revista pensamiento penal

Las redes sociales de encuentros y la seguridad

Por Gustavo Sain

@grsain

Históricamente la tecnología ha oficiado como intermediaria para que las personas puedan contactarse entre sí para establecer algún tipo relación sentimental. La era analógica estuvo caracterizada por las emisiones radiales nocturnas de citas y los programas televisivos al estilo del histórico "yo me quiero casar y usted" de Roberto Galán. En radio, estos programas -o micros dentro de los programas- constaban en que dos personas para que dialoguen entre sí al aire para que se "conozcan" para que luego la producción proveyera los números telefónicos a los protagonistas para se puedan encontrarse en persona. En los programas televisivos de este estilo, un grupo de hombres y mujeres –en su mayoría adultos mayores- se presentaban frente a la cámara con el objetivo de elegir una posible candidata para pasar el resto de su vida, un verdadero reality show del amor.

Ya en la década del 90 con la digitalización de las comunicaciones y la llegada de Internet, el advenimiento de las líneas telefónicas de encuentros y los chats eróticos en sitios web específicos anticipaban una nueva era en materia de encuentros a distancia. Con la popularización de la red comienzan a surgir los sitios de citas, donde a partir de una suscripción con tarjeta de crédito el usuario podía interactuar virtualmente con otras personas a través de los servicios de comunicación que brindaba la plataforma. Pero con la llegada de los *smartphones* o celulares inteligentes comenzaron a aparecer aplicaciones específicas conocidas comúnmente como redes sociales de encuentros, tales como Tinder, Badoo o Happn entre otras, la mayoría de ellas de uso gratuito en sus funciones básicas.

Estas redes representan un catálogo de personas en línea que a diferencia de lo que sucede en el mundo físico, uno puede intentar algún tipo de acercamiento con alguien en base preferencias personales del usuario establecidas previamente. En base a la "ficha de datos" de un perfil de usuario -foto, identidad de género, edad y preferencias

sexuales, entre las más comunes- el interesado o interesada puede contactarse en la plataforma mediante un "me gusta" o manifestación de afinidad. Muchas de estas aplicaciones se encuentras asociadas al GPS del celular, lo que permite la interrelación a través de la cercanía por zona geográfica de acuerdo a la localización de un usuario al momento de loguearse. En estos casos la aplicación oficia de amigo "presentador" que intermedia brindando diferentes opciones al usuario en base a esos criterios de búsqueda que se establecen de antemano.

Si bien estas aplicaciones son presentadas para hacer amistad o búsqueda de parejas, su uso mayoritario es el contactar gente para establecer relaciones sexuales. Las relaciones estables se pueden dar o no pero el inicio de las mismas de da en forma inversa a las relaciones que se establecían antes del auge de los entornos multimedia, donde después de un acercamiento cara a cara entre dos personas en un ámbito específico se podía saber si "se gustan" o no tras una serie de intercambios y encuentros presenciales previos. El éxito de las redes sociales de encuentro es que evita en contacto cara a cara inicial para los rituales convencionales de conquista ya que los vínculos entre usuarios comienzan sabiendo que entre ambos hay cierta afinidad en base a algún criterio de preferencia.

A partir del caso de violencia que involucró a Gerardo Birillis -médico anestesista- y Belén Torres una chica de 20 años que había conocido a través de Tinder, algunos medios de comunicación pusieron el ojo en estas aplicaciones y sitios web calificándolos como "riesgosos". Si bien es cierto que a través de Internet se puede ocultar la verdadera identidad de una persona, el principal riesgo es no saber quién se encuentra del otro lado de la pantalla a partir de las condiciones de anonimato que provee la web. Más allá de esta condición de seguridad a tener en cuenta como regla básica de seguridad, las recomendaciones no varían demasiado con los primeros contactos que una persona inicia con un desconocido.

Algunas recomendaciones para el uso de estos servicios y aplicaciones son:

- En primer lugar, antes de establecer un encuentro cara a cara con un usuario, se recomienda establecer previamente un intercambio vía webcam con la otra persona para verificar que quien está detrás de la pantalla es quien dice ser. Como se señaló anteriormente la red permite la construcción de identidades ficticias con el simple uso de una fotografía de las miles que hay en la web y la elección de un nombre falso, inclusive de otro sexo.

- Una vez producidos diferentes intercambios virtuales dentro de estas redes, si dos personas deciden conocerse cara a cara, se recomienda que el encuentro se realice en un lugar neutral, ni en la casa del usuario ni del interesado/a. en este caso un lugar público, un café, un bar, un boliche, -donde haya gente- o en un espacio abierto como una plaza por ejemplo.

- Si tras varias comunicaciones previas los usuarios acuerdan tener relaciones sexuales en el primer encuentro, que el encuentro sea en un hotel y no en ningún domicilio particular.

- Muchas de estos servicios permiten vincular el perfil con otras redes sociales como el caso de Tinder, que asocia la foto y los datos personales del usuario al perfil de Facebook. Ahí todo cambio que realice en Facebook se va a ver reflejado en Tinder. En este caso se recomienda configurar la privacidad de la información de figura en la biografía de pública a privada y no volcar datos como domicilio, colegio o empresa, numero de celular en estos sitios.

- Hay que tener en cuenta que Tinder, por ejemplo, cuando se usa desde el celular utiliza el GPS para geolocalizar contactos cercanos. Si bien no muestra la ubicación exacta dice que tal o cual persona se encuentra a cierta cantidad de metros desde donde se conecta el usuario. Esto se debe tener en consideración en términos de la seguridad física de las personas ante cualquier eventualidad.

Por otro lado hay cuestiones que no tienen que ver con un buen uso o uso responsable de los usuarios de estas redes sociales y que también existen factores como **la seguridad de la información que brindan los proveedores de servicio de internet**, que no depende de las distintas precauciones que pueden tomar los usuarios de estos entornos virtuales. Los usuarios tienen que tener esto en consideración a la hora de analizar qué datos e información van a volcar en estos sitios o que material intercambian dentro de los chats o foros -fotos, videos, audios, etc.- ya que otra regla de seguridad de Internet es que *nada es invulnerable en términos de seguridad informática*.

Un ejemplo de esto sucedió con Ashley Madison, la red social de encuentros de infieles más popular del mundo. Con más de 40 millones de usuarios en todo el mundo y publicitada como la mejor vía para tener aventuras sexuales fuera del marco de una pareja formal, mediante el pago de un abono mensual con tarjeta de crédito los usuarios se suscriben bajo condiciones de estricta discreción. En 2015 un grupo de hackers saboteó la base de datos de la empresa y con ellas los nombres, direcciones de correo electrónico, números de tarjeta de crédito y todo tipo de conversaciones privadas de sus usuarios. Intentos de extorsión, chantajes fraudulentos -donde se pedía dinero a cambio de filtrar esos datos a su pareja fueron moneda común por varios meses.

Por ultimo está el tema del **sexting**, es decir, la práctica que consiste el intercambio de material multimedia –audios, fotos y videos- de producción propia con contenido erótico y/o pornográfico mediante servicios y aplicaciones de Internet. Si bien la mayoría de las redes sociales de encuentros solo habilitan un chat para que los usuarios puedan intercambiar entre sí, lo más común es que a través del mismo los usuarios con mayor afinidad intercambien celulares para tener un contacto más personalizado. Sea como primer acercamiento antes de un encuentro o como fin en sí mismo, esta práctica también es conocida como *cibersexo*. En primer lugar no sabemos lo que la otra persona va a hacer con ese material porque no tenemos confianza, obviamente el riesgo acá es la *viralización, es decir, la reproducción masiva por diferentes servicios y aplicaciones de Internet*.

Inclusive pese a que cualquiera de los protagonistas no vulnere la intimidad de un usuario filtrando ese material, si alguno de los mismos lo almacena en su dispositivo –computadora, tablet o celular- corre el riesgo de que sea extraviado, robado, e inclusive también pueda ser hackeado. También los fallos de seguridad de las empresas proveedoras de servicio, como sucedió en el caso Ashley Madison. La recomendación en estos casos es que no lo practiquen, si asi todo deciden hacerlo, que los involucrados no se retraten los rostros que permita la identificación de la identidad de la persona frente a una posible publicación en la web.

**Especialista en cibercrimen, asesor de la Dirección nacional de Política Criminal del Ministerio de Justicia y DDHH de la Nación y profesor universitario.*