La PRIVACIDAD en los servicios de **Internet**

Rafael **Ponce Medellín**
Jorge A. **Ruiz Vanoye**
Gabriel **González Serna**

Con la creciente popularidad que han tomado las redes sociales surgen cuestionamientos sobre el impacto que estas tienen en las personas. Uno de los cuestionamientos que más fuerza ha tomado se refiere a la privacidad, es decir, qué tanta información se puede dejar publicada al alcance de todos, así como la manera en que esta puede ser usada, inclusive en contra de los mismos usuarios.

Personas con diversas intenciones se pueden enterar de las actividades que alguien ha realizado, los lugares que ha visitado o a los que asiste frecuentemente, momentos embarazosos, entre otros datos. Las redes sociales son una ventana hacia los hábitos, gustos, actividades, es decir, la vida misma de las personas.

Para muchas personas es muy fácil publicar en su red social todo tipo de información sin tomar en cuenta las consecuencias de no delimitar quiénes pueden tener acceso a qué contenidos. Esto puede y ha acarreado problemas, desde personas que han perdido su trabajo, divorcios, etcétera.

Y si eso no fuera suficiente, se suma otra variable a la información que se hace pública: la localización. El abaratamiento de tecnologías como el GPS ha hecho posible que se tome en cuenta el factor geográfico dentro de las redes sociales, permitiendo que los usuarios puedan indicar en qué lugar se encuentran o dónde fue tomada una foto. Si bien la información geográfica puede ser útil para distintos fines (como saber qué hay alrededor de un lugar, encontrar contactos o lugares cercanos, llevar un mejor registro de colecciones de fotos al saber dónde fueron tomadas, etc.), esto abre nuevas consideraciones y medidas de seguridad que las personas deben tomar en cuenta antes de subir y publicar en alguna red social.

Hemos entrado a una era donde todo lo que se publique, haga o diga, quedará registrado. Una era en la que destacan distintos medios sociales, cada uno con sus propios dilemas con respecto a la privacidad, como se verá a continuación.

EL CASO DE FACEBOOK

Los comienzos de Facebook se remontan a una red social exclusiva para un entorno universitario que quedó a disposición del público en septiembre de 2006, convirtiéndose con el paso de los años en la red social con más usuarios del planeta. Sin embargo, al pasar de ser una red universitaria a una red mundial, la información que se había estado publicando empezó a quedar al alcance de cualquiera, con lo que los usuarios fueron perdiendo cada vez más su privacidad. Esto llevó a que Facebook cambiara sus políticas de privacidad (como se puede apreciar en *La evolución de la privacidad en Facebook* [1]).

Al quedar esta información al alcance de otros, se ha planteado un número de cuestionamientos distintos acerca de qué tan válido y ético es aprovechar estos datos para diversos fines ajenos a la misma red social. Por ejemplo, existen compañías que visitan el perfil de sus aspirantes a empleados para obtener una perspectiva distinta de la persona, ajena a su currículum; esta acción, sea justa o no, sólo muestra el hecho de lo que alguien puede hacer: tomar información de la vida personal de un usuario y usarla en su contra. Como contramedida para evitar estas situaciones, en Alemania se encuentra en estudio una ley que prohibiría que las empresas tomen en cuenta el perfil de Facebook de los candidatos a un trabajo, marcando una diferencia entre lo que es la vida personal del postulante y su aspecto profesional.[2]

Otro dilema relacionado con Facebook recae en las aplicaciones que se ejecutan sobre esta plataforma. Un gran número de ellas consisten en simples preguntas del tipo: color favorito, artista preferido, frases de alguna celebridad, etcétera aplicaciones inocentes y comunes, pero que bien pueden permitir que los desarrolladores tengan libre acceso a la información de los usuarios y de sus contactos, como lo demostró la American Civil Liberties Union.[3] La única advertencia de seguridad que se muestra al usuario de estas aplicaciones es un mensaje que la mayoría de los usuarios acepta sin más consideraciones. Esta organización también demostró que Facebook no toma en cuenta la veracidad y confiabilidad de los creadores de aplicaciones, limitándose a que sólo indiquen si aceptan los términos del servicio, sin dar un mayor seguimiento.

Estatua para adivinación. Etnia Yoruba, Nigeria.

Estatua para adivinación. Etnia Yoruba, Nigeria.

Finalmente, otro problema relacionado con la invasión a la privacidad en Facebook, es que guarda una referencia de las personas que se han importado desde las listas de correos de sus usuarios, aunque estas personas no se hayan registrado. Estas listas quedan guardadas hasta que de manera explícita se les elimine. Esta situación fue alertada por el gobierno de Alemania como una manera de proteger la privacidad de sus ciudadanos.[4] Facebook no es el único medio en Internet que ha tenido problemas con la privacidad de las personas. Con el avance de las tecnologías para la geolocalización se han formado redes sociales alrededor de estas, que también han tenido sus dificultades.

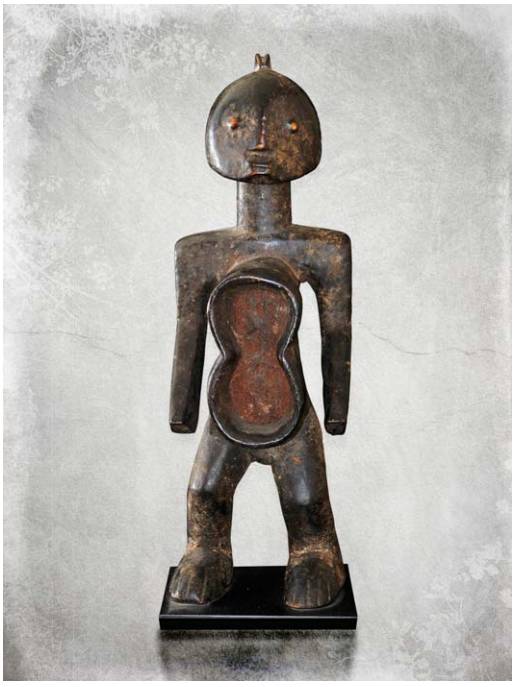
PRIVACIDAD EN LA GEOLOCALIZACIÓN

Poco a poco han surgido redes sociales basadas totalmente en la geolocalización (Foursquare, Gowalla) o la implementación de características de geolocalización en medios sociales ya existentes (Twitter, Facebook, etc.). El uso descuidado de estos medios puede ocasionar problemas de privacidad al publicar información de manera abierta, permitiendo así que cualquiera pueda conocer dónde se encuentra alguien o los lugares que visita. Un ejemplo del mal uso de esta información por terceros es el de una persona que publicó en Foursquare que salía a comer y, estando en el lugar de reunión, recibe una invitación telefónica a salir por parte de un desconocido que leyó esta información. La víctima siente que su privacidad ha sido violada, pese a que ella misma publicó abiertamente dónde y en qué momento se encontraba.[5]

El problema no se restringe sólo a lo que los usuarios publican de manera explícita, sino también a la información que se puede extraer de las fotos que publican. Una simple foto puede contener información como fecha, detalles de la foto y de la cámara y, con la ayuda de dispositivos como los GPS, también pueden incluir la localización geográfica de donde fue tomada. Si bien esto puede ayudar para organizar la colección de fotos de una persona, la publicación descuidada de imágenes en la red brinda información a terceros sin que el dueño de la imagen se percate, como se verá en el caso siguiente.

¿INVITANDO A LOS ASALTANTES?

Tomando en cuenta que el servicio de Twitter soporta geolocalización de los *tweets* (es decir, los mensajes que publican los usuarios), esta información podría ser usada con otros fines. Prueba de ello es que en fechas recientes surgió un sitio Web que tomaba en cuenta la localización de los tweets para informar cuándo un usuario no se encontraba en casa; dicho sitio se llamaba: PleaseRobMe.com (Por favor róbame, página actualmente fuera de servicio). De manera semejante a este sitio, se presentó *I Can Stalk U* (Te puedo robar, http://icanstalku.com/), el cual se basa en la información que se puede obtener de imágenes vía Twitter. Dentro del sitio se muestra la información del *tweet* original, la localización de la foto en un mapa, así como la fotografía en cuestión. El objetivo del sitio es alertar a los usuarios a que tomen precauciones sobre la información que comparten, siendo que actualmente muchas cámaras y teléfonos celulares ya cuentan con dispositivos GPS y pueden etiquetar automáticamente una foto con datos sobre su geolocalización.



Copa antropomórfica para el vino de palma. Etnia Koro, Nigeria.

LOS PROBLEMAS DE GOOGLE

Google maneja una gran cantidad de información sobre los usuarios y, por lo mismo, varios países han llamado a poner especial atención en el manejo que se haga de la privacidad por parte de esta compañía. Entre estos países se encuentran Francia, Alemania, Israel, Italia, Irlanda, Países Bajos, Nueva Zelanda, España, Reino Unido y Canadá, que han solicitado a Google que proteja la privacidad de sus usuarios.[6] Pero, ¿qué ha motivado a que estos países decidieran manifestar su preocupación por la manera en que Google maneja la información personal? Una de las causas se debe al servicio de Google Buzz y su problemático inicio.

Google Buzz se trata de un intento de Google por presentar un servicio de microblogging y de red social, de manera semejante (pero no igual) a otros servicios como Twitter. Durante el lanzamiento, se pretendía automatizar la importación de contactos de correo de Gmail de una persona para ponerlos como sus seguidores dentro de Buzz. El resultado fue un rotundo error; si bien inicialmente la intención parecía buena, el problema radicó en que este listado de contactos quedaba visible de manera pública. Esto tiene una importancia mayor si se considera que la información de disidentes iraníes quedaba descubierta, contactos anónimos de periodistas se volvían públicos, entre otros sucesos de índole más particular.

Google corrigió y cambió esta situación, sin embargo el impacto negativo ya se había propagado, lo que llevó a que en ciudades como Washington y San Francisco se realizaran demandas colectivas por parte de la comunidad de usuarios afectada por estos fallos. Otra consecuencia fue que el FTC (Federal Trade Commerce) solicitó una investigación por la violación de leyes federales en Estados Unidos sobre la escucha e intercepción de comunicaciones.[7] Google también tiene problemas a causa de su servicio Google Street View, servicio que muestra imágenes panorámicas de distintas partes del mundo con gran nivel de detalle. Uno de los métodos que Google utiliza para capturar estas imágenes es a través de vehículos que recorren las ciudades tomando fotos estereoscópicas del lugar que esté visitando. Estas capturas han mostrado transeúntes caminando, vehículos, fachadas de las casas, e incluso situaciones hilarantes de personas que al saber que el vehículo de Google va a pasar, aprovechan su creatividad y realizan algún montaje para, que al ser retratados, aparezcan así en el servicio de mapas. Pero no todas las personas están de acuerdo en que su rostro aparezca así de fácil en Internet. Para tranquilizar a quienes se oponen a ello, Google empezó a difuminar los rostros de las personas; sin embargo, en Alemania consideraron que este servicio viola la intimidad de los ciudadanos. A partir de ello, en dicho país consideraron que es el mismo Google quien tendría la obligación de pedir permiso a los ciudadanos para que aprueben la publicación de imágenes de sus casas, ya que en caso contrario se consideraría una intromisión a la propiedad privada.[8]

Otro ejemplo ocurrió en España, en donde se llevó ante los tribunales a Google en un caso también relacionado de manera indirecta con Street View. Mientras que los vehículos de Google tomaban fotos panorámicas de los lugares que visitaban, también interceptaban información de las redes Wi-Fi que encontraban en el camino. A causa de lo mismo, en Corea del Sur la policía confiscó los datos de los servidores de las oficinas de Google, por la presunta recolección ilegal de información personal.[9] Desde Google se han disculpado

por este error, el cual califican de accidental.[10] Por lo menos en Estados Unidos, Google salió bien librado legalmente de esta situación gracias a las distintas medidas que comenzó a implementar para proteger la privacidad de los usuarios; sin embargo, en otros países, aún continúa el litigio contra Google.

RECOMENDACIONES GENERALES

Para concluir, con base en los puntos anteriormente expuestos, se muestra una recapitulación a tener en cuenta, así como herramientas de utilidad para minimizar el riesgo de vulnerar la privacidad propia dentro de una red social.

- Configurar el nivel de privacidad deseado. Siempre se debe estar consciente de que la información que se publica en los medios sociales puede ser difundida o accedida por otros, por lo que se debe hacer uso de las distintas directivas y configuraciones existentes en cada red y delimitar a qué se puede tener acceso y por parte de quiénes. Algunas herramientas para su uso en Facebook son, por ejemplo, PrivacyDefender, la cual valora qué tan pública es la información que un usuario muestra en su cuenta y permite ajustar automáticamente la configuración de privacidad al nivel elegido; por su parte, PrivacyCheck califica la privacidad de la cuenta de un usuario y muestra la información que pudo extraer de la cuenta en cuestión.
- Limitar el acceso de terceros a nuestra localización geográfica. En las redes sociales que utilizan geolocalización debe tenerse cuidado para que sólo un grupo determinado de personas pueda enterarse de esta información. Caso contrario, puede haber sorpresas, ya sea por encontrarse a gente no deseada en un punto de encuentro, o por avisar, de forma abierta, que la persona no se encuentra en casa, como se vio previamente.
- Eliminar o tener en consideración la información que se puede obtener de fotos. Existen herramientas, tanto gratuitas como de paga, que ayudan a eliminar las etiquetas que se agrega a las fotos y datos como la fecha y lugar en que fueron tomadas. Algunos ejemplos son JPEG & PNG Stripper y GeoTag Security.

Al final, depende de cada persona el cuidado que le dé a la información que publica, siendo cada uno responsable de lo que comunica y a quién lo comunica.

REFERENCIAS

[1] McKeon M. The Evolution of privacy on Facebook, http://mattmckeon.com/facebook-privacy/, última visita: octubre 2010.

[2] Alemania prohibiría usar Facebook como filtro para contratar personal, www.lanacion.com.ar/nota.asp?nota _ id=1298396, última visita: octubre 2010.

[3] Perez S. What Facebook Quizzes Know about You, www.readwriteweb.com/archives/what _ facebook _ quizzes _ know _ about _ you.php, última visita: octubre 2010.

[4] Shiels M. Germany officials launch legal action against Facebook, BBC News, http://news.bbc.co.uk/2/hi/technology/8798906.stm, última visita: octubre 2010.

[5] http://blog.sheasylvia.com/post/809428679, última visita: octubre 2010.

[6] Letter to Google Inc. Chief Executive Officer, http://www.priv.gc.ca/media/nr-c/2010/let _ 100420 _ e.cfm, última visita: octubre 2010.

[7] www.genbeta.com/a-fondo/buzz-y-la-privacidad-google-comienza-a-recibir-demandas-colectivas-como-panes, última visita: octubre 2010.

[8] http://alt1040.com/2010/05/google-pide-disculpas-por-robar-datos-de-redes-wifi, última visita: octubre 2010.

[9] The New York Times, Police in South Korea Raid Google's Office, http://www.nytimes.com/2010/08/11/technology/11google.html _ r=2&ref=technology, última visita: octubre 2010.

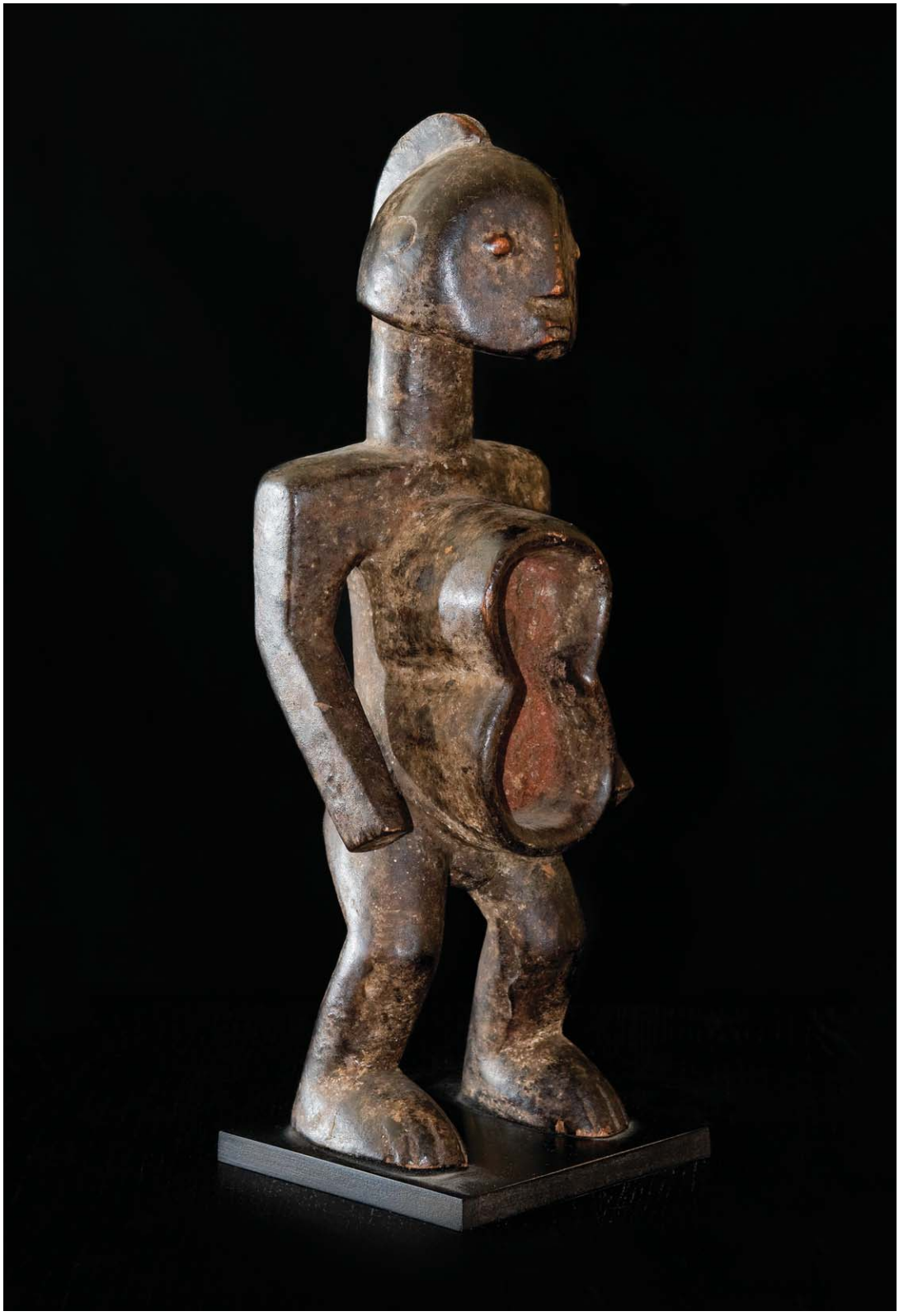
[10] http://bitelia.com/2010/08/google-cede-a-las-presiones-de-alemania-y-permite-borrar-imagenes-de-street-view, última visita: octubre 2010.

Rafael Ponce Medellín
Centro Nacional de Investigación y Desarrollo Tecnológico
rafaponce@cenidet.edu.mx

Jorge A. Ruiz Vanoye
Universidad Popular Autónoma del Estado de Puebla

Gabriel González Serna
Internado Palmira

Copa antropomórfica para el vino de palma. Etnia Koro, Nigeria.



Copa antropomórfica para el vino de palma. Etnia Koro, Nigeria.