

TITULO: Tecnología para la prevención e investigación en casos de violencia contra la mujer

Texto ampliado del PPT difundido en el aula virtual de UNED del 8 de agosto 2017.

AUTORA: Dra. Nora A. Cherñavsky\*

### Introducción:

Las tecnologías de la información y comunicación (TIC s) han optimizado la posibilidad de las mujeres de trabajar en red obteniendo claros resultados en favor de poder compartir experiencias e intentar buscar soluciones al problema de la violencia de género.

Es un medio propicio para realizar campañas contra este tipo de violencia, ayudar a las víctimas y promover imágenes de mujeres libres de estereotipos en los medios de comunicación.<sup>1</sup>

Por otra parte el medio digital, por sus características técnicas de acceso y de anonimato, brindan un espacio de oportunidad favorable al incremento del delito en general y en particular para los acosos, hostigamientos, amenazas y extorsiones, que encuentran en este entorno un ambiente propicio que les permite llegar más fácilmente a un número de víctimas mayor e indeterminado, careciendo del contacto físico que resulta necesario en el mundo “real” y que saca partido también de la “desterritorialización” y descentralización que posee Internet, lo que permite evadir los controles jurisdiccionales que existen en el mundo físico.

La difusión y reproducción de contenidos se ve facilitada y aumentada exponencialmente por la acción de los motores de búsqueda que facilitan la localización y acceso y optimizan la búsqueda de los usuarios, debatiéndose actualmente su responsabilidad por el enlace a contenidos ilegales creados por terceros.<sup>2</sup>

Los dispositivos móviles han facilitado la comunicación, pero como expresan algunas autoras también pueden convertirse en un elemento de control hacia las mujeres y se han convertido “en uno de los primeros artefactos a ser destruidos por el compañero durante reacciones violentas.”<sup>3</sup>

---

<sup>1</sup> <http://www.genderit.org/en/index.shtml?w=r&x=96306>

<sup>2</sup> En Argentina el caso se debatió en “Rodríguez, María Belen c/ Google inc y otros s/ daños” CSJN 12-10-2014.

<sup>3</sup> <http://www.genderit.org/en/index.shtml?w=r&x=96314>

En Internet como espacio público los usuarios pueden brindar y acceder a todo tipo de contenidos e información que circula libremente por la red. Así también ese mismo espacio resulta apto para la difusión de contenidos ofensivos, de odio o discriminatorios, los que son reproducidos a través de la creación de falsos perfiles que utilizan datos e imágenes ajenas para ocultar su identidad.

#### Las cifras del delito por género consumado a través de las tecnologías:

En la Argentina, según cifras de 2015 del MPF de consultas territoriales por género, las mismas corresponden en un 70 por ciento a mujeres. En tanto la cifra disminuye al 59 por ciento cuando se trata del delito de femicidio, y aumenta notablemente hasta alcanzar cifras superiores al 80% <sup>4</sup>cuando la consulta se refiere a acosos, extorsiones, amenazas, ciberodio, discriminación en razón de género, difusión y o publicación de imágenes íntimas no autorizadas por la red.

#### Principales delitos que afectan a la mujer, por su condición de tal, cometidos mediante uso deTICs

- a) Hostigamientos, amenazas y extorsiones a través de redes sociales y mensajeros de WhatsApp en dispositivos móviles.
- b) Captación de imágenes de abuso de niñ@s
- c) Captación por las redes de mujeres y niñas para explotación sexual y/o laboral.
- d) Captación por las redes de mujeres y niñ@s para la trata de personas.
- e) Captación de imágenes de niñas y adolescentes para producción y distribución de pornografía infantil.
- f) Difusión de imágenes íntimas sin autorización a través de acceso indebido a dispositivos o introducción de malware en las computadoras de las víctimas para apropiarse de claves y así obtener datos e imágenes en forma subrepticia.
- g) Difusión no autorizada de imágenes íntimas de mujeres, previamente compartidas en pareja o con amigos para pasarla a los contactos de la víctima o en algunos casos para publicarlas en sitios de pornografía o de acompañantes sexuales, menoscabando así la dignidad de la persona afectada<sup>5</sup>.
- h) Difusión no autorizada de imágenes íntimas en las redes sociales y en el ámbito laboral y afectivo de la mujer para humillarla, hostigarla y producir un daño grave a su imagen social y laboral. (puede tratarse de ex parejas, compañeros de trabajo, etc)

---

<sup>4</sup> Se está elaborando la estadística específica 2016/2017 en el seno de la UFECI y de la UFEM, que funcionan en el ámbito del Ministerio Público Fiscal de la Nación.

<sup>5</sup> Esta difusión no autorizada de imágenes íntimas no está penalizada en la Argentina, salvo que el medio utilizado sea el acceso indebido a computadoras o correos electrónicos o introducción de malware (daño informático) para captar claves. Existen diversos proyectos de ley en el Congreso Nacional: S-2180/15 S-2119/16, 5893-D-2016, entre otros.

- i) Estafas cometidas en redes sociales donde las que las mujeres caen víctimas en función de falsas promesas amorosas por un lado, y por el otro extorsiones que afectan también en gran medida al varón que accede al intercambio de imágenes de desnudo a través de la “web cam” y luego es extorsionado para no difundirlas. (sextorsion).

Internet ha permitido no sólo optimizar y favorecer la comunicación, la libertad de expresión y el acceso a la información sino que como consecuencia no deseada del uso de las redes ha incrementado y brindado nuevos medios para la difusión y reproducción de contenidos ilícitos y otros abusos contra mujeres y niños.<sup>6</sup>

La legislación argentina sanciona en el art. 128 del CPA la producción, financiamiento y difusión de imágenes “pornográficas” de niños y niñas en situaciones sexualmente explícitas o exhibiendo partes íntimas, como así también la tenencia de estas imágenes con “inequívocos fines de distribución”. Actualmente hay en danza proyectos de ley para penalizar la SIMPLE TENENCIA de imágenes sexualmente explícitas de menores, sin requerir tales fines de distribución y aun cuando dicha posesión sea mínima.

Como se refleja en la exposición del 8 de agosto<sup>7</sup>, existe actualmente entre amigos y parejas una conducta socialmente difundida y aceptada que se conoce por su denominación en inglés “SEXTING”, que consiste el intercambio libre y consentido de fotos generalmente tomadas con el celular en posiciones seductoras de tipo sensual o eventualmente con connotaciones sexuales.

Esta conducta se convierte en “SEXTORSION” (denominación en inglés) que consiste como lo grafica la diapositiva 5<sup>8</sup> en la siguiente etapa de extorsión a la víctima previamente filmada con el celular o mediante la cámara web del computador, solicitándole dinero para no difundir dichas imágenes entre sus contactos o bien solicitándole más imágenes de ella o de alguna amiga o parienta para rescatar las

---

<sup>6</sup> Tal como se grafica en la conferencia de la autora del 8 de agosto de 2017 en la página web de UNED.

<sup>7</sup> Diapositiva 4

<sup>8</sup> Ibid.5

anteriores<sup>9</sup>. Es posible también que dichas imágenes el autor las hubiera “secuestrado” directamente de la computadora de la víctima a través de la introducción de un virus o malware en el navegador de la víctima, lo que le permite apropiarse de las mismas y difundirlas mediante este “ardid tecnológico”.

#### Valoración de las conductas descriptas:

En la legislación argentina, a través de la incorporación en el derecho interno de las Convenciones de Derechos Humanos de la mujer<sup>10</sup>, la ley 26485<sup>11</sup>, en su artículo 4 describe todas aquellas conductas que menoscaban e inferiorizan a la mujer en relación al varón y que por lo tanto se consideran que son generadoras de violencia contra la mujer y cuyo texto conviene reproducir:

“Art. 4: Se entiende por violencia contra las mujeres toda conducta, acción u omisión, que de manera directa o indirecta, tanto en el ámbito público como en el privado, basada en una relación desigual de poder, afecte su vida, libertad, dignidad, integridad física, psicológica, sexual, económica o patrimonial, como así también su seguridad personal. Quedan comprendidas las perpetradas desde el Estado o por sus agentes.

Se considera violencia indirecta, a los efectos de la presente ley, toda conducta, acción omisión, disposición, criterio o práctica discriminatoria que ponga a la mujer en desventaja con respecto al varón”

Por ser mayoría las mujeres sometidas a amenazas y extorsiones en la red, estas conductas afectan sus derechos a una vida libre y sin violencia. En efecto, la mujer, por su condición de tal, se ve más severamente afectada que el varón en la consideración

---

<sup>9</sup> Como refiere Mary Anne Franks (2015), quien ha elaborado una Guía para Reguladores: “ tanto como 3.000 sitios web publican “pornografía de venganza” y ese material íntimo es asimismo ampliamente distribuido sin consentimiento a través de redes sociales, blogs, correos electrónicos y mensajes de texto. La Cyber Civil Rights Initiative (CCRI) es contactada por un promedio de 20-30 víctimas cada mes. La tecnología y las redes sociales han permitido a los abusadores externalizar distribuidamente (crowd-source) su acoso y también ha permitido a los individuos inescrupulosos aprovecharse de ello.<sup>3</sup> No hay duda que existe un derecho claramente vulnerado, tales conductas son violatorias del derecho a la privacidad de las personas. Ver también: “La Regulación de la Pornografía no consentida en Argentina. Diciembre 2015 CELE (Centro de Estudios en Libertad de Expresión y Acceso a la Información). Franks Mary Anne “Revenge Porn” Law: A Guide to Policymakers en End Revenge Porn. Citado en Internet y Derechos Humanos Aportes para la Discusión en América Latina, Universidad de Palermo - Facultad de Derecho- Eduardo Bertoni Compilador. 2015

<sup>10</sup> CEDAW <http://www.un.org/womenwatch/daw/cedaw/cedaw25years/content/spanish/Convention-CEDAW-Spanish.pdf> Y Convención de Belem do Pará <http://www.oas.org/juridico/spanish/tratados/a-61.html>

<sup>11</sup> Ley de protección integral para prevenir, sancionar y erradicar la violencia contra las mujeres en los ámbitos en que desarrollen sus relaciones interpersonales, publicada en el Boletín Oficial Argentino del 14-abr-2009

social, laboral, familiar y afectiva, cuando sus imágenes íntimas son difundidas masivamente y/o por venganza de una ex pareja, son subidas a sitios pornográficos. Estas conductas afectan seriamente lo que la doctrina ha dado en llamar “reputación digital” y colocan a la mujer en una situación de desigualdad y desventaja respecto del varón, lo que en los términos de las Convenciones de Derechos humanos y de la ley 26.485 en particular, constituye violencia.

La diapo 7 grafica como la captación de mujeres y niñas con fines de trata y explotación sexual o laboral se da cada vez más frecuentemente a través de las redes sociales. Tal acción generalmente se consume a través de **falsos perfiles de Facebook o de otras redes sociales, en las que el usuario fraudulento**, tienta a mujeres y niñas vulnerables con una participación en falsas campañas publicitarias, venta de lencería, etc solicitándoles fotos y todo tipo de imágenes a cambio de prometerles una buena paga o trabajos mejor pagados.

De ahí la importancia que la investigación de estos delitos se lleve a cabo no sólo sobre perfiles individuales de usuarios sino también de los grupos cerrados de Facebook que ofertan dudosas búsquedas laborales muy bien remuneradas. También deben tenerse en cuenta en la investigación de pornografía y venta de mujeres y niñas, a aquellas plataformas donde se intercambian imágenes pornográficas de mayores, que suelen ser muchas veces indicio de que dichas mujeres son tratadas o explotadas y de aquellos sitios en los que se suben o comparten imágenes de niños y niñas menores de 18 años abusadas sexualmente.

La diapo 8 grafica las acciones de captación de mujeres y niñas y demuestra que a los medios y fines tradicionales se agrega muy fuertemente el Internet.

La diapo 9 grafica al delito de “*grooming*” (art. 131 CPA), que es la conducta deliberada de un adulto de acosar sexualmente a un niño o niña mediante el uso de Internet.

La conducta delictiva se consume generalmente mediante un perfil falso en una red social, sala de chat, foro, el perfil se hace pasar por un chico o una chica para entablar una relación de amistad y ganarse la confianza del niño o niña con el fin de disminuir sus inhibiciones, obtener imágenes íntimas que concluyen en la 4 etapa y la más peligrosa que es la extorsiva, en la que generalmente se consume el abuso sexual de la víctima.

La diapo 10 señala grafica estas etapas del “*grooming*”.

De ellas se desprende que la cuarta etapa es la más peligrosa, por lo que la prevención para que dicho delito no se consume debería comenzar tanto en la familia como en los colegios en etapas anteriores en las que la niña o niño comienza a tener contactos con desconocidos a través de dispositivos conectados a Internet (lo que habría que enseñar a evitar), ello a fin de evitar que establezcan lazos de confianza con desconocidos y evitar el abuso.

Dificultades para la investigación de los delitos informáticos:

Por ser delitos transnacionales, es decir con consecuencias en diferentes jurisdicciones, tiene los problemas de

- i) La determinación de la jurisdicción, esto es cuál es el juez que se hace cargo de la investigación y cómo se determina el Juez natural.
- ii) Determinación del lugar en que se llevó a cabo el hecho investigado (competencia territorial)
- iii) Cuáles son los tipos penales a considerar para fundar la competencia (competencia material)
- iv) Problemas de conexidad con otra causa en trámite para acumular (competencia por conexidad) dado que generalmente hay varias causas de violencia iniciadas.

La elección de una u otra jurisdicción resulta aún más dificultosa cuando tenemos que investigar delitos informáticos, ya que en estas modalidades delictivas la conducta se produce en un lugar y puede afectar a diferentes personas en distintos territorios, con el uso de una simple y única herramienta: una computadora conectada a la red.

#### Importancia de la dirección IP

En la investigación de delitos informáticos, resulta determinante un elemento característico y propio de esta temática: la dirección IP (Internet Protocol).

La dirección IP identifica una conexión a internet desde un dispositivo (computadora de escritorio o portátil, celular, tableta o cualquier otro aparato con conexión a internet incluso televisores inteligentes, heladeras) en un momento determinado.

Estas direcciones IP, que son únicas a través de toda la red de redes están formadas por un grupo de cuatro segmentos (ej. 200.55.243.205, el número mínimo es 0.0.0.0. y el máximo 255.255.255.255.)

Se encuentran distribuidas mundialmente en bloques y son asignadas a los clientes por los proveedores del servicio de internet -ISP- (ej "Fibertel" -de Cablevisión Argentina S.A)

#### Características de la evidencia digital:

Se trata de una prueba que es volátil y puede ser fácilmente duplicada o alterada, por lo que hay que preservar la cadena de custodia, que es el control que se efectúa tanto de las personas que recogen la evidencia como de cada persona o entidad que posteriormente tiene la custodia de la misma. La cadena de custodia debe contener un identificador unívoco de la evidencia, de las fechas en las que los artículos fueron recogidos o transferidos, datos sobre el responsable que realizó la recolección, datos sobre la persona que recibe la evidencia y los datos de las personas que acceden, el momento y la ubicación física, número del caso, y una breve descripción de cada elemento. El pasaje de la evidencia de un sitio a otro y las tareas realizadas, cualquier

cambio inevitable potencial en evidencia digital será registrado con el nombre del responsable y la justificación de sus acciones. El objetivo de la cadena de custodia es garantizar la autenticidad de la evidencia que se utilizará como prueba dentro del proceso.

### Conclusiones útiles para la prevención y la investigación de los delitos cometidos mediante el uso de las TIC s:

Sin perjuicio de que actualmente el niño/niña maneje mejor que el adulto los dispositivos tecnológicos, lo cierto es que hay que CAPACITARLOS para que aprendan a distinguir que como en el mundo físico, hay contenidos privados, que forman parte de su intimidad y que no deben ser divulgados ni compartidos con extraños, explicando los riesgos que ello conlleva.

Que la difusión indiscriminada de imágenes, puede generarle daños no sólo en el mundo digital sino en el mundo físico ya que podría ser objeto de graves burlas por parte de sus compañeros.

Se les debe enseñar a las niñ@s y mujeres a no caer víctimas de otros delitos contra el patrimonio como las estafas u otros delitos que puedan afectar desde su integridad corporal hasta su vida.

Para la investigación de estos delitos es especialmente útil peritar los dispositivos utilizados por los atacantes, y solicitar todos los datos de suscripción y eventualmente de contenido de usuario al proveedor de servicio de telefonía o de red, por las vías de procedimiento habilitadas dentro de los procesos legales.

Resulta importante investigar y conocer el entorno de redes sociales que utiliza el atacante, sus contactos y “amigos” en las redes, preservar contenidos y así obtener datos útiles para la investigación que almacenan las empresas proveedoras del servicio de alojamiento de datos por internet o de telefonía fija y móvil.

Tengamos en cuenta que Internet es en parte un espacio “privado” donde la intimidad de los datos personales del usuario deberían estar protegidos por las leyes de Protección de Datos Personales y resguardados de un uso ilegítimo, pero que también brinda un espacio “público” de intercambio de contenidos e información.

En esta autopista informativa, los proveedores de servicio cumplen también un rol muy importante ya que son empresas que intermedian entre el usuario y los múltiples contenidos generados en la red, cuya ubicación y disponibilidad facilitan y enlazan. En Argentina, como en otros países se ha discutido el rol de estos Proveedores de Servicio y si tienen o no responsabilidad civil por enlazar a contenidos ilícitos generados por terceros usuarios.

\*Profesora Adjunta Regular de la Universidad de

Buenos Aires

