

Impacto y evolución de las redes sociales digitales: libertades y derechos

Carlos G. Gregorio

Introducción

Es claro que Internet se ha desarrollado como un espacio propicio para la comunicación, el acceso a la información y el conocimiento, la transparencia gubernamental, la expresión y todo ello rodeado de una atmósfera de creatividad e innovación. No por ello la satisfacción es plena, por un lado existen muchos aspectos sensibles y también la evolución futura es un enigma. La discusión que se hará entonces en este documento se concentrará —más que nada— en cómo las decisiones del presente perfilarán la evolución y optimización de las aplicaciones del futuro en un contexto de libertades y derechos.

Uno de los aspectos y expectativas básicas es que este desarrollo sea armonioso con el respeto de los derechos humanos, y en este sentido existen al menos dos aspectos preocupantes: evitar que se creen concentraciones de poder¹ y garantizar los derechos de las personas o grupos que devienen vulnerables como consecuencia de esta espiral

¹ La evolución histórica de los derechos humanos ha estado caracterizada por evitar las concentraciones de poder; comenzando por las monarquías absolutistas, los gobiernos de facto, y también los excesos de los gobiernos elegidos democráticamente.

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

de innovación.

Se comenzará por una discusión sobre los riesgos, fundamentalmente porque los logros y las nuevas oportunidades que se han generado son innegables. También es impensable una marcha atrás, solo se trata aquí de discutir los ajustes necesarios.

El marco legal en que ocurre esta evolución aparece como fundamental, porque el sistema de incentivos o regulaciones es el que determina la inversión y el que orienta la creatividad.

Es probable que hoy no sea posible —aun— contar con recomendaciones claras sobre cómo resolver los problemas, garantizar los derechos y maximizar las libertades; pero si es posible contribuir a este debate —en momentos muy acalorado y polarizado— con investigación, una visión ampliada y una identificación respetuosa de algunos consensos incipientes.

1. Riesgos

Los problemas y los riesgos suelen darse a conocer en estilo anecdótico, por casos particulares que resuenan en los medios, por críticas o denuncias. Pueden mencionarse dos categorías: los riesgos para la privacidad, intimidad o para la autodeterminación de los datos personales o la imagen; la otra categoría está definida por riesgos no virtuales, que no son nuevos, pero que se han recreado, o se ha modificado quiénes son ahora víctimas potenciales. Se incluyen los casos de fraude, robo de identidad y otros ciberdelitos, pero en este documento se trabajará con mayor profundidad la situación de los niños, niñas y adolescentes por su doble condición de nativos digitales y grupo vulnerable.

A partir de varios documentos recientes se ha puesto en evidencia la preocupación por los niños y adolescentes en el ciberespacio y la necesidad de complementar los marcos regulatorios, en particu-

camente. En este caso las empresas que hacen sus negocios en internet crecen e incrementan su posición de poder y el usuario está a merced de su oferta y a la aceptación de las condiciones de uso. Las leyes de transparencia se aplican a los gobiernos, pero las empresas en internet se escudan en los secretos comerciales y paradójicamente se presentan como *servicio público*, que en una atmósfera de aparente gratuidad ofrecen servicios y aplicaciones.

CARLOS G. GREGORIO

lar la *Child Online Protection Initiative* del la Unión Internacional de Telecomunicaciones (del 18 de mayo de 2009); *Opinion 5/2009 on online social networking*, del Grupo Europeo de Trabajo del Artículo 29 (del 12 de junio de 2009) analizadas también en la perspectiva del *Acordo que põe fim à disputa judicial entre o Ministério Público Federal de Brasil e a Google* (del 1 de julio de 2008); el *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. / Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc.* (del 16 de julio de 2009).

Estos documentos han sido recientemente complementados por un documento elaborado en el Berkman Center for Internet & Society de la Harvard University² y por un estudio llevado adelante por iniciativa de la Comisión Europea.³

Estos documentos podrían resumirse en el reconocimiento de problemas, en particular para niños y adolescentes, generalmente ilustrados por casos particulares, y algunas veces presentados en forma dramática por los medios, que han motivado un llamado de atención que intenta recordar que vigencia de los derechos fundamentales (en particular la Convención de los Derechos del Niño) y la necesidad de una visión más amplia que incluya las nuevas tecnologías.

Por un lado se reconocen algunos riesgos intrínsecos pero se enfatizan algunos riesgos contextuales que se magnifican en particular en los países en vías de desarrollo.⁴ La descripción de estos riesgos para los niños y adolescentes supone un conjunto de neologismos: *pharming*, *clickjacking*, gusanos, *cookies*, *ciberbullying*, *grooming* y

² Urs Gasser, Colin Maclay & John Palfrey, 'Working towards a deeper understanding of digital safety for children and young people in developing nations: an exploratory study by the Berkman Center for Internet & Society at Harvard University, in collaboration with UNICEF', (16 de junio de 2010).

³ Sonia Livingstone, Leslie Haddon, Anke Gorzig & Kjartan Olafsson *et al.*, 'Risks and safety on the internet: the perspective of European children (initial findings from the EU Kids Online survey of 9—16 years old and their parents', (21 de octubre de 2010).

⁴ En un estudio reciente Gasser, Maclay y Palfrey analizan la vulnerabilidad *online* de los niños y adolescentes desde la óptica del país en que acceden a Internet. El enfoque del estudio acepta la existencia en las nuevas tecnologías de una multiplicidad de nuevas oportunidades para los niños y adolescentes, pero también hace

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

sexting.⁵ Para los adultos uno de los riesgos que aun no reciben una respuesta adecuada es el de difamación y el uso indebido de la imagen.

Si hubiera que señalar algún factor reiterativo en la proliferación de estos riesgos, aparece inmediatamente el anonimato y la posibilidad que éste ofrece de suplantar una identidad, simular una edad o personalidad determinada y evadir toda responsabilidad. Al mismo tiempo se verá más adelante que el anonimato es un elemento clave en la evolución de Internet y que no puede —ni sería deseable— suprimirle *manu militari*.

En este orden de ideas nace también el *Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes*,⁶ (*Memorándum de Montevideo*) quizás interpretando que la protección de datos sería el primer paso de una garantía integral de derechos.

un exhaustivo análisis de los riesgos que se han percibido, destacando en forma reiterada que existen mucha información anecdótica y de casos puntuales que han ganado los medios, pero al mismo tiempo muy pocos datos obtenidos sistemáticamente. El estudio incluye una hipótesis subyacente que postula que no son iguales los riesgos para los niños y adolescentes de los países industrializados que para aquellos de los países en vías de desarrollo. En esta vía de argumentación surgen una serie de consideraciones, entre ellas las que se refieren a “riesgos altamente contextuales” y a una sucesión de “historias trágicas en la cobertura de la prensa” que se complementan con la debilidad del estado de derecho y la falta de instituciones robustas. En definitiva la argumentación apunta a la necesidad de disponer de datos empíricos sobre victimización para justificar intervenciones en el balance de los derechos del niño con otros derechos fundamentales (y eventualmente con la libertad de expresión). Los riesgos para los niños y adolescentes en el uso de las nuevas tecnologías de información y comunicación no son nuevos riesgos, sino en su mayoría una redistribución de los riesgos preexistentes que ahora afectan diferentes poblaciones en distintos grados y fundamentalmente se expanden en una atmósfera de excesiva confianza, y por tanto, baja precaución y prevención. Por esa razón las políticas de seguridad son más críticas en los países en vías de desarrollo, dado que a los riesgos próximos se suman los globales, y las exiguas prevenciones locales reciben un magro apoyo desde los países industrializados.

⁵ Pablo Pérez San-José, Cristina Gutiérrez Borge, Susana de la Fuente Rodríguez, Laura García Pérez y Eduardo Álvarez Alonso, *Guía de introducción a la Web 2.0: aspectos de privacidad y seguridad en las plataformas colaborativas*, INTECO, (2011). Disponible en: <http://www.inteco.es/file/pc8SqNjSy4wtSH7Ap15n5Q>

⁶Ver www.ijjusticia.org/Memo.htm

CARLOS G. GREGORIO

2. Niños, adolescentes y otros grupos vulnerables

Los riesgos son muy angustiantes para los niños y adolescentes; en un instante pueden pasar de un ambiente de juego y comunicación a estar siendo molestados o acosados por contenidos o personas que tratan de aprovecharse de ellos. Los niños y adolescentes suelen vivir estos eventos en soledad, pues temen que al confiarse en sus padres, la primera reacción de ellos será quitarles la conectividad. Aun cuando confíen en sus padres, el escenario más frecuente es que los padres no saben a quién acudir y que solo en muy pocos casos es posible, o remover los contenidos ofensivos, o identificar a los autores

En efecto, los nativos digitales han incorporado formas de socialización de las que les es muy difícil prescindir, pero las fallas en el sistema educativo y el halo de impunidad que rodea la intervención en Internet, han generado la situación en que niños y adolescentes son tanto víctimas como victimarios.

Las plataformas de relacionamiento (redes sociales digitales) son para los adolescentes un espacio obligado. En primer lugar porque son nativos digitales. También están siendo obligados a socializar de ese modo; nuestros abuelos hacían nuevas amistades en la “plaza”, nuestra generación en los “*shoppings*”, pero para los adolescentes de hoy es más difícil usar el espacio público, por la falta de seguridad y por las distancias en la nueva arquitectura de las ciudades.

Los intentos de solución son aun débiles: los filtros (o controles parentales) son ineficaces, no solo porque sería absurdo impedirles el acceso a las redes sociales, sino también si se considera que al mismo tiempo se desarrollan todos los días nuevos *proxis* para garantizar la libertad de información, que también anonimizan la conexión. Soluciones como la adoptada en otros medios de comunicación, como el horario de protección en la televisión, carecen de sentido en la red. Los filtros y el dominio .xxx recientemente aprobado luego de una larga discusión, podrían prevenir ciertos accesos, pero quedan muchas preguntas abiertas. También están las *helplines* y las *hotlines*.⁷

⁷ Las *helplines* reciben llamadas, son un canal para que los niños u otros en su nombre, presenten situaciones conflictivas. Pueden ser desde adolescentes deprimidos

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

El *Memorándum de Montevideo* hace algunas recomendaciones que interpretan el consenso, como la de reforzar el sistema educativo con una marcada visión preventiva; pero también sugiere explorar líneas de intervención que tienen menor consenso —y que serán analizadas más adelante, pero que introducen la visión de una región (América Latina) que suma algunos factores difíciles de administrar (acceso y conexión predominantemente desde cibercafés, y un nivel mayor de riesgos contextuales).

Otros riesgos son poco claros e incluyen otros grupos vulnerables (como por ejemplo los trabajadores y los inmigrantes) y devienen de la disponibilidad de mucha información de carácter personal que es publicada pensando que se trata de una comunicación (grupal) privada pero que —de acuerdo a algunas reglas del sitio donde se colocan, pueden ser utilizadas con otras finalidades; los aspectos más preocupantes en este caso es la discriminación laboral que pueda generarse por la debilidad con que se garantiza el derecho al olvido. En este sentido —y ya entrando en un análisis quizás exageradamente especulativo— los juegos *online* son capaces de generar mucha información sobre la personalidad y podrían ser utilizados como un test psicológico en tiempo real; así rasgos personales como la agresividad o un excesivo detallismo podrían ser determinantes en la selección laboral, que podría desplazarse a buscar patologías antes que identificar habilidades.

3. Oferta de redes de relacionamiento

Es natural que un espacio tan dinámico e innovador con Internet esté matizado por una oferta difusa. Los ajustes de las aplicaciones ofrecidas son permanentes y están basadas generalmente en

a educadores sociales en un barrio que saben de un caso de abuso sexual y quieren informarse adónde derivar. Muchas situaciones de violencia se presentan a través de las líneas de ayuda. Ver *Child Helpline International* – www.childhelplineinternational.org y CAI Virtual (require registro previo) www.delitosinformaticos.gov.co. Las *hotlines* se dedican específicamente a identificar delitos en el ciberespacio. Deberían tener la tecnología y los conocimientos para ver dónde están alojados los contenidos, estudiar si ellos constituyen delito en esa jurisdicción, contactarse con las autoridades locales para que avancen, y en paralelo avisarle al proveedor para que baje los contenidos. Ver SaferNet Brasil – www.safernet.org.br y ASI México <http://asi-mexico.org>.

CARLOS G. GREGORIO

la aceptación y en las respuestas de los usuarios.

Muchas empresas (por ejemplo líneas aéreas), noticieros de televisión (por ejemplo CNN), ONGs e incluso instituciones del Estado,⁸ difunden información y facilitan la participación en sus sitios en *Twitter* y *Facebook*: son usuales las frases “síguenos en *Twitter*” o “estamos en *facebook*”.

No se trata de establecer un relacionamiento, ni de ser amigo de una empresa gigantesca. En la práctica el mismo intercambio de información y las mismas expectativas podrías satisfacerse desde un sitio web, pero consultados algunos de directivos de empresas o de ONGs dijeron preferir redes sociales “porque los usuarios están más acostumbrados”. Esto quiere decir que las redes sociales tienen un atractivo especial (que no es sociabilizar en red) sino ofrecer a los usuarios una lógica de contenidos preestablecida y común, una modalidad de participación e invitar a usar un lenguaje al que ya están acostumbrados. Para un usuario experimentado puede ser difícil encontrar en un sitio de gobierno, o de una empresa, o de una ONG la información que busca; debe enfrentarse primero a ... ¿dónde están las cosas que busco? (puede ayudarse con el mapa del sitio, pero es muy probable que quede desilusionado, o con el buscador del sitio, y es probable que no resulte muy útil, y ... luego de varios intentos se encuentra la información o abandona la búsqueda. ¿Qué ocurriría —entonces— con un usuario que habitualmente maneja solo su correo y su red social? ... muy probablemente sienta que Internet es una gran complicación.

Entonces Facebook y Twitter (y no necesariamente otras plataformas de relacionamiento) ofrecen y tienen el monopolio de un lenguaje,⁹ las cosas están donde ya se está habituado a encontrarlas ... como estas redes son muy populares, es un terreno conocido para una población económicamente muy interesante. No parece muy racional que una oferta de relacionamiento se convierta en un estándar de lenguaje; sería entonces quizás más inteligente promover estándares para disponibilizar información en los sitios

⁸ Ver facebook.com/us.embassy.montevideo

⁹ Estas redes deben ser naturalmente monopólicas, pues quien está en una pequeña está incomunicado de la mayoría. Al inicio en algunos países los usuarios se caracterizaban por adherir a alguna red en particular —como *Orkut* en Brasil y la India, o *Tuenti* para los jóvenes en España— pero esta tendencia tiende a revertirse y ahora todos quieren estar en la “común”.

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

web cuando está dirigida a usuarios en forma masiva, así cada sitio tendría dos opciones, la estandarizada y la “creativa” (esa versión que incluye “saltar la introducción” y un despliegue de imágenes y arboles de decisión para organizar la información).

Esto explica —en parte— el éxito de las redes sociales: redes dentro de la red, que mantienen cautivos a los usuarios. Que los mantienen dentro de un mercado complejo (el producto ofertado es solo la punta de un ovillo) y poco claro (se presentan como gratuitas, pero la moneda es la información personal — y cuanta más información mejor).

Del análisis de la oferta y de la demanda surgen algunas preguntas sobre las redes sociales —prefiriendo aquí el término plataformas de relacionamiento: ¿qué es comunicación? y ¿qué es comunicación grupal?, ¿cuándo existe expresión?, ¿cuándo la intensidad es la asociación? ¿Cómo encontrar información, conocimiento u opinión pertinente? Y fundamentalmente si los diseños y aplicaciones ofrecidas, diferencian o confunden estas expectativas, y si privilegian u opacan los derechos y libertades que están detrás de cada una de ellas. ¿Existe libertad de diseño?

4. Libertades, derechos y políticas públicas

Existen varias expectativas predominantes en Internet, que se refieren a más libertad de expresión, acceso a la información, transparencia y las posibilidades de comunicación y asociación.

Acceso a la información, conocimiento y transparencia es una expectativa significativamente lograda. También existen logros para las posibilidades de comunicación interpersonal y grupal, con matices y críticas (hay quienes piensan que la comunicación es de contenido muy trivial —algunos dice que es mas cotilleo que relacionamiento; que los ciudadanos están sobrepasados de información pero mucho menos comunicados que antes, en fin este es el debate).

Sobre la libertad de expresión —quizás la expectativa mas sustantiva— se podría decir que está en desarrollo, con logros puntuales muy extraordinarios. Hay quienes dicen que si bien existen hoy muchas más posibilidades de expresarse, también se ha señalado

CARLOS G. GREGORIO

que es menos posible ser oído, producir impacto y generar transformaciones significativas. El impacto de una idea publicada en un artículo en un periódico de gran circulación —de lectura obligada— o difundida por televisión, no es igual a que aparezca en un *blog* que en la mayoría de los casos es conocido solo por quienes piensan igual y que es muy difícil de encontrar por la saturación de las búsquedas en Internet.

Dice Balkin, “las decisiones más importantes que afectarán el futuro de la libertad de expresión, no ocurrirán en el ámbito del derecho constitucional; ellas serán las decisiones sobre el diseño tecnológico, las regulaciones legislativas y administrativas, la formación de nuevos modelos de negocios, y las actitudes colectivas de los usuarios finales”.¹⁰ En consecuencia es posible inferir que la libertad de expresión debe ser repensada a la luz de la capacidad y potencialidad de internet.

Hoy uno de los incentivos que opera sobre los desarrollos y diseños de aplicaciones de relacionamiento se remiten a la sección 230 de la *Communications Decency Act* de los EE.UU. en la que los proveedores son inmunes frente a acciones judiciales por contenidos —denominada protección para el buen samaritano.¹¹ Section 230(c)(1) “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider”.

En los EE.UU. la Primera Enmienda es determinante en este análisis. Rebecca Tushnet encuentra que la discusión teórica sobre la libertad de expresión se centra en la implicaciones de “enfocarse en quien habla” versus “enfocarse en la audiencia”.¹² Por ejemplo Barron señala un profundo interés en proveer a los ciudadanos de un amplio acceso a puntos de vista conflictivos y a asuntos poco corrientes, no porque quienes tienen ideas disruptivas tengan dere-

¹⁰Jack M. Balkin, “The Future of Free Expression in a Digital Age” (January 29, 2009). *Pepperdine Law Review*, Vol. 36, 2008. Disponible en SSRN: <http://ssrn.com/abstract=1335055>

¹¹www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000230----000-.html

¹²Rebecca Tushnet, “Power Without Responsibility: Intermediaries and the First Amendment”, 76, *Geo. Wash. L. Rev.*, 101 (2008). Disponible en SSRN: <http://ssrn.com/abstract=1205674>

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

cho a ser oídos, sino porque la sociedad tiene un especial interés en oírlos.¹³

Estos argumentos son fundamentales al momento de discutir sobre los diseños de las aplicaciones de Internet en las que la libertad de expresión está en juego. Mientras que hoy existen diseños que facilitan expresarse, no tienen un desarrollo semejante aquellos que permiten encontrar puntos de vista conflictivos u opiniones en temas atípicos. O sea mientras que las plataformas de relacionamiento, y en particular los *blogs*, las posibilidades de comentar noticias y muchas más aplicaciones se abrojan (o autodefinen) como herramientas de libertad de expresión —y de hecho han incrementado la posibilidad de expresarse— simultáneamente se ha tornado mucho más complejo encontrar opiniones.

Continúa Rebecca Tushnet: “una teoría de la libertad de expresión centrada en la audiencia, no puede aceptar que la Primera Enmienda es satisfecha por la no intervención del gobierno en el mercado ... fundamentalmente porque las estructuras privadas que la ley habilita determinarán qué puede oír la audiencia y en qué manera puede responder”.

Como operan entonces los mecanismos para oír: la primera respuesta es que este es el *rôle* de los buscadores —pero los buscadores más populares son cero-transparentes y en algunos casos abiertamente no neutrales.¹⁴ Otros mecanismos se centran en el interés de los medios clásicos (prensa escrita y televisión) de motivar mecanismos de participación en línea, para seleccionar algunas intervenciones. Pero cualquier selección —hasta la más honesta y con intención de neutralidad— no deja de ser una parte del discurso.

¹³Jerome A. Barron, “Access to the Press—A New First Amendment Right”, *Harv. L. Rev.*, (80), 1641, 1641, 1653–54 (1967).

¹⁴Los buscadores tienen una función esencial en el acceso a la información, sin embargo los algoritmos de búsqueda son un secreto industrial, y en la práctica no todos los sitios web están indexados. Usar un buscador eficientemente exige habilidades bastante desarrolladas, no esperables al menos en un ciudadano común. Mientras que la oferta de redes sociales es muy grande porque existe un rédito en términos de perfiles y datos personales, existe escasez de herramientas para encontrar información. La neutralidad de los buscadores puede evaluarse con un ejercicio muy simple: buscando un hotel por su nombre y ciudad, “normalmente” aparecen en los primeros resultados los sitios de los revendedores de habitaciones de hoteles (¿... es que están en esas posiciones porque pagan por ellas?), y buscando cuidadosamente en la tercera o cuarta página aparece el “sitio web oficial” del hotel (normalmente si el hotel es pequeño y de pocos recursos).

CARLOS G. GREGORIO

Otros intentos apuntan a usar estadísticas sobre los comentarios en las redes sociales; por ejemplo dicen “la palabra más utilizada esta semana en *Twitter* ha sido ...” ... pero adaptando un antiguo refrán “aunque tú en la estadística estés presente, tu voz para la audiencia está ausente”.

5. Expectativas y derechos en las plataformas de relacionamiento

Cuando el Grupo del Artículo 19 se preocupa por algunos aspectos presentes de las redes sociales: “Cuando el acceso a la información del perfil va más allá de los contactos elegidos, en particular, cuando todos los miembros que pertenecen al servicio de red social pueden acceder a un perfil o cuando los datos son indexables por los motores de búsqueda, el acceso sobrepasa el ámbito personal o doméstico. Del mismo modo, si un usuario decide, con perfecto conocimiento de causa, ampliar el acceso más allá de los «amigos» elegidos, asume las responsabilidades de un responsable del tratamiento de datos. En la práctica, se aplica entonces el mismo régimen jurídico que cuando una persona utiliza otras plataformas tecnológicas para publicar datos personales en Internet”. Finalmente dice que aunque la *excepción doméstica* no se aplique debe establecerse un equilibrio entre la libertad de expresión y el derecho a la intimidad.¹⁵

Cabe preguntarse o inferir entonces que mientras no exista indexación de los contenidos y si el número de amigos es “razonable” el usuario no está “expresándose” sino “comunicándose”. Es difícil de responder pero es una hipótesis muy fértil. No parece muy razonable que quien tenga una expectativa de expresión quiera voluntariamente limitar su audiencia y reducir la probabilidad de que su opinión sea encontrada (ciertamente si solo quiere evitar el acceso de quien puede perseguirle o discriminarle por sus ideas).

Este manto de optimismo bajo el cual se colocan derechos, expectativas y diseños no va más allá de un ejercicio de imaginación para desmitificar el concepto de que el mejor escenario posible para que las nuevas tecnologías evolucionen y se desarrollen sólo son las

¹⁵Por ejemplo en España la *Ley Orgánica de Protección de Datos* dice: “El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación: a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas”.

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

reglas del mercado.

No huelga insistir, sin lugar a dudas desde la generalización de Internet una de las expectativas de impacto en las instituciones democráticas es que las aplicaciones en Internet producirían un notable incremento en el derecho a la libre expresión.¹⁶

Tabla 1. Aplicaciones sociales digitales.

	COMUNICACIÓN INTERPERSONAL	COMUNICACIÓN GRUPAL	EXPRESIÓN NO INTERMEDIADA	EXPRESIÓN INTERMEDIADA
DERECHOS EN EXPECTATIVA	derecho a la comunicación derecho al a privacidad de las comunicaciones		libertad de expresión derecho a la imagen	
EJEMPLOS	teléfono	Facebook Orkut	Twitter, blogs, wikileaks, YouTube, “comente esta nota”	“medios” en su sentido clásico
	teléfono móvil correo electrónico			
CONTENIDOS Y ACCESO	no intervención de las comunicaciones sin orden judicial	sin indexación ¹⁷	indexado	indexado
		robots identifican valoraciones a las reglas del sitio ¹⁸	(a veces con moderador que aplica las reglas del foro)	(con editor responsable)
IDENTIFICACIÓN	identificador de llamadas IMEI - SIM card ¹⁹ teléfono público ²⁰	pseudónimo posible (criterio de aceptación de amigos)	pseudónimo posible	pseudónimo casi-imposible
AUDIENCIA	los interlocutores muchos	el grupo o los “amigos”	absolutamente todos	los lectores, televidentes, etc.
RIESGOS PARA LOS NIÑOS Y ADOLESCENTES	bajo	alto	medio	casi nulo

¹⁶La libertad de expresión implica dos derechos, *viz.* el derecho a la libre expresión, y el derecho a no expresarse, a quedarse en silencio y a retener la información propia.

¹⁷En realidad no es siempre así, dependiendo de la red social y del nivel de privacidad seleccionado el contenido puede ser indexado por los buscadores universales en Internet (*Google, Yahoo, Bing*, etc.).

¹⁸En muchas aplicaciones se incluyen *robots* que analizan contenidos privados con fines de enviar publicidad comercial, esto supone una disminución del derecho a los datos personales y a la privacidad de las comunicaciones. Su aceptación es discutible, pero su generalización abre también la posibilidad de utilizar estos robots para detectar situaciones de acoso, difamación o contenidos ilegales.

¹⁹El IMEI (*International Mobile Equipment Identity*) y la SIM card (*Subscriber Identity Module*) tienden a hacer que cada teléfono móvil pueda ser identificado (y asociado generalmente a una persona), en algunos países cambiar estos códigos es considerado un delito.

²⁰Ciertamente el teléfono público abre la posibilidad de llamas totalmente anónimas

CARLOS G. GREGORIO

En efecto en los últimos años se ha observado una transformación positiva en la libre expresión de ideas y opiniones; pasando de un modelo intermediado por empresas característico del pasado, a un conjunto de aplicaciones en Internet que permiten la expresión y manifestación de ideas en forma directa (como los *blogs*, la posibilidad de comentar notas en los periódicos virtuales y en alguna medida algunas redes sociales como *Twitter*).

El balance de este proceso aun no es claro; si bien existen hoy muchas más posibilidades de expresarse, también se ha señalado que es menos posible ser oído, producir impacto y generar transformaciones significativas. El impacto de una idea publicada en un artículo en un periódico de gran circulación —de lectura obligada— o difundida por televisión, no es igual a que aparezca en un blog que en la mayoría de los casos es conocido solo por quienes piensan igual y que es muy difícil de encontrar por la saturación de las búsquedas en Internet.

Este análisis remite a una discusión de cuáles son las aplicaciones disponibles en Internet conocidas genéricamente como *redes sociales*, cómo son usadas (*i.e.* cuáles son las expectativas de los usuarios) y cuáles serían los derechos que intentan priorizar.

En algunas redes sociales la expectativa predominante de los usuarios podría definirse como “un mecanismo de comunicación grupal asincrónico”. Por ejemplo en las entrevistas a los niños y adolescentes sobre quiénes ellos creen que leen sus contenidos en redes sociales y quiénes ven sus fotos, la respuesta inmediata es “mis amigos”.

Otras redes sociales como *Twitter*, o los blogs tienen una clara expectativa de ejercitar el derecho a expresarse (aun cuando algunos crean cuentas cerradas sólo para sus amigos).

La dificultad de diseñar una aplicación (un “medio de comunicación” en el sentido amplio propio del contexto de Internet) que maximice al mismo tiempo la privacidad de las comunicaciones y la libertad de expresión parece difícil (o imposible), y es probable que las aplicaciones disponibles actualmente tengan aun pautas confusas

que genera cierto riesgo, sin embargo el bajo nivel de conflictos asociados hace este riesgo relativamente admisible, en particular porque quien recibe la llamada tiene el control suficiente para interrumpirla.

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

sobre cual expectativa satisfacen. En este sentido es clara la consternación del Grupo del Artículo 19 al ver que la “excepción doméstica” puede haber perdido sentido cuando se refiere a usuarios de redes sociales con varios miles de amigos, así como en la contradicción de la indexación en los grandes buscadores de los contenidos de las redes sociales.²¹

6. Sistema de responsabilidades

Una vez más, la expectativa de libertad de expresión es de alguna forma una prioridad. Pero qué hacer con las cosas que entran por la ventana ... pornografía infantil, apología del delito, datos confidenciales y de seguridad nacional, difamación, uso indebido de la imagen, exposición de los niños y adolescentes a contenidos inadecuados, violentos, la explotación sexual, o a la pornografía, etc.

El enfoque tradicional del derecho es desarrollar un sistema de responsabilidades para reprochar y en la práctica disminuir los riesgos y proteger los derechos. Pero estando en medio la libertad de expresión el sistema legal ha evolucionado evitando convertirse en un mecanismo de represión o cesura indirecta. Por esa razón muchos países han eliminado las sanciones penales —con privación de libertad— para algunos delitos como por ejemplo el de difamación (muchas veces usado para perseguir a disidentes políticos).

En los medios clásicos (prensa escrita, radio, televisión) las responsabilidades estaban definidas con cierta claridad por la figura de editor responsable, pero con los nuevos “medios” en Internet, instantáneos, anónimos y ampliamente accesibles la dilución de la responsabilidad ha ampliado la posibilidad de expresarse pero también ha generado abusos y víctimas.

La responsabilidad penal se aplica en algunas legislaciones. El ejemplo más resonante y reciente es el caso *Associazioni Vivi-Down vs. Google Italy s.r.l.* en Italia, donde se han aplicado sanciones penales a cinco directivos de *Google* por la publicación en *YouTube* de

²¹Opinión 5/2009.

CARLOS G. GREGORIO

un video que ridiculiza a un niño con síndrome de Down (pero las penas de prisión previstas por la ley se han dejado en suspenso).²² También en España se aplican multas a intermediarios y colaboradores necesarios, pero la cuantía de estas multas es muy baja.

El otro ejemplo muy interesante son las sanciones civiles aplicadas en Brasil. Por ejemplo en una decisión del Tribunal de Justicia del Estado de Rio de Janeiro, Brasil, un operador de telefonía móvil fue encontrado responsable por los daños morales a una cliente de la operadora que recibió insultos bajo la forma de mensajes de texto anónimos enviados a través del sitio web de la empresa.²³

También pueden traerse a colación una serie de conflictos que en los últimos años se han observado en Brasil y que están vinculados al uso de la red social *Orkut*, y que han derivado en una serie de procesos judiciales penales y civiles.²⁴ Las primeras reacciones del Ministerio Público en Brasil fueron al descubrirse que se utilizaba *Orkut* para compartir imágenes de pornografía infantil, situación que fue sucesivamente investigada por la Policía Federal de Brasil. El gran número de delitos identificados en el contexto de *Orkut* y los procesos penales derivados de ellos llevaron a la empresa *Google* a firmar un acuerdo con el Ministerio Público Federal y con la organización *SaferNet* para colaborar —bajo pena de multas muy significativas— con las autoridades en la persecución de estos delitos.²⁵

Paralelamente comenzaron en Brasil a generarse una serie de demandas civiles, la mayoría de ellas por difamación, derecho a la propia imagen y algunas por pornografía infantil en las que se demandaba a *Google* por los daños morales.²⁶

²²Ver la sentencia completa en: http://speciali.espresso.repubblica.it/pdf/Motivazioni_sentenza_Google.pdf

²³Ver *C.M.P. vs. Nextel Telecomunicações Ltda* (18 de octubre de 2010) se afirma que el riesgo está en una falla en la prestación del servicio al usuario al permitir que cualquier persona envíe mensajes vía Internet sin identificarse, no ofreciendo así a los consumidores el nivel de seguridad al que tienen derecho. La condena (4.000 reales) es insignificante.

²⁴La red social *Orkut* es propiedad de *Google* y tiene predominancia solo en Brasil y la India.

²⁵Ver www.safernet.org.br/site/sites/default/files/TACgoogleMPF_0.pdf, *Térmo de ajustamento de conduta, entre La Procuradoria da Republica no Estado de São Paulo, Google Brasil Internet Ltda. e SaferNet Brasil* (2 de julio de 2008).

²⁶Casos similares han sido decididos en el mismo sentido en Argentina -incluso

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

Existen algunas notas características en estos procesos judiciales: (1) se inician en juzgados de menor cuantía denominados en Brasil *Juizados Especiais*, sin formalidades, no requieren el patrocinio de un abogado y no existen costas judiciales. El damnificado presenta una demanda contra un usuario de *Orkut* que solo conoce por un *nickname* (pseudónimo o nombre de fantasía) y subsidiariamente contra *Google* solicitando que revele la identidad del usuario; (2) el juez libra una orden a *Google* para que informe la identidad del usuario detrás del nombre de fantasía bajo una pena de 5.000 reales por día mientras no satisfaga esta información.²⁷

En primer lugar *Google* adujo que los usuarios aceptaban los tribunales de los EE.UU. al adherir como usuarios de *Orkut*; la respuesta de la justicia de Brasil fue que esa aceptación es nula y que la jurisdicción de los tribunales brasileños es irrenunciable. En segundo lugar *Google do Brasil* (a quien estaban dirigidas las demandas) argumentó ser solo una oficina de representación; la justicia brasileña respondió que el uso del nombre *Google* y su calidad de representación, así como la capacidad para recolectar los pagos de los servicios de publicidad la hacían solidariamente responsable, y por tanto podía ser desmanda.

En una importante cantidad de casos *Google do Brasil* no ha podido identificar a la persona física detrás de los perfiles, entonces los jueces condenaban a *Google do Brasil* a pagar los daños morales que rondan los 10.000 reales por caso.

unos años antes, como *S. M. y L. E. vs Jujuy Digital y Jujuy.com-* pero en un número relativamente mucho más pequeño. La diferencia radica en un mayor nivel de acceso a la justicia que existe en Brasil que justifica litigar por cuantías indemnizatorias significativamente bajas. Ver el caso *Proteção Associação Civil vs. Facebook, Inc.* (decidido el 11 de mayo de 2010), www.ijlac.org/jurisprudencia/components.php?name=Articulos&artid=104 que trata de un grupo de adolescentes que creó un perfil en *Facebook* para convocar a sus compañeros de escuela a ausentarse un día determinado y concurrir a un espacio público a festejar su rebeldía, la decisión judicial se limita a ordenar a *Facebook* la remoción del contenido. En el mismo sentido *P. O. vs. Facebook Inc.* Pero en el caso de difamación de una figura pública, www.ijlac.org/jurisprudencia/components.php?name=Articulos&artid=107

²⁷Esta es una multa media, hay algunas variaciones de un juzgado a otro; equivale a unos 2.800 dólares por día. No en todos los casos *Google do Brasil* es el demandado, también existen casos contra *Fotolog* y *Facebook* y contra personas físicas cuando son identificables.

CARLOS G. GREGORIO

En el momento de la redacción del *Memorándum de Montevideo* se entendió que ambos procesos en Brasil —civiles y penales— representaban una de las experiencias más interesantes en América Latina y que habían sido determinantes para la firma de los convenios de colaboración entre la empresa *Google* y las autoridades judiciales. Por esa razón se incluyó en el capítulo correspondiente a *Recomendaciones para la Aplicación de las Leyes por parte de los Estados* el siguiente párrafo:

10.1. ...Se debe fortalecer el uso de la responsabilidad civil extracontractual objetiva como mecanismo regulatorio para garantizar los derechos fundamentales en las aplicaciones en la Sociedad de la Información y Conocimiento, Internet y redes sociales digitales. Las sanciones judiciales por los daños derivados tienen la ventaja de ser una respuesta inmediata, eficiente y capaz de desincentivar los diseños peligrosos. Este tipo de responsabilidad civil se fundamenta en el interés superior del niño.²⁸

Este párrafo permite traer algunos conceptos necesarios para analizar el marco regulatorio, por ello se tornan pertinentes las siguientes consideraciones: (1) la recomendación se limita a los casos en los que un niño o adolescente es víctima, y en este sentido se hace referencia explícita al interés superior del niño; (2) la frase desincentivar diseños peligrosos alude a responsabilidad por productos elaborados y no a una simple responsabilidad por contenidos.

En este sentido las más recientes decisiones judiciales en Brasil fundan su condena en un diseño peligroso (responsabilidad por productos elaborados) encontrado por los jueces en la aplicación *Orkut*, fundamentalmente al ver que viabilizan una anonimidad ab-

²⁸Claramente inspirado en la *Declaración de Principios sobre Libertad de Expresión*, de la Comisión Interamericana de Derechos Humanos de la Organización de Estados Americanos (octubre de 2000): “10. Las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público. La protección a la reputación debe estar garantizada sólo a través de sanciones civiles, en los casos en que la persona ofendida sea un funcionario público o persona pública o particular que se haya involucrado voluntariamente en asuntos de interés público. Además, en estos casos, debe probarse que en la difusión de las noticias el comunicador tuvo intención de infligir daño o pleno conocimiento de que se estaba difundiendo noticias falsas o se condujo con manifiesta negligencia en la búsqueda de la verdad o falsedad de las mismas”. [Aprobada durante el 108° Período Ordinario de Sesiones de la CIDH].

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

solita, y en el hecho de que ésta es una actividad lucrativa para la empresa.²⁹

Los argumentos de *Google* frente a las decisiones judiciales en Brasil se remiten a la sección 230 de la *Communications Decency Act* de los EE.UU. en la que los proveedores son inmunes frente a acciones judiciales por contenidos —denominada protección para el *buen samaritano*.³⁰ Sin embargo las condenas en Brasil son por la responsabilidad derivada de productos elaborados, aplicaciones que incluyen la posibilidad de operar en forma anónima, y no necesariamente por un contenido en particular; debe tenerse en cuenta adicionalmente que la Constitución Política de Brasil garantiza la libertad de expresión pero excluye el anonimato.

Artigo 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: ... IV — é livre a manifestação do pensamento, sendo vedado o anonimato; V — é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem; ...

Se dice también que un sistema de sanciones civiles podría crear una censura indirecta con la consiguiente pérdida de libertad de expresión. Sin embargo la cuantía de las indemnizaciones en Brasil es muy moderada y puede ser interpretada como un suave incentivo a mejorar las condiciones de seguridad de las aplicaciones y está muy lejos de ser un riesgo económico para la empresa —es más bien una parte mínima de la externalidad negativa que existe en toda industria.³¹

En España se han observado alguna variabilidad en la jurisprudencia, fundamentalmente por la introducción de concepto de

²⁹Ver *R. S. B. v. Google do Brasil Internet Ltda.* Sobre el anonimato como una protección de quien ejerce su derecho a expresarse puede verse el caso *John Doe v. Cabill* 884 A.2d. 451, 456 (Del. 2005) donde el proveedor del servicio conoce pero no puede revelar la identidad del usuario hasta que medie una orden judicial. Sin embargo el anonimato al que se refieren los casos de *Orkut* se crea cuando un usuario en una red social puede crear su perfil en un ciber-café y operar en una forma tal que es imposible de identificar (anonimato irreversible).

³⁰www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000230----000-.html

³¹En Brasil el proyecto de ley del Marco Civil de Internet dice: Artículo 19. El pro-

CARLOS G. GREGORIO

“cooperador necesario” que ha desplazado en algunos casos al de “conocimiento efectivo”.³² La mayoría de los casos de difamación o atentado contra el honor hay ido por la vía civil, solo ocasionalmente se ha acudido también a la vía penal, con resultados desiguales.³³ Por ejemplo el casos de la concejala del ayuntamiento de Santa Brígida, condenada por intromisiones ilegítimas al *honor* de tres personas por los comentarios que se publicaron al pie de varios de sus artículos: en el fundamento jurídico sexto *“Por todo lo expuesto, y sin perjuicio de lo que debe añadirse en el fundamento de derecho siguiente, procede la condena de la demandada, en cuanto que la misma es titular del blog en cuestión, la cual, evidentemente, pudo restringir o eliminar los mensajes que han sido objeto de análisis en el presente procedimiento evitando con ello su divulgación. A este respecto, es necesario indicar que no se conoce la persona concreta autora de los comentarios, debiéndose exigirse a la titular del blog donde se produce la difusión un deber de diligencia con relación a los mensajes que acceden al blog”*.³⁴ La sentencia fue revocada por la Audiencia de Gran Canarias y esta revocación declarada firme el 10 de marzo de 2011.³⁵

En el caso Mafius se dice *“que el recurrente es el creador de la blog, determinando su temática, y responsable de su mantenimiento, que admite comunicaciones anónimas y, pese al indiscutible contenido ofensivo, que no podía ser ignorado, del comentario de 18 de abril decide su mantenimiento hasta fechas muy posteriores, tal proceder aparece como propio de la autoría por cooperación necesaria del artículo*

veedor de conexión a Internet no será responsable por daños derivados de los contenidos generados por terceros. Artículo 20. El proveedor de servicios de Internet sólo puede ser responsable por daños derivados de los contenidos generados por terceros si, después de intimado para cumplir orden judicial, no tomase medidas para, en el marco de su servicio y dentro del plazo establecido, tornar indisponible el contenido señalado como dañoso.

³²Antoni Rubí Puig, “El requisito del ‘conocimiento efectivo’ en las SSTs, Sala Primera, de 9 de diciembre de 2009 y 18 de mayo de 2010”, *Revista para el Análisis del Derecho* (www.indret.com).

³³Miquel Peguera, *La administración de un foro no implica responsabilidad penal por los comentarios vertidos en él por terceros* (caso elcomentario.tv), (2009) — <http://responsabilidadinternet.wordpress.com/2009/10/11/caso-elcomentario-tv/>

³⁴<http://victoriacasas.blogspot.com/2009/02/se-acabo-paso-pagina.html>

³⁵<http://victoriacasas.blogspot.com/2011/03/la-sala-declara-firme-la-sentencia-por.html>

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

28.b) del Código Penal. No se trata de coartar la libertad y sí, simplemente, de señalar que la libertad lleva aparejada la responsabilidad por el uso que se hace de la misma.³⁶

En la vía civil en el caso *Ramoncín contra alasbarricadas.org* el Tribunal Supremo de Madrid establece una indemnización civil de 6.000 €, a los que hay que sumar 5.300 € de gastos judiciales.³⁷

La moderación de contenidos de acuerdo con las reglas del sitio es tanto una posibilidad como una consecuencia de las reglas de responsabilidad.³⁸

Sobre la responsabilidad de los buscadores se han suscitado algunos casos. La Audiencia provincial de Barcelona ha resuelto que los buscadores no violan la propiedad intelectual cuando hacen y disponibilizan un *cache* de un texto protegido.³⁹ Recientemente la Cámara de Apelaciones Civil de la Ciudad de Buenos Aires ha establecido que los buscadores no son responsables por los contenidos de los sitios que indexan.⁴⁰ Sin duda sentencias judiciales muy plau-

³⁶Sentencia 96/2007 de la Audiencia Provincial de Madrid, Sección 3ª, de 26 de febrero de 2007. Sentencia del Juzgado de Primera Instancia e Instrucción núm. 5 de Arganda del Rey, de 30 de junio de 2006.

³⁷Disponible en <http://s.libertaddigital.com/doc/sentencia-del-supremo-que-condena-a-la-web-alasbarricadas-a-indemnizar-a-ramoncín-41912140.pdf> En Italia la ley establece la responsabilidad objetiva: artículo 16 de la Legge 31 dicembre 1996, N. 675 – www.parlamento.it/parlam/leggi/966751.htm y artículo 2050 del Código Civil.

³⁸Para este procedimiento se ofrecen algunos prototipos como www.keepcon.com. Keepcon ha desarrollado una tecnología que es capaz de detectar los contenidos de riesgo según las reglas definidas por cada cliente. Se hace automáticamente y si algún contenido es dudoso se modera manualmente con otra herramienta informática para facilitar el trabajo: <http://www.keepcon.com/esp/index.php> Santiago Siri, uno de sus creadores de la herramienta www.meaningtool.com que es capaz de detectar las partes relevantes de un texto de internet, saber de qué trata un documento colgado en la Red e incluso “hacer interpretaciones políticas de los textos” o de los “sentimientos” con los que se ha escrito algo. Asegura Siri: “es la única posibilidad costo-efectiva de acompañar el crecimiento”; “necesitamos una brújula para orientarnos”, “el sistema puede arrojar luz sobre un texto que con una lectura humana no llegaría”; el fin es “resolver la sobredosis de información que hay en internet”; “necesitamos una brújula para orientarnos”; “el sistema puede arrojar luz sobre un texto que con una lectura humana no llegaría”.

³⁹*Aleix P. L. vs. Google Spain*, 17/9/2008 – www.interiuris.com/blog/wp-content/uploads/sentencia_google.pdf

⁴⁰*V. D. C. vs Google Inc. y Yahoo de Argentina S.R.L.* 11/8/2010 — www.diariojudicial.com/documentos/Agosto2010/Bandana_Google_Yahoo.pdf

CARLOS G. GREGORIO

sibles dado que los buscadores son absolutamente necesarios para navegar en Internet.

Pero si la tendencia es que los buscadores sean un negocio opaco y sin responsabilidad alguna, cuál será la tendencia futura de las capacidades de búsqueda. Si la libertad de expresión tiene una fuerte componente en el derecho a encontrar información, como los buscadores evolucionarán en este sentido.⁴¹

7. Tratamiento de la difamación en los EE.UU.

Las decisiones judiciales —publicadas— en los EE.UU. muestran un perfil diferente; normalmente se trata de alguien que estima que determinada información en un blog es difamatoria y pone en marcha el mecanismo establecido para identificar un responsable.⁴² El tribunal puede ordenar o denegar la identificación y para ello se han articulado estándares, fundamentalmente son precedentes relevantes los casos *Dendrite v. Doe* (New Jersey) y *Doe v. Cahill*, (Delaware).

⁴¹En este sentido una experiencia personal del autor puede dar una perspectiva interesante. Hace diez años y para entender como operaban los buscadores y su capacidad de hacer accesibles contenidos en forma totalmente neutral desarrolle un sitio web para mi perro (que se llama *Manchitotauro*) e inscribí ese sitio en la opción que los principales buscadores tienen para solicitar que se indexe un contenido. El sitio fue dado de baja el año pasado y durante diez años y pese a la insistencia el sitio de *Manchitotauro* nunca fue indexado. Simultáneamente desarrolle otros sitios con otros contenidos en el mismo servidor pero incluí enlaces a ellos en el sitio de mi institución, estos si fueron indexados pese a que no solicite la indexación. La pregunta es ¿existe responsabilidad por no indexar? ¿es censura?

⁴²Por ejemplo, en *Rules on Civil Proceedings in the Trial Court, Rule 224. Discovery Before Suit to Identify Responsible Persons and Entities*. (a) Procedure. (1) Petition. (i) A person or entity who wishes to engage in discovery for the sole purpose of ascertaining the identity of one who may be responsible in damages may file an independent action for such discovery. (ii) The action for discovery shall be initiated by the filing of a verified petition in the circuit court of the county in which the action or proceeding might be brought or in which one or more of the persons or entities from whom discovery is sought resides. The petition shall be brought in the name of the petitioner and shall name as respondents the persons or entities from whom discovery is sought and shall set forth: (A) the reason the proposed discovery is necessary and (B) the nature of the discovery sought and shall ask for an order authorizing the petitioner to obtain such discovery. The order allowing the petition will limit discovery to the identification of responsible persons and entities and where a deposition is sought will specify the name and address of each person to be

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

Los proveedores de los servicios disponen normalmente de muy pocos elementos de identificación: los que provee el usuario como nombre, dirección de correo electrónico, quizás un teléfono o una dirección; y los que obtiene por medios tecnológicos basados en la conexión a Internet. Al ser conectividad predominante identificable es probable que existan muy pocos casos de anonimato irreversible. La actitud de los jueces —y los estándares definidos— tiende a proteger, y establecer los límites, de la expresión anónima.⁴³

8. Abordajes para una evolución armoniosa —con los derechos y libertades— de las redes sociales

Ya se han presentado algunos abordajes legales clásicos —como el de la responsabilidad civil— pero han surgido también otras visiones sobre las que se propone edificar el futuro de Internet.

8.1. La neutralidad como abordaje

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.

La neutralidad de la red ha sido materia legislativa en Chile por la Ley 20.453 del 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 arbitrari-

examined, if known, or, if unknown, information sufficient to identify each person and the time and place of the deposition.

⁴³Expresarse en forma anónima es una forma de garantizar a quien se expresa que no existirán represalias o discriminación, es también al mismo tiempo una forma de facilitar la difamación, invasiones sobre el derecho a la propia imagen, comisión

CARLOS G. GREGORIO

amente 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*:

Artículo 2. El uso de Internet en Brasil se fundamenta en el reconocimiento de la escala mundial de la red, el ejercicio de la ciudadanía en los medios digitales, los derechos humanos, la pluralidad, la diversidad, la apertura, la libre empresa, la libre competencia y la colaboración, y observará los siguientes principios:

I – Garantía de la libertad de expresión, comunicación y manifestación del pensamiento;

II – Protección de la privacidad;

III – Protección de datos personales, de acuerdo con la ley;

IV – Mantenimiento y la garantía de neutralidad de la red;

V – Preservación de la estabilidad, seguridad y funcionalidad de la red a través de medidas técnicas compatibles con las normas internacionales y fomentando el uso de mejores prácticas;

VI – Preservación de la naturaleza participativa de la red.

Pero el proyecto de ley en Brasil no hace una definición de los alcances de la neutralidad, como en el caso de la ley chilena; otras definiciones como la de Julio Alonso: “que la inteligencia, los servicios se ponen en los extremos de la red, y la red en sí trasmite todo sin mirar ni jerarquizar ni priorizar”. El problema radica en que la neutralidad tecnológica es un concepto en extremo difuso y polivalente, alguna de sus interpretaciones se asemeja a afirmar la

de delitos —como el de pornografía infantil— o apología del delito, por citar los más frecuentes. Aquí es difícil establecer un balance al estilo de William Blackstone, que podría —por ejemplo— decir “*es preferible que 10 personas sean difamadas a que a una se le impida expresarse anónimamente*”. Cuando Blackstone dijo en 1769 “*para la ley, es preferible que diez culpables escapen a que un inocente sufra*” sentó las bases del equilibrio entre debido proceso y seguridad ciudadana. William Blackstone, *Commentaries on the Laws of England, Book the Fourth, Chapter the Twenty-Seventh: Of trial, and conviction*.

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

neutralidad ética característica de las leyes de la evolución biológica, y la aceptación que los individuos más débiles o las poblaciones menos adaptadas están destinadas a desaparecer en aras de un ideal evolutivo; escenario inadmisibles en las sociedades humanas y desde una visión de derechos humanos.

Como refiere Justine Nolan “Hoy, la capacidad económica de las corporaciones transnacionales va mucho más allá de la capacidad económica de los países en las que ellas operan, y su músculo político es también mucho más grande que la habilidad de algunos Estados para regularlas efectivamente. Este poder debería estar acompañado de responsabilidad”.⁴⁴

Por su parte Hans Ulrich Buhl y Günter Müller afirman: “El problema real no es el ‘ciudadano transparente’ que está a la merced de un ‘Estado controlador’, sino en el hecho 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

Entonces preocupa la existencia de concentraciones de poder en la red frente a la expectativa de que el centro de la evolución debe ser el ciudadano y el quien logre empoderarse.

Balkin considera que el *rôle* de los jueces es menor “estoy persuadido sobre la trayectoria de los futuros debates políticos, nuestra atención se desplazará crecientemente a cuestiones de diseño —tanto institucional como tecnológico— que están significativamente más allá de la competencia judicial”.⁴⁶ También Balkin preconiza la “libertad de diseño” pero su afirmación se limita solo al contexto de los juegos en línea.⁴⁷

⁴⁴Justine Nolan, “With Power comes Responsibility: Human Rights and Corporate Accountability”, *UNSW Law Journal*, Volume 28(3), 582. Disponible en SSRN: <http://ssrn.com/abstract=1556443>

⁴⁵Hans Ulrich Buhl y Günter Müller, “The ‘Transparent Citizen’ in Web 2.0: Challenges of the ‘Virtual Striptease’”, *Business & Information Systems Engineering*, (4)2010, 203-206.

⁴⁶Jack Balkin, “Media Access: A Question of Design”, *George Washington Law Review*, 76, (2008), p. 933 – <http://ssrn.com/abstract=1161990>

⁴⁷Jack Balkin, “Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds”, *Virginia Law Review*, 90, (2004) – <http://ssrn.com/abstract=555683>

CARLOS G. GREGORIO

Todos estos argumentos llevan a preguntarse cuan neutrales pueden ser los operadores de Internet —manteniendo su modelo de negocios—, y cuáles serán los mecanismos, estímulos o incentivos para determinar una red en la que el poder este en manos de los ciudadanos, y se prevenga adecuadamente la victimización.

8.2. La educación como abordaje

El abordaje educativo —que concita uno de los mayores consensos— es aquel que ve como estrictamente necesaria una educación de los usuarios para prevenir los riesgos y para aprovechar al máximo las ventajas de la sociedad de la información y el conocimiento. Este abordaje está dirigido a todos pero fundamentalmente a los niños, niñas y adolescentes y de preferencia en la enseñanza regular. Existe una analogía interesante sobre este abordaje, se remonta a los años 60 en los que se generalizó la bolsa plástica y simultáneamente comenzaron a producirse muchos accidentes de muerte por sofocación —en particular en los niños entre 3 y 5 años. El tema fue una conmoción durante esos años, y se crearon muchas campañas de concientización y en el plano legislativo se reguló la colocación de mensajes impresos en las mismas bolsas plásticas. Hoy parece un tema superado, ni existen estadísticas con este tipo de accidente y —podría decirse— que la prevención de este riesgo fue inculturizada. Si debe decirse que se aprobaron algunas leyes —que aun están vigentes— por las que las bolsas plásticas utilizadas en juguetes y otros objetos que pueden estar al alcance de los niños debían llevar perforaciones. O sea este ejemplo muestra una combinación de educación y disminución del riesgo.

El *Memorándum de Montevideo* hace un fuerte llamado a establecer políticas educativas y no hace sino coincidir con otros documentos y con la tendencia mayoritaria.

Aunque la prevención y educación para el uso seguro y responsable es una recomendación que cuenta con amplio consenso en el concierto internacional,⁴⁸ no por ello es necesariamente una tarea

⁴⁸Este objetivo fue incluido como Meta n° 24 en el *Plan de Acción sobre la Sociedad de la Información y del Conocimiento de América Latina y el Caribe* (eLAC2015) aprobado en la ciudad de Lima el 23 de noviembre de 2010 en la Tercera Conferencia Ministerial convocada por CEPAL.

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

sencilla en América Latina y el Caribe. Varios países de la región están embarcados en programas “un ordenador por niño”,⁴⁹ pero estas políticas públicas no han sido acompañadas con la inserción en los programas regulares de enseñanza de educación para un uso seguro de las nuevas tecnologías. Este desfase está acompañado por la dificultad de capacitar a profesores y rectores, y por la falta de recursos económicos en los presupuestos educativos para atender estas necesidades. Existen ONGs en la región que ofrecen la realización de talleres de prevención en las escuelas, pero es una oferta externa y que debe ser pagada por las escuelas que las solicitan; esta modalidad incide diferencialmente en las escuelas privadas que disponen de recursos adicionales.

Si bien las políticas de responsabilidad social empresarial puede ser un recurso muy valioso para solventar al menos las etapas iniciales de generación de los contenidos educativos y la capacitación de los profesores, muchos operadores (de conectividad, de aplicaciones en Internet y de telefonía móvil) no muestran en la región los mismos estándares de responsabilidad social empresarial que ostentan en sus países de origen.

8.3. La identificación como abordaje

Dado que la causa principal de la mayoría de los riesgos es el anonimato —y la sensación de impunidad que se deriva de él— muchos piensan que es necesario incrementar los sistemas de identificación de los usuarios.

En primer lugar puede decirse que el anonimato irreversible,⁵⁰ es una ilusión. Si es posible si una persona cree una cuenta de correo electrónico en un ciber-café, a partir de ella cree una cuenta en una red social o hace un comentario a una nota en un periódico; si tiene un cuidado extremo en que su opinión esté escrita en un lenguaje neutro, sea tan sucinta como pueda ser, y además realice todo esto

⁴⁹Varios países de la región están embarcados en programas “un ordenador por niño”, el Plan Ceibal en Uruguay es el que está más adelantado.

⁵⁰Ver Gabriela Mendoza Correa, *La protección de las niñas, niños y adolescentes y el principio de anonimato aplicado a la Sociedad de la Información y el Conocimiento. Una reflexión sobre la no-identificación funcional en el nuevo entorno tecnológico*, (publicado en esta misma obra).

CARLOS G. GREGORIO

por única vez ... probablemente su anonimato sea irreversible. Pero la dirección IP ya lo ubica geográficamente, el idioma utilizado y el tema abordado reducen el círculo; y su estilo de lenguaje aporta más información. Pero Internet tiene sus reglas de negocios, y la libertad de expresión —en particular la expresión anónima— no es un buen negocio.

En las aplicaciones teóricamente gratuitas de Internet —fundamentalmente las redes sociales— el negocio consiste en acumular información adjudicable a un perfil: cuanta más información se posea del usuario, más probable es encontrar una publicidad que le interese.⁵¹ Pero más información implica la pérdida del anonimato irreversible, o sea las redes sociales y su modelo de negocio no son el espacio adecuado para expresarse anónimamente. Muchos periódicos tienen la posibilidad de “comentar una nota” en un diseño en el que el anonimato irreversible es mucho más real, aun así muchos periódicos han decidido no habilitar esta posibilidad para evitar los riesgos y porque tiene sus costos de moderación para retirar los comentarios que no cumplen con las reglas del sitio; o sea si bien es un producto interesante para los lectores es encarado siempre como un plus y no como el negocio principal.

Para ahondar en el análisis histórico se puede mencionar el caso *Dreiffus*: este caso comenzó en 1894 cuando un documento llamado el “*bordereau*” que contenía información militar francesa fue encontrado por el servicio secreto francés en un cesto para papeles en la embajada alemana; el documento fue analizado y se dijo haber identificado como autor al capitán del ejército francés Alfred Dreyfus, utilizando un proceso geométrico y probabilístico para analizar la caligrafía.⁵² Enjuiciado por un tribunal militar, fue condenado a prisión perpetua y desterrado en la Isla del Diablo situada en la costa de la Guayana francesa. El caso mostró la debilidad del proceso judicial y fue un hito en la historia del antisemitismo.⁵³

⁵¹ Las redes sociales no necesitan identificar al usuario, solo necesitan un perfil completo; pero un perfil (que incluya fotos, vinculación a perfiles de amigos y muchos datos más) está a un paso muy pequeño de un proceso de individualización.

⁵² F. Taroni, C. Champod, y P. Margot, “Forerunners of bayesianism in early forensic science”, *Jurimetrics J.*, 38, (1988), pp. 183-200.

⁵³ Ver Jean Jaures, *Les Preuves* disponible en http://fr.wikisource.org/wiki/Les_Preuves y Émile Zola, *J'Accuse*, disponible en www.pitbook.com/textes/pdf/jaccuse.pdf

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

Este como otros casos muestran la permanente intensión de identificar y los riesgos que cualquier proceso de identificación encierra. También muestra que siempre se esconden otros intereses y prejuicios en cómo se identifica. Pero también muestran que la información preexistente se usa para triangular la identidad del autor de un texto, una hoja de caligrafía es nada comparada con miles de datos relacionales con que hoy contamos: contactos, amigos, correos recibidos y enviados, imágenes, direcciones IP, browser y muchas cosas más. Es la cantidad de información la que atenta contra el anonimato irreversible, pero también hay intentos de institucionalizar la identificación.

En agosto de 2010 Telefónica de España S.A. anunció la compra de la red social *Tuenti* con la intensión de expandir sus operaciones en Brasil, Argentina y otros países de América Latina, especialmente entre el sector de los adolescentes y los jóvenes. Esta noticia preanuncia y explica un cambio en la conectividad a Internet, que en América Latina migraría de la predominancia de los cibercafés a un uso de las redes sociales en forma concurrente desde los teléfonos móviles. Es muy probable que de concretarse este cambio, todo el escenario de riesgos se modifique. Al mismo tiempo podría ser una excelente noticia para los niños y adolescentes de América Latina y sus derechos; en particular porque *Tuenti* ha mostrado su compromiso con la legislación aplicable al firmar un acuerdo con la Agencia Española de Protección de Datos y también porque *Telefónica* ya cuenta con políticas de responsabilidad social en la región.

En alguna medida, en la mayoría de los países de América Latina, la conexión por teléfono móvil es identificable a una persona física, es decir que un perfil de red social quedará más probablemente identificado a un usuario que en la modalidad de acceso anterior.⁵⁴ Si se acepta que el anonimato absoluto y la suplantación de identidad en los espacios de chat, redes sociales y otras aplicaciones en Internet es una de las causas de vulnerabilidad de los niños y

⁵⁴Recientemente el Tribunal Constitucional Alemán ha dictado una sentencia en la que ordena al legislador implementar una serie de requisitos para el almacenamiento de los datos de las telecomunicaciones y que los datos solo pueden ser utilizados para acciones judiciales si se sospecha un delito grave y utilizados en forma preventiva si existe un peligro concreto. También dice que no pueden guardarse registros de las llamadas a líneas telefónicas de ayuda que garanticen el anonimato.

CARLOS G. GREGORIO

adolescentes, un mayor nivel de identificación reducirá los riesgos para los niños y adolescentes, claro está esta reducción no será absoluta pues existen muchos teléfonos móviles no identificados — porque son antiguos o porque provienen de un mercado de segunda mano— pero esto es un aspecto factible de mejorar con la colaboración de las empresas y la responsabilidad de los usuarios. También algunos aspectos de diseño de las redes sociales podrían reducir los riesgos, como ser criterios más seguros para la aceptación de amigos.

También se sabe que los teléfonos móviles introducen nuevas vulnerabilidades para los niños y adolescentes; Gasser, *et al.* describen la modalidad de intercambio de imágenes —en algunos casos de pornografía infantil— a cambio de la acreditación de saldo, riesgo que ha sido también advertido en varios países de América Latina, que se suma a otros riesgos asociados a la cámara de video y a la posibilidad de transferir archivos entre teléfonos móviles.⁵⁵ La responsabilidad civil también podrá ser aplicada, pero tendría un impacto positivo ya que son mucho más viables los diseños alternativos.

En definitiva existe una expectativa mayor de identificación en un contexto de comunicación pero no es así en plataformas para la expresión.

9. Problemas venideros

Sin duda el problema recién comienza y ni siquiera están claramente individualizados todos los problemas. ¿Cómo expandir un espacio de libertades con herramientas legales pensadas durante siglos para territorios delimitados? ¿Cómo conciliar el anonimato y resolver la protección del derecho al honor? ¿Cómo llevar a escala la educación y la prevención? ¿Cómo se prevendrá la discriminación injusta basada en perfiles?

⁵⁵También la adhesión a redes sociales vinculadas a un teléfono móvil rompe la ilusión de gratuidad que hoy ostentan. Cuando en realidad en los servicios ‘gratuitos’ en Internet la moneda de pago son los propios datos personales y la aceptación de publicidad, esta nueva modalidad se parecería a incluir una aplicación más en el precio del paquete de conectividad.

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

El carácter comercial de la red es una fuerte perturbación. Supongamos un espacio de expresión anónima basado en el espíritu de generosidad que si existe en internet (al estilo de los *wiki*), quizás pueda ser muy poco atractivo en la medida que no está relacionado con una noticia —y entonces falla el derecho a oír (o encontrar). O si está relacionado con una pregunta (como hace CNN) ... la formulación de la pregunta es ya una limitación. ¿Quién selecciona los comentarios que se mencionan, con qué criterio? ¿se hacen estadísticas y se busca representar las tendencias? ¿Las mayoritarias o las minoritarias? ... en definitiva ¿Cómo se pasa de la nube a los medios clásicos? ... o sea ¿solo los medios clásicos son la caja de resonancia adecuada de la expresión y las redes de expresión son solo un incremento en las “fuentes”?

La libertad de asociación es también otra incógnita. Sin duda la red ha mostrado resultados efectivos para movilizar y potenciar los movimientos sociales. Pero aun no se sabe a ciencia cierta cómo funciona y si puede ser controlado desde fuera.

La participación de los adolescentes —desprevenidamente— en algunas conductas delictivas (cyberbullying, pornografía infantil —incluyendo la auto-pornografía—, extorsión, entre otras) serán un desafío en muy poco tiempo para los sistemas de justicia penal de adolescentes. Un sistema que se caracteriza ya por su dificultad de atender al adolescente infractor respetando sus derechos, abusando de la internación e ignorando la necesidad de programas de inserción en libertad y basados en la comunidad.

Conclusiones

Obviamente estamos frente a un conjunto de expectativas, intereses y problemas que por el momento parecen inconciliables ... también estamos frente a víctimas y grupos vulnerables, que están perplejos ante la inmovilidad de las instituciones de garantía de sus derechos. No se avizora hoy cual será la solución, pero es estimulante que continúe el debate y que se profundice el debate legal —desde un marco intelectual y académico.

Es muy probable que predomine el debate y la discusión sobre la libertad de expresión. Internet es un territorio en evolución,

CARLOS G. GREGORIO

por eso los estímulos e incentivos que existan hoy serán los que definan su futuro.

La inmunidad de la Section 230(c)(1) crea un importante incentivo hacia el desarrollo de herramientas de libertad de expresión, e inhibe otros mecanismos que podrían llevar hacia un equilibrio de derechos. En parte como afirma Bakin los diseños son claves para el futuro de internet, y para los diseñadores y proveedores es muy cómodo incluir la libertad de expresión en cualquier aplicación para evadir responsabilidades; diferenciar comunicaciones privadas, comunicaciones grupales y espacios de expresión no dejaría de garantizar la libertad de ; mientras exista una oferta razonable de aplicaciones para expresarse —incluyendo a la expresión anónima irreversible— las expectativas estarán satisfechas.

Quizás hoy no es posible optar por ningún abordaje en particular. Si hubiera silencio, aceptación y complacencia... tendríamos el futuro comprometido ... se trata de mantener vivos los incentivos y los estímulos para quienes desarrollan y dan forma a Internet busquen un equilibrio saludable y armonioso.