caso de que no desee que esto suceda, debe ingresar a su cuenta y chequear que no tenga ningún móvil asociado (Configuración de la cuenta > Celular). Luego, desde su teléfono, como un **Blackberry**, debe presionar el menú Opciones y

en *Twitter*, es en principio público, esto es, cualquier persona, en cualquier lugar del mundo en que se encuentre podrá acceder a lo publicado por ser parte de la famosa "comunidad *Facebook*" o "comunidad *Twitter*"; salvo que en el momento en que tiene lugar la registración en la red, se configure con especial atención la política de privacidad, permitiendo acceder a los contenidos, ya sean fotos, textos, videos, solamente a los llamados "amigos" que se suponen serian personas con las cuales nos vinculamos en la red social a las cuales conocemos de antemano en el caso de *Facebook*; o solamente en el caso de los llamados "seguidores" en el caso de *Twitter*.

Es tal el impacto de las redes sociales en nuestras vidas, que seguramente la mayoría de los uruguayos[35] que tiene *Facebook* hoy en día tienen la "suerte" de contar con miles y miles de "amigos", con lo cual podemos señalar que el concepto de "amigo" en las redes sociales del mundo virtual difiere sin lugar a dudas del concepto de "amigo" en nuestra vida real, aunque claro está no podemos seguir insistiendo en la existencia de un mundo virtual y de un mundo real.

Es tal el impacto de las redes sociales en nuestras vidas, que seguramente la mayoría de los uruguayos que tiene *Facebook* hoy en día tienen la "suerte" de contar con miles y miles de "amigos", con lo cual podemos señalar que el concepto

desmarcar la casilla que dice Aplicación Contactos. Allí también están Aplicación Calendario y Aplicación Mensajes. En **iPhone, iPod e iPad**, dentro de Opciones > Amigos, se activa o se desactiva la función de sincronización, que permite tomar los amigos del directorio telefónico y vincularlos en *Facebook*.

4. Bloquear las cookies que registran la navegación

Un buen número de usuarios no ve con buenos ojos que las redes sociales usen su información de navegación para personalizar anuncios publicitarios y así maximizar sus ganancias. Para evitarlo, es necesario **desactivar las llamadas "cookies"**. En *Twitter*, esto se hace desde Configuración > Cuenta y se desmarca la opción Personalización. En cuanto a *Facebook*, no está preciso cómo hacerlo, pero con desactivar los datos compartidos a las aplicaciones será suficiente. Con respecto a Google Plus, que se vale del historial del buscador, se ingresa a la solapa Editar perfil y donde dice Servicios, se hace clic en la opción Ver historial. Allí se puede desactivar el registro de la navegación y borrar el historial preexistente.

35 Según <http://www.observa.com.uy> (09.08.2012): Más de un millón de uruguayos usan redes sociales: La novena edición del Perfil del Internauta dejó en evidencia la supremacía de *Facebook* y la diversificación de los usos en internet. El 99% usa *Facebook* y el 11% *Twitter*. *Facebook* es el uso más mencionado (el 99% de los uruguayos que usan redes están en *Facebook*) y a una distancia importante de los demás. Es el medio que más se utiliza para chatear, triplicando el MSN, es prácticamente lo único que se usa para subir fotos y cuadruplica el uso de Youtube para subir videos. Más de la mitad de los usuarios de *Facebook* entra todos los días. El usuario promedio tiene unos 400 amigos y ese número crece muy fuertemente cuanto menor es la edad (640 entre los que tienen menos de 20 años). Los usos más mencionados de *Facebook* son chatear (73% lo hace "habitualmente"), compartir enlaces (48%), comentar el estado de sus amigos (47%), subir fotos (44%) y escribir comentarios sobre sí mismos (30%).

de "amigo" en las redes sociales del mundo virtual difiere sin lugar a dudas del concepto de "amigo" en nuestra vida real, aunque claro está no podemos seguir insistiendo en la existencia de un mundo virtual y de un mundo real.

5 La neutralidad tecnológica y las administraciones públicas

5.1 El principio de neutralidad tecnológica

En este punto debe resaltarse especialmente que toda normativa que regule aspectos tecnológicos o íntimamente relacionados con la Sociedad de la Información debe partir de la neutralidad tecnológica, de tal forma que todos los aspectos regulados permitan cubrir diferentes situaciones particulares, con independencia de las características tecnológicas con las que cuente.[36]

El mundo cambió drásticamente en la última mitad del siglo XX. Transformación que es perceptible en nuestros días y que tiende a continuar. Esta revolución se hace latente con mayor claridad en el uso de las nuevas tecnologías, vislumbrándose así el nacimiento de una cuarta generación de derechos humanos, en los que la universalización del acceso a la tecnología, la libertad de expresión en la web y la libre distribución de la información juegan un papel fundamental y son elementos esenciales para su definición.[37]

Internet es visto como un espacio propicio para extender las libertades, en consecuencia se propone que no debe hacerse ninguna intervención —o quizás mínima— en la red, esta es la opinión de un grupo significativo y es la visión predominante entre los usuarios —aun cuando evaden discutir o minimizan el tema de los riesgos. Por esta característica difusa la neutralidad suele expresarse en diferentes niveles y con diferentes consecuencias.[38]

[36] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Disponible en internet: <http://www.agpd.es>.

[37] ORNELAS, Lina. – *El derecho de las niñas, niños y adolescentes a la protección de sus datos personales: evolución de derechos y su exigencia frente a la redes sociales*; Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes; Memorándum de Montevideo; Carlos G. Gregorio – Lina Ornelas, Compiladores; IIJusticia – Instituto de Investigación para la Justicia, IFAI –Instituto Federal de Acceso a la Información y Protección de Datos; México, 2011, p. 27.

[38] GREGORIO, Carlos G. – *Impacto y evolución de las redes sociales digitales: libertades y derechos*; Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes; Memorándum de Montevideo; Carlos G. Gregorio – Lina Ornelas, Compiladores; IIJusticia – Instituto de Investigación para la Justicia, IFAI –Instituto Federal de Acceso a la Información y Protección de Datos; México, 2011, p. 63 y siguientes.

Según Miguel Osio Zamora, el principio de neutralidad tecnológica supone que la Ley debe permanecer neutral en cuanto a los tipos de tecnología y el desarrollo de las mismas, por demás cambiantes en forma constante. La Ley no debe inclinarse u orientarse a un tipo de tecnología, ni limitarse a una forma de transmitir los mensajes. Esto es de suma importancia, debido a que no sólo puede excluir tecnologías existentes, sino quedar obsoleta en un período relativamente corto.[39]

Para las empresas productoras de software y tecnología este concepto alude a la neutralidad del Estado, permitiendo que el mercado se regule mediante la oferta y la demanda. Las empresas de software privativo que promueven la neutralidad tecnológica plantean que los proveedores de software libre y los proveedores de software privativo compitan libremente entre ellas manteniendo así el *status quo* de los monopolios que se han impuesto mundialmente y rechazando la posibilidad de perder el control de áreas que le reportan a estas empresas extraordinarias ganancias, como lo son las administraciones publicas. Este tipo de neutralidad es denominada neutralidad formal, aludiendo a la igualdad de concurrencia y a la no discriminación entre tecnologías ante una necesidad que los Estados necesitan solventar.[40]

Contraponiéndose a esta acepción del término, encontramos una interpretación que entiende que la neutralidad tecnológica marca la actitud que debe tomar la administración pública respecto de un proveedor que a través del transcurso del tiempo ha adquirido una posición de preeminencia por sobre las demás empresas. Este tipo de neutralidad es denominada horizontal y demanda al Estado la activa adopción de políticas de adquisiciones que favorezcan alternativas. Esta posición es defendida por aquellas empresas que no poseen fuerte presencia en el mercado y consideran que el mismo estado debe regular y crear un ámbito de igualdad de concurrencia.[41]

[39] OSIO ZAMORA, Miguel. – *El comercio electrónico. Los mitos de una Ley sobre la materia*; TPA: Publicaciones y eventos, artículos de opinión. Disponible en internet: <http://www.tpa.com.vw/art_e_comerce/>.

[40] LOFEUDO, Ismael. – *La neutralidad tecnológica del Estado y la defensa común como mandato constitucional*; Grupo de Estudio de la complejidad en la Sociedad de la Información (GECSI). Universidad Nacional de La Plata, Facultad de Ciencias Jurídicas y Sociales, Argentina. Disponible en internet: <http://www.gecsi.unlp.edu.ar/>.

[41] LOFEUDO, Ismael. – *La neutralidad tecnológica del Estado y la defensa común como mandato constitucional*; Grupo de Estudio de la complejidad en la Sociedad de la Información (GECSI). Universidad Nacional de La Plata, Facultad de Ciencias Jurídicas y Sociales, Argentina. Disponible en internet: <http://www.gecsi.unlp.edu.ar/>.

5.2 La neutralidad tecnológica como nueva tecnología de identificación electrónica

Para regular el uso de las nuevas tecnologías de identificación electrónica, siguiendo a Trivelli González, podemos adoptar dos perspectivas: una tecnológicamente específica u otra tecnológicamente neutra:[42]

a) La primera implica establecer un marco jurídico particular y determinado que regulara un proceso de identificación y tecnología definida.

b) La segunda, en cambio, establece disposiciones sobre la base de las funciones que cumple o puede cumplir cualquier tecnología de identificación, sin importar el proceso y la estructura que utiliza para identificar, sino el cumplimiento de los requisitos que exige. Tal cual acontece con la Ley Modelo de la Comisión de las Naciones Unidas sobre el derecho mercantil internacional sobre firmas electrónicas de 2001. Esta ley, establece entre sus objetivos que "[...] Al incorporar a su derecho interno los procedimientos prescritos por la Ley Modelo para todo supuesto en el que las partes opten por emplear medios electrónicos de comunicación, un Estado estará creando un entorno legal neutro para todo medio técnicamente viable de comunicación comercial".

La incorporación de este principio a un texto legal permite su aplicación sin que los cambios o modificaciones o avances de la tecnología de identificación menoscaben su vigencia. Ello en la medida en que las funciones y efectos jurídicos de los procesos aseguren la integridad de la información, la autenticidad del documento electrónico, la identificación de las partes, la función del "no repudio" y la confidencialidad.[43]

La neutralidad tecnológica consiste en "no comprometer el sistema jurídico a una determinada tecnología, permitiendo que la firma electrónica acceda a modernizaciones destinadas a mantener su eficiencia de empleo, operación, almacenamiento y mecanismos de transmisión".[44]

[42] TRIVELLO GONZÁLEZ, María Paz. – *El principio de neutralidad tecnológica en la Ley Nº 19.799*; Revista Chilena de Derecho Informático. Facultad de Derecho. Universidad de Chile. Disponible en internet: <http://www.derechoinformatico.uchile.cl/>.

[43] TRIVELLO GONZÁLEZ, María Paz. – *El principio de neutralidad tecnológica en la Ley Nº 19.799*; Revista Chilena de Derecho Informático. Facultad de Derecho. Universidad de Chile. Disponible en internet: <http://www.derechoinformatico.uchile.cl/>.

[44] TRIVELLO GONZÁLEZ, María Paz. – *El principio de neutralidad tecnológica en la Ley Nº 19.799*; Revista Chilena de Derecho Informático. Facultad de Derecho. Universidad de Chile. Disponible en internet: <http://www.derechoinformatico.uchile.cl>.

La neutralidad de la red ha sido materia legislativa en Chile por la Ley 20.453 de 18 de agosto de 2010: *Artículo 24 H*. "Las concesionarias de servicio público de telecomunicaciones que presten servicio a los proveedores de acceso a Internet y también estos últimos, entendiéndose por tales, toda persona natural o jurídica que preste servicios comerciales de conectividad entre los usuarios o sus redes e Internet: a) No podrán arbitrariamente bloquear, interferir, discriminar, entorpecer ni restringir el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet, así como cualquier otro tipo de actividad o uso legal realizado a través de la red".

En Brasil existe un proyecto de ley denominado "Marco Civil para Internet en Brasil".

Hans ULRICH y Gunter MULLER señalan que el problema real no es el "ciudadano transparente" que está a la merced de un "Estado Controlador", sino en el hecho de que ningún Estado en el mundo puede protegernos contra la amenaza de anarquía en la red. Por eso los grandes recolectores de datos como *Google*, *Facebook*, *Microsoft* y muchas más empresas parecen monitorear todo —y no existe aún un genuino guardián identificable.[45]

6 La autorregulación como instrumento para la protección de los datos personales y de la seguridad en la redes sociales

6.1 La importancia de la autorregulación

Para resolver las dificultades y lagunas en la normativa estatal, incluso, internacional, ante el ritmo vertiginoso de los avances tecnológicos, así como para superar aspectos complejos de la propia naturaleza de Internet como son la territorialidad indefinida de la Red y la frecuente multinacionalidad de las partes, se han fomentado desde el Estado la creación de códigos de conducta específicos que sirvan para minimizar los riesgos asociados a estos servicios y resolver los posibles problemas por un cauce más rápido y sencillo.

El valor de la autorregulación resulta especialmente relevante en un ámbito que, como el que analizamos, no parece conocer de fronteras territoriales. En efecto, las plataformas en las que las redes sociales se fundamentan, en no pocas ocasiones, se encuentran situadas fuera de la Unión Europea, principalmente en Estados Unidos, por lo que, en el momento del registro, los datos serán trasladados

[45] GREGORIO, Carlos G. – *Impacto y evolución de las redes sociales digitales: libertades y derechos*; Ob. Cit, p. 63 y siguientes.

a los servidores y oficinas situados en ese país. Es, en consecuencia, necesario y plausible que las políticas de privacidad de las redes sociales que, en el espacio territorial mundial.

6.2 Códigos de conducta y redes sociales

En este sentido, es la propia legislación española la que fomenta, desde el artículo 18 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de Información y Comercio Electrónico (LSSI-CE), la creación de una serie de códigos de conducta que, combinados con sistemas de solución extrajudicial de conflictos, permitan mejorar las relaciones en Internet.[46]

Concretamente, la LSSI-CE dice lo siguiente: "Las Administraciones públicas impulsarán, a través de la coordinación y el asesoramiento, la elaboración y aplicación de códigos de conducta voluntarios, por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores, en las materias reguladas en esta Ley".

Frente a todos los riesgos señalados, la autorregulación es un método para proteger los derechos de los usuarios de redes sociales —sin, por supuesto, suplir a la normativa en materia de protección de datos.

Los códigos de conducta y las condiciones de uso constituyen una buena forma de solventar los posibles conflictos que puedan surgir en el uso de estas plataformas, y brindan una herramienta básica e imprescindible a los prestadores de dichos servicios ante posibles demandas de usuarios de las mismas. Los códigos de conducta son una forma de regulación interna, y funcionan como un contrato entre los proveedores del servicio y sus usuarios. En el caso de un uso que vulnere la ley, son los poderes judiciales y los gobiernos los que aplican los mecanismos que consideren necesarios, siguiendo los procedimientos ordinarios (denuncia, investigación, juicio y sentencia), solicitando a cada parte los datos que considere necesarios.[47]

Así, el pasado 10 de febrero de 2009 se anunciaba el *Acuerdo Europeo para mejorar la seguridad de los menores que utilizan redes sociales* a iniciativa de la

[46] PÉREZ SAN JOSÉ, Pablo. Observatorio de Seguridad de la Información. Instituto Nacional de las Tecnologías de la Comunicación (INTECO). Revista de la Agencia de Protección de Datos de la Comunidad de Madrid.

[47] PÉREZ SAN JOSÉ, Pablo. Observatorio de Seguridad de la Información. Instituto Nacional de las Tecnologías de la Comunicación (INTECO). Revista de la Agencia de Protección de Datos de la Comunidad de Madrid.

Comisión Europea y firmado por diecisiete de las redes sociales más importantes que operan en Europa, reconociendo su responsabilidad respecto a los riesgos potenciales que pueden encontrar en sus webs los niños y adolescentes (revelación de datos personales, ciberacoso, acoso sexual, etc.).

La finalidad de este código de conducta de las redes sociales para la protección de los menores es minimizar, limitar y/o erradicar estos riesgos, mediante las siguientes medidas:[48] a) Proporcionar un botón de "denuncia de abusos" fácil de utilizar y accesible, que permita a los usuarios denunciar, con un solo clic, contactos o comportamientos inadecuados de otros usuarios; b) Asegurarse de que todos los perfiles y listas de contactos en línea de los usuarios de los sitios web registrados como menores de 18 años estén predeterminados como "privados"; c) Asegurarse de que los perfiles privados de los usuarios menores de 18 años no puedan buscarse (ni en los sitios web ni a través de motores de búsqueda); d) Garantizar que las opciones de privacidad estén destacadas y sean accesibles en todo momento, de manera que los usuarios puedan averiguar fácilmente quién puede ver lo que cuelgan en línea: si sólo sus amigos o todo el mundo; y, e) Impedir que los menores de edad utilicen sus servicios: si una red social está dirigida a adolescentes de más de 13 años, a los menores de esa edad debe resultarles difícil registrarse.

Paralelamente se han desarrollado otras iniciativas similares en este ámbito, como son la *Social Networking Guidance* publicada por el Ministerio del Interior del Reino Unido en abril de 2008; el compromiso del británico *Interactive Advertising Bureau*, relativo a la publicidad en redes sociales, o el *Joint statement on key principles of social networking safety*, una serie de acuerdos suscritos entre *Myspace* y *Facebook* con 49 fiscales generales estatales en los Estados Unidos, en enero de 2008.

Este último se define asimismo como un potencial modelo de conducta adoptar por otras redes sociales, con medidas similares al Acuerdo europeo, pero también otras que destacan por su singularidad:[49] a) Los perfiles de menores 14 y 15 años serán automáticamente privados, se impedirá el contacto con adultos. Existirá, además, la posibilidad de bloquear a todos los usuarios mayores de 18

[48] PÉREZ SAN JOSÉ, Pablo. Observatorio de Seguridad de la Información. Instituto Nacional de las Tecnologías de la Comunicación (INTECO). Revista de la Agencia de Protección de Datos de la Comunidad de Madrid.

[49] PÉREZ SAN JOSÉ, Pablo. Observatorio de Seguridad de la Información. Instituto Nacional de las Tecnologías de la Comunicación (INTECO). Revista de la Agencia de Protección de Datos de la Comunidad de Madrid.

años; b) Los perfiles menores de 14 y 15 años solo podrán agregar contactos que conozcan previamente su nombre y apellidos y su email ("solo amigos" automático); a los perfiles de los menores con 16 y 17 años se les aplicará por defecto, pero será modificable; c) Se aplicará una política de "bloqueo de edad" (*Age locking*) para los perfiles ya existentes, que no se podrán modificar hasta que el usuario no cumpla los 18 años; d) Acceso restringido a contenidos y links para adultos; y, e) Herramientas y formación a padres y educadores, con un servicio de atención a padres, el desarrollo y distribución gratuita de un programa de control parental, y la posibilidad de incluir en un registro el email de sus hijos para evitar su acceso a las redes sociales.

En este sentido, los códigos de conducta constituyen un instrumento autorregulatorio fundamental para el desarrollo seguro y confiable de los servicios de Internet y la protección de la privacidad y seguridad de sus usuarios. Y un buen ejemplo de su aplicación y utilidad, desde el punto de vista de la protección de los datos personales, son los acuerdos de buenas prácticas y compromisos éticos que están alcanzando los proveedores de redes sociales.

7 Conclusiones

A lo largo del presente trabajo abordamos los principales lineamientos de la protección de datos personales en las redes sociales digitales, teniendo presente por un lado, los impactos de la llamada "Web 2.0" conocida como la "Web de las redes sociales", y por otro, que el modelo de crecimiento de estas plataformas se basa fundamentalmente en un proceso "viral", con posibilidades de crecimiento de tipo exponencial y quizás desconocidas en cuanto a sus impactos.

Se destacaron conceptos claves como el acceso seguro, la identidad digital, las condiciones de uso y política de privacidad, la neutralidad tecnológica y la autorregulación en el mundo de la Web 2.0 con millones y millones de personas[50] colaborando, compartiendo y participando en un canal multidireccional abierto que permite lograr la máxima interacción entre los usuarios y les ofrece nuevas posibilidades de colaboración, expresión y participación.

Dada la gran cantidad de datos personales que los usuarios publican en sus perfiles, estos se convierten en auténticas "identidades digitales" que facilitan un

[50] En este sentido, existen redes sociales, como *Facebook*, en las que ya existen más de 200 millones de usuarios y con su *chat* supera la barrera de los 1000 millones de mensajes electrónicos diarios. Otro dato que, a este respecto, podemos poner de relieve, a tenor de ciertos estudios de carácter empírico, es que dentro de las primeras veinte posiciones de los 500 sitios *Web* más visitados a nivel internacional existen cuatro redes sociales cuales son *Facebook*, *MySpace* y *Hi5*.

rápido conocimiento de datos de contacto, preferencias y hábitos del usuario. El consentimiento que presta el usuario es válido en el momento en que decide aceptar, la política de privacidad y condiciones de uso de la plataforma que constan en el formulario de registro.

Evidentemente, esto no obsta a que resulte exigible que las políticas de privacidad deban ser transparentes, accesibles y claras. La configuración de la privacidad y las condiciones de uso de una de las redes sociales, sino la más representativa y masiva que existe en la actualidad, como *Facebook* ha despertado sucesivas controversias entre los millones de usuarios en el mundo.

Quizás y más allá de consejos esenciales para proteger nuestros datos en Internet, a los cuales hemos hecho referencia, debemos tener presente que todo lo que se publica en *Facebook* como en *Twitter*, es en principio público, esto es, cualquier persona, en cualquier lugar del mundo en que se encuentre podrá acceder a lo publicado por ser parte de la famosa "comunidad *Facebook*" o "comunidad *Twitter*"; salvo que en el momento en que tiene lugar la registración en la red, se configure con especial atención la política de privacidad, permitiendo acceder a los contenidos, ya sean fotos, textos, videos, solamente a los llamados "amigos" —que se suponen serian personas con las cuales nos vinculamos en la red social a las cuales conocemos de antemano— en el caso de *Facebook*; o solamente en el caso de los llamados "seguidores" en el caso de *Twitter*.

Es tal el impacto de las redes sociales en nuestra vida, también llamada "Vida 2.0" caracterizada por la transformación de lo cotidiano en los tiempos de las redes sociales electrónicas,[51] que seguramente la mayoría de los uruguayos[52] que tiene

[51] El 78% de los usuarios de las redes sociales admite que no puede controlar el tiempo que les dedica. Esta es una de las conclusiones principales de una investigación realizada por la Facultad de Comunicación de la Universidad de Montevideo (UM) sobre el uso de estos formatos electrónicos, la primera en su tipo en el país. Este estudio también revela que si bien el 71% siente temor a perder su privacidad, un 76% ya la considera parte de su rutina. ¿Algo más? El promedio de conexión a estas redes es de una hora y once minutos al día. Su utilidad más valorada, señalada por el 78% de los consultados, es intercambiar fotos con su universo de "amigos". **Vidas 2.0: "La Transformación de lo cotidiano en los tiempos de las redes sociales electrónica" Facultad de Comunicación de la Universidad de Montevideo (UM).**

[52] Según <http://www.observa.com.uy> (09.08.2012): Más de un millón de uruguayos usan redes sociales: La novena edición del Perfil del Internauta dejó en evidencia la supremacía de *Facebook* y la diversificación de los usos en internet. El 99% usa *Facebook* y el 11% *Twitter*. *Facebook* es el uso más mencionado (el 99% de los uruguayos que usan redes están en *Facebook*) y a una distancia importante de los demás. Es el medio que más se utiliza para chatear, triplicando el MSN, es prácticamente lo único que se usa para subir fotos y cuadruplica el uso de Youtube para subir videos. Más de la mitad de los usuarios de *Facebook* entra todos los días. El usuario promedio tiene unos 400 amigos y ese número crece muy fuertemente cuanto menor es la edad (640 entre

Facebook hoy en día tienen la "suerte" de contar con miles y miles de "amigos", con lo cual podemos señalar que el concepto de "amigo" en las redes sociales del mundo virtual difiere sin lugar a dudas del concepto de "amigo" en nuestra vida real, aunque claro está no podemos seguir insistiendo en la existencia de un mundo virtual y de un mundo real.

Tenemos la esperanza de que este trabajo sea un aporte, más que a la problemática de las redes sociales con sus riesgos y amenazas, a la nueva realidad que nos toca vivir, inimaginable años atrás y absolutamente desconocida en lo viene, en el futuro cercano, dado el crecimiento exponencial de las nuevas tecnologías y de las nuevas aplicaciones.

The Protection of Personal Data in Social Networks

Abstract: Throughout this work we will consider the main guidelines for the protection of personal data in social networks. We refer to the impact of the "Web 2.0" and social networking Web on the traditional concept of the protection of personal data in both its normative and doctrinaire in their livelihoods. Our tour begins in the present situation of the problems in the European Union and in the world, bearing in mind that the growth model of these platforms is primarily based on a viral process, with potential for exponential growth and perhaps unknown in their impacts. Hence, a possible breach of personal data of users of social networking transforms into the central object of our work, highlighting key concepts such as secure access, digital identity, technological neutrality and self-regulation codes of conduct. The biggest challenge will be how to respond to the questions posed to millions of people around the world about the impacts and risks increasingly sensitive to set out to be part of the "cyberspace" these days.

Key words: Privacy policy. Social network. Web 2.0. Secure, digital identity. Technological neutrality. Autoregulation. Codes of conduct.

Referencias

BERNIER, Chantal – *El Memorándum de Montevideo: un marco de referencia para la protección de los datos personales de los jóvenes en Internet en la región Iberoamericana*; Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes; Memorándum de Montevideo; Carlos G. Gregorio – Lina Ornelas, Compiladores; IIJusticia – Instituto de Investigación para la Justicia, IFAI –Instituto Federal de Acceso a la Información y Protección de Datos; México, 2011.

los que tienen menos de 20 años). Los usos más mencionados de *Facebook* son chatear (73% lo hace "habitualmente"), compartir enlaces (48%), comentar el estado de sus amigos (47%), subir fotos (44%) y escribir comentarios sobre sí mismos (30%).

CAMPAÑA, Farith Simon – *El enfoque de derechos en el "Memorándum de Montevideo"*; Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes; Memorándum de Montevideo; Carlos G. Gregorio – Lina Ornelas, Compiladores; IIJusticia – Instituto de Investigación para la Justicia, IFAI –Instituto Federal de Acceso a la Información y Protección de Datos; México, 2011.

DELPIANO, Héctor M. – "*Derechos Fundamentales y Habeas Data en el Uruguay"*, Anuario de Derecho Administrativo, Tomo IX. F.C.U, Montevideo 2002.

– "*Protección de datos personales y acción de habeas data. La Ley Nº 18.831"*, Anuario de Derecho Administrativo, t. XV. F.C.U, Montevideo 2008.

DELPIAZZO, Carlos E. – "*A la búsqueda del equilibrio entre privacidad y acceso"* en "Protección de Datos Personales y Acceso a la Información Pública" Dr. Carlos Delpiazzo- Coordinador, Instituto de Derecho Informático, Facultad de Derecho de la Universidad de la República, F.C.U./AGESIC, Montevideo 2009.

DURÁN MARTÍNEZ, Augusto. – "*Derecho a la protección de datos personales y al acceso a la información pública – Hábeas Data, Leyes Nº 18.331, de 11 de agosto de 2008 y Nº 18.381, de 17 de octubre de 2008"* (A.M.F., 2º Edición actualizada y ampliada, Montevideo 2012.

GREGORIO, Carlos G. – *Impacto y evolución de las redes sociales digitales: libertades y derechos*; Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes; Memorándum de Montevideo; Carlos G. Gregorio – Lina Ornelas, Compiladores; IIJusticia – Instituto de Investigación para la Justicia, IFAI –Instituto Federal de Acceso a la Información y Protección de Datos; México, 2011, p. 63 y siguientes.

LOFEUDO, Ismael. – *La neutralidad tecnológica del Estado y la defensa común como mandato constitucional*; Grupo de Estudio de la complejidad en la Sociedad de la Información (GECSI). Universidad Nacional de La Plata, Facultad de Ciencias Jurídicas y Sociales, Argentina. Disponible en internet: <http://www.gecsi.unlp.edu.ar/>.

LÓPEZ JIMÉNEZ, David – *La protección de datos de carácter personal en el ámbito de las redes sociales electrónicas: el valor de la autorregulación*; Universidad de Alcalá de Henares. Servicio de Publicaciones, 2009.

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Disponible en internet: <http://www.agpd.es>.

OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN (INTECO). *Guía de introducción a la Web 2.0: aspectos de privacidad y seguridad en las plataformas colaborativas*. España, Febrero 2011. Disponible en internet: <http://observatorio.inteco.es>.

ORNELAS, Lina. – *El derecho de las niñas, niños y adolescentes a la protección de sus datos personales: evolución de derechos y su exigencia frente a la redes sociales*; Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes; Memorándum de Montevideo; Carlos G. Gregorio – Lina Ornelas, Compiladores; IIJusticia – Instituto de Investigación para la Justicia, IFAI –Instituto Federal de Acceso a la Información y Protección de Datos; México, 2011.

OSIO ZAMORA, Miguel. – *El comercio electrónico. Los mitos de una Ley sobre la materia*; TPA: Publicaciones y eventos, artículos de opinión. Disponible en internet: <http://www.tpa.com.vw/art_e_comerce/>.

PESCHARD MARISCAL, Jacqueline – *Protección de las niñas, niños y adolescentes en el ámbito digital: responsabilidad democrática de las instituciones de gobierno y de las agencias de protección de datos*; Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes; Memorándum de Montevideo; Carlos G. Gregorio – Lina Ornelas, Compiladores; IIJusticia – Instituto de Investigación para la Justicia, IFAI –Instituto Federal de Acceso a la Información y Protección de Datos; México, 2011.

PÉREZ SAN JOSÉ, Pablo. Observatorio de Seguridad de la Información. Instituto Nacional de las Tecnologías de la Comunicación (INTECO). Revista de la Agencia de Protección de Datos de la Comunidad de Madrid.

PIÑAR MAÑAS, José Luis. –*"Guía del Derecho Fundamental a la protección de datos de carácter personal"*, (Agencia Española de Protección de Datos, 2004). La información de esta Guía puede ser ampliada en Servicio de Atención al Ciudadano. Disponible en internet: <http://www.agpd.es>.

– *¿Existe la privacidad? Inauguración del curso académico 2008/2009*, Madrid, Publicaciones de la Fundación Universitaria San Pablo CEU.

– "El derecho fundamental a la protección de datos. Contenido esencial y retos actuales. En torno al nuevo Reglamento de Protección de Datos". En PIÑAR MAÑAS, José Luis y CANALES GIL, Álvaro, *Legislación de Protección de Datos*, Madrid, Iustel.

ROTONDO TORNARÍA, Felipe. –"*Protección de datos: su régimen jurídico. Derecho subjetivo. Regulación*" en "Nuevos aspectos de las relaciones administrativas", Instituto de Derecho Administrativo; Carlos Delpiazzo -Coordinador (F.C.U., Instituto de Derecho Administrativo –Facultad de Derecho – Universidad de la República; Montevideo 2011), p. 257 y siguientes.

RIZO GARCÍA, Marta – "*Redes. Una aproximación al concepto*". Universidad Autónoma de la Ciudad de México. Disponible en internet: <http://sic.conaculta.gob.mx/centrodoc_documentos/62.pdf>.

SCHIAVI, Pablo.– *El control del acceso a la información pública y de la protección de datos personales en el Uruguay"*, Universidad de Montevideo. Facultad de Derecho. Montevideo, 2012.

–"*El Acceso a la Información Pública en el Uruguay"* en Estudios de Derecho Administrativo, Nº 3/2011, DURÁN MARTÍNEZ, Augusto, Director (Editorial La Ley Uruguay, Montevideo 2011).

TRIVELLO GONZÁLEZ, María Paz. – *El principio de neutralidad tecnológica en la Ley Nº 19.799*; Revista Chilena de Derecho Informático. Facultad de Derecho. Universidad de Chile. Disponible en internet: <http://www.derechoinformatico.uchile.cl/>.

VÁZQUEZ PEDROUZO, Cristina. –"*El régimen jurídico del acceso a la información pública y la protección de datos personales"* (Revista de Derecho y Tribunales, Nº 15, A.M.F., Montevideo 2011).

Informação bibliográfica deste texto, conforme a NBR 6023:2002 da Associação Brasileira de Normas Técnicas (ABNT):

SCHIAVI, Pablo. La protección de los datos personales en las redes sociales. A&C – Revista de Direito Administrativo & Constitucional, Belo Horizonte, ano 13, n. 52, p. 145-178, abr./jun. 2013.

Recebido em: 08.10.2012
Aprovado em: 20.04.2013