225

Cuadernos y Debates

Libertad de expresión e información en Internet

Amenazas y protección de los derechos personales

LORETO CORREDOIRA Y ALFONSO
LORENZO COTINO HUESO (dirs.)

CENTRO DE ESTUDIOS POLÍTICOS Y CONSTITUCIONALES

225

Libertad de expresión e información en Internet

Amenazas y protección de los derechos personales

LORETO CORREDOIRA Y ALFONSO
LORENZO COTINO HUESO (dirs.)

Catálogo general de publicaciones oficiales:
http://www.publicacionesoficiales.boe.es/

De esta edición, 2013:

Plaza de la Marina Española, 9
28071 Madrid
http://www.cepc.gob.es
Twitter: @cepcgob

NIPO: 005-13-028-9
ISBN: 978-84-259-1561-1
Depósito Legal: M. 13719-2013

Realización: Imprenta ROAL
Gamonal, 5 - 28031 Madrid

Impreso en España - *Printed in Spain*

Impreso en papel reciclado

Índice

El futuro de la vida pública y privada en las redes sociales

Óscar Jaramillo[1]
Profesor Doctor de Derecho de la información,
Universidad Mayor, Santiago de Chile

I. Introducción

Miedo, rechazo, son algunas de las reacciones que se han producido después que Facebook anunciara cambios a sus políticas de gobierno (Facebook's Governance).

El anuncio realizado a fines de noviembre de 2012 y que ha causado revuelo dentro de la prensa tecnológica y de los sitios de defensa de los derechos humanos en los entornos digitales, no es más que la punta del iceberg: de la desarticulación del concepto de los público y lo privado.

Estamos frente a un escenario en el cual los mundos digitales y analógicos se funden en uno sólo, lo que nos obliga a redefinir los conceptos de vida privada y pública. En uno en que la ubicuidad de los teléfonos inteligentes (smartphones) permite que cada aspecto de la vida de las personas sea registrado, procesado y almacenado en bases de datos. Ya no estamos hablando de la página web que leyó la semana pasada, sino que del registro de cada uno de los lugares que ha estado, combinado con la lectura de sus mensajes, correos electrónicos y el almacenaje de información antrométrica que permite reconocer el rostro de una persona apenas una fotografía es subida a una red social.

Si partimos desde la base de que las redes sociales jugaron un rol fundamental en la generación de la llamada Primavera Árabe, el Movi-

[1] Estudio realizado en el marco del Proyecto MINECO «Régimen jurídico constitucional del Gobierno 2.0-Open government. Participación y transparencia electrónicas y uso de las redes sociales por los poderes públicos» (DER2012-37844).

miento de los Indignados en Europa, o de los Estudiantes en Chile, podremos darnos cuenta que la forma en que se definan los conceptos de lo público y lo privado en dichos entornos digitales tiene grandes implicancias en la vida política, social y económica de las naciones alrededor del globo.

La caída de los gobiernos en Túnez, Egipto y Libia, sumado a la guerra civil que aún sacude a Siria, son un recordatorio de que en este momento es imposible dividir el mundo real, material, del virtual. La revolución que estalló en el Medio Oriente en los grupos de Facebook, gracias a un video de Youtube y que elevó a Twitter al nivel del ágora de los antiguos griegos, no afectó a los gobiernos de Second Life u otros mundos virtuales. Derrocó a los gobiernos reales, a las dictaduras que durante años trataron de controlar los medios de comunicación y a sus audiencias.

Las redes sociales no sólo cambiaron la forma en que las nuevas generaciones (nativos digitales) socializan, sino que también la manera en que debemos definir lo público y lo privado.

Sería bastante fácil recurrir a la figura del Gran Hermano de la novela 1984, para retratar la situación actual. Sería de verdad sencillo recordar que cada smartphone que funcione bajo el sistema operativo IOS o Android guarda la información de cada comentario que realizamos en Facebook, que sabe quiénes son nuestros contactos en Whatsapp, que el GPS registra cada lugar en el que estamos y que Siri, ese asistente virtual que tanto amamos, aprende a diferenciar nuestros estados de ánimo. Sería de verdad sencillo decir que el Gran Hermano no está observándonos desde nuestra muralla, como en la novela de Orwell, sino desde el bolsillo de los habitantes de gran parte de este planeta.

Pese a que nuestra realidad no sea distópica y que estamos alejados del mundo creado por George Orwell, la desarticulación de lo público y lo privado en las redes sociales, plantea cambios que atañen a lo social y político.

Los cambios propuestos por Facebook a su política de privacidad, son importantes porque marcan una tendencia que desdibuja los límites de lo privado en los entornos digitales y apuntan hacia la transformación de la información personal en mercancía.

Tal como lo señala la carta enviada por Marc Rotenberg[2] y Jeffrey Chester[3] al fundador de Facebook, Marc Zuckerberg, los cambios

[2] Presidente de Electronic Privacy Information Center (EPIC).

[3] Presidente de Center for Digital Democracy.

suponen el abandono de una norma fundamental, que los usuarios son ciudadanos en una comunidad y no, datos en un algorismo publicitario[4].

Estos cambios, van más allá de una cuestión que afecta sólo a la vida privada de las personas, sino que a la forma en que se producen los movimientos sociales. Es por eso que vale la pena preguntarnos cómo se han visto afectados los conceptos de vida privada y pública, a partir de la ubicuidad de las redes sociales.

La tesis de este artículo es que las redes sociales han redefinido los conceptos de vida pública y privada más allá de los entornos digitales, debido a que afecta la forma en que las personas socializan. Básicamente lo que deseamos es ver, desde el punto de vista del derecho a la información, qué sucede con los conceptos de vida pública y privada.

Antes de poder centrarnos en ello, debemos detenernos brevemente en dos aspectos que pueden parecer desconectados entre sí: el funcionamiento de las redes sociales y los conceptos tradicionales de vida pública y privada.

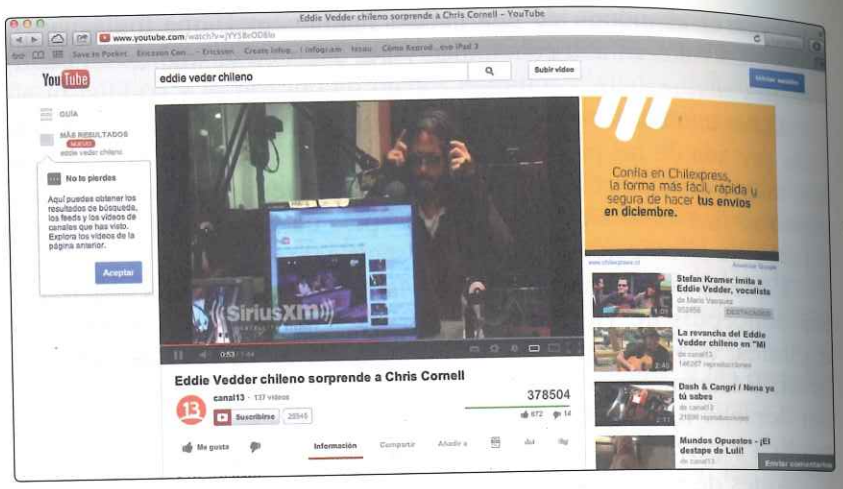
II. Redes sociales: Más allá de «Facebook»

Para poder entender qué es lo que sucede con la vida pública y la privada en las redes sociales, antes es necesario conocer su mecánica y la forma en que la información se difunde a través de ellas.

De esta manera podremos apreciar la forma en que afectan a ambos conceptos y cómo son redefinidos a medida de que es produce la viralización de los mensajes. Para ello abordaremos un caso que nos sirve para ilustrar la mecánica de las redes sociales. Nos referimos a los casos del Eddie Vedder Chileno.

En el 2011, Canal 13 realizó un programa de talentos con corte de reallity Show, Mi nombre es. El objetivo era escoger al mejor imitador chileno. Dentro de las rondas eliminatorias, se presentó Javier Díaz, quien imitó a Eddie Vedder, vocalista del grupo norteamericano, Pearl Jam.

[4] ROTENBERG, Marc; CHESTER, Jeffrey, «Facebook's proposed changes to its data use and site gobernance policies», E*lectronic Privacy Information Center*. 2012. (*http://epic.org/privacy/facebook/EPIC-CDD-Ltr-to-FB-Data-Use.pdf*)



Un adolescente chileno que escuchó la imitación y que estuvo en desacuerdo de que Javier Díaz fuera eliminado, subió el video a Youtube. Días después el video fue comentado por otras personas en Facebook y Twitter. Incluso llegó a ser trending topic en Chile. La noticia fue rescatada por algunos portales como Terra Chile (Terra.cl). De ahí pasó a otros portales extrajetos, como Terra Perú. Finalmente, el video fue comentado por Chris Cornell, ex vocalista de Soundgarden, quien tiene un programa de radio en los Estados Unidos. Ese hecho fue comentado en las redes sociales nuevamente. Y al igual que antes, fue noticia en portales y diarios electrónicos chilenos. Después de eso fue noticia en la versión impresa de diarios nacionales y de ahí, pasó a la televisión. Una vez que el hecho fue noticia en la televisión, pasó a lo que los sociólogos denominan como opinión pública.

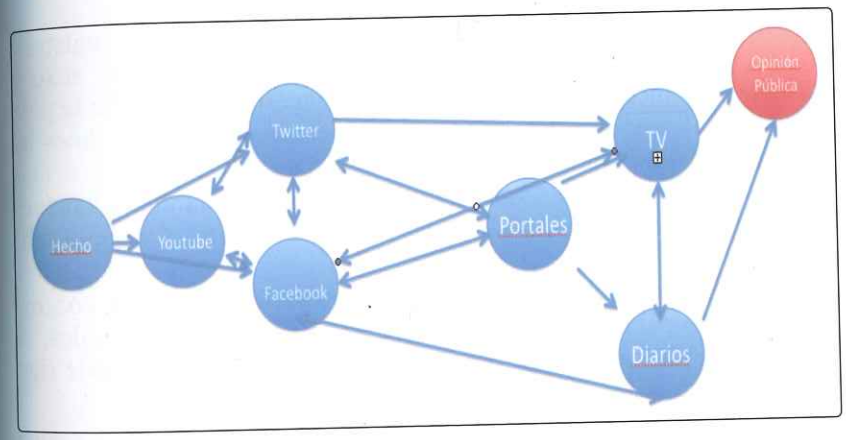
Bastó que los diarios de circulación nacional y los programas de espectáculos hablaran del tema, para que el mismo canal llamara al Eddie Vedder Chileno para que participara en la segunda temporada del programa, el cual ganó finalmente.

Hemos tomado este ejemplo en particular, porque nos demuestra que las redes sociales por sí solas (Youtube, Facebook, Twitter, Whatsapp o Miso) no bastan por sí solas para que un tema llegue a la opinión pública.

Necesariamente, la información necesita ser recogida por los medios de comunicación tradicionales para que sea de dominio público. Otro ejemplo es lo que sucedió con el hit musical de 2012, Gang-

nam Style, del cantante coreano, PSY. La canción partió como un video exitoso en Youtube. Cuando la televisión dio cuenta de su éxito en las redes sociales, su número de visitas en Youtube subió a tal punto, que se convirtió en el video más visto de la historia.

Eso nos lleva a un punto interesante. Para que un hecho entre a la esfera de lo público, requiere de la participación de los medios de comunicación tradicionales (radio, prensa y televisión). Sin embargo, no podemos considerar como algo privado si un acontecimiento es es comunicado a nuestros mejores 500 amigos, tal como sucede en Facebook. La red social sería algo intermedio, que está entre lo público y lo privado.



Teniendo claro ese hecho, podemos introducirnos en nuestro análisis y ver qué sucede con la vida privada y la pública en las redes sociales.

III. La vida privada en las redes sociales

Hace unos momentos afirmamos que el desdibujamiento de lo público y lo privado en las redes sociales, no se circunscribe sólo a los entornos digitales, que su impacto alcanza a todos los aspectos de la vida humana. Para entender dicha afirmación debemos analizar el funcionamiento interno de las redes sociales y, más específicamente, la forma en que las redes sociales recopilan información privada.

En primer lugar, hay que considerar que la información de carácter privado que está en las redes sociales proviene de cinco fuentes básicas: el mismo usuario que entrega información de manera voluntaria, otros usuarios de las mismas redes sociales que publican información sobre nosotros, empresas asociadas y no asociadas a las redes sociales que recolectan información sobre nosotros, la misma red social que registra y procesa información sobre nuestras actividades y, por último, los motores de búsqueda (buscadores) que indexan los perfiles y los ponen a disposición de cualquier usuario de Internet.

Con respecto a la información entregada por el propio usuario ésta es variada, pero en la mayor parte de los casos cae dentro de la categoría de datos sensibles.

Un ejemplo de ello es lo que sucede en Facebook. Al registrarse las personas entregan información como el nombre, edad, sexo y correo electrónico. Una vez que la persona ya está registrada se le pide que llene el campo de información que incluye una serie de datos de carácter sensible como ciudad de residencia, ciudad de nacimiento, teléfono básico y celular, estado civil, con quién está casado, quiénes son los hijos, los amigos, intereses, tendencias políticas y credo religioso.

Toda la información que hemos enumerado más arriba conforma sólo el perfil del usuario. A eso hay que sumar los contenidos, la mayor parte de carácter personal, que suben las personas a este tipo de plataformas.

Nos referimos a las fotografías y videos sobre cumpleaños, matrimonios, reuniones sociales y todo tipo de eventos de carácter familiar. En Chile, es común que los adolescentes publiquen en Facebook un álbum de fotografías cada vez que se juntan con amigos, que van de paseo a la playa o al mall de compras.

A ello hay que sumar los comentarios a las noticias que leen y comparten las personas, y que también pueden ser realizados en Twitter. O si nos vamos a Miso, allí pueden compartir y comentar las series y películas de televisión que están viendo.

Cabe señalar, que esta forma social de consumir la prensa y la televisión, entrega datos sobre el pensamiento político y religioso de las personas. Y también sobre los estados de ánimo de los sujetos.

No es necesario realizar un análisis de discurso para intuir la orientación política de una persona, a partir de los comentarios que realiza en Twitter o Facebook sobre un hecho político de relevancia o un atentado terrorista.

En la ilustración anterior vemos los comentarios a una noticia sobre el llamado conflicto mapuche en Chile realizados en Facebook, en los queda de manifiesto el pensamiento político de las personas.

No obstante, la mayor parte de los problemas a los que se ve enfrentado la vida privada en las redes sociales, proviene de la información personal subida por terceras personas. En la actualidad, ésta es una de las principales formas en las que se realiza el *cyberbullying*.

Básicamente consiste en postear información que atente contra el honor de una persona o, simplemente, realizar amenazas. También se utilizan fotografías comprometedoras o injuriosas.

Los mecanismos para realizar este tipo de acciones son tres, básicamente. El primero de ellos se basa en el etiquetado o tageado de fotografías o videos. Cualquier persona puede publicar una fotografía sobre nosotros y etiquetarla con nuestro nombre, para que de inmedia-

to todos nuestros contactos sepan que alguien ha publicado una foto nuestra. Hay que sumar el hecho de que las publicaciones que nuestros amigos realizan en nuestro muro, son comunicados tanto a nuestros amigos, como a los amigos de mi amigo.

Asimismo hay que considerar que redes sociales como Facebook, poseen programas de reconocimiento facial que permiten identificar (etiquetar) de manera automática a un usuario cuando alguien sube una fotografía. La única forma de evitar aquello, es desactivando esa función desde la configuración de privacidad de la red social.

Una segunda forma es a través de robo o uso no autorizado de un dispositivo móvil, como un teléfono inteligente o una tableta. Debido a que los dispositivos móviles funcionan bajo el esquema de apps (aplicaciones) y no desde la web, para abrir una red social, con el perfil del usuario, sólo se necesita abrir la aplicación correspondiente a la red social. Tanto la clave, como el nombre de usuario, se colocan al instalar la aplicación. Desde ese momento, no es necesario volver a colocarla.

Basta con que un adolescente deje olvidado el teléfono inteligente arriba de una mesa, para que otro lo tome y publique información vergonzosa para él o que injurie a otra persona, desde su propia cuenta de Twitter o Facebook. Es por eso que es recomendable bloquear con clave todos los dispositivos móviles.

La tercera forma consiste en el *hackeo* de cuentas de correo electrónico y de redes sociales. Por lo general, el objetivo de este tipo de suplantación de identidad es hacer juicios racistas o discriminatorios, para que la persona a la cual le *hackearon* la cuenta, sea objeto de un repudio de carácter social.

Cabe señalar, que en la actualidad para realizar este tipo de prácticas no es necesario conocimientos de programación. Para ello, se utiliza lo que se conoce como ingeniería social y programas de nivel de usuario, que circulan por la web.

A ello hay que sumar el hecho de que cuando un amigo mío utiliza una aplicación como un juego o cuestionario que no pertenece directamente Facebook, también comunica datos personales de mi propiedad a dicha empresa externa.

«Si tu amigo se conecta a un aplicación o sitio web, estos podrán acceder a tu nombre, fotografía, sexo, ID de usuario, y aquella información que hayas compartido con «todos». También podrán acceder a tus conexiones, pero no podrán acceder a tu lista de amigos»[5].

[5] FACEBOOK, «Política de privacidad de Facebook». *Facebook Site Governance*, 2011. http://www.facebook.com/note.php?note_id=10150163927665301

Tal como podemos observar en la cita anterior, cada aplicación que utilizamos en Facebook no sólo da acceso a nuestra información personal, sino que también a la de nuestros contactos. Por lo que el simple hecho de que un amigo nuestro instale una aplicación en su perfil, también constituye un peligro para nuestra vida privada.

Esto constituye un atentado en contra de la autodeterminación informativa y al concepto mismo de vida privada. Por lo mismo, es necesario que realicemos una pequeña reflexión de carácter conceptual antes de proseguir.

Autores como Herrán y Desantes señalan que el límite entre la vida privada y la vida pública es puesto por la misma persona, al determinar qué es lo que comunica o pone a disposición de los medios de comunicación masivos.

Lo privado, en tanto, se rige por medio de la confidencialidad. Según Herrán la confidencialidad es «aquello que se revela a alguien con la intención o el ánimo de que no sea develado a los demás sin el consentimiento del interesado»[6].

Claramente en este caso esa condición no es cumplida. Tampoco cuando un amigo nuestro publica algo en nuestro muro y ello es comunicado no sólo a nuestros «amigos», sino que también a los «amigos de nuestros amigos».

Es allí donde se rompería la autodeterminación informativa, porque perderíamos control de poder decidir qué es público y qué no lo es. Y lo que es más importante, qué es lo que quiero comunicar a una persona y no a otra.

Tal como lo señala las políticas de privacidad de Facebook, el objetivo del sitio es comunicar o compartir información con «todos». Si bien es cierto que Facebook permite restringir el acceso a nuestros datos personales, la configuración por defecto para la protección de datos personales es mínima y sigue la política de *opt-out*.

Es decir, la configuración por defecto tiende a compartir la información con todos y con los «amigos de mis amigos». Para poder tener un mayor nivel de protección, es el mismo usuario el que debe restringir el acceso a la información a través de los controles de la configuración de privacidad.

Otro aspecto interesante a considerar es el tipo de información personal que las redes sociales pueden recolectar y procesar, para producir nuevo conocimiento.

[6] HERRÁN, Ana Isabel, *La violación de la intimidad en la protección de los datos personales*, Ed. Dykinson, Madrid, 1998, p. 16.

Además de todos los datos que los usuarios entregan a redes sociales como Facebook y que ya analizamos, hay que considerar que recolectan toda la información sobre nosotros que es publicada por otros usuarios.

A lo anterior hay que sumar las prácticas de intromisión y monitoreo que realizan las redes sociales. Por monitoreo entenderemos como el registro y vigilancia de cada una de las acciones que las personas realizan en las redes sociales. La intromisión, en tanto, es la práctica de utilizar *cookies*, *bugs*, *worms* u otro tipo de *software* espía con el fin de buscar información dentro del disco duro o memoria *flash* del dispositivo digital del usuario.

Cada vez que una persona accede a una red social desde un teléfono celular u otro dispositivo móvil, el sitio almacena el número de teléfono y la ubicación de la persona. En el caso de hacerlo desde un computador, almacena la dirección IP, la ubicación, el nombre del ISP[7] que utiliza, el sistema operativo y hasta el tipo de procesador que tiene el PC.

En ambos casos se puede saber el *browser* del usuario y los sitios web que visitó antes y después de entrar a la red social. Asimismo es posible averiguar el buscador que utiliza, junto con los términos de búsqueda usados recientemente. A ello hay que sumar una serie de parámetros más técnicos como el tipo de pantalla o programas cargados en el dispositivo móvil o computador.

Además recolectan y procesan información sobre todas las actividades realizadas por los usuarios, lo cual les permite realizar perfiles «personalizados» sobre la conducta de sus usuarios. La mayor parte de estos perfiles son empleados con fines publicitarios, para entregar anuncios «a la carta».

Gmail, el popular servidor de correo electrónico gratuito, posee *bots* que leen todos los mensajes, los clasifican y procesan para determinar qué publicidad entregarnos, de acuerdos a nuestros intereses, edad y ubicación geográfica.

Si usted le envía correos electrónicos a sus amigos para organizar un partido de fútbol el día domingo, lo más común sería que se encontrara con avisos sobre las canchas que podría arrendar cerca de su hogar.

Como podemos observar, la cantidad de información privada que circula por las redes sociales es bastante. Pero lo más importante, es que es información de carácter sensible. En muchos casos va más allá de lo privado y entra en la esfera de lo íntimo.

[7] Internet Service Provider.

Una aplicación creada por Facebook a fines de 2012, permite acceder a la información personal que dicha red social almacena sobre un usuario. Lo interesante del caso es que esa herramienta nos da una imagen bastante precisa de la información que se almacena. Va desde todos los mensajes enviados y recibidos, el texto de todos los chats, todo lo que hemos escrito en nuestro muro y en el de otros, todo lo que se ha escrito en nuestro muro, todas las fotografías que hemos subido o que otras personas han publicado, pero aparecemos en ellas, los nombres de los contactos borrados, bloqueados, pasando por el registro de cada sesión activa que hemos tenido en Facebook, con día, hora, duración, dirección IP, datos de geolocalización, registro del equipo que utilizamos, hasta los datos de reconocimiento facial.

Asimismo existe la posibilidad de recolectar esa información, por parte de la red social, de las empresas que crean aplicaciones para dichas redes, por los contactos de los usuarios y hasta por los contactos de los contactos (amigos de los amigos en el lenguaje de Facebook), y procesarla para obtener conocimiento de carácter íntimo de cada uno de los usuarios.

A través del monitoreo de los cambios de relaciones, publicaciones de estado, conversaciones, comentarios y fotografías y videos publicados, es posible saber qué le está pasando a una persona, cuál es su estado del ánimo o cuáles son sus problemas.

Una última forma en la que a través de la cual la información personal de un usuario de una red social es recolectada, es la indexación por parte de los motores de búsqueda. Todas las redes sociales que están basadas en formatos web, como Facebook, Twitter, Hi5 o Myspace, pueden ser indexadas por los buscadores.

El problema no es que el buscador sólo realice una copia de nuestro perfil, sino que lo pone a disposición de todos los usuarios de Internet. El *googleo* (poner el nombre de una persona en un buscador para ver cuál es la información disponible sobre él) es una práctica habitual por parte de los empleadores antes de contratar a una persona. ¿Qué pasaría entonces si se encontraran con una fotografía comprometedora que otra persona subió a una red social? La respuesta es obvia.

Uno de los mayores problemas de las redes sociales es ése, debido a que la autodeterminación informativa desaparece al perder la persona el control de su información personal, debido a que queda sujeto a la actuación de terceros. Terceros que van desde amigos, desconocidos, hasta la misma red social y los motores de búsqueda.

IV. La configuración de lo meta público

Como consecuencia de lo anterior, se configura una nueva esfera de lo público: la red social. Si nos remontamos a los trabajos de Desantes, él identificaba tres espacios: lo íntimo, lo privado y lo público[8].

Los definía como una especie de esferas o capas de cebolla (una afuera de la otra) que se situaban desde el núcleo de la personalidad hacia afuera. Según Desantes el espacio de lo íntimo corresponde a las experiencias, creencias, convicciones y sentimientos que definen la personalidad de un individuo[9]. Es nuestro mundo propio. No obstante, Herrán afirma que «lo íntimo, pues, no se identifica con lo secreto o desconocido para terceros; va más allá porque representa la propia esencia de cada individuo en cuanto ser humano, su propia individualidad»[10].

Lo que señala Herrán es que lo íntimo no es necesariamente secreto, sino que son todos aquellos sentimientos, experiencias y sucesos que la persona se guarda para sí mismo, que no los comenta, pero que pueden ser observados por el círculo cercano a la persona.

La desarticulación de los espacios íntimos y privados, se produce porque dicha observación antes, sólo podía ser realizada por el círculo más cercano del individuo. Es decir, por quienes tenían un vínculo físico y/o emocional prolongado o cercano con la persona.

La red social virtualiza dicho vínculo, debido a que permite ejercer la vigilancia través de los mecanismos de monitoreo e intrusión, por parte de sujetos que no mantengan, necesariamente, un vínculo emocional o físico con la persona.

Lo que podríamos plantear es que al contrario de lo que señala Herrán, la red social reduce la esfera de lo íntimo a lo secreto, a aquello que no es posible deducir a través de la observación o monitoreo, en este caso.

Por otra parte, la vida íntima es todo aquello que consideramos que no debemos poner en conocimiento del público en general, «pero que a pesar de eso no son determinantes para definir los sentimientos o la personalidad de alguien»[11].

[8] DESANTES, José María, «El derecho fundamental a la intimidad», Estudios Públicos, N.° 46, 1992, p. 270.

[9] DESANTES, José María, *Información y derecho*. Pontificia Universidad Católica de Chile. Santiago, 1990, p. 32.

[10] HERRÁN, Ana Isabel. *Op. cit.*, p. 2.

[11] JARAMILLO, Óscar, *Derecho a la información en los portales y buscadores de la web*. Tesis para obtener el grado de Doctor en Ciencias de la Información, Universidad Complutense de Madrid. Prof. guía: CORREDOIRA, Loreto, 2003, p. 133.

En términos sencillos, es todo aquello que comunicamos a nuestro círculo cercano, compuesto por la familia y amistades. Una de las características esenciales de la vida privada, es que se rige por el concepto de confidencialidad y de la autodeterminación informativa. Es la propia persona quien define que forma parte de lo íntimo, lo público y lo privado.

Lo público es todo aquello que es comunicado a la población en general a través de los medios de comunicación masivos o por archivos y registros de consulta general.

Lo que hace la red social es convertir la esfera de lo privado en público, debido a que todo lo que publique en ella no está regido por el concepto de confidencialidad, por lo que de inmediato se pierde la autodeterminación informativa. Tal como pudimos observar anteriormente, todo lo publicado en una red social pasa rápidamente de nuestro círculo de contactos a los contactos de nuestros amigos. Por eso podemos decir que no hay confidencialidad.

Si aceptáramos el hecho de que las redes sociales se mantienen dentro del ámbito de lo privado, tendría que ser una definición bastante amplia, en la cual el círculo de amistades estaría compuesto por cientos de personas.

No obstante, esta nueva esfera compuesta por la red social, se diferencia de la vida pública en términos de masividad. La diferencia está en que a pesar de la gran cantidad de visitas, la red social se mantiene dentro de un ámbito más *underground*, por llamarlo de alguna manera. Y tal como lo dijimos anteriormente, para que una información sea de conocimiento de la opinión pública, requiere de la participación de los medios de comunicación tradicionales.

Desde un punto de vista sociológico, no contiene los elementos propios de la fama, tal como los define Gubern. Dicho de otro modo, la masividad otorgada sólo por la red social no asegura que una persona forme parte del *star system* o telecracia.

Eso último está reservado sólo aquellas personas que hagan la transición hacia los medios de comunicación tradicionales y, en especial, a la televisión.

V. La delegación

La masividad no es la única diferencia entre la esfera de la red social y de lo público. Tanto o más importante es lo que Desantes denomina como la delegación del sujeto universal del derecho a la información.

En términos desantianos, el derecho a la información es ejercido por delegación por los medios de comunicación y los profesionales de la comunicación[12]. Al menos, eso es lo que sucede dentro del ámbito de los medios tradicionales, tales como la prensa, radio y televisión.

Pero en las redes sociales y en todos los medios de la Web 2.0, el derecho a la información es ejercido de manera directa por el titular universal, sin ningún tipo de intromisión por parte de los profesionales de la comunicación o de los medios de comunicación.

Es el sujeto universal quien recibe, investiga y difunde información sin ningún tipo limitaciones ni fronteras, a través de la red social. Al igual que lo que sucede con las esferas de los público y privado, las redes sociales y la Web 2.0 desarticulan el campo deontológico, tal cual como lo conocemos.

El objeto tradicional de los medios de comunicación es la información. Es la producción y difusión de mensajes lo que da origen a las llamadas industrias culturales, en términos frankfurtianos.

No obstante, el objeto de la Web 2.0 no está en la producción de información. Los responsables de Youtube, Facebook, MySpace o Hi5 no hacen videos, noticias, ni ningún tipo de contenidos.

Ellos se limitaron a crear una plataforma para que sean los propios usuarios quienes generen y difundan los contenidos. Es por esa razón que los desafíos éticos propios del ejercicio del periodismo y del resto de las profesiones asociadas a los medios de comunicación masivos, recaen ahora en los usuarios de las redes sociales.

Preguntas tan clásicas como debo publicar o no, recaen ahora en niños de doce años, que carecen de la madurez, el desarrollo ético, valórico y emocional para dimensionar las consecuencias que puede tener la decisión de subir a la red un video, por inocente o simple que pueda parecer en un principio.

Es por eso que desde un punto de vista ético y deontológico, la responsabilidad de quienes administran las redes sociales es aún mayor. Su rol no es el de un medio tradicional o de un profesional de la comunicación. Su pregunta no es de si debe o no publicar, ni su compromiso más básico debe radicar en el deber de informar, asociado a la esencia misma de la vida democrática de los Estados.

Sus preguntas son qué hacer frente a los casos de grooming, sexting, pedofilia, bullying o ciber odio que circulan a través de las plataformas que ellos mismos crearon.

[12] DESANTES, José María, *Información y derecho. Op. cit.*

La pregunta central es si la creación de complicadas y grandilocuentes políticas de privacidad y uso de las redes sociales son suficientes como para asegurarnos que están cumpliendo con el compromiso ético y legal, que está asociado a su accionar comunicacional.

Muchas de ellas están redactadas en términos tan complicados y ubicadas en lugares tan poco visibles que hacen que sea casi imposible que sean leídas y menos, entendidas, por la mayor parte de los usuarios de las redes sociales.

Al leerlas queda la impresión que su objetivo es de desligar responsabilidades en el caso de que sucediera algo, en vez de formar conciencia sobre los peligros asociados al uso poco reflexivo de las redes sociales.

Es por eso que el administrador de la red social adquiere un compromiso ético importante, pero que no es el mismo que los medios de comunicación tradicionales, ni el de los periodistas.

Su compromiso no está en el deber de informar para que la opinión pública reciba la información necesaria para que pueda ejercer su voto de manera informada.

Su compromiso debiera estar con la educación y mediación en los conflictos éticos, para sean los propios usuarios quienes respeten los principios de personalidad y comunidad, de los que hablaba Desantes.

No queremos decir con esto que los administradores de las redes sociales y los ISP's deban convertirse en ciberpolicías, que monitoreen constantemente la red para evitar que se produzcan delitos al interior de ella.

Nos referimos que al momento de crear una red que permite que todas las personas con acceso a Internet puedan efectivamente ejercer su derecho a la información de manera directa, sin ningún tipo de delegación, adquieren el compromiso ético de formar a esas personas para que puedan ejercer sus derechos y deberes de manera libre.

¿Puede un administrador de una red social refugiarse en su política de uso y no hacer nada frente a casos de pedofilia que se vehiculen a través de su plataforma?

Dado el estado actual de la cuestión, la política de uso sería suficiente como para deslindar responsabilidades desde el punto de vista legal. Bastaría con que borrara de su servidor los contenidos cuestionados, cuando se lo solicitaran los tribunales de justicia.

Sin embargo, eso sería una medida pírrica porque el administrador sabría que sería demasiado tarde, que el contenido ya habría sido

copiado, descargado y vuelto a subir en cientos o miles de servidores y computadores alrededor de todo el mundo. Más aún si fueron indexados por un buscador.

Frente a eso hay dos alternativas: ejercer mecanismos de control o de educación. Lamentablemente todo mecanismo de control está condenado al fracaso debido a factores éticos y técnicos.

La única forma de evitar que un usuario suba un video que compromete a otra persona, es impidiéndoselo. Es decir, ejerciendo la censura y evitando que se suban videos, se tageen contenidos o se publiquen mensajes en el muro de una persona. Si hiciéramos eso, atentaríamos en contra del derecho a la información de las personas.

Por otra parte, todos los mecanismos de control de contenidos de tipo tecnológico y que no siguen una lógica totalitaria, han demostrado su bajo nivel de efectividad. Los programas de filtrado y etiquetado o el uso de *bots* para identificar los contenidos nocivos e ilegales tienen grandes falencias debido a su incapacidad para reconocer el contexto. Además su gran limitación radica en que sólo pueden leer palabras y no imágenes, por lo que basta con que un video sobre pedofilia sea tageado o etiquetado con términos inocentes, para que pase los filtros.

La otra alternativa es educar a los usuarios de las redes sociales para que sean conscientes de sus derechos y deberes asociados al ejercicio del derecho a la información.

En este rol formativo no sólo deben participar los administradores de las redes sociales. También deben hacerlo los padres y la escuela, debido al papel formativo que juegan dentro de la sociedad. Además es necesario que dentro de toda esta discusión se incluya, además, a las autoridades políticas y legislativas de cada nación.

De lo contrario, pude suceder que se repitan fórmulas altamente restrictivas como el modelo australiano para evitar el flujo de pornografía por la red o soluciones ya fracasadas, como responsabilizar a los ISP's.

El modelo australiano lo que propone es la creación de un muro de fuego o *firewall* que aísle al país de todos los contenidos que provienen de otros países. Es lo que se conoce como zonificar la red, para que el usuario sólo pueda navegar por una especie de intranet o Internet de carácter nacional.

El segundo paso consiste en un acceso a Internet sin ningún tipo de neutralidad, en la cual se guarda registro de cada una las actividades que los usuarios realizan en la Web a través de códigos identificatorios.

Dicho de otro modo, a cada usuario se le asigna una IP específica y el ISP está obligado a guardar registro de cada una de sus actividades en línea, además de filtrar los puertos para evitar que se conecte a redes P2P, para compartir archivos, o de cualquier otro tipo que no sea autorizada.

Un tercer paso es tener control sobre los servidores de alojamiento y de los buscadores, para que los usuarios sólo puedan acceder a los contenidos aprobados por el gobierno.

Ése es el modelo que está en discusión en Australia y que se emplea en países como Corea del Norte y China. De esa manera podríamos, técnicamente, evitar la publicación de contenidos ilegales y nocivos. Sin embargo, el costo sería altísimo, ya que convertiríamos la red en un Estado policial que negaría de manera rotunda el derecho a recibir información por parte del titular universal del derecho a la información.

Es por eso que la autorregulación debe ser realizada por los propios usuarios, debido a que son ellos quienes confeccionan y suben los contenidos a las redes sociales.

En tanto, el rol mediador se refiere a que el administrador de la red social debe estar capacitado para resolver conflictos de carácter ético entre usuarios. Asimismo debe ser capaz de saber cuáles son las acciones que debe seguir cuando un problema trascienda la esfera de lo ético y caiga dentro de lo ilegal.

Un ejemplo de ello es lo sucedido en foros de corte tecnológico, en los que los administradores deben intervenir cuando un usuario hace una pregunta de carácter básico, lo cual muchas veces hace que personas con mayores conocimientos técnicos los descalifiquen por «ignorantes». En esos casos los administradores deben recordarles a los usuarios que guarden la compostura, que descalifiquen y que el rol del foro es ayudar a las personas.

Otro ejemplo es lo que sucedió en Chile cuando un usuario del blog Fayerwayer publicó en un posteo el *link* hacia una base de datos con información confidencial de aproximadamente seis millones de personas.

El *link* fue removido apenas los administradores del sitio se dieron cuenta de ello y realizaron una denuncia a la Brigada del Cibercrimen de la Policía de Investigaciones para que investigara los hechos.

Al igual que la neutralidad, es necesario que se garanticen otros dos derechos en las redes sociales y en los entornos digitales. Nos referimos al derecho al olvido y al de simplicidad.

El derecho a la simplicidad en las condiciones de uso y privacidad, parte desde la base de que toda información debe ser veraz y oportuna. tal como lo hemos dicho anteriormente, las políticas de privacidad y las condiciones de uso se caracterizan por su complejidad en términos legales y por ser muy extensas. En mucho casos superan los 20 folios con largueza.

Al ser tan largas y estar en un lenguaje casi críptico, las personas se limitan a clickear acepto, sin siquiera leer. Cabe recordar que una de las tácticas más efectivas de ejercer la desinformación es, justamente, a través de saturarnos de información innecesaria. Ése es el caso de gran parte de las políticas de privacidad de muchas redes sociales.

Asimismo para que el derecho al olvido pueda ejercerse en las redes sociales, es necesario que se restrinja la indexación de los perfiles por parte de los motores de búsqueda. No se saca nada con borrar una fotografía desde Facebook, si está disponible en la base de datos de un buscador. Además el buscador produce un efecto multiplicador del contenido, que hace que para cuando se ejerza el derecho al olvido ya esté circulando por toda la red.

VI. Antes del cierre

McLuhan planteaba que el hombre creaba la tecnología, pero que esta terminaba moldeando al hombre. La forma en que las redes sociales han redefinido los conceptos de vida privada y pública, no afectan sólo a los entornos digitales, sino que a toda la sociedad. Ahí radica la importancia de este tema.

La arquitectura misma de las redes sociales apunta a que toda la vida de las personas transite hacia lo público. En una época en que la transparencia se pone de moda, la pregunta pareciera ser hasta qué punto estamos dispuesto a que así sea.

Esa es la razón por la que es necesario saber cómo se produce el tránsito desde lo privado a lo público en las redes sociales. Cuál es el tipo de información que el usuario entrega de mutuo propio y cuál, a través de terceros o de la acción de las redes sociales, al recopilar, almacenar y procesar el verdadero rastro digital

que deja al vehiculizar sus relaciones sociales a través de las redes sociales.

Éste es un campo que debe formar parte de la alfabetización digital de las generaciones actuales y de las futuras. También debe ser el inicio de una discusión en la que se planteen nuevos derechos y deberes, no ya para profesionales de la comunicación, sino que para usuarios-personas comunes y corrientes.