VIOLENCIA DE GÉNERO Y NUEVAS TECNOLOGÍAS, UNA RELACIÓN CONFLICTIVA

Carlos Igual Garrido
Capitán del EMUME Central de la Guardia Civil

Resumen

La compleja relación entre la violencia contra las mujeres (VCM) y las tecnologías de información y comunicación (TIC) genera distintos escenarios que afectan a los derechos de las mujeres. Las TIC pueden utilizarse como una herramienta para prevenir o combatir la violencia contra las mujeres, mientras que por otro lado la VCM puede facilitarse mediante el uso de las TIC. A diferencia de otros ámbitos como por ejemplo el uso de las TIC y los menores, la relación entre las TIC y la VCM ha tenido poca atención tanto en las políticas como en los recursos empleados para su prevención.

En este artículo se van a nominar y definir las formas de violencia perpetradas contra las mujeres a través de las nuevas tecnologías de la información (TIC), y también se van a señalar ciertas prácticas para proteger los derechos de la mujer y prevenir la violencia contra las mujeres.

1 MANIFESTACIONES DE LA VIOLENCIA CONTRA LAS MUJERES EN EL MUNDO DIGITAL

A menudo se dice que las tecnologías como Internet o los teléfonos móviles son un arma de doble filo. El acoso, el hostigamiento, los insultos y las amenazas a las mujeres se realizan con frecuencia a través de los teléfonos móviles, mensajes de texto o correos electrónicos. Pero al mismo tiempo, las TIC son plataformas que las mujeres pueden utilizar para defender su derecho a una vida libre de violencia. En el estudio "*Women & mobile: A global opportunity*" [1] el 93% de las mujeres entrevistadas se sentían más seguras y el 85% se sentían más independientes gracias a su teléfono móvil. No es una coincidencia que los teléfonos móviles de las mujeres sean los primeros objetos personales destruidos en las agresiones de las parejas violentas en Argentina[2].

Aunque a veces identificamos la violencia con la violencia física, aquella puede adoptar muchas formas diferentes. Así, aunque la violencia relacionada con la tecnología puede derivar en violencia física, es más habitual que las víctimas experimenten una violencia más psicológica.

Dentro de la categoría de VCM relacionada con la tecnología existen diferencias en la prevalencia de la violencia y cómo se manifiesta debido a una combinación de factores:

- ¿Quiénes son los autores? (por ejemplo, la pareja, familiares, extraños, la sociedad).
- La plataforma tecnológica utilizada por los autores (por ejemplo, el teléfono móvil, las redes sociales, SMS, correos electrónicos, páginas web, cámara web, etc.).

[1] GSMA Development Foundation *Women & mobile: A global opportunity* www.mwomen.org/Research/women-mobile-a-global-opportunity_1

[2] Cristina Peralta*: Violence against women and information communication technologies* (APC WNSP, 2009) www.genderit.org/content/argentina-violence-against-women-and-informationcommunication-technologies

- La naturaleza de la violencia (por ejemplo, el acoso, el acoso online, la violencia de pareja, la justificación cultural de la violencia contra las mujeres, agresión sexual, la violencia dirigida a determinados colectivos de mujeres).
- El tipo de agresión (por ejemplo, las amenazas, el chantaje, el robo de identidad, el espionaje de las comunicaciones online y la grabación y/o distribución de imágenes no autorizadas).
- El daño que experimenta la víctima (por ejemplo, daño físico, daño psicológico, daño sexual, daños económicos, daños a la privacidad o daño al honor)
- Las características sociales y personales de la víctima (por ejemplo, nivel cultural, nacionalidad, raza, edad, la existencia de una discapacidad o cualquier otro tipo de vulnerabilidad).

Con fines descriptivos, podemos utilizar la clasificación realizada por la "*Association for Progressive Communications Women´s*"[3] de la violencia contra las mujeres relacionada con la tecnología, que la engloba en cinco grandes categorías:

1. **El acoso online**, que constituye uno de las formas más visibles de la VCM relacionada con la tecnología. Implica desde acosar a mujeres mediante mensajes (SMS, whatsapp, etc.) a publicar en las redes sociales comentarios en los perfiles de las mujeres, sus amigos, su familia etc.
2. **La violencia en el ámbito de la pareja**, donde se usa la tecnología como forma de violencia (acoso, insultos, amenazas), como forma de control o como forma de extorsión para impedir que la mujer abandone la relación. Por ejemplo algunas mujeres tienen miedo de abandonar relaciones abusivas debido a las amenazas de divulgación de imágenes íntimas o comunicaciones privadas por parte de sus parejas.
3. **La violencia culturalmente justificada contra las mujeres**, cuando la tecnología juega un papel en la creación de una cultura de la violencia contra las mujeres o en su justificación. Puede variar desde algo tan aparentemente banal como la difusión de una broma sexista que apoya la idea de que las mujeres son menos valiosas que los hombres, hasta la creación de un grupo en una red social que promueva diferentes formas para drogar a las mujeres y abusar de ellas.
4. **Violación y abuso sexual**, donde se utiliza la tecnología para rastrear el movimiento y las actividades de una víctima, o para proporcionar información sobre su ubicación o cuando una agresión sexual se graba y distribuye online. En otros casos puede utilizarse las nuevas tecnologías para contactar con mujeres y atraerlas a una cita donde serán agredidas sexualmente.
5. **Violencia dirigida a las comunidades**, ciertos colectivos, asociaciones, partidos políticos conocidos por su apoyo a las mujeres o a las víctimas de VCM, pueden ser víctimas de ataques a través de las nuevas tecnologías en forma de insultos, amenazas o ataques cibernéticos. Incluso muchas Blogueras han sido atacados en sus blogs por defender posturas favorables a las mujeres.

Las víctimas de violencia de género, por la especial relación que mantienen con sus agresores, son más vulnerables a sufrir violencia mediante las nuevas tecnologías, esta violencia puede

[3] Association for Progressive Communications Women´s Networking Support Programme "Map it. End it. Take Back the Tech!" GenderIT.org 16 November 2011 ww.genderit.org/feminist-talk/map-it-end-it-take-backtech

realizarse de diferentes formas, algunas de las cuales analizamos de forma detallada a continuación.

1.1 Ciber-control de la pareja

Las nuevas tecnologías nos permiten estar interconectados permanentemente con nuestra familia, nuestros amigos o nuestro trabajo. Esta disponibilidad puede amenazar nuestra privacidad, y convertirse en una forma control total en todo tiempo y lugar.

Pero especialmente las víctimas de violencia de género deberían ser conscientes de qué información comparten en internet para saber hasta qué punto están expuestas al escrutinio de sus parejas o ex parejas y reducir su vulnerabilidad.

1.1.1 *Información personal en internet*

"*Internet es lo más cercano a una máquina perfecta de vigilancia que el mundo ha conocido. Todo lo que se hace en la Red es registrado; cada email enviado, cada sitio visitado, cada fichero descargado, cada búsqueda realizada son grabados y archivados en algún sitio, ya sea en los servidores de nuestro proveedor de Internet o en los servicios de la "nube" a los que accedemos…"* [4]

Internet recoge toda la información que publicamos bien en redes sociales, en blogs, haciendo un comentario sobre un producto que hemos comprado, pero también la información que otras personas publican sobre nosotros, por ello es conveniente conocer dónde y qué buscar para saber cuan expuestos estamos al escrutinio de los demás.

1.1.2 Redes sociales, blogs, páginas web.

Las redes sociales han revolucionado la forma de relacionarnos. Los usuarios de estas aplicaciones publican su vida e información privada de forma accesible para millones de personas.

Sin embargo las víctimas de la violencia de género pueden ser vulnerables a nuevas agresiones o pueden experimentar acoso a través de estas redes sociales. Para estas mujeres preservar la información sobre su ubicación y su privacidad a menudo es necesario para su propia seguridad y la de sus hijos.

Las víctimas y sus amigos o familiares deben ser conscientes que la información privada que publican en las redes sociales, presenta un potencial riesgo que puede multiplicarse simplemente pulsando el botón de "compartir".

Incluso a veces se publica más información de la que las víctimas son conscientes, por ejemplo si en un restaurante fotografiamos un plato que nos ha sorprendido y la publicamos en nuestra cuenta de Twitter, aunque no revelemos el nombre del restaurante, de forma automática la fecha, hora y localización exacta de dónde hemos hecho la fotografía se comparte con el resto de los usuarios de la red, sólo habrá que utilizar alguna de las muchas herramientas de búsqueda de tweets[5] en internet para que aparezcamos señalados en un mapa con una precisión asombrosa.

También las víctimas deben ser especialmente cautas con la información que revelan en las redes sociales, y deben tener presente que habitualmente su agresor conocerá las palabras que

[4] *http://www.kriptopolis.org/osint-inteligencia-open-source*

[5] http://www.welivesecurity.com/la-es/2014/09/18/creepy-geolocalizacion-tweets-al-descubierto/

utiliza habitualmente como nombres de usuario, sus cuentas de correo electrónico, o sus contraseñas habituales. Otras veces le bastará con conocer cierta información personal para identificarla.

Un ejemplo de cómo conocer cierta información personal de una víctima puede permitir encontrar su perfil en una red social, independientemente del nombre que utilice, pude realizarse mediante las opciones de Facebook de búsqueda de personas por su localización, aficiones, lugar de nacimiento, trabajo, etc. Es obvio que el agresor conocerá información personal sobre su pareja o ex pareja que podrá utilizar para buscar su nuevo perfil de facebook.

Sería también recomendable comprobar la configuración de privacidad que las víctimas poseen en las redes sociales y ajustarla a un nivel seguro, aunque no debe olvidarse que aunque se publique información accesible solo por los amigos, si éstos la comentan o la comparten, estará disponible para los contactos de esos amigos y así sucesivamente.

Por otro lado es importante que las víctimas sepan que los navegadores Web registran la historia de navegación en Internet y esta información puede ser utilizada por los agresores para conocer las páginas visitadas, si la víctima ha buscado información sobre asistencia o denuncias o incluso si ha consultado direcciones en busca de refugio.

1.1.3 Información que otros publican sobre ti.

Cualquiera puede publicar información sobre otra persona, amigos, familiares, la empresa donde trabaja, instituciones oficiales, bancos, etc. La primera medida que debe adoptar una víctima para protegerse es ser consciente de cuanta información personal sobre ella está disponible en internet. Para ello conviene conocer las principales fuentes que pueden ser el origen de estos datos.

1.1.3.1. Registros públicos

Internet refleja el contenido de distintos registros oficiales: boletines, resultados de oposiciones, ayudas, concursos públicos, edictos judiciales, etc. En todos ellos puede encontrarse el nombre complete y DNI, ciudad de residencia, titulaciones académicas, estudios realizados, etc. Esta información puede ser luego utilizada para nuevas búsquedas, por ejemplo introduciendo el número del DNI en Google.

1.1.3.2 Amigos, familia y compañeros de trabajo

Muchas organizaciones y empresas tienen páginas web o perfil en redes sociales que muestran las actividades de sus miembros. Si usted participa en una actividad formativa del AMPA del colegio de sus hijos, participa en una conferencia, en una excursión realizada por un club de aire libre, su nombre, y su imagen puede aparecer en la página web.

Pero para el que fue pareja, marido o compañero de una víctima de violencia, muchas veces les será más fácil llegar a ellas a través de las publicaciones de sus hijos, si éstos aparecen inscritos en una carrera popular es deducible que su madre estará el día de la competición, o si aparecen en la graduación en el colegio también es seguro que su madre asistirá a este evento, y eso cuando no son los menores directamente los que publican fotos en las redes sociales con sitios donde han pasado las vacaciones, el fin de semana o su residencia actual. Las madres deberían educar a sus hijos a que sean tan cautos a la hora de compartir su información privada como lo son ellas.

1.1.4 Cómo puedo saber qué información sobre mi aparece en internet.

La primera opción debería ser la utilización de buscadores genéricos como Google, Bing o Yahoo. Una búsqueda entre comillas, de por ejemplo "nombre y apellidos" arrojará resultados mucho más exactos que si se hace de forma general. Otros términos que convendría buscar serían el DNI, el número de teléfono, y las direcciones de correo electrónico o nicks utilizados habitualmente en las redes sociales. El resultado nos mostrará la información que sobre nosotros está disponible en la red, aunque no será toda, ya que mucha no está indexada en estos buscadores.

De la misma forma, será conveniente conocer cuanta información compartimos en las redes sociales, para ello Facebook, Twitter, Tuenti, Instagram o Flickr, tienen herramientas de búsqueda, tendremos que introducir tanto nuestro nombre como nuestro correo electrónico, al que muchas veces está vinculado el perfil. También conviene realizar la búsqueda a través del perfil de un amigo, familiar o conocido, incluidos nuestros hijos, ya que el agresor es posible utilice esta forma a la hora de buscar información sobre su ex pareja.

Tampoco debemos olvidar redes profesionales como Linkedin, que incluyen información sobre nuestra actividad profesional y nuestros contactos.

1.1.5 Borrado de información.

Si tras la búsqueda de información privada en internet una víctima descubre información personal y desea borrarla, ¿cómo puede hacerlo?

La primera opción sería solicitar el borrado de la información a los administradores de los buscadores como Google o Yahoo, podría dirigirse directamente a ellos[6], pero no debemos olvidar que ellos simplemente muestran la información disponible en otros sitios web que son el verdadero origen. Para borrar completamente la información, se necesita dirigirse al administrador de cada uno de estos sitios y solicitar su borrado.

La mayoría de las redes sociales también tienen una opción para denunciar la existencia de contenido ofensivo o degradante y permiten eliminar la cuenta de forma permanente (por ejemplo en Facebook[7]), esta opción será recomendable para víctimas de violencia de género que quieran crear un nuevo perfil y evitar el escrutinio de su agresor.

En otros sitios es posible que para acreditar la identidad de la persona que solicita la retirada de información se le requieran datos personales complementarios que podrían ser contraproducentes, es decir si para que una página donde aparece nuestro correo electrónico nos solicitan nuestro nombre, apellidos, dirección física y número de teléfono, puede ser preferible no continuar con el proceso.

En otros casos, si la información publicada es constitutiva de calumnias, amenazas o injurias puede denunciarse con el fin de identificar a la persona que publicó esa información, aunque muchas veces si la página web que aloja esta información está alojada en países que no suelen dar respuesta a las peticiones de información de las autoridades españolas (los denominados paraísos digitales), será difícil obtener los datos necesarios para identificar al autor.

[6] https://support.google.com/websearch/troubleshooter/3111061?hl=es
[7] https://www.facebook.com/help/www/224562897555674

2 CONSEJOS SOBRE PRIVACIDAD PARA LAS VÍCTIMAS DE VIOLENCIA DE GÉNERO.

La amenaza que las nuevas tecnologías puede suponer a la seguridad de la mujeres víctimas de violencia puede ser muy real, tanto que determinadas organizaciones que las apoyan han alertado que mujeres víctimas de violencia de género que estaban refugiadas en casas de acogida seguras eran localizadas por sus ex parejas, mediante la información que compartían tanto ellas como sus familiares y conocidos en las redes sociales.

En otros países, por ejemplo en Australia, las asociaciones de ayuda a las víctimas de violencia de género les realizan cuestionarios sobre las medidas de seguridad que adoptan las víctimas en sus teléfonos móviles u ordenadores, así se incluyen preguntas como ¿quién configuró su teléfono móvil?, ¿quién creó su cuenta de Facebook u otra red social?, ¿quién puede tener acceso a sus contraseñas?, de esta forma pueden detectar posibles fallos de seguridad que podrían exponer la privacidad de las víctimas.

A petición de la Unidad de Atención a la Violencia del Ayuntamiento de Madrid, se elaboró por el EMUME Central de la Guardia Civil, un decálogo de consejos para incrementar la seguridad y privacidad de las mujeres víctimas de violencia de género en las nuevas tecnologías:

1. Utilice un ordenador seguro, si su ordenador lo configuró o utilizó su ex pareja es posible que no lo sea. Haga que un experto lo examine o utilice el de una biblioteca, cibercafé o el de una persona de confianza.
2. Cree nuevos perfiles en las redes sociales: Facebook, Instagram, etc. y configure el máximo nivel de privacidad sobre sus publicaciones.
3. Si pertenece a asociaciones o grupos, pídales que no publiquen sus datos en internet, ni fotografías donde usted aparezca, igualmente en el colegio de sus hijos.
4. Cuando busque trabajo en internet, sea prudente con la información que publique como número de teléfono o domicilio. Como forma de contacto publique una dirección de correo nueva.
5. Pida a sus amigos que no etiqueten en las redes sociales su nombre en las fotografías, o publiquen fotos, vídeos o cualquier otra información sobre su estado actual, domicilio, aficiones, etc.
6. Configure una alerta de Google con su nombre y apellidos[8], también puede incluir su correo electrónico o su número de teléfono, ésta alerta enviará a su correo cualquier información que aparezca en internet sobre usted.
7. Tenga más de una cuenta de correo y utilícelas para diferentes usos: particular, trabajo, redes sociales.
8. En las cuentas de correo menos seguras, las que utiliza para sus redes sociales o foros, no utilice información personal para su registro (nombre: Agustina de Aragón).

[8] https://support.google.com/alerts/?hl=es

9. Evite contraseñas débiles tanto para acceso a su ordenador, cuentas de correo electrónico, y los teléfonos móviles (evite los patrones de desbloqueo, es más seguro la utilización de contraseñas con números).
10. No use contraseñas que utilizó mientras vivía con su pareja ni use como pregunta de seguridad para recuperar contraseñas información conocida por él.
11. Compruebe la seguridad de los teléfonos móviles de sus hijos, desactive la opción de geolocalización y si sospecha de ellos, borre toda la información y restablezca la configuración de fábrica (puede hacerlo en cualquier tienda de telefonía).
12. Utilice alguna aplicación en su teléfono móvil que le permita solicitar ayuda en caso de agresión, puede utilizar Cibercops[9] que le permite una comunicación inmediata con los servicios policiales españoles.

3 LOS TELÉFONOS MÓVILES COMO INSTRUMENTO DE ACOSO A LAS VÍCTIMAS.

"*El ciberacoso se puede definir como una forma de invasión en el mundo de la víctima de forma repetida, disruptiva y sin consentimiento, usando las posibilidades que ofrece Internet*".[10]

El ciberacoso como forma de ejercer violencia sobre la pareja o ex pareja supone una dominación sobre la víctima mediante estrategias humillantes que afectan a la privacidad e intimidad, además del daño que supone a su imagen pública. Su efecto acumulativo es básico.

En efecto, puesto que el ciberacoso como instrumento para agredir a la pareja se produce generalmente sin que haya coincidencia física, la reiteración se convierte en la estrategia de invasión de la intimidad más utilizada por los acosadores.

El uso más simple del teléfono móvil como herramienta de acoso sería el envío masivo de textos amenazantes y llamadas, especialmente a través de aplicaciones de mensajería instantánea como WhatsApp, aunque también puede hacerse por SMS.

De hecho, el acoso a través de los mensajes a móviles, es uno de los problemas que más están creciendo en todo el mundo. La difusión de los programas de mensajería instantánea tipo Whatsapp, Line u otros, ha traído la gratuidad de los mensajes, por lo que pueden enviarse cientos cuando no miles de mensajes sin coste alguno. Un ejemplo de este tipo de agresiones puede verse en la noticia aparecida en internet[11] sobre un joven estudiante condenado por un Juzgado de Ferrol por acosar a su ex novia mediante el envío de 2.147 mensajes de WhatsApp en un mes.

En un reciente estudio realizado en Australia[12], entre profesionales que trabajaban con víctimas de violencia de género, afirmaban que el 82% de las víctimas habían denunciado ser acosadas a través de su teléfono móvil o redes sociales.

---

[9] https://alertcops.ses.mir.es

[10] **"**EL CIBERACOSO COMO FORMA DE EJERCER LA VIOLENCIA DE GÉNERO EN LA JUVENTUD: UN RIESGO EN LA SOCIEDAD DE LA INFORMACIÓN Y DEL CONOCIMIENTO" Ministerio de Sanidad, Política Social e Igualdad. Centro de Publicaciones. 2014.

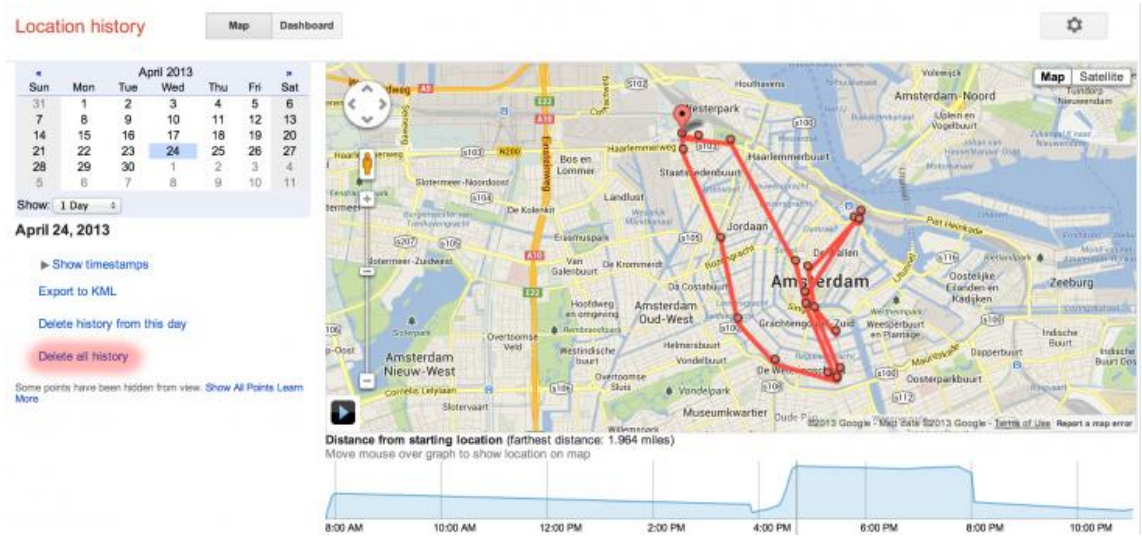
[11] http://www.tecnopasion.com/condenado-acosar-ex-novia-whatsapp-2238/

[12] http://smartsafe.org.au/wp-content/uploads/2013/09/SmartSafe-Findings-Booklet.pdf

Sin embargo la tecnología de los teléfonos móviles puede ser utilizada de formas mucho más complejas para controlar o espiar a las víctimas. De nada sirve que una mujer víctima de violencia de género cambie de domicilio, de ciudad, incluso de país, o se refugie en una casa de acogida si es posible encontrarla a través del rastro que deja su teléfono móvil, sus publicaciones en las redes sociales o su correo electrónico.

Continuamente nuestros teléfonos móviles envían información nuestra sobre nuestra posición, nuestra identidad o hábitos de navegación. Un estudio realizado por la Penn State University, Duke University, junto con Intel Research Labs,[13] reveló una lista de aplicaciones Android que enviaban información del usuario, sin permiso explícito de éste, a servidores propiedad de empresas de anuncios publicitarios. En el estudio pusieron a prueba 30 aplicaciones populares al azar, de 12 categorías distintas y comprobaron que, para su sorpresa, la mayoría de ellas hacían un uso indebido de la información de los usuarios de los móviles en los cuales estaban instaladas. Entre la información enviada figuraba el número de teléfono, el código IMSI, y más de la mitad de las aplicaciones testeadas estaban enviando información GPS sobre la ubicación del móvil a servidores de terceros, sin permiso explícito o implícito del usuario: Entre las aplicaciones testeadas figuraban aplicaciones meteorológicas, juegos, prensa, lectores de códigos de barras, antivirus, etc.

Podemos decir que los Smartphone son en realidad un dispositivo de geolocalización en nuestro bolsillo. Hagamos la prueba, si nuestro dispositivo posee el sistema operativo Android, podemos entrar en la página https://maps.google.com/locationhistory/b/0/ después de haber iniciado nuestra sesión en google (o Gmail) y aparecerá nuestra posición en los últimos días, meses o años, con una inquietante precisión.



Esto es debido a que tendremos activado en nuestro móvil la opción de "permitir que Google use los datos de ubicación para obtener unos mejores resultados de búsqueda y otros servicios". A esto se une que muchos teléfonos móviles tienen activada la función de geolocalización de fotos, que añade la ubicación geográfica a las fotos realizadas con el móvil, y la envía junto con ésta en formato exif que puede ser leído por cualquier persona que acceda a la imagen.

Pero Android no es el único sistema que geolocaliza las imágenes, Iphone añade la geolocalización automáticamente en cada foto que realiza, siempre que tengamos el GPS

[13] http://appanalysis.org/

activado y tenga una posición reciente y válida cuando hacemos la foto. Las coordenadas geográficas de donde se ha tomado la foto se añaden a los datos EXIF, junto con información como la exposición, apertura, etc. Esto queda incorporado al archivo jpg de la foto.

También nuestro navegador, ya sea en nuestro ordenador, tablet o móvil puede enviar nuestra localización cuando vemos una página web, podemos comprobarlo en la página http://norfipc.com/internet/saber-mi-localizacion-ubicacion-geografica.php, que mostrará de una forma precisa nuestra posición a partir de distintas fuentes de información disponibles a través de la red como es la dirección IP, los nodos Wi-Fi disponibles y otros que dependen de funcionalidades del dispositivo como las torres de telefonía celular GSM/CDMA y el GPS, si está incluido.

3.1 La ciber-extorsión a las víctimas de violencia de género.

Después de un periodo más o menos prolongado de convivencia en pareja, es muy posible que se compartan videos, fotografías o conversaciones de actividades privadas e íntimas, incluso de índole sexual.

Actualmente la proliferación de redes sociales, páginas web, blogs, grupos de mensajes y chats permite que un agresor pueda distribuir a cientos, miles o millones de personas esas imágenes privadas de forma que humillen a las víctimas y a su entorno. La sola amenaza de distribuir esas imágenes puede servir para obligar a las víctimas a realizar actos contra su voluntad.

También puede utilizarse la manipulación de las imágenes fotográficas reales de las mujeres para componer imágenes pornográficas que se publicarán en páginas webs de contactos sexuales y que suelen ir acompañadas de datos personales como su nombre, teléfono o dirección real, lo que ocasionará que la víctima reciba múltiples llamadas obscenas o solicitudes sexuales de personas que no conoce.

4 EVIDENCIAS DEL ACOSO EN LOS TELÉFONOS MÓVILES INTELIGENTES (SMARTPHONES

En casos de acoso, cuando se utilizan aplicaciones de mensajería instantánea como Whatsapp o Line, la identificación del autor es posible tan pronto como la víctima denuncia los hechos, puesto que estos servicios están asociados al titular de la línea telefónica.

En estos casos, la preservación de la prueba, podría realizarse tanto mediante la exhibición ante la policía o los jueces del texto del mensaje amenazante, tanto directamente desde el teléfono, como a través de una captura de la pantalla y remisión posterior. No obstante, en todos los casos, será necesario conservar en el dispositivo original el contendido de las conversaciones, imágenes, vídeos para que en caso necesario puedan ser sometidos a un análisis forense.

Sin embargo existe cierto riesgo en aceptar como prueba, la mera exhibición de los mensajes de texto y whatsapps en el terminal. De hecho éstos pueden ser manipulados o totalmente falsificados, como se puede ver en una publicación la Asociación de Internautas[14] que documenta aplicaciones gratuitas que permiten crear o modificar mensajes recibidos tanto de WhatsApp como SMS, de forma fácil y sin conocimientos técnicos.

[14] http://www.internautas.org/html/8474.html

Efectivamente existen aplicaciones para teléfonos móviles y para sus distintos sistemas operativos (Android, Blackberry, Iphone) que se encuentran al alcance de cualquier usuario y aunque habitualmente los utilizan los adolescentes para hacer bromas, su utilización para falsificar pruebas es posible. Estas aplicaciones lo que hacen es modificar o crear mensajes falsos en el teléfono en el que se han instalado, mensajes que o bien nunca se enviaron o se enviaron con otro texto desde otro terminal. La detección de este tipo de falsificaciones no es sencilla, exige un completo análisis forense de los dispositivos que por su coste y el tiempo que se emplea no se justifica salvo que existan suficientes indicios de la alteración de los mensajes.
También es posible enviar mensajes SMS falseando el número del remitente, la técnica conocida como SMS Spoofing, exige conocimientos avanzados de técnicas de hacking y es utilizada habitualmente para el envío masivo de SMS para obtener claves de acceso a bancos.

Por otro lado, también puede instalarse un troyano en un terminal móvil y de forma remota enviar un mensaje o SMS desde ese terminal con un texto amenazante sin que el titular del teléfono tenga conocimiento.

5 SPYWARE, APLICACIONES PARA EL ESPIONAJE DE LAS VÍCTIMAS

Aunque los programas informáticos creados para el control más o menos legal de la actividad de un terminal han existido siempre, desde los antiguos "keyloggers", que capturaban el texto introducido a través de un teclado, con objeto de capturar contraseñas, hasta los programas de control parental instalados para monitorizar la actividad de los menores en internet, sin embargo ha sido con el auge de los dispositivos móviles cuando estos programas han llegado a su máximo nivel de control del usuario, ya que permiten conocer tanto la actividad que se realiza a través de ellos como los lugares a los que acude el usuario y los más sofisticados pueden servir de micrófonos y cámaras encubiertas.

Y es que el objetivo de estas aplicaciones es controlar la actividad de la víctima las 24 horas del día, sin su consentimiento y sin ser conscientes de esta vigilancia.

Una simple búsqueda en Google de "aplicaciones para espiar a tu esposa" permite acceder a miles de páginas donde se informa de detallada cómo configurar el móvil de tu pareja para conocer sus ubicaciones, movimientos y acciones. Otras páginas informan o comercializan aplicaciones que permite conocer si la pareja es infiel.

Estas aplicaciones, la mayoría de pago, son de fácil instalación, sólo se necesita acceder durante escasos minutos al teléfono móvil de la víctima, y una vez instaladas son invisibles para la víctima, que en el peor de los casos verá reducido el tiempo de uso de su batería o un mayor gasto en el tráfico de datos.

Las posibilidades de estas aplicaciones son varias, desde la geolocalización permanente de la víctima hasta el envío al ordenador del agresor de una copia de todos los mensajes enviados o recibidos por ella, sus comunicaciones por Whatsap, sus SMS e incluso las llamadas de voz realizadas o recibidas. Las versiones más sofisticadas permiten incluso activar de forma remota la cámara o el micrófono del móvil espiado, sin que la víctima se aperciba, y obtener tanto imágenes como sonidos del entorno. Este tipo de tecnología sería similar a la intervención ilegal de la línea telefónica o de la correspondencia privada de la víctima.

Aunque pueda parecer que estas herramientas corresponden más a grandes agencias de inteligencia u organizaciones criminales complejas, lo cierto es que en internet, cualquiera por menos de 100€, puede conseguir aplicaciones similares, sólo necesitará acceder menos de un minuto al móvil de la víctima para instalarlo.

Tampoco en estos casos debe olvidarse que una forma de localizar a las víctimas son los hijos que conviven con la víctima, en determinados casos los agresores habían regalado a sus hijos smartphones con spyware o con configuraciones que permiten su localización.

Pero la seguridad no solo debe restringirse a los dispositivos móviles, ordenadores de sobremesa, tablets y más recientemente televisiones con la función smartTV, pueden ser configurados para obtener imágenes y enviarlas por internet a direcciones de los agresores.

La respuesta de las víctimas no puede ser renunciar a las posibilidades que ofrecen las nuevas tecnologías, que son una forma de comunicación inmejorable para buscar redes de apoyo y colaboración, mantener el contacto con su familia.

Por todo lo anteriormente expuesto, sería recomendable, proporcionar a las víctimas de violencia de género, otra serie de consejos, éstos sobre la seguridad de su teléfono móvil:

- Proteja su teléfono con una clave que solo Ud. conozca y no la comparta con nadie.
- Cuando no lo necesite, desconecte la geolocalización de su teléfono móvil.
- Nunca instale en su teléfono móvil aplicaciones procedentes de fuentes desconocidas.
- Utilice un antivirus gratuito que detecte la existencia de spyware o malware en su terminal, por ejemplo "CONAN MOBILE"[15]

6 APLICACIONES PARA LA PROTECCIÓN A LAS VÍCTIMAS.

Las víctimas de violencia de género también pueden utilizar sus dispositivos móviles como recurso para evitar volver a sufrir una agresión, la localización GPS, junto con distintas aplicaciones que permiten alertar a la policía en caso de necesidad puede ser una ayuda inestimable para la víctima en cuando se vea amenazada.

En España, y desarrollada por la Secretaría de Estado de Seguridad, está disponible la aplicación AlertCops, que puede descargarse gratuitamente para dispositivos móviles Android y Apple[16], y mediante la cual la usuaria, una vez registrada, puede generar una alerta, seleccionando, a través de iconos, la opción que mejor describa la situación: robo o atraco, agresión, agresión sexual, acoso escolar, desaparición de personas, etc. que quiera reportar a las FCSE, a continuación tanto la alerta, como la localización exacta de su terminal será remitida a las Salas Operativas de la Guardia Civil o Cuerpo Nacional de Policía.

Además permite que el agente que reciba la comunicación pueda dirigirse por chat al ciudadano para obtener más información. La utilización de iconos, además de que la aplicación está disponible en varios idiomas, permite su utilización por extranjeros o personas con discapacidad auditiva.

[15] http://www.osi.es/es/conan-mobile
[16] https://alertcops.ses.mir.es

A partir de octubre de 2015, esta aplicación incluirá una opción para víctimas de violencia de género que permitirá alertar a los servicios policiales en caso de una agresión o amenaza de este tipo.

Además de esta aplicación, otras administraciones han desarrollado aplicaciones para teléfonos móviles para ayudar a las víctimas de violencia de género:

- Libres[17]: herramienta de ayuda a mujeres que incluye llamada al 016 y testimonios de víctimas.
- ¡No te pases![18], desarrollada por el Ayuntamiento de Santa Cruz de Tenerife, ofrece información sobre la violencia de género y su prevención.

Por último, como iniciativa sorprendente, en Estados Unidos, está disponible la aplicación iEAA (Evidentiary Abuse Affidavit)[19], desarrollada por la abogada especialista en violencia de género Susan Murphy-Milano, y que consiste en una aplicación para teléfono móvil que crea un testamento vital que combina declaraciones en vídeo de la víctima, documentos, información sobre el agresor y otra serie de evidencias para poderse utilizar en el caso de que la mujer muera o desaparezca. Toda esta información es almacenada online y disponible para los investigadores en caso de que la víctima tenga un desenlace trágico. Sin embargo lo deseable de un recurso es que evite tener que llegar a esta solución.

[17] Disponible en Google Play, https://play.google.com/store/apps/details?id=com.fraileyblanco.android.libres y en https://itunes.apple.com/es/app/libres/id582602376?mt=8
[18] Disponible en Google Play, y en https://play.google.com/store/apps/details?id=pixitec.notepases
[19] http://www.documenttheabuse.com