Módulo 3. Ilícitos en las redes sociales

Unidad 3.1 Principales ilícitos en el ámbito del *social media*

3.1.1 *Spam* y *phishing*

Una de las prácticas más frecuentes en el ámbito de internet es el llamado *spamming*, que consiste en el envío masivo de correos electrónicos no solicitados (*spam*), normalmente con fines publicitarios o promocionales. Aunque, también puede esconder finalidades delictivas, como ser la apropiación de datos confidenciales a los efectos de cometer una estafa, el envío de virus informáticos para dañar los sistemas del destinatario o bien, la saturación o interrupción de las comunicaciones producto de la enorme cantidad de mensajes que ingresan en un servidor en un lapso de tiempo muy breve.

Hacemos esta aclaración porque el *spamming* como tal, no es un delito conforme a la legislación argentina. En otros países, en cambio, está tipificado como un ilícito, más allá de que el *spammer* no tenga como finalidad cometer un fraude u otro delito mediante el envío de estos correos electrónicos masivos. En consecuencia, en primer lugar, examinaremos la práctica del *spamming* y su regulación legal en el país, para luego analizar su vinculación con el *phishing*, que sí es una conducta tipificada como delito por el Código Penal.

Se denomina *spam* "a cualquier mensaje no solicitado que normalmente tiene como finalidad ofertar, comercializar, o tratar de despertar el interés respecto de un producto, servicio o empresa" (Vaninetti, 2010, p. 189). Consiste en el "envío indiscriminado y no solicitado de publicidad mediante el correo electrónico" (Fernández Delpech, 2014, p. 395). El *spam* tiene la enorme ventaja para el remitente de permitirle publicitar o promocionar sus productos o servicios a un público masivo a un costo ínfimo, dado que no conlleva gastos de folletería, propaganda televisiva o radial, basta simplemente con tener una cuenta de correo electrónico remitente, acceso a Internet, una base de datos con las cuentas de correo electrónico de los destinatarios y, en general, un programa que permita automatizar los envíos, a los efectos, entre otras cosas, de segmentarlos y evitar los filtros anti-*spam* que suelen tener instalados los destinatarios. Es por eso que, actualmente,

constituye una de las formas más utilizadas para publicitar productos o servicios en internet.

No obstante, los beneficios que el *spam* tiene para el remitente revisten su contrapartida en perjuicios para el destinatario, vinculados fundamentalmente al uso de ancho de banda para descargar esos correos, la necesidad de actualizar los filtros anti-*spam*, la pérdida de tiempo y productividad producto de la necesidad de eliminarlos, la fragmentación del disco duro del dispositivo del receptor del correo electrónico, la caída del sistema, la pérdida de correos electrónicos que no son *spam* y que el destinatario desea recibir y -cuestión no menor- la afectación de la intimidad y privacidad.

La violación a la intimidad y privacidad de las personas está dada, entre otras cosas, por la manera o los medios utilizados normalmente por los *spammers* para obtener las direcciones de correo electrónico de los destinatarios:

- Compra de bases de datos ilegales.
- Programas espías.
- *Cookies*.
- Cadenas de mails en las que se dejan visibles las listas de contactos.
- Datos sacados de sitios web en los cuales normalmente figuran las direcciones de contacto y de empleados de una empresa u organización.
- Foros o blogs donde los participantes dejan sus datos de contacto.
- Las propias redes sociales en las que la información de perfil del usuario suele ser pública y en las que muchas veces figura la cuenta de correo electrónico.
- El ingreso ilegal en servidores de correo electrónico (*hacking*).

  La prueba de ensayo y error a través de la cual los *spammers* generan direcciones aleatorias mediante determinados programas informáticos y van comprobando cuáles de ellas son direcciones válidas y cuáles no.

Bien se ha señalado que:

> La ilegalidad del spam como elemento violatorio de la intimidad está a su vez dada en que para su funcionamiento necesariamente se deben recolectar previamente direcciones de correo electrónico que se alojan en 'bases de datos' conjuntamente con otros datos de

> sus titulares (gustos, preferencias de consumo, etcétera) obtenidos en la navegación que realizan los usuarios por Internet para ofrecerle un producto o servicio determinado que encaje en su perfil de consumidor. (Vaninetti, 2010, p. 192).

Y si recordamos los requisitos que establece la Ley de Protección de Datos Personales respecto de la recolección y tratamiento de ese tipo de datos (visto en el módulo 2) claramente surge que esa recolección es ilegal en la mayoría de los casos, porque se realiza sin el consentimiento del titular del dato (en este caso, el titular de la cuenta de correo electrónico) y sin el debido registro de la base de datos ante el organismo encargado de la aplicación de la mencionada ley.

A nivel internacional, existen dos sistemas respecto de cómo regular el *spam*:

1) **Sistema *opt in*:** es un sistema **cerrado**, ya que conforme a él, solamente se pueden enviar correos electrónicos publicitarios o promocionales a quienes expresamente lo hayan solicitado. En este caso, el envío solo es lícito si el destinatario ha prestado previamente su consentimiento a tales efectos de manera expresa.

2) **Sistema *opt out*:** sistema **abierto** según el cual se pueden enviar correos electrónicos publicitarios o promocionales a cualquier persona hasta tanto esta solicite expresamente que no se le envíen más. En este caso el envío es lícito hasta tanto el destinatario manifieste expresamente que no desea recibir más este tipo de correos electrónicos.

Señala Fernández Delpech que:

> En algunos países donde se ha implantado el sistema *opt out*, se ha creado además el sistema de las listas negativas de correos, estableciendo sitios de Internet en donde los usuarios pueden inscribir sus direcciones de correos, con la finalidad de que no se les envíe correo electrónico publicitario. A partir de la inscripción en dichas listas se invierte la regla dejando de ser, respecto de ese usuario, un sistema abierto o de *opt out* y pasado a ser un sistema cerrado o de *opt in*, en el cual el envío desde ese momento se torna ilícito. (Fernández Delpech, 2014, p. 396)

Como dijimos, a diferencia de otros países, en Argentina no hay una regulación específica para el *spam*. No obstante, es de aplicación el artículo 27 de la Ley N°

25.326 de Protección de Datos Personales, que regula las bases de datos con fines de publicidad. En ese sentido, dispone lo siguiente:

> **1 -** En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.
>
> **2-** En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.
>
> **3-** El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo.[1]

A su turno, el Decreto 1558/2001, reglamentario de la Ley N° 25.326, aclara este punto cuando establece que:

> En toda comunicación con fines de publicidad que se realice por correo, teléfono, correo electrónico, Internet u otro medio a distancia a conocer, se deberá indicar, en forma expresa y destacada, la posibilidad del titular del dato de solicitar el retiro o bloqueo, total o parcial, de su nombre de la base de datos. A pedido del interesado, se deberá informar el nombre del responsable o usuario del banco de datos que proveyó la información.[2]

Este plexo normativo se complementa con la Resolución 4/2009 de la Dirección Nacional de Protección de Datos Personales, que regula esta opción para solicitar el retiro o bloqueo de los datos personales y dispone que, en las comunicaciones mencionadas (publicidad directa a través del correo electrónico y de Internet, entre otros medios), el emisor de la comunicación "debe incorporar un aviso que informe

---

[1] Art. 27- Ley N.° 25.326 (2000). Protección de los Datos Personales. Honorable Congreso de la Nación Argentina.

[2] Art. 27- Decreto 1558/2001 (2001). Protección de los datos personales. Poder Ejecutivo Nacional.

al titular del dato sobre los derechos de retiro o bloqueo total o parcial (…) el mecanismo que se ha previsto para su ejercicio y la transcripción [de las normas citadas]"[3]. Además, dispone que cuando se trata de comunicaciones:

> (…) no requeridas o consentidas previamente por el titular del dato personal, deberá advertirse en forma destacada que se trata de una publicidad. En el caso de realizarse dicha comunicación a través de un correo electrónico deberá insertarse en su encabezado el término único "publicidad".[4]

En resumidas cuentas, la normativa establece lo siguiente:

1. Está permitida la formación de bases de datos con fines de publicidad que establezcan perfiles de consumidores.
2. Los datos deben recabarse de documentos accesibles al público o, en caso de no derivar de esa fuente, contar con el consentimiento del titular del dato.
3. El titular del dato puede ejercer sin cargo el derecho de acceso a la información que está recabada en la base de datos.
4. El titular del dato puede ejercer el derecho de retiro o bloqueo de los datos que estén en esa base de datos, para lo cual el emisor de la publicidad (remitente del correo electrónico) debe informar acerca de su derecho y del mecanismo para ejercerlo.
5. Tratándose de correos electrónicos publicitarios o promocionales, el asunto de estos solo debe contener la palabra **publicidad**.

Más allá de la cuestión de si se cumple o no en Argentina con toda esta normativa (pensemos solamente en la cantidad de correos electrónicos publicitarios que recibimos a diario y cuyo asunto no incluye el término "publicidad"), un punto interesante es determinar por cuál de los sistemas ha optado nuestra ley.

A primera vista, podría decirse que la opción ha sido por el sistema *opt out*, dado que consagra el derecho del destinatario a solicitar el retiro o bloqueo de su dirección de correo electrónico de las bases de datos publicitarias; en suma, a los fines de no recibir publicidad mediante correo electrónico o internet, el destinatario

[3] Art. 1- Resolución 4/2009 (2009). Protección de los datos personales. Dirección Nacional de Protección de Datos Personales.

[4] Art. 2- Resolución 4/2009. Op. cit.

debe ejercer ese derecho solicitando el retiro o bloqueo. Sin embargo, si tenemos en cuenta que el artículo 27 de la ley establece que los datos deben recabarse de documentos de acceso público o, caso contrario, con el consentimiento del titular, podría pensarse que, en los casos en que no se recaben de documentos de acceso público, el sistema será el *opt in*, en la medida en que se requiere el consentimiento del titular y como vimos en el módulo 2, para obtener el consentimiento se debe dar a conocer la finalidad del tratamiento de los datos.

Un tema íntimamente relacionado con este es el Registro Nacional No Llame, creado por la Ley N° 26.951, cuya autoridad de aplicación también es la Dirección Nacional de Protección de Datos Personales. Conforme a dicha ley y según los artículos 1 a 15, se establece que cualquier usuario del servicio de telefonía, en cualquiera de sus modalidades (básica, móvil, servicios de radiocomunicaciones, móvil celular, de comunicaciones móviles y de voz IP, así como cualquier otro tipo de servicio similar en el futuro), que manifieste su voluntad de no ser contactado por quien publicitare, ofertare, vendiere o regalare bienes o servicios, podrá inscribirse en el mencionado registro, a partir de lo cual no podrá ser contactado por quienes realicen publicidad directa a través de servicios de telefonía, salvo supuestos de excepción, como la existencia de un vínculo contractual previo con el usuario o las llamadas de quienes hayan sido expresamente permitidas por el usuario inscrito.

Podría decirse que este registro adopta la modalidad de lista negativa dentro del sistema *opt out*, conforme a lo que vimos anteriormente, lo cual facilita el ejercicio del derecho de bloqueo, dado que el usuario del servicio, en lugar de tener que ejercerlo respecto de cada empresa que haga publicidad directa, lo ejerce una sola vez ante el registro y las empresas están obligadas a consultarlo y a bloquear a quienes se hayan inscrito.

El registro comprende las comunicaciones a través de voz IP (como lo es Skype, por ejemplo), las llamadas o SMS a teléfonos celulares, la mensajería instantánea a través de una plataforma móvil (por ejemplo, WhatsApp), pero no abarca al correo electrónico, dado que se limita solamente a las comunicaciones telefónicas.

A nivel jurisprudencial del país surge el caso sobre *leading case* en materia de *spam* que data del año 2006 (Juzgado Nacional de Primera Instancia en lo Civil y Comercial Federal N.° 3, T., G. D. y otro c. Cosa, Carlos A. y otro. s/habeas data - art. 43 C.N.-, 7 de abril de 2006, disponible en http://www.derecho.uba.ar/rev_comunicaciones/ed010/jurisprudencia.htm). El caso se inició cuando dos conocidos abogados especialistas en derecho informático presentaron ante la justicia una acción de *hábeas data* en los términos de la Ley N°25.326, y argumentaron que sus datos personales se encontraban registrados en una base de datos utilizada por una empresa que enviaba *spam* con el fin de publicitar la venta de sus productos. Agregaron, además, que a pesar de que

habían solicitado vía correo electrónico el cese de estos envíos, los demandados continuaban su accionar.

El juez hizo lugar a la acción promovida y ordenó a los demandados que permitieran a los accionantes acceder a los datos personales que tenían almacenados, luego proceder a su eliminación y cesar en el tratamiento de estos. Para ello, se basó en los siguientes argumentos, que son muy importantes para tener en cuenta porque dejan claros varios aspectos que hemos tratado al hablar del *spam*:

1. Dado que los demandantes habían solicitado el cese del envío de *spam*, la actividad de los demandados consistente en continuar con sus envíos de correos electrónicos implica una invasión en la esfera de su intimidad y de su tranquilidad, violando los derechos personalísimos contemplados en el artículo 1071 bis del Código Civil (artículo 1770 del Nuevo Código Civil y Comercial); en suma, el *spam* viola el derecho a la intimidad o privacidad de las personas y por ende, deviene en una actividad ilícita, máxime cuando los destinatarios solicitaron el cese y el remitente hizo caso omiso de dicha solicitud.

2. El *spam* genera daño a los destinatarios atento al tiempo de descarga que requiere identificar, seleccionar y borrar los correos no solicitados, así como también al incremento en el costo de recepción y procesamiento y la necesidad de implementar sistemas para bloquear los virus que se pueden dispersar.

3. El proceso de fragmentación del disco duro que tiene lugar durante el almacenamiento y la eliminación de los correos no solicitados irroga un perjuicio a los destinatarios, que se traduce en una notable disminución de la velocidad de almacenamiento y obtención de información.

4. El hecho de que los destinatarios requieran el cese de la actividad a través de internet y no por un medio tradicional (carta documento, por ejemplo) no obsta a la validez de dicho pedido. Por ende, en los casos de envío de *spam*, se puede solicitar el cese mediante una vía similar: un correo electrónico enviado al remitente.

5. La oferta de transferencia de bases de datos a terceros con la finalidad de enviar publicidad y promocionar un servicio que posibilita el envío de correos electrónicos y oculta la dirección remitente (*spam*), viola lo dispuesto en la Ley N° 25.326, dado que dicho accionar dificulta el ejercicio del derecho de acceso a la referida base de datos.

Dijimos al comenzar el tratamiento de este tema que el *spam* normalmente se utiliza con fines meramente publicitarios o promocionales, aunque puede esconder también finalidades delictivas.

Justamente, una de las formas de utilizar el *spam* para la comisión de ilícitos se relaciona con el llamado *phishing*, que es una modalidad de fraude o estafa realizada comúnmente, aunque no es exclusiva de internet, bajo la modalidad de envíos masivos de correos electrónicos dirigidos a clientes de entidades financieras o negocios en los cuales tienen fondos o crédito y mediante los cuales se les solicita que ingresen a un hipervínculo a los efectos de actualizar sus datos (usuario y contraseña del servicio de *homebanking*, número de cuenta bancaria, número de tarjeta de crédito, etcétera).

A los fines de ganar la confianza de la víctima, se suele usar una serie de ardides, tales como informarle que, ante la sospecha de que personas inescrupulosas están haciendo uso de sus datos, la entidad ha procedido a suspender el uso de la cuenta hasta que el cliente verifique sus datos a través de la página web del banco a la cual tiene que acceder vía el hipervínculo que se le ofrece en el correo electrónico, o bien que, debido a una actualización del sitio web para mejorar su seguridad, se requiere que el cliente verifique los datos (usuario y contraseña o números de cuenta o tarjeta).

Una vez que el usuario pincha el hipervínculo, se le abre una ventana con una página web similar a la oficial de la entidad financiera de la cual es cliente (página espejo), pero que, en realidad, es una página falsa administrada por el *phisher* quien, a partir de los datos capturados procede a realizar una disposición patrimonial mediante la suplantación de la identidad de la víctima.

Ahora bien, como dijimos, el *phishing* puede realizarse vía *spam*, pero también puede llevarse a cabo por otros medios. En el caso particular de las redes sociales, puede realizarse mediante alguna aplicación que se utiliza a través de la cuenta de Facebook, en cuyo caso el *phisher* crea una página similar a la de la red social y cuando el usuario de la aplicación pincha allí, se le abre la falsa página donde consigna sus datos de ingreso (correo electrónico y contraseña) con los que el *phisher* puede acceder luego a la verdadera cuenta que la víctima tiene abierta en la red social.

A nivel legal, el *phishing* encuadra en el tipo penal del fraude informático, incorporado como modalidad especial de defraudación en el artículo 173, inciso 16, por la Ley N°26.388 de Delitos Informáticos en los siguientes términos: "El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de

datos"[5], por lo que prescribe la misma pena (prisión de un mes a seis años) que el artículo 172 estipula para el delito de defraudación en general (estafa).

La jurisprudencia local ha receptado la figura del *phishing* en un caso resuelto en 2010 (Álvarez de La Chica, 2010). La denuncia había atribuido a los procesados haber llevado a cabo maniobras de fraude mediante la técnica de manipulación informática conocida por *phishing* (página paralela), mediante la cual obtuvieron el código de transferencia y número de tarjeta de crédito del damnificado para poder operar en las cuentas bancarias de la víctima, desde la cual realizaron transferencias de dinero. Los imputados admitieron la transferencia bancaria desde la cuenta de la víctima a la cuenta de uno de ellos, pero alegaron que esta tenía como causa la compra por parte de la víctima de una camiseta de fútbol a través de Facebook.

La cámara confirmó el procesamiento de los computados en calidad de coautores del delito de defraudación previsto en el artículo 173, inciso 16, del Código Penal, toda vez que el descargo efectuado no resultaba creíble, pues más allá de que se logre localizar al supuesto comprador de la camiseta, los procesados no presentaron nada para avalar la transacción comercial alegada. Además, el monto supuestamente abonado era por demás elevado en relación con el producto que la víctima habría comprado.

3.1.2 *Bullying*

En el módulo 1 vimos que una de las problemáticas más importantes en el ámbito del *social media* tiene que ver con los menores de edad y su capacidad jurídica para abrir una cuenta en una red social. Las redes sociales establecen pautas sobre edad mínima de los usuarios para abrir una cuenta y el sistema automáticamente inhabilita a los usuarios que no alcanzan el mínimo exigido. Asimismo, explicamos que no hay una edad mínima uniforme, tanto en los términos y condiciones de uso de las plataformas, cuanto en la legislación de los diferentes países.

Si a esto le sumamos las facilidades que tiene un menor de edad para abrir una cuenta en una red social, navegar por páginas de internet, *chatear*, utilizando todo tipo de dispositivos, nos daremos cuenta de que la problemática de los menores de edad asume dimensiones importantes. Pensemos en esto: ¿cuántos niños o adolescentes conocemos que tienen celulares con acceso a internet? ¿Cuántos sabemos que tienen una cuenta abierta en una red social? ¿Cuántos usan WhatsApp? ¿Cuántos participan en juegos *online*?

---

[5] Art. 173, inc. 16- Ley N.° 26.388 (2008). Código Penal de la Nación Argentina. Honorable Congreso de la Nación Argentina.

Precisamente, una de las cuestiones más críticas respecto de los menores de edad en internet es la del **acoso**. Y hablamos de acoso para referirnos a dos prácticas diferentes, que muchas veces pueden confundirse, pero que deben, y de hecho, son tratadas por las leyes de manera diferente: nos referimos al *cyberbullying* y al *grooming*.

El *bullying* es el acoso de un menor de edad por parte de sus pares. Los casos típicos ocurren en el ámbito escolar, en los clubes, en el barrio, en suma, en los ámbitos donde los menores suelen relacionarse con otros menores. Cuando el acoso de un menor por parte de otros menores ocurre en el ámbito de internet, estamos en presencia del llamado *cyberbullying*, práctica consistente en "ser cruel con otra persona mediante el envío o publicación de material dañino o la implicación en otras formas de agresión social usando Internet u otras tecnologías digitales" (Vaninetti, 2010, p. 84).

Esta práctica puede asumir diferentes formas: imágenes o videos de agresiones físicas difundidas por la red, difusión de imágenes deformadas o de fotos con comentarios injuriantes o burlones de algún compañero de la escuela, creación de cuentas o grupos en las redes sociales con el objeto de burlarse o denigrar a un compañero de la escuela, envío de textos ofensivos o intimidatorios mediante celulares o *chats*, etcétera.

Sin lugar a dudas, el *cyberbullying* afecta a los menores que son víctimas de este, cuyas prácticas generan consecuencias negativas a nivel psicológico, autoestima, integración con los pares, rendimiento escolar, etcétera. No obstante, a nivel legal, no hay una normativa específica que regule esta temática y solo se cuenta con la Ley N° 26.892 de Promoción de la Convivencia y el Abordaje de la Conflictividad Social en las Instituciones Educativas, conocida como ley *antibullying*.

El otro tipo de acoso por internet al que hicimos referencia es el llamado *grooming*, que se refiere a lo siguiente:

> (…) las conductas y acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad, creando una conexión emocional con el mismo, con el fin de disminuir las inhibiciones del niño y poder abusar sexualmente de él. (Fernández Delpech, 2014, p. 213)

Uno de los medios más empleados por pedófilos y pederastas para llevar a cabo esta práctica aberrante son los *chats* de las redes sociales. En general, estos personajes abren cuentas en las redes sociales con perfiles falsos, simulando ser menores de edad para tomar contacto con menores, ganar su confianza y comenzar

el acoso mediante *chats* privados. Los someten emocionalmente para obtener imágenes o videos pornográficos de las víctimas, o bien intentan generar un encuentro real con ellas para abusar sexualmente.

> El proceso de grooming, comúnmente, puede durar semanas o incluso meses, variando el tiempo según la víctima y que suele pasar por las siguientes fases: 1) El adulto procede a entablar lazos emocionales (de amistad) con el menor. En algunos casos, a través de internet pueden simular ser otro niño o niña;
>
> 2) El adulto va obteniendo datos personales y de contacto del menor;
>
> 3) Utilizando tácticas como la seducción, la provocación, el envío de imágenes de contenido pornográfico, consigue finalmente que el menor se desnude o realice actos de naturaleza sexual. Entonces puede iniciarse el acoso, chantajeando a la víctima para obtener cada vez más material pornográfico o tener un encuentro físico con el menor para abusar sexualmente de él. (Schneider, 2014, p. 212)

En Argentina, la Ley N° 26.904, sancionada en 2013, incorporó al Código Penal la figura del *grooming* en el artículo 131, en los siguientes términos:

> Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.[6]

A nivel jurisprudencial, en un caso de 2014, una persona mayor de edad arribó al país para encontrarse con una menor de 14 años, con quien mantenía una relación virtual a través de Facebook y WhatsApp. La menor abandonó su hogar y se dirigió hacia donde se alojaba el adulto y allí mantuvieron relaciones íntimas. El juez lo procesó por los delitos de estupro y *grooming*. La Cámara mantuvo la decisión solo respecto del estupro, dado que quien mantuvo conversaciones inapropiadas con una

[6] Artículo 131, Ley N.° 26.904 (2013), incorporación a la Ley N.° 26.388 (2008). Código Penal de la Nación Argentina. Honorable Congreso de la Nación Argentina.

menor a través de redes sociales y la involucró en actividades de alto contenido erótico no puede ser procesado por el delito de *grooming*, pues el contacto entre ellos se inició cuando todavía no había sido dictada la ley 26.904.

En otro caso resuelto de 2013 (Tribunal en lo Criminal N.° 1 de Necochea, Buenos Aires, F., L. N. s/ corrupción de menores agravada, 5 de junio de 2013, recuperado de https://aldiaargentina.microjuris.com/2013/07/30/grooming-condena-al-imputado-quien-se-contactaba-con-una-menor-mediante-internet-acosandola-y-enviando-material-de-contenido-sexual/), los padres de una menor denunciaron que su hija había recibido mensajes instantáneos con contenido sexual y lenguaje obsceno en su dirección de correo electrónico. Luego se confirmó que había recibido correos en los cuales se adjuntaron fotografías de menores realizando actividades sexuales explícitas. El Tribunal en lo Criminal condenó al imputado a la pena de prisión por el delito de promoción de la corrupción de menor agravada por la edad de la víctima y su comisión mediante engaño (Reuters, 2016).

En ese marco, la doctrina sentó que:

> El *grooming* debe ser definido como un proceso abusivo, facilitado por el uso de las nuevas tecnologías, que implica la interacción comunicacional de un adulto con un menor, a través del despliegue de una conducta deliberada para captar su atención y confianza, con el objeto de obtener imágenes sexuales o lograr un encuentro sexual. (Tribunal en lo Criminal N.° 1 de Necochea, Buenos Aires, F., L. N. s/ corrupción de menores agravada, 5 de junio de 2013, recuperado de https://aldiaargentina.microjuris.com/2013/07/30/grooming-condena-al-imputado-quien-se-contactaba-con-una-menor-mediante-internet-acosandola-y-enviando-material-de-contenido-sexual/)

También traemos a colación el resonado caso de 2012, que tuvo mucha repercusión mediática, ocasión en la que una maestra sanjuanina fue descubierta en el momento en que estaba por tener sexo con un alumno suyo menor de edad, luego de haberlo acosado por Facebook e incitado para que tuvieran un encuentro íntimo. Los padres supieron del hecho, por la advertencia de compañeros del menor de edad, e hicieron la correspondiente denuncia policial. La policía actuó a tiempo y detuvo a la maestra.

3.1.3 Calumnias e injurias

En el módulo 1, decíamos que uno de los aspectos más críticos del *social media* es el de intimidad o privacidad de las personas, dado que el surgimiento de internet y el auge de las redes sociales, blogs, foros, etcétera, sumados a la casi omnipresencia de los dispositivos móviles, han corrido notablemente la línea entre lo público y lo privado y han generado una exposición pública nunca vista en la historia. Vimos toda la problemática relacionada con el uso del social media y la afectación de la intimidad y privacidad de las personas y repasamos algunos casos que han resuelto los tribunales de justicia en nuestro país.

Sin duda, otro de los aspectos críticos del *social media*, que está emparentado con lo anterior, es el del honor de las personas. En efecto, una de las características salientes del *social media* -y que lo diferencia de manera sustancial con los medios tradicionales de expresión y comunicación- es que ha posibilitado que cualquier persona que cuente solamente con un dispositivo con conexión a internet, se convierta en productor de contenidos y no meramente en consumidor, como sucedía en la época de los medios tradicionales o analógicos (radio, periódico, revistas, televisión). Incluso, hoy en día se habla de *prosumers/prosumidores* para hacer referencia justamente a los usuarios de la web 2.0, que son consumidores y productores de contenidos al mismo tiempo.

Vimos que estos avances han ampliado enormemente las posibilidades de expresarse e informarse, lo cual sin dudas es muy positivo. Pero también conlleva riesgos. Y uno de ellos es que muchas personas creen que por el solo hecho de tener un blog, una cuenta abierta en una red social o estar registrados en un foro pueden decir lo que quieran, respecto de quienes quieran y ante quienes quieran, sin consecuencias de ningún tipo. Pueden hablar mal públicamente de una persona, afectar su honra, buen nombre, crédito o fama libremente, dado que la tecnología les da la posibilidad. Es así como vemos proliferar en las redes sociales, por ejemplo, contenidos injuriantes o difamatorios, insultos, agresiones, etcétera, proferidas por un particular hacia otro particular o hacia personas públicas. Esto nos lleva al tema de la vigencia y alcance del derecho al honor en el *social media* y a sus correspondientes conductas atentatorias, a saber: las injurias y calumnias.

El honor puede ser definido como el conjunto de cualidades valiosas atribuibles a una persona. En ese sentido, presenta dos aspectos claramente diferenciables:

1. **Subjetivo:** refiere al juicio que cada persona se forma sobre sí misma, sobre su propia dignidad y, en este sentido, se habla del honor en cuanto **autovaloración**, porque es el propio sujeto el que se atribuye esas cualidades valiosas.

2. **Objetivo:** refiere al juicio que las demás personas se forman sobre otra y, en este sentido, se habla del honor en cuanto **crédito**, **fama** o **reputación**,

> dado que es la comunidad la que le atribuye a una persona determinadas cualidades valiosas.

Huelga decir que las posibilidades de afectar el honor subjetivo en las redes sociales son mucho mayores que las de afectar el honor objetivo, porque es muy difícil conocer cuál es la valoración que tiene de sí mismo cada uno de nuestros contactos, seguidores o amigos en una red social, más aún en los casos de quienes utilizan estos medios sin restricciones en cuanto al círculo de personas que conforman su red de contactos.

Otra cuestión que es preciso tener en cuenta es que el grado de afectación del honor no es el mismo si se trata de personas públicas o notorias que si se trata de particulares, atento a que, tal como lo ha resuelto la Corte Suprema de Justicia de la Nación:

> (…) las personas 'comunes' son más vulnerables que los funcionarios públicos o las celebridades (modelos, actores, etcétera), puesto que estos últimos tienen mayor acceso a los medios periodísticos para replicar las falsas imputaciones. Esto hace que los particulares necesiten una amplia tutela frente a los ataques a su reputación, dando lugar a la llamada 'protección fuerte del ciudadano común', frente a la 'protección débil del funcionario público. (Vibes, 2013).

El honor puede ser afectado por dos tipos de conductas ilícitas:

1. **Injurias**: son conductas consistentes en ofensas genéricas al honor. Por ejemplo, decirle a otro que es un tonto, ingrato, aprovechador, insensible, feo y, en general, imputaciones que atribuyen al afectado cualidades no valiosas y genéricas, que no constituyen un delito penal. En el ámbito de las redes sociales este tipo de conductas es moneda corriente.

2. **Calumnias:** son injurias especializadas por el tipo de imputación u ofensa que consisten en la falsa atribución al ofendido de haber cometido un delito tipificado por la ley penal que dé lugar a la acción penal pública; por ejemplo, atribuirle a una persona haber cometido un robo de determinado objeto, propiedad de determinada persona en determinada fecha y lugar. En el ámbito de las redes sociales, este tipo de conductas no es tan frecuente entre particulares, aunque se han presentado casos que han sido resueltos por los tribunales. Pero, en materia de atribución de conductas delictivas a funcionarios públicos, es una práctica casi

cotidiana por parte de particulares que, desde sus cuentas personales, atribuyen a políticos haber cometido delitos de toda naturaleza.

En nuestra legislación, el honor tiene resguardo tanto desde un punto de vista civil, como penal. Así, el Nuevo Código Civil y Comercial dispone en su artículo 1740:

> Reparación plena. La reparación del daño debe ser plena. Consiste en la restitución de la situación del damnificado al estado anterior al hecho dañoso, sea por el pago en dinero o en especie. La víctima puede optar por el reintegro específico, excepto que sea parcial o totalmente imposible, excesivamente oneroso o abusivo, en cuyo caso se debe fijar en dinero. En el caso de daños derivados de la lesión del honor, la intimidad o la identidad personal, el juez puede, a pedido de parte, ordenar la publicación de la sentencia, o de sus partes pertinentes, a costa del responsable.[7]

Es decir, en caso de lesiones al honor de las personas, el damnificado podrá solicitar la reparación plena del daño, así como la publicación de la sentencia a cargo del responsable del daño.

En el ámbito penal, el Código Penal tipifica como delictivas tanto las injurias como las calumnias en el título: delitos contra el honor. El artículo 110 tipifica la figura básica de la injuria en los siguientes términos:

> El que intencionalmente deshonrare o desacreditare a una persona física determinada será reprimido con multa. En ningún caso configurarán delito de injurias las expresiones referidas a asuntos de interés público o las que no sean asertivas. Tampoco configurarán delito de injurias los calificativos lesivos del honor cuando guardasen relación con un asunto de interés público[8].

Por su parte, la calumnia está regulada en el artículo 109, que dispone:

---

[7] Art. 1740- Ley N° 26.994 (2014). Código Civil y Comercial de la Nación. Honorable Congreso de la Nación Argentina.

[8] Art. 110- Ley N° 26.388 (2008). Código Penal de la Nación Argentina. Honorable Congreso de la Nación Argentina.

> La calumnia o falsa imputación a una persona física determinada de la comisión de un delito concreto y circunstanciado que dé lugar a la acción pública, será reprimida con multa de pesos tres mil ($ 3.000) a pesos treinta mil ($ 30.000). En ningún caso configurarán delito de calumnia las expresiones referidas a asuntos de interés público o las que no sean asertivas.[9]

Finalmente, destacamos el artículo 113, que puede ser de aplicación en el entorno del *social media*, especialmente en las redes sociales, dada la facilidad que tienen los usuarios de republicar en sus cuentas lo publicado por otros usuarios:

> El que publicare o reprodujere, por cualquier medio, injurias o calumnias inferidas por otro, será reprimido como autor de las injurias o calumnias de que se trate, siempre que su contenido no fuera atribuido en forma sustancialmente fiel a la fuente pertinente. En ningún caso configurarán delito de calumnia las expresiones referidas a asuntos de interés público o las que no sean asertivas.[10]

Está claro que estos delitos pueden ser cometidos en las redes sociales, blogs, sitios webs o foros de Internet, atento a que la norma penal no limita su comisión a un medio determinado, más aún si tenemos en cuenta que estas normas fueron modificadas en 2009, es decir, con posterioridad a la sanción de la Ley N° 26.388, razón por la cual si el legislador hubiera considerado que los tipos penales estaban limitados a un determinado medio, no comprensivo de internet, seguramente hubiera agregado esa aclaración.

3.1.4 Otros delitos en el entorno *online*

El *social media* es un caldo de cultivo para la comisión de ilícitos y delitos de distintas naturalezas. Ya no nos sorprende ver en los noticieros informes sobre nuevas modalidades delictivas vinculadas al uso de blogs, sitios webs y redes sociales, como pueden ser el acoso de menores de edad, la propagación de *software* malicioso (virus informáticos), las injurias y calumnias o la violación de los derechos de

[9] Artículo 109- Ley N° 26.388. Op. cit.
[10] Artículo 113- Ley N.° 26.388. Op. cit.

propiedad intelectual vinculados a la subida y descarga de videos, música, libros o imágenes protegidas por las leyes.

Podríamos decir que en el ámbito del *social media* hay tantas modalidades delictivas como usos posibles de estas tecnologías o como las hay en el mundo real. Pero es importante dejar claro que desde un principio, por más nombres que pongamos a los ilícitos y aunque presenten particularidades vinculadas al propio avance de las tecnologías, en materia penal rigen algunos principios fundamentales:

- **Principio de legalidad:** es el famoso principio **no hay delito sin ley previa**, de modo que por más aberrante que pueda ser una conducta, por más reprochable que puede llegar a ser desde el punto de vista moral o social, si una ley previa al hecho no dispone expresamente que esa conducta es un delito, entonces no lo es.

- **Reserva:** todo lo que no está expresamente prohibido por la ley está permitido.

- **Tipificación:** justamente, la ley penal tiene que tipificar esa conducta, es decir, establecer claramente el hecho y las condiciones que deben darse para que una conducta sea delictiva. Por ejemplo, que sea realizada con dolo, a sabiendas, ilegítimamente, etcétera.

- **Prohibición de la analogía**: aunque una conducta sea parecida en aspectos relevantes con otra conducta que está tipificada como delictiva, si la ley no la tipifica expresamente, entonces no constituirá un ilícito penal.

- **Territorialidad**: aun cuando internet no tiene límites territoriales y trasciende todas las fronteras físicas, la legislación en general y en particular la legislación penal, son territoriales. De manera que una conducta puede ser ilícita en un país y lícita en otro, por más que dos personas que están a pocos kilómetros de distancia entre sí hayan realizado exactamente el mismo acto.

Por ende, a la hora de hablar de los ilícitos en el ámbito del *social media*, lo primero que tenemos que hacer es determinar qué conductas están tipificadas como delitos por la legislación penal, en concreto, por la legislación penal argentina.

Otro punto que se debe tener en cuenta es que hay delitos que pueden ser cometidos tanto en el mundo real como en internet, mientras que otros son propios de internet o, más precisamente, de las tecnologías informáticas.

Respecto de los primeros, internet solamente es un medio más para su comisión, mientras que en relación al segundo tipo, internet se convierte en la plataforma

indispensable para su comisión. Por ejemplo, una persona puede injuriar a otra a través de cualquier medio idóneo para hacerlo, incluyendo las redes sociales, páginas webs, blogs, foros, etcétera, mientras que el llamado *phishing* o la violación de una comunicación electrónica solamente pueden ser cometidos a través de internet.

Para la primera categoría de delitos bastan las leyes penales tradicionales que son de plena aplicación en el ámbito de internet, mientras que para la segunda hace falta una legislación específica. En ese sentido, debemos decir que hasta la sanción en 2008 de la Ley N° 26.388, conocida como Ley de Delitos Informáticos, no había en Argentina normas penales que tipificaran expresamente a los denominados delitos informáticos, aunque eso no implicaba que no se aplicaran normas penales tradicionales, como por ejemplo, las de la Ley de Propiedad Intelectual, o las normas del Código Penal, en la medida en que tipifican delitos susceptibles de llevarse a cabo en el ámbito de internet, o el caso de injurias. Por entonces, los jueces tenían criterios dispares a la hora de aplicar los tipos penales tradicionales a las nuevas modalidades de comisión de ilícitos en internet.

La Ley N° 26.388 incorporó al Código Penal varias normas que abarcan algunas de las modalidades delictivas presentes en el *social media*. Posteriormente, en 2013 fue sancionada la Ley N° 26.904 que como vimos, incorporó al Código Penal la figura del *grooming*. En consecuencia, podríamos decir que el marco normativo en materia de ilícitos en las redes sociales está dado por las figuras incorporadas al Código Penal por las leyes mencionadas y por aquellas que tipifican conductas susceptibles de cometerse en cualquier ámbito (como las injurias), aunque se está trabajando a nivel legislativo a los fines de incorporar otras figuras que quedaron fuera de la regulación legal como por ejemplo, el robo de la identidad digital.

Veamos, entonces, algunas de las figuras incorporadas por las mencionadas leyes con ejemplos de posibles ilícitos en las redes sociales:

a. **Pornografía infantil:** es un delito tipificado por el artículo 128 del Código Penal, luego de la reforma de la Ley N° 26.388.

> Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales. [11]

[11] Art. 128- Ley N°26.388 (2008). Código Penal. Modificación. Honorable Congreso de la Nación.

> También se especifica el castigo por el empleo de cualquier medio, incluidas las nuevas tecnologías, entre ellas, las redes sociales. Se prevé una pena de prisión de 6 meses a 4 años.
>
> Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descritas en el párrafo anterior con fines inequívocos de distribución o comercialización.[12]

Es importante notar que no se castiga la mera posesión de material con pornografía infantil, como en otros países, sino solamente cuando se la tiene con fines inequívocos de distribución o comercialización. En materia de redes sociales, esta figura puede estar asociada al delito de *grooming*, en la medida en que muchos casos el acosador se acerca al menor de edad a través de un perfil falso y luego procura que el menor le envíe imágenes o videos con contenido sexual que, muy probablemente, debido al tipo de perfil psicológico de los pedófilos y pederastas, terminan divulgando a otros delincuentes.

b. **Violación de comunicaciones electrónicas:** se trata de un delito tipificado por los artículos 153 y 155 del Código Penal, luego de la reforma de la Ley N° 26.388 (2008). La nueva normativa tipifica como delitos la violación, apoderamiento y desvío de comunicación electrónica y la publicación de la misma. Para estas figuras, prevé penas de prisión de 15 días a 1 año, en tanto que para el caso del delito de publicación de una comunicación electrónica, una multa de $1500 a $100.000. Está claro que las comunicaciones que realizan los usuarios en el ámbito del *social media* encuadran perfectamente en el concepto de comunicación electrónica. Es importante tener en cuenta que cuando las comunicaciones están abiertas al público en general, quien acceda a ellas no cometerá el delito en cuestión, sin perjuicio de que el empleo que posteriormente haga de esa información pueda configurar otro delito. Por ello, cobra relevancia para los usuarios determinar qué comunicaciones quieren hacer públicas y cuáles no, antes de publicar información en alguna de las redes sociales. Un caso muy común en las redes sociales es la publicación de *chats* privados mantenidos con otro usuario, sobre todo cuando se trata de *chats* en los que hay insultos o agravios. El canal del *chat* tiene la característica de ser privado, justamente porque es una comunicación exclusiva entre quienes participan allí, de modo que la publicación de esas conversaciones podría encuadrar en el tipo del artículo 155:

[12] Art. 128- Ley N°26.388. Op. cit.

> (…) el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros[13].

c. **Acceso a un sistema informático (*hacking*):** se trata de un delito tipificado por el artículo 153 bis del Código Penal, luego de la reforma de la Ley N° 26.388.

> Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.[14]

Muchas veces el acceso a un sistema informático es el paso previo para la comisión de otros delitos o simplemente, sirve a los efectos de extraer información valiosa almacenada en el sistema al que se accede. En este sentido, es importante tener en cuenta que la propia interacción en las redes sociales, así como la exposición pública de información, puede facilitarles a los *hackers* el acceso a los sistemas del usuario de la red social, tal como vimos en el video de impacto socio-productivo.

Tanto la implementación de medidas de seguridad tecnológicas como la conciencia y responsabilidad en la administración de la información personal son mecanismos muy útiles para prevenir estos ataques.

Destacamos un caso resuelto en 2014 (disponible en http://dpicuantico.com/sitio/wp-content/uploads/2015/03/Tecnolog%C3%ADa-Jurisprudencia-2015-03-11.pdf), en el que una abogada denunció a su expareja, abogado también, aduciendo que este había accedido ilegítimamente a la

[13] Art. 155- Ley N° 26.388. Op. cit.
[14] Art. 153 bis- Ley N° 26.388. Op. cit.

información de su muro en Facebook, a través de la colaboración que le había prestado su hermana, con el fin de ofrecer aquella información como prueba en el juicio de divorcio que la abogada había promovido en su contra, al argumentar que la conducta encuadraba en el delito regulado en el artículo 153 bis del Código Penal.

Los imputados fueron sobreseídos. La denunciante recurrió al sobreseimiento hasta que la causa llegó al Tribunal Superior de Justicia de la ciudad de Buenos Aires, que rechazó el recurso, sosteniendo que:

> (…) el sobreseimiento de los imputados por la intrusión a un sistema o dato informático de acceso restringido por manifiesta atipicidad no es arbitrario si fue fundado en que la usuaria de una red social voluntariamente compartió su información y, así, aceptó exponer una parte de su privacidad al difundir ciertos datos personales -como fotos y comentarios- a través de Internet, por cuanto no cumpliría con el requisito típico de acceso sin la debida autorización, puesto que uno de sus contactos -"amigo" de Facebook- al cual se le permitía acceder a los datos, los facilitó a quien no tenía ese permiso, todos ellos argumentos razonables y suficientes para sustentarla. (Reuters, 2016)

d. **Fraude informático:** delito tipificado por el artículo 173, inciso 16 del Código Penal, luego de la reforma de la Ley N° 26.388, figura que vimos al analizar el *phishing*, que es una modalidad de fraude informático, aunque no la única. La Ley de Delitos Informáticos también ha introducido la figura de la defraudación "mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos"[15]. En este caso se prevé una pena de prisión de 1 mes a 6 años. El apoderamiento de datos relacionados con cuentas bancarias o tarjetas de crédito o débito es una de las modalidades más frecuentes de estafa informática. Los medios van desde las técnicas de ingeniería social hasta el mencionado *phishing*. En este sentido, cobran relevancia las medidas que puedan adoptar los usuarios de redes sociales, tanto respecto de las personas con quienes intercambian información (los contactos dentro de la

[15] Art. 173, inciso 16- Ley Nº 26.388. Op. cit.

red), como respecto de los sitios a los que acceden por invitación de otro usuario o la información que dejan en esos sitios.

e. **Daño informático:** delito tipificado por los artículos 183 y 184 del Código Penal, luego de la reforma de la Ley N°26.388. Dicha ley sanciona a quien: "(…) alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos, o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños"[16].

Se prevé una pena de prisión de 15 días a 1 año, que aumenta a prisión de 3 meses a 4 años cuando la acción se ejecuta en datos, documentos, programas o sistemas informáticos públicos o en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

En esta figura, encuadran los virus informáticos, que son programas de computación destinados a causar daños, aunque no encuadraría el *spyware*, salvo que este cause un daño o esté destinado a causarlo. Es interesante destacar que la ley contempla el caso de quien daña un dato, documento, programa o sistema informático, así como el de quien comercializa, distribuye, hace circular o introduce un virus en un sistema informático, aun cuando no se produzca ningún daño en el sistema infectado.

Las redes sociales son propicias para este tipo de accionar, dado que el intercambio de archivos o la descarga de material subido por los usuarios pueden involucrar casos de virus informáticos. Medidas relacionadas con la precaución a la hora de abrir o descargar material, así como contar con antivirus y *firewalls* auténticos y debidamente actualizados, ayudan a prevenir este tipo de ataques. (Bruera, 2009, http://www.informaticalegal.com.ar/2009/12/26/%C2%BFcuales-son-los-delitos-informaticos-que-se-pueden-cometer-por-facebook/)

[16] Art. 183- Ley N° 26.388. Op cit.

Unidad 3.2 Jurisprudencia de interés

3.2.1 Caso Taringa

El caso Taringa ha sido el más resonante en Argentina en materia de violación de los derechos de propiedad intelectual en internet. La causa tuvo su origen en una denuncia presentada por la Cámara Argentina del Libro contra los responsables del sitio de *linksharing* Taringa, alegando que estos facilitaban a los usuarios de la plataforma la posibilidad de publicar hipervínculos a diferentes contenidos, algunos de los cuales eran obras protegidas de titularidad de sus representados (libros jurídicos y de informática). También les proporcionaban un buscador que permitía ubicar los hipervínculos de los contenidos demandados por los usuarios, lo cual facilitaba, de ese modo, la violación de los derechos de propiedad intelectual.

El juez decretó el procesamiento de los imputados como partícipes necesarios en la comisión del delito del artículo 72 de la Ley de Propiedad Intelectual, que vimos en el módulo 3. Los denunciados apelaron el procesamiento. En abril de 2011, la Cámara Nacional de Apelaciones en lo Criminal y Correccional, sala VI, confirmó el procesamiento argumentando que:

Los imputados, a través de su sitio, permitían que se publiciten obras que, finalmente, eran reproducidas sin consentimiento de sus titulares y que, aunque eso ocurría a través de la remisión a otro espacio de internet, lo cierto es que, justamente, tal posibilidad la brindaba su servicio. (Cámara Nacional de Apelaciones en lo Criminal y Correccional (2015). Botbol Hernán y otros s/ sobreseimiento, sala V, MJ-JU-M-92305-AR | MJJ92305 | MJJ92305. Disponible en https://aldiaargentina.microjuris.com/2015/06/05/sobreseimiento-de-responsables-del-portal-taringa-por-reproduccion-sin-autorizacion-de-obras-de-borges/).

Agregó, que si bien los autores del hecho finalmente serían los usuarios que subieron la obra al *website* y los que la bajan, lo cierto es que el encuentro de ambos obedece a la utilización de la plataforma Taringa, por cuanto sus responsables son, al menos, "partícipes necesarios de la maniobra y, además, claros conocedores de su ilicitud" (Cámara Nacional de Apelaciones en lo Criminal y Correccional (2015). Botbol Hernán y otros s/ sobreseimiento, sala V, MJ-JU-M-92305-AR | MJJ92305 | MJJ92305. Recuperado de https://aldiaargentina.microjuris.com/2015/06/05/sobreseimiento-de-responsables-del-portal-taringa-por-reproduccion-sin-autorizacion-de-obras-de-borges/).

El segundo episodio de Taringa en la justicia tuvo lugar en 2015, cuando María Kodama, viuda y heredera del escritor Jorge Luis Borges, presentó una denuncia

contra los responsables del sitio por violación de la propiedad intelectual cuando el sitio publicó los hipervínculos a las obras completas del escritor. A diferencia del caso anterior, el juez dictó el sobreseimiento de los denunciados. Kodama apeló y la Cámara confirmó el sobreseimiento argumentando que:

> Los contenidos cuestionados se ubicaban a través de links direccionados por las páginas denunciadas es decir que no eran parte del contenido de estas, sino material ajeno, por lo que no se verifica una conducta positiva de reproducción ilegítima de obra ajena ni una violación al deber objetivo de cuidado, no existiendo una obligación de verificar ex ante el material de intercambio, sino posteriormente cuando este es denunciado, lo que ocurrió en el caso donde contenidos en cuestión fueron dados de baja… [y que, por otra parte] las ganancias, producto de la publicidad referenciadas por el recurrente, no constituyen en una eventual maniobra defraudatoria el desplazamiento patrimonial requerido por la norma, en tanto lo que la víctima -titular de los derechos de propiedad intelectual- sufre, en todo caso, es el lucro cesante por las sumas que en base al derecho de autor se habrían dejado de percibir por el acceso gratuito habilitado. (Cámara Nacional de Apelaciones en lo Criminal y Correccional, 5 de mayo de 2015, Botbol Hernán y otros s/ sobreseimiento, sala V, https://aldiaargentina.microjuris.com/2015/06/05/sobreseimiento-de-responsables-del-portal-taringa-por-reproduccion-sin-autorizacion-de-obras-de-borges/)

En definitiva, claramente se puede ver que, en nuestro país, aún no está definida la responsabilidad de sitios web de *linksharing* -como efectivamente es el caso de Taringa- en materia de violaciones a los derechos de propiedad intelectual.

3.2.2 Google y las modelos

Sin duda alguna, uno de los temas más controvertidos respecto a internet, fue el de la afectación de la imagen y honor de las modelos a partir de la práctica de utilizar sus imágenes para promocionar sitios web de contenido erótico o pornográfico.

La utilización de imágenes de modelos famosas por parte de los mencionados sitios web tiene un claro propósito promocional y lucrativo: captar la atención de los visitantes bajo el supuesto de que efectivamente en estos sitios encontrarán

contenido erótico o pornográfico de modelos, lo cual genera mayor tráfico, con el consecuente beneficio económico o de posicionamiento en la web.

Ahora bien, en general, esos sitios son anónimos, razón por la cual se hace muy difícil denunciar esas prácticas y reclamar el cese de esa utilización ilícita y la consecuente indemnización por los daños y perjuicios ocasionados a las víctimas, el cual es ostensible atento a que son personas cuya imagen constituye su herramienta de trabajo, además claro está, de la afectación de su honor.

Esto nos retrotrae a la temática analizada en el módulo 3 respecto del uso de imágenes de terceros y la afectación de los derechos a la imagen y a la intimidad. Allí habíamos dicho que el uso no autorizado de la imagen de un tercero viola el derecho a la imagen, protegido por el artículo 31 de la Ley N°11.723, pero que eventualmente, podría afectar otros derechos como la intimidad o el honor que son derechos personalísimos.

Ante la dificultad de denunciar y demandar a los responsables de los mencionados sitios eróticos o pornográficos, la opción es ir contra los motores de búsquedas, a los efectos de que bloqueen el acceso a los mencionados sitios cuando un usuario realice una búsqueda de la persona en cuestión y, eventualmente, reclamar los daños y perjuicios, en caso de que los buscadores no respondan al reclamo efectuado.

Entonces, surge la cuestión de si los buscadores son responsables y qué tipo de responsabilidad tienen:

1) Objetiva: responden por el riesgo de la cosa.

2) Subjetiva: responden solamente por culpa o dolo.

Recordemos también que a diferencia de otros países, Argentina no tiene legislación interna que implemente los tratados de la OMPI (Organización Mundial de la Propiedad Intelectual) sobre internet, con toda la legislación sobre puertos seguros (*safe harbours*).

Y bien, el caso es que muchas modelos argentinas famosas demandaron ante la justicia a Google y Yahoo! por no haber bloqueado el acceso a sitios eróticos o pornográficos que usaban ilícitamente sus imágenes y, por tanto, afectaban su derecho a la imagen y su honor.

El *leading case* en la materia fue resuelto por la Corte Suprema de Justicia de la Nación en 2014.

La modelo había interpuesto una demanda de daños y perjuicios contra Google Inc. (la cual amplió posteriormente contra Yahoo! de Argentina SRL), argumentando que:

> (…) se había procedido al uso comercial y no autorizado de su imagen y que, además, se habían avasallado sus derechos personalísimos al habérsela vinculado a determinadas páginas de Internet de contenido erótico y pornográfico. Pidió también el cese del mencionado uso y la eliminación de las señaladas vinculaciones. (CSJN, Buenos Aires, Rodríguez, María Belén c/Google Inc. s/daños y perjuicios, sentencia del 28 de octubre del 2014, Fallos 401)

El juez de primera instancia hizo lugar a la demanda y consideró que: "las demandadas habían incurrido en negligencia culpable "al no proceder a bloquear o impedir de modo absoluto la existencia de contenidos nocivos o ilegales perjudiciales a los derechos personalísimos de la actora, a partir de serles comunicada la aludida circunstancia" (CSJN, Buenos Aires, Rodríguez, María Belén c/Google Inc. s/daños y perjuicios, sentencia del 28 de octubre del 2014, Fallos 401)

De allí deriva la condena a Google y a Yahoo! por parte del juez de primera instancia a pagar una indemnización y, además, dispuso también "la eliminación definitiva de las vinculaciones del nombre, imagen y fotografías de la actora con sitios y actividades de contenido sexual, erótico y pornográfico" (CSJN, Buenos Aires, Rodríguez, María Belén c/Google Inc. s/daños y perjuicios, sentencia del 28 de octubre del 2014, Fallos 401).

El fallo fue apelado y la Cámara Nacional de Apelaciones en lo Civil lo revocó parcialmente, rechazando el reclamo contra Yahoo! y admitiéndolo contra Google, aunque, en este último caso, redujo la indemnización y dejó sin efecto la sentencia de primera instancia en cuanto este disponía la eliminación de las mencionadas transcripciones. La cámara encuadró la eventual responsabilidad de los llamados motores de búsqueda (como Google y Yahoo!) en el ámbito de la responsabilidad subjetiva y descartó que pudiera aplicarse responsabilidad objetiva basada en el riesgo de la cosa. Por otra parte, atento a que la modelo no había intimado extrajudicialmente a las demandadas, sino que, por el contrario, había pedido y obtenido directamente medidas cautelares, no se podía achacar negligencia en el accionar de los motores de búsqueda. No obstante, Google fue condenado en el tema relativo a los llamados *thumbnails* (son las versiones en miniatura de las imágenes) que contenían la imagen de la actora, por entender que Google debió haber requerido el consentimiento de aquella, de acuerdo con lo impuesto por el artículo 31 de la Ley N°11.723.

El caso llegó finalmente a la Corte Suprema de Justicia que, en fallo dividido, confirmó la sentencia de la cámara. Los argumentos dados por la mayoría de los vocales, en términos reducidos, fueron los siguientes:

En el caso no se trata de la responsabilidad atribuible a una página de Internet por la indebida publicación o reproducción de imágenes, sino a un mero intermediario, cuya única función es servir de enlace con aquella. En suma, los buscadores son intermediarios, no editores de contenidos.

Los motores de búsqueda responden civilmente por el contenido que les es ajeno, pero conforme a la responsabilidad subjetiva, es decir, solamente después de que han tomado efectivo conocimiento de la ilicitud de ese contenido, si tal conocimiento no fue seguido de un actuar diligente. Sería la aplicación de la doctrina del *safe harbour* al ámbito jurisprudencial argentino.

A los efectos del efectivo conocimiento requerido para responsabilizar en forma subjetiva a un buscador de Internet por los contenidos que le son ajenos, si la naturaleza ilícita de estos es palmaria y resulta directamente de consultar la página web, basta con una comunicación fehaciente del damnificado o, según el caso, de cualquier persona, sin requerir ninguna otra valoración ni esclarecimiento. Pero, en los casos en que el contenido dañoso importe eventuales lesiones al honor o de otra naturaleza que exijan un esclarecimiento en sede judicial o administrativa, corresponde exigir la notificación judicial o administrativa competente. En suma, dependiendo del caso en cuestión, se puede exigir al buscador que actúe ante una mera denuncia o pedido informal o será necesaria una actuación administrativa o judicial.

La sentencia que dejó sin efecto el pronunciamiento que dispuso la eliminación definitiva de las vinculaciones del nombre, la imagen y las fotografías de una modelo con sitios y actividades de contenido sexual, erótico y pornográfico a través del buscador de Internet demandado, para que no puedan ser utilizadas en el futuro, debe ser confirmada, pues toda restricción en la materia tiene una fuerte presunción de inconstitucionalidad. Es decir, tiene plena vigencia la garantía constitucional de la libertad de expresión y toda medida que esta restrinja debe ser interpretada restrictivamente. (CSJN, Rodríguez, María Belén c/Google Inc. s/daños y perjuicios, sentencia del 28 de octubre del 2014, Fallos 401)

Posteriormente, la corte se ha expresado en el mismo sentido en otros casos, remitiendo a los argumentos dados en el caso Rodríguez, como por ejemplo, en el caso Virginia Da Cunha con Yahoo! de Argentina SRL y otros daños y perjuicios, el cual fue resuelto por la Corte Suprema de Justicia de la Nación Argentina el 30 de diciembre de 2014.

3.2.3 Facebook y libertad de expresión

Traemos nuevamente a colación el fallo sobre la materia anteriormente reseñado. En el caso, el denunciante solicitó:

> (…) una medida autosatisfactiva para que se le ordene a Facebook Argentina SRL, sobre la cuenta en dicha red social bajo el dominio o titular, la inmediata "eliminación, supresión o retiro de todo contenido o datos referidos al Instituto Médico Modelo Sociedad Anónima y sus diversas acepciones o referencias, así como el bloqueo, baja y cierre definitivo de dicha cuenta, imponiendo adicionalmente que se abstenga de habilitar el uso de enlaces, blogs, foros o grupos que injurien y lesionen la imagen, marca, identidad comercial y empresarial de la razón social reclamante.
>
> (…) Relata que allí se difunden y publican acusaciones relacionadas con los servicios médicos que se brindan, que son infundadas e irrazonables y lesionan la imagen, reputación y trayectoria médica y comercial de la empresa. (Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Buenos Aires, Instituto Médico Modelo S.A. c/ Facebook Argentina S.R.L. s/ medida autosatisfactiva, 18 de junio de 2014, fallo 654)

Agregó, además, que "el derecho a la libre expresión no es absoluto, puesto que encuentra una frontera cuando colisiona con otros derechos: la reputación y la imagen" (Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Buenos Aires, Instituto Médico Modelo S.A. c/ Facebook Argentina S.R.L. s/ medida autosatisfactiva, 18 de junio de 2014, fallo 654).

El juez rechazó la medida y la Cámara de Apelaciones confirmó la decisión. En lo que respecta al tema de nuestro interés, la cámara señaló que:

> La naturaleza de los derechos involucrados exige una precisa determinación de los intereses en juego. Es que para decidir acerca de la medida solicitada, no cabe, en principio, equiparar los derechos personalísimos con los patrimoniales. Esto no implica que estos últimos no sean susceptibles de una tutela judicial precautoria, pero el juicio de valor que debe hacerse en tal supuesto es diferente, habida cuenta de que la tutela pretendida podría poner en tensión esos derechos con otros amparados en forma directa por la Constitución Nacional, como la libertad de expresión y de información de toda la sociedad. (Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Buenos Aires, Instituto Médico Modelo S.A. c/ Facebook Argentina S.R.L. s/ medida autosatisfactiva, 18 de junio de 2014, fallo 654)

Es decir, a la hora de evaluar este tipo de casos, hay que sopesar adecuadamente los derechos que están en juego y claramente, los derechos patrimoniales (por ejemplo, la imagen de una empresa) no están en un pie de igualdad con la libertad de expresión, máxime si no se había identificado al titular de la cuenta desde la cual se difamaba a la empresa.

En segundo lugar, el tribunal sostuvo que:

> Menos admisible aún resulta la pretensión de imponer a la demandada un control preventivo y discrecional para el futuro sobre la circulación de contenidos que eventualmente pudieran afectar los derechos de la actora, puesto que implica una restricción general y para el futuro, que podría comprometer la búsqueda, recepción y difusión de información e ideas, derecho garantizado por la Constitución Nacional y por la ley 26.032. (Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Buenos Aires, Instituto Médico Modelo S.A. c/ Facebook Argentina S.R.L. s/ medida autosatisfactiva, 18 de junio de 2014, fallo 654)

Es decir, no puede ordenarse a Facebook que censure preventivamente los contenidos publicados por los usuarios de la red social, dado que, como vimos, lo que rige es la responsabilidad ulterior por los daños que eventualmente pudieran derivar del ejercicio de la libertad de expresión (ver comentario a este caso en Molina Quiroga, 2014).

3.2.4 Jurisprudencia sobre agravios

Veamos ahora algunos casos jurisprudenciales referentes a agravios (injurias o calumnias) en el ámbito del *social media*. En un caso resuelto en 2009, el juez ordenó a Facebook:

> La suspensión cautelar de los discursos vertidos respecto de la actora que contengan procacidades y, de no ser posible obrar parcialmente, suprimirlos en su totalidad, ya que los calificativos utilizados en referencia a ella por algunos de los miembros del portal que se cuestiona aparecerían sin lugar a dudas directamente agraviantes de su derecho al honor, ofensivos incluso de personas de su familia y ello no puede justificarse. (Juzgado Nacional de Primera Instancia en lo Civil, Buenos Aires, L. R. I. c/ Facebook Incorporated s/ medidas precautorias, 2009)

Además, agregó que:

> El derecho de prensa radica en el reconocimiento de que todos los hombres gozan de la facultad de publicar sus ideas por la prensa sin el previo contralor de la autoridad, pero no de la subsiguiente impunidad de quien utiliza la prensa como un medio para cometer delitos y causar daños por culpa o negligencia, es por ello que un estricto equilibrio entre la libertad de expresión y el respeto a los derechos personalísimos lleva a ordenar la suspensión cautelar solicitada por la actora para suprimir los discursos vertidos sobre ella en el portal de internet cuestionado, pero limitada estrictamente a los contenidos alojados dentro de los comentarios de los participantes del grupo que importen improperios, no así los restantes. (Juzgado Nacional de Primera Instancia en lo Civil, Buenos Aires, L. R. I. c/ Facebook Incorporated s/ medidas precautorias, 6/10/2009 MJ-JU-M-59162-AR | MJJ59162 | MJJ59162)

En otro caso resuelto en 2012 (Juzgado Civil y Comercial, Formosa, B. C. c/ Facebook Argentina S.A. s/ medida autosatisfactiva, 2012), una mujer se presentó ante la justicia para requerir una medida autosatisfactiva contra Facebook Argentina SRL, donde solicitó de manera inmediata el bloqueo, cancelación o cierre

definitivo de una cuenta existente en esa red social debidamente individualizada. Además pidió que Facebook se abstuviera en el futuro a habilitar el uso de enlaces, blogs, foros, grupos, sitios de *fans*, que injurien, ofendan, agredan, vulneren, menoscaben o afecten la intimidad personal o la actividad comercial de su persona, alegando que en la mencionada página se atacaba su honor y el de su empresa.

En ese marco, se entendió que:

> (…) se ha lesionado el derecho al honor de la actora, el cual es entendido como uno de los principales bienes espirituales que el hombre siente, valora y sublima colocándolo dentro de sus más preciadas dotes. Es una cualidad moral del ánimo, que puede ser herida, sufrir menoscabo, y que suele ser defendida con el mismo ahínco, con la misma fuerza de quien se afana entre la vida y la muerte. (Juzgado Civil y Comercial, Formosa, B. C. c/ Facebook Argentina S.A. s/ medida autosatisfactiva, 2012)

El juez ordenó a Facebook:

> (…) la urgente e inmediata eliminación de todo contenido o datos referidos a la actora o a la empresa que administra, que obren insertos o publicados en el sitio referido en la demanda, debiendo asimismo la empresa demandada abstenerse en el futuro de habilitar el uso de enlaces, blogs, foros, grupos o sitios de fans, que injurien, ofendan, agredan, vulneren, menoscaben o afecten la intimidad personal y/o la actividad comercial de la reclamante. (Juzgado Civil y Comercial, Formosa, B. C. c/ Facebook Argentina S.A. s/ medida autosatisfactiva, 2012)

En otro caso resuelto en 2013 (Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Buenos Aires, V. J. O. y otro c/ Facebook Argentina S.R.L. s/ medida autosatisfactiva, 2013) el Secretario General de un sindicato solicitó una medida autosatisfactiva a fin de que se ordenara a Facebook Argentina SRL la inmediata cancelación de toda cuenta abierta o que se pretendiera abrir a nombre de una ex abogada del sindicato o su marido (hermano del Secretario General), como de cualquier cuenta asociada a los correos de titularidad de ellos, disponiendo la inmediata eliminación de los sitios que individualizaba y haciendo cesar y

abstenerse en el futuro de habilitar el uso de enlaces, blogs, foros, grupos, sitios de *fans* o cualquier otro espacio web de www.facebook.com en los que se injurie, difame, agreda, vulnere, ofenda, menoscabe, acose, intimide o afecte de cualquier manera, directa o indirectamente, el nombre, el honor, la imagen, la intimidad y la integridad del Secretario General o del sindicato.

El juez de primera instancia rechazó el pedido y la Cámara de Apelaciones confirmó la sentencia, ya que entendió que no se encontraba acreditada la verosimilitud del derecho, atento a que el peticionante de la medida:

> (…) funda la responsabilidad de la administradora de la red social demandada, como proveedora de los medios para difundir las expresiones que califica como dañosas, en las 'Normas Comunitarias' y en su inacción ante la denuncia formulada, pero no acreditó siquiera haber formulado reclamo alguno a la empresa contra la cual dirige su pretensión cautelar. (Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Buenos Aires, V. J. O. y otro c/ Facebook Argentina S.R.L. s/ medida autosatisfactiva, 2013)

Y que, adicionalmente,:

> Si bien la actora atribuye la autoría de los textos cuestionados solo a las personas de su hermano y cuñada, no se advierte óbice para que dirija su reclamo contra ellos, y ni siquiera los ha intimado extrajudicialmente a cesar en la conducta que considera que afecta sus derechos. (Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Buenos Aires, V. J. O. y otro c/ Facebook Argentina S.R.L. s/ medida autosatisfactiva, 2013)

Referencias

Álvarez de La Chica, F. (12 de agosto de 2010). *Boletín Oficial de la Junta de Andalucía - Histórico del BOJA*. Recuperado de http://www.juntadeandalucia.es/boja/2010/158/3.

Bruera, H. (2009) *¿Cuáles son los delitos informáticos que se pueden cometer por Facebook?* Recuperado de http://www.informaticalegal.com.ar/2009/12/26/%C2%BFcuales-son-los-delitos-informaticos-que-se-pueden-cometer-por-facebook/

Cámara Nacional de Apelaciones en lo Civil y Comercial Federal "Instituto Médico Modelo S.A. c/ Facebook Argentina S.R.L. s/ medida autosatisfactiva" (18 de junio de 2014). Fallo 654. Disponible en https://aldiaargentina.microjuris.com/2014/05/16/no-procede-el-bloqueo-de-una-cuenta-de-facebook-por-comentarios-difamatorios-si-no-se-identifica-al-usuario/.

Cámara Nacional de Apelaciones en lo Criminal y Correccional "Botbol Hernán y otros s/ sobreseimiento" (5 de mayo de 2015). MJ-JU-M-92305-AR | MJJ92305 | MJJ92305. Disponible en https://aldiaargentina.microjuris.com/2015/06/05/sobreseimiento-de-responsables-del-portal-taringa-por-reproduccion-sin-autorizacion-de-obras-de-borges/.

Corte Suprema de Justicia de la Nación "Rodríguez, María Belén c. Google Inc. s/ daños y perjuicios" (sentencia del 28 de octubre del 2014). Fallos 401. La Ley, 2014-F, 401, AR/JUR/50173/2014. Disponible en http://tuespaciojuridico.com.ar/tudoctrina/wp-content/uploads/2014/10/Fallo-Corte-buscadores-de-internet.pdf.

Decreto N° 1558/2001 (2001). *Protección de los datos personales*. Poder Ejecutivo Nacional.

Fernández Delpech, H. (2014). *Manual de derecho informático*. Buenos Aires: Abeledo Perrot.

Juzgado Nacional de Primera Instancia en lo Civil N° 46, Buenos Aires "L. R. I. c/ Facebook Incorporated s/ medidas precautorias", 6/10/2009. MJ-JU-M-59162-AR | MJJ59162 | MJJ59162

Juzgado Nacional de Primera Instancia en lo Civil y Comercial Federal N.° 3, Buenos Aires, "T., G. D. y otro c/ Cosa, Carlos A. y otro" (7 de abril de 2006).

Recuperado de http://www.derecho.uba.ar/rev_comunicaciones/ed010/jurisprudencia.htm

Ley N.° 11.723 (1933). *Régimen Legal de la Propiedad Intelectual*. Honorable Congreso de la Nación Argentina.

Ley N.° 25.326 (2000). *Protección de los Datos Personales*. Honorable Congreso de la Nación Argentina.

Ley N.° 26.388 (2008). *Código Penal de la Nación Argentina*. Honorable Congreso de la Nación Argentina.

Ley N.° 26.904 (2013). *Incorporación a la Ley N.° 26.388 (4 de junio de 2008). Código Penal de la Nación Argentina*. Honorable Congreso de la Nación Argentina.

Resolución 4/2009 (2009). *Protección de los datos personales*. Dirección Nacional de Protección de Datos Personales.

Schneider, M. V. (28 de mayo de 2015). Grooming: ciberacoso a menores de edad. *Revista de derecho de familia y las personas, 6(5)*, 211-216.

Thomson Reuters - La Ley (12 de julio de 2016). *Doctrina del día: el grooming una nueva modalidad delictual*. Recuperado de http://thomsonreuterslatam.com/2016/07/doctrina-del-dia-el-grooming-una-nueva-modalidad-delictual/.

Tribunal en lo Criminal N.° 1 de Necochea "F., L. N. s/ corrupción de menores agravada, Sup. Penal 20" (5 de junio de 2013). recuperado de https://aldiaargentina.microjuris.com/2013/07/30/grooming-condena-al-imputado-quien-se-contactaba-con-una-menor-mediante-internet-acosandola-y-enviando-material-de-contenido-sexual/.

Tribunal Superior de la Ciudad Autónoma de Buenos Aires "F., J. C. y otra s/ inf., artículo 153 bis del Código Penal" (1 de octubre de 2014). RDP 2015-1-165. Disponible en http://dpicuantico.com/sitio/wp-content/uploads/2015/03/Tecnolog%C3%ADa-Jurisprudencia-2015-03-11.pdf.

Vaninetti, H. A. (2010). *Aspectos jurídicos de Internet*. La Plata: Librería Editora Platense.

Vibes, F. P. (14 de febrero de 2013). Alcances y límites de la libertad de expresión en Internet. *Revista Argentina Jurídica La Ley, A*(2013), pp. 805-813.