

LA DESARTICULACIÓN DE LO PÚBLICO Y LO PRIVADO EN LAS REDES SOCIALES

Dr. Oscar Jaramillo

Profesor titular del Instituto de Comunicación y Nuevas Tecnologías de la Universidad Mayor, Chile

En noviembre de 2007 los medios chilenos se estremecieron con la circulación por distintas redes sociales de un video en el que una escolar de 14 años mantenía sexo oral con un compañero de curso en un parque de Santiago.

El hecho causó un alto impacto mediático, por lo que el Consejo Nacional de Televisión (CNTV) rápidamente prohibió la exhibición de video y les advirtió a las cadenas de TV que de lo contrario, serían acusadas de distribuir material pedofílico.

El video fue grabado con un teléfono celular por otro escolar, el cual lo envió vía inalámbrica (Bluetooth) a sus compañeros dentro del colegio. Como una verdadera bola de nieve el video comenzó a ser enviado de manera indiscriminada por Bluetooth.

Mucha gente recibió el mensaje a su teléfono celular sin siquiera saber quién se lo enviaba, ni quererlo. Sólo lo recibía por estar al alcance de la red inalámbrica de quien lo enviaba.

De ahí alguien tuvo la idea de subir el video a Youtube. Con posterioridad el portal El Antro publicó el enlace al video y de ahí la noticia pasó en sólo cosa de horas a las portadas de noticieros y programas de farándula y opinión periodística.

Casos como el anterior no son nuevos dentro de las redes sociales y se suman a los de Edgard y Star Wars Kids, por nombrar sólo algunos de los que existen a nivel internacional.

Fenómenos como el sexting, en el cual adolescentes de 13 a 15 años se toman fotografías de corte erótico o abiertamente pornográfico, con el único objetivo de recibir posteos de admiración en sus fotologs, constituyen otra arista de la desarticulación del concepto de vida privada en las redes sociales como Facebook, Hi5 o Youtube.

A partir de los ejemplos anteriores cabe preguntarse si existe o es posible tener vida privada desde el momento en que las redes sociales comienzan a adquirir ubicuidad.

Al parecer la respuesta sería no o, al menos, eso es lo que indicaría el estado del arte actual.

LA VIDA PRIVADA

Antes de poder proseguir y realizar un análisis de lo que sucede con la vida privada en las redes sociales, es necesario aclarar cuál es la información nuestra que está en dichas plataformas digitales, para ver de esa manera si son un espacio público o privado.

En primer lugar, hay que considerar que la información de carácter privado que está en las redes sociales proviene de cuatro 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 y, por último, la misma red social que registra y procesa información sobre nuestras actividades.

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.

En la práctica es posible reconstruir diarios de vida audiovisuales de los adolescentes, a partir de las fotografías y videos publicados en la red social. A ello hay que sumar

que el muro de la plataforma es utilizada como herramienta de comunicación intra e inter personal.

¿Por qué podemos decir que es intra personal? Porque los usuarios publican sus pensamientos, sentimientos y estados de ánimos, el estado de sus relaciones sentimentales, la música que están escuchando y que evocaciones le trae ello.

Es interpersonal porque dialogan con otras personas, más allá de sea una comunicación entre avatares como plantean algunos autores. Hay un diálogo entre personas sobre cuestiones que van desde lo más trascendental a lo más mundano. Pero lo interesante del caso, es que estos diálogos quedan registrados y son comunicados a todos los contactos o amigos.

Cuando publico algo en el muro de Pedrito, no queda sólo entre él y yo. Es comunicado a todos los contactos de Pedrito y los míos. Y junto con enterarse de este diálogo tienen la capacidad de involucrarse en él.

Es como si pudiéramos hablar por teléfono o chatear, pero con la diferencia de que quede un registro de él y existan quinientas personas escuchándonos y con la posibilidad de interactuar con ellas.

Cuando interactuamos en las redes sociales estamos poniendo o exponiendo una parte de nuestras vidas al resto de las personas o contactos que conforman nuestra red.

A esto hay que sumar la posibilidad de publicar enlaces a contenidos 1.0, como noticias o sitios web, hacer críticas de libros, chatear o jugar en línea con usuarios alrededor del mundo, los que necesariamente deben ser contactos o "amigos" míos.

Esa es sólo una parte de la información que las personas entregan voluntariamente y que circula por las redes sociales. Hay que sumar la que otros usuarios pueden publicar sobre nosotros.

La capacidad de taguear o etiquetar permite asociar una fotografía o un video a un usuario específico. Cualquier persona puede publicar una fotografía sobre nosotros y etiquetarla con nuestro nombre para que de inmediato todos nuestros contactos sepan que alguien ha publicado una foto nuestra.

Muchas veces sucede que esa fotografía o video no es precisamente la que más nos conviene según nuestras intenciones avatáricas. 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.

A ello hay que sumar el hecho de que cuando un amigo mío utiliza una aplicación como un juego o cuestionario que no pertenece a 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”¹⁴.

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”¹⁵.

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.

¹⁴ Facebook Site Governance. Política de privacidad de Facebook. Marzo 2010.
http://www.facebook.com/note.php?note_id=10150163927665301

¹⁵ A.I. Herrán, “La violación de la intimidad en la protección de los datos personales”. Ed. Dykinson. Madrid, España. 1998. P. 16.

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.

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 ISP¹⁶ 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

¹⁶ Internet Service Provider.

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 acuerdo 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.

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.

Uno de los mayores problemas de las redes sociales es éste, el cual está asociado a la posibilidad de procesar la información, cuestión que desde hacer data mining o sacar simples consecuencias a partir de lo que se está observando. Es por eso que podemos considerar a la red social como un espacio público, pese a que en un principio el acceso esté restringido por clave a los contactos de la persona.

LA CONFIGURACIÓN DE LO META PÚBLICO

Para poder terminar de dimensionar la desarticulación de lo público y lo privado, es necesario volver al ejemplo con el que iniciamos la ponencia. En el caso del video de la adolescente que mantuvo relaciones sexuales con un compañero de curso en un parque de Santiago, el Edgard o el de Star Wars Kid, todos mantienen la misma lógica de difusión.

En los tres el video es subido a las redes sociales y allí se va propagando de manera viral. Es observado por los “amigos” y los “amigos de los amigos” (contactos de los contactos) de la persona que subió el video. A su vez estas personas decidieron compartirlo con sus contactos y así sucesivamente. Sin embargo, hasta ese momento se mantiene dentro de los límites de la red social en la cual fue publicado.

Con el paso de los días el video llega hasta el conocimiento de un blog con un alto número de visitas, quien publica el link hacia la red social en donde está alojado.

El salto desde el blog, hasta los medios de comunicación tradicionales como los diarios, revistas y televisión, es casi instantáneo. En primer momento la utilización de videos de carácter privado, que circulaban a través de la redes sociales, estuvo restringido a programas de entretenimiento y farándula.

Los ejemplos más clásicos los constituyeron los videos de índole sexual de figuras de la farándula internacional como Paris Hilton o Pamela Anderson.

En la actualidad es posible observar la utilización de videos registrados con teléfonos celulares o cámaras de seguridad que fueron subidos a las redes sociales, en noticiarios de grandes cadenas nacionales e internacionales.

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

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 individuo¹⁷. 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”¹⁸.

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.

¹⁷ J.M. Desantes, Información y derecho. 1º Ed. Pontificia Universidad Católica de Chile. Santiago, Chile. 1990. P. 32.

¹⁸ A.I. Herrán, Op. cit. p. 2.

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”¹⁹.

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 o miles de personas.

¹⁹ O. Jaramillo, 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. 2003. P. 133.

Es lo que le sucedió en el mes de marzo de 2010 a una universitaria chilena que para aprovechar el viaje de sus padres decidió organizar una fiesta en la casa. Las invitaciones las realizó a través de Facebook y Hi5.

Casi de inmediato pudo apreciar el poder convocatorio de las redes sociales, cuando en vez de llegar sus amistades más cercanas, pudo comprobar que afuera de la casa de sus padres había más de tres mil quinientas personas.

El alboroto llegó a tales proporciones que la muchedumbre debió ser dispersada por fuerzas especiales (antimotines) de la policía (Carabineros). El hecho figuró al día siguiente en todos los noticiarios centrales de la televisión chilena.

A partir de lo anterior, podemos plantear que la esfera de lo público se rearticula en una nueva configuración en la cual adquiere dos niveles: la red social y los medios de comunicación masivos (diarios, revistas, televisión).

Podemos plantearlos como dos niveles aparte debido a que la esfera de la red social tiene características distintas. En términos de masividad es menor, generalmente, que los medios tradicionales.

Sin embargo, hay que considerar que hay videos de origen chileno que están en Youtube, como los de Narco Henríquez, Para Bolas para Todos o el Osito Gomi Lalo, que tienen más de dos millones de visitas.

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.

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.

LA DELEGACIÓN

Casos como los que hemos planteado anteriormente, conllevan también una desarticulación de las consideraciones éticas y legales asociadas a los medios de comunicación tradicionales.

En términos desantianos, el derecho a la información es ejercido por delegación por los medios de comunicación y los profesionales de la comunicación. 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 de limitaciones ni fronteras, a través de la red social. Al igual que lo que sucede con las esferas de lo 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.

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.

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, atentariamos 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, puede 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 aisle 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 de 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.

ANTES DEL CIERRE

Como podemos observar, la desarticulación de lo público y privado en las redes sociales tiene consecuencias directas en la formación de responsabilidades desde el punto de vista ético.

En esta ponencia hemos identificado dos esferas dentro de lo público. Una directamente relacionada con las redes sociales y otra, con los medios de comunicación tradicionales.

Por otra parte hemos visto que la alarma pública, por llamarla de algún modo, se produce cuando un contenido (video) pasa de la red social a la televisión o los diarios.

Es importante recalcar este hecho porque es ahí cuando se produce el mayor daño a la honra de la persona afectada por el contenido, porque pasa de una condena o vergüenza de carácter local o restringida, a una de carácter nacional e internacional.

El hecho de que el contenido sea público en la red, no justifica o autoriza al medio de comunicación ni al periodista para que lo divulgue a través de la televisión o los diarios.

Lo que proponemos es que en ese momento se reintroduzca la autodeterminación informativa y sea la persona la que decida si autoriza o no, la difusión del contenido.

Para poder tomar la decisión de publicar o no, habría que considerar si estamos frente a un personaje público o privado y si el hecho tiene un interés público real. Es necesario hacer esta aclaración porque la mayor parte de los videos que pasan de la red a la televisión no afectan a la vida democrática, no son constitutivos de delito y sólo producen un daño gratuito a la honra de personas comunes y corrientes.

Un caso distinto sería si esas imágenes corresponden a autoridades y que las acciones ahí relatadas afectan al ejercicio público de sus funciones. Como podemos observar, el tratamiento que los medios de comunicación deben darle a dichos contenidos es el mismo que deben otorgarle a cualquier imagen, video o información de carácter privado.

Es aquí donde termina por reconfigurarse la desarticulación de lo público y lo privado en las redes sociales. Por paradójico y contradictorio que pueda parecer, los medios de comunicación deben considerar como privado esta nueva esfera de lo público, llamada redes sociales.

Es la única forma efectiva de minimizar los daños a la honra de las personas producida por la contracción de la vida privada a partir de la irrupción de las redes sociales. En los casos analizados, la sola circulación de los videos a través de la redes sociales produjeron un gran daño a la honra de las personas, como para agregar a eso la condena de carácter nacional.

Si bien es cierto que la red social es en sí misma un espacio público, es necesario que los medios de comunicación masivos (radio, prensa y televisión) tomen los resguardos para no afectar la honra de personas comunes y corrientes, que en ningún momento tuvieron la intención de ser famosos o aparecer en los medios.

BIBLIOGRAFÍA

A. Herrán, La violación de la intimidad en la protección de los datos personales. Ed. Dykinson. Madrid, España. 1998.

Facebook Site Governance. Política de privacidad de Facebook. Marzo 2010.
http://www.facebook.com/note.php?note_id=10150163927665301

L. Lessig, Code. Version 2.0. Basic Books. New York, USA. 2006.

J.M. Desantes, Información y derecho. 1º Ed. Pontificia Universidad Católica de Chile. Santiago, Chile. 1990