Ciberacoso
y violencia de género en redes sociales

Análisis y herramientas de prevención

Coordinadora: María Ángeles Verdejo Espinosa

Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

Capítulo VIII

Privacidad, factor de riesgo y protección en la violencia digital contra las mujeres

Jorge Flores Fernández[1]

En la nueva sociedad digital, las mujeres de todas las edades (niñas, adolescentes, jóvenes y más adultas) vuelven a ser el principal grupo de personas victimizadas. El ciberacoso sexual, el maltrato y la ciberviolencia de género tanto psicológica como sexual son auténticas plagas contra las que toda medida, sin excepción, debe ser activada. Una de estas medidas es el fomento de la cultura de la privacidad como es estrategia de prevención y protección individual y colectiva.

Cuando PantallasAmigas inició su andadura en 2004 la privacidad no era una de sus prioridades. Sin embargo, dos años más tarde, al popularizarse los llamados "blogs" y servicios al estilo Fotolog donde los y las usuarias se convertían en editoras de información, pasó a ser uno de los ejes de nuestra acción preventiva. Con las redes sociales, privacidad y datos personales han pasado al primer plano. Sirve de ejemplo cómo Facebook, que acaba de cumplir diez años, presionado por las autoridades europeas y por las y los usuarios, anunció mejoras en la protección de la privacidad y datos de los usuarios cuando se encontraba a escasos días de salir a Bolsa.

1 Director de PantallasAmigas.

Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

1. Privacidad como derecho y factor de protección

A finales de 2013 la Asamblea del Naciones Unidas ratificó un documento donde destacaba el derecho a la privacidad en la era digital. Pero, al margen de eso, la privacidad es un factor de protección de primer orden: cuanto menos se sepa de una persona, menos vulnerable es. En una sociedad digital donde existe una asimetría de poder tan grande entre víctima y victimario es preciso no dar ningún tipo de ventaja a quienes usan las posibilidades y herramientas de la Red para hacer daño. Ejercer la violencia digital es fácil, rápido y queda muchas veces impune.

En Internet todas y todos somos podemos ser más fácilmente victimizados. Si bien el objetivo final es que no hubiera personas violentas o que éstas no pudieran llegar a hacer daño, mientras esto no sea así está a nuestro alcance tratar de disminuir las víctimas o bien el daño que les es infligido; la cultura de la privacidad es una buena aliada para ello.

2. Privacidad en las redes sociales: nosotras, las demás personas y la red social

Nuestra privacidad depende cada vez menos de nosotras o nosotros mismos y más del resto de personas y de las redes sociales (o cualquier tipo de software que nos ayuda a socializarnos y, sobre todo, a socializar nuestra información).

Está en nuestras manos publicar una determinada información o imagen pero esa decisión no siempre se toma de la manera adecuada bien porque no somos conscientes de dónde puede llegar a parar esa información o porque desconocemos el funcionamiento de la red social o bien porque hemos configurado de manera inadecuada nuestras opciones de privacidad.

Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

No obstante, es mucho más frecuente que sean las demás personas con las que generalmente compartimos momentos las que más afectan a nuestra privacidad. Haber participado o ser testigo de ello les hace creerse con derecho a contarlo a los cuatro vientos… y el problema es que la información corre no como un reguero de pólvora, sino como cientos entrelazados. Un caso especialmente lesivo es el de las etiquetas en las fotografías de las redes sociales mediante las cuales alguien, sin previo aviso ni permiso, identifica a una persona en una imagen asociándola a su perfil. Ese acto aparentemente tan liviano supone algo tan grave como hacerla visible en la fotografía lo que significa decir en muchos casos qué, con quién, cómo y dónde se encontraba. Es nuestra vida contada por otras personas a golpe de etiquetas.

Sin duda, quien tiene más capacidad para salvaguardar nuestra privacidad en las redes sociales son las propias redes, esto es, el software que las gestiona y quienes deciden cómo cada plataforma va a funcionar y, por lo general, no lo hacen bien. Por supuesto, hay excepciones y grados pero Facebook, la referencia, no se caracteriza por su celo en el asunto. Su misión parece más bien dejar abiertos a los ojos de los demás nuestros datos y actos lo que, a la vez, genera un efecto dominó. Por ello es de aplicación la conocida frase "si no eres el cliente, eres el producto"... y Facebook es gratis. Analicemos algunas de las prácticas que podemos observar en redes sociales:

- Mueven información, la agitan, la expanden, la multiplican. Aprovechan cualquier ocasión para tratar que las personas sepan algo nuevo sobre sus contactos: una imagen nueva, un comentario, un "me gusta", un nuevo "amigo"…

Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

- Insisten en que participes con mensajes que te incitan a opinar, a etiquetar… lo que genera a su vez visibilidad sobre lo que tú haces.
- Disponen de determinadas funciones cuyo alcance nos cuesta imaginar y que, por lo general, implican socialización de la información más allá de lo esperado. Se presentan como una forma de facilitarnos las cosas, de ayuda, o directamente funcionan sin aviso en un discreto pero efectivo segundo plano. Un ejemplo tan claro como extremo de esto es la función de reconocimiento facial que dice nacer con la intención de ahorrarnos el trabajo de etiquetado manual.
- Analizan con precisión nuestros intereses, datos, contactos y actividad dentro de la red social y en función de los mismos trazan nuestro perfil para actuar sobre él de forma interesada u ofrecérselo segmentado a terceras empresas.
- Permiten la entrada de aplicaciones externas como pequeños juegos o programas que, aunque sean de uso voluntario y gratuito, están accediendo a datos, muchas veces innecesarios, que poseen de sus usuarios sin que estos sean debidamente avisados.
- Realizan cambios importantes en su forma de funcionamiento o propiedades, incluso en aspectos tan importantes como la privacidad, sin avisar de manera suficiente a los usuarios para que se adapten a las nuevas condiciones. Provocan cierta sensación de premura y temporalidad que desemboca finalmente en que los usuarios desistan: "para qué revisarlo si no tengo tiempo; no sé muy bien cómo funciona ahora, no entiendo del todo qué va a cambiar y quién sabe cuándo lo van a volver a reajustar".

Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

Personalmente creo que algunas redes sociales no tienen ninguna intención de que controlemos nuestra privacidad. Por la presión de las autoridades, especialmente en Europa, y de los usuarios van haciendo pequeños cambios que, aunque son avances, nunca compensan las concesiones que en otras áreas van logrando, por lo que el saldo a la fecha es cada vez más negativo para el usuario/consumidor. Eso sí, anunciando cambios logran tres objetivos:

- Conseguir que creamos que podemos llegar a gestionar nuestra privacidad y que a ellos el asunto les importa.
- Entretenernos mientras hablamos de ello o intentamos saber qué suponen los cambios en realidad.
- Hacernos desistir de conocer cómo funciona su entorno o bien crear confusión sobre un modo de operar al que ya nos habíamos acostumbrado.

Viendo que el control de nuestra privacidad está en nuestras manos solo en una muy pequeña parte, la protección de datos personales que desarrollan las autoridades debe completarse con nuestra protección personal, proactiva y compartida, de los datos.

3. Smartphones: malware, Apps y geolocalización

Sin darnos cuenta, tenemos un ordenador en el bolsillo que se llama *smartphone*. Un computador que sirve para mantener conversaciones telefónicas pero desde el que hacemos muchas otras cosas como acceder a nuestro correo electrónico, interactuar en las redes sociales u orientarnos usándolo como brújula o navegador al estar dotado de GPS. Se trata también de un ordenador al que agregamos nuevos progra-

Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

mas que descargamos de Internet, las Apps (abreviatura de aplicaciones en inglés). Al llevarlo siempre encima lo dotamos de nuevas funcionalidades que nos pueden ser útiles y guardamos información muy personal en él.

Sin embargo, estas posibilidades que sí usamos llevan consigo problemas que no llegamos a valorar en su justa medida y que pueden afectar a nuestra privacidad. Mencionamos a continuación algunos de ellos:

- Malware: como ordenadores que son están sujetos a software malicioso que, entre otras cosas, puede espiar nuestros datos y claves de acceso.
- Apps: son programas que instalamos en nuestro terminal pero de los que no siempre tenemos garantías de que vayan a respetar lo que allí pueden encontrarse.
- Geolocalización: disponen de las coordenadas de posición en cada momento y no siempre somos conscientes de lo que este dato puede suponer, en especial en combinación con otras informaciones.

Otras situaciones, aunque de diferente índole, donde podemos vernos en apuros es en caso de pérdida o robo, en especial si las claves de acceso están grabadas y sin protección.

4. El rastro de la navegación y el valor añadido de datos combinados

Las *cookies* son pequeños ficheros que se van grabando en nuestro equipo cuando navegamos. Son pistas, datos muy diversos que las páginas consultadas van dejando. En ocasiones, nos identifican para facilitar el uso de nuestros programas y que no tengamos, por ejemplo, que meter el usuario y

Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

la clave cada vez que entremos a Facebook. También ayudan a que nos aparezca un entorno personalizado, inteligente, sensible al contexto. En otros casos, sirven para indicar dónde estamos y qué hacemos al navegar. Un uso inadecuado o abusivo de estas informaciones puede crear problemas de seguridad y privacidad.

Cuando en Marzo de 2012 Google comenzó a aplicar su nueva política unificada de privacidad, las consecuencias no se hicieron esperar y desde la Unión Europea se puso en duda que cumpliera las normas comunitarias de protección de datos al combinar informaciones de los clientes en sus diferentes servicios (buscador, red social, correo electrónico…). Se trata de informaciones que, convenientemente cruzadas, aportan una nueva dimensión de conocimiento sobre la identificación, hábitos, y ámbito relacional de las y los usuarios. De nuevo, la industria justificaba un menoscabo de nuestra privacidad con la excusa de buscar un servicio más personalizado.

5. El Derecho al olvido

Desde la Comisión Europea se han venido preparando una serie de cambios legislativos en materia de privacidad y protección de datos personales que incluyen lo que se ha dado en llamar "el derecho al olvido". Es un concepto algo complejo de acotar y complicado de articular pero se puede concretar en las palabras de la propia Comisaria de Justicia: "los datos pertenecen a las personas y si un usuario quiere retirar del servicio los datos que ha puesto, debe poder hacerlo".

La memoria eterna que tiene la Red o las bases de datos de los servicios, incluyendo a los buscadores, supone en ocasiones, por evocación de datos no pertinentes, muy antiguos, caducos e incluso inciertos, una intromisión a nuestra privacidad, honor e imagen.

Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

6. Diez recomendaciones para mejorar tu privacidad

- Impide la entrada de *malware* al ordenador o dispositivo móvil, es el primer paso.
- Usa claves de acceso que no sean fáciles de descubrir, no las cedas y cámbialas periódicamente.
- Elige y configura tu navegador teniendo en cuenta el control de las *cookies*.
- Presta atención a las opciones de privacidad de las redes sociales. Asegúrate de que sabes lo que significan y revísalas de vez en cuando. Pon especial interés en las relativas al etiquetado.
- Tu privacidad depende de las personas con las que te relacionas. Tenlo siempre en cuenta y contribuye a una cultura del uso responsable de la información personal; es una cuestión colectiva.
- La defensa de tu privacidad debe ser proactiva. Es preciso que dejes tu postura clara al respecto para evitar equívocos y velar porque sea respetada.
- Presta atención al servicio de geolocalización y a los metadatos en las fotografías.
- Bloquea el acceso a tu *smartphone* con un código de seguridad.
- Antes de instalar una App en el móvil valora si realmente merece la pena y cuáles los permisos de acceso que exigen que concedas para ello.
- Pequeños datos y detalles se van acumulando y conformando tu perfil a lo largo del tiempo. Tenlo en cuenta y limita lo que entregas.

Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

7. Recursos para el fomento de la cultura de la privacidad y la protección de datos personales

A continuación se citan algunos recursos de utilidad para la educación en la cultura de la privacidad:

- Canal YouTube de PantallasAmigas, con abundantes vídeos sobre el tema, es el mayor canal educativo mundial de Internet Safety con más de 25 millones de visualizaciones y 50.000 personas suscritas.
  https://www.youtube.com/user/pantallasamigas

- Directorio de referencias sobre privacidad y protección de datos personales.
  http://www.proteccionprivacidad.com/

- Oficina de Seguridad del Internauta, con herramientas gratuitas de diagnóstico de malware y antivirus.
  http://www.osi.es

- Web con información sobre *sexting*.
  http://www.sexting.es

- Web con información sobre sextorsión.
  http://www.sextorsion.es

Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528