Título Vidas Observadas en la Red

Tipo de Producto Divulgación

Autores Galmarini, Luciano

Código del Proyecto y Título del Proyecto

A14S20- Espionaje comercial con robo de información confidencial

Responsable del Proyecto

Lo Giudice, María Eugenia

Línea

Derecho Informático

Área Temática

Derecho

Fecha

2015

INSOD
Instituto de Ciencias Sociales y Disciplinas Proyectuales

UADE
FUNDACIÓN UADE

VIDAS OBSERVADAS EN LA RED

Por Luciano Galmarini

Internet, cuyo origen fue exclusivamente militar -con el proyecto ARPANET-, no fue pensada para el uso masivo de las personas. Sin embargo, provocó un impacto similar al que en su momento sucedió con la Imprenta de Gutenberg.

Desde el punto de vista de la libertad de expresión, Internet es el paradigma que ha permitido confluir los distintos medios de comunicación conocidos hasta su aparición. Pero coincidentemente ha significado un avance sobre la intimidad y privacidad que no ocurría con los medios tradicionales.

El auge de las redes sociales ha contribuido a que una gran cantidad de datos personales que antes estaban reservados circulen en la nube de internet formando una especie de Big Data. Hoy todo está en la red. La gente ha hecho una identificación casi total de su vida real con la vida virtual. Todo tiene que comentarse en Twitter, postearse en Facebook, mostrarse en Instagram con "*selfies*" o "*braggies*", subirse a Youtube o buscarse en Google. Y lo que no termina de comprender, es que detrás de estos sitios webs que forman parte de nuestra vida diaria, hay terceros interesados en "ver" nuestros rastros con fines totalmente diversos.

La mayoría de las personas no tiene noción de que al abrir una cuenta de perfil en una red social, está celebrando un contrato electrónico de "Log-in", por el cual acepta los términos y condiciones fijados por el Sitio, los que normalmente están ubicados en la denominada "*low taffic*". Las políticas de privacidad presentan la particularidad que pueden ser modificadas en cualquier momento por el sitio sin el debido aviso a sus usuarios. Esta situación puede hacer disponible información que un usuario había restringido, hasta tanto ajuste su configuración de privacidad. Además, al abrir la cuenta el usuario le da una serie de permisos al sitio para que disponga de los datos personales para cederlos a terceros.

A esto hay que agregar el tema de las "*cookies*", que son archivos que se instalan en nuestras computadoras y dispositivos móviles cuando navegamos por los sitios, y que permiten la recopilación de datos de los usuarios, para formar un perfil *online* de sus gustos, intereses, preferencias, hábitos de consumo y hasta la capacidad de compra, a los fines de luego poder enviarles publicidad a través del *spam* o de *pop ups*. La pregunta es, si todos los usuarios conocen el uso de las "*cookies*", y la finalidad de las mismas.

Además hay que agregar el aumento exponencial de dispositivos móviles con tecnología "*I-mode*" (conexión a la red), que a su vez permiten descargar una gran cantidad de aplicaciones del tipo "*social networking*" y la posibilidad de conexión a través de redes inalámbricas (la más conocida es *Wi-Fi*) que hacen muy vulnerable la privacidad de los usuarios. En el primer supuesto, lo relacionado a aplicaciones y *plug-ins* de descargas (mayormente de juegos), permite que terceros accedan a una gran cantidad de datos, sin que los usuarios tengan conciencia de ello. Y en el segundo caso, la gente no entiende que cuando alguien dejó abierta una conexión a una red, no lo hizo por descuido, sino para que las personas "muerdan el anzuelo" y utilicen dicha conexión, poniendo sus claves y nombres de usuarios, los cuales luego serán captados.

Otra cuestión está dada en las técnicas de reconocimiento facial a través de sistemas biométricos. La herramienta de Facebook, "*deep face*" permite que un tercero pueda etiquetar una con un 99 % de

certeza, igualando la capacidad de reconocimiento del ojo humano. Por caso, el llamado "Proyecto Chicas Bondi – Sin pose sin permiso", en el cual una persona tomaba fotografías de jóvenes mujeres que viajaban en distintas líneas de colectivo y luego las subía a Facebook, Twitter, Instagram y Tumbrl, trajo el gran inconveniente, además de la violación de los derechos personalísimos (intimidad, honor, dignidad, imagen) que permitió que cualquier usuario de Facebook que pasara el mouse por el rostro de alguna de las chicas fotografiadas, las etiquetara, exponiéndolas a un serio riesgo al ser fácilmente identificables por su nombre y apellido, rostro, vestimenta, línea de colectivo y el recorrido que hacían. Si a esto se suma los datos que la propia joven subió a su perfil, habrá quedado totalmente expuesta en su intimidad.

A esto hay que sumarle que, luego de los sucesos del "*9/11*", se sancionaron varias leyes en Estados Unidos, que permiten una suerte de recopilación y monitoreo de datos de redes sociales y sitios webs, como la "*Patriot Act*" o la "*Cyber Intelligence Sharing Protection Act*" (conocida como *CISPA*), que legitiman y permiten la posibilidad de controlar Internet a través del intercambio de datos personales entre el Gobierno de Estados Unidos y empresas privadas, con el objetivo de evitar, lo que dichas leyes llaman, "amenazas cibernéticas".

Por otra parte, no podemos olvidarnos de las recientes revelaciones que ha hecho Snowden, acerca de que la Agencia de Seguridad Nacional de los Estados Unidos habría estado involucrada en presuntos casos de espionaje a ciudadanos y el mundo empresarial, a través de programas como "*Prism*", "*Mystic*" o "*XKeyScore*", que pueden buscar "metadatos" (la información que no se ve a simple vista y que queda registrada en memorias, temporales, etc.).

Si la gente tomara noción de que cualquier cosa que haga en Internet está siendo vista por alguien, nadie más se conectaría a una red. No hay una región más expuesta que otra, ya que Internet borra las fronteras de los países. Cualquier región, menos la llamada "*Five Eyes*" (un acuerdo entre Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda) ha sido, está siendo y será monitoreada por algún sistema de inteligencia estatal.

El Derecho Informático estudia el impacto de las TICs (Tecnologías de la información y la comunicación) en la sociedad y el mundo jurídico. Surge como una necesidad de adaptar las distintas disciplinas a los cambios e implicancias que genera el uso de la tecnología, permitiendo conocer y entender cuáles son los interrogantes y conflictos que plantean las TICs.

Los principales conflictos están dados por:

- violación a los derechos personalísimos a través de comentarios injuriantes, uso de imágenes sin consentimiento, lesión a la intimidad y dignidad, y casos de cyberbullying, a través de las redes sociales, blogs e incluso en los resultados que arrojan los buscadores (como el caso de las thumbnails).
- víctimas de modalidades delictivas como phishing, pharming, skimming, ransomware, hacking, estafas a través de comercio electrónico.
- en relación a menores, delitos de pornografía infantil, grooming y sexting, "robo de identidad".
- violación a la privacidad del correo electrónico, recepción de spam con publicidad no deseada, inserción de cookies en los navegadores, monitoreo del email corporativo.

En algunos aspectos Argentina tiene normas de avanzada, aunque aún no existen tribunales específicos, salvo algún caso puntual -como el sistema de solución de conflictos de nombres de

dominio-, como la Ley 25.326 de “Datos Personales” (que se aplica a aspectos muy novedosos como la prestación de servicios de datos informatizados a través de la “Cloud Computing”), la Ley 24.766 de “Confidencialidad”, la Ley 25.036 de “Software”, la Ley 25.506 de “Firma Digital”, la Ley 26.388 de “Delitos Informáticos”, la Ley 26.685 de “Expediente Electrónico”, la Ley 26.904 de “Grooming”, y Resoluciones administrativas sobre el registro de “Nombres de Dominio”.

Sin embargo hay cuestiones que aún no han sido normadas, como la privacidad del correo electrónico en el ámbito laboral, la no tipificación de ciertos delitos como el robo de identidad digital, el robo de datos como tal (phishing, pharming, keylogger, skimming), el tratamiento del cyberbullying. No obstante, debe destacarse la labor de los jueces, que han tenido que resolver cuestiones bien complejas, como la privacidad del e-mail del trabajador (distinguiendo si es corporativo o privado, si hay o no manual de uso de herramientas informáticas y si el trabajador fue notificado del mismo), o la violación de los derechos personalísimos en las redes sociales, y lo han hecho con muy buen criterio, a pesar de no tener normas específicas al respecto.

En lo relativo a la protección de los datos personales, la Ley 25.326 permite la recopilación de información por parte de las bases de datos, siempre y cuando cumplan con las condiciones de licitud que la misma estipula, en cuanto a la forma de obtener el consentimiento, que debe ser libre, expreso e informado, la calidad sobre el tratamiento de los datos en cuanto a las formas de recopilarlos y tratarlos, inscripción en la DNPDP (Dirección Nacional de Protección de Datos Personales), y una política de seguridad informática y confidencialidad, en base a las Directivas que dicta la DNPDP.

La ONTI (Oficina Nacional de Tecnologías de la Información) fija estándares de seguridad para los organismos públicos y a su vez controla que sean cumplidos; también coordina las soluciones ante los intentos de ataque a las redes informáticas públicas.

En el ámbito privado hay políticas de resguardo de la información que se ajustan a la Ley 24.766, que protege toda información considerada como secreto, en cualquier tipo de soporte, como medios electrónicos, magnéticos, discos ópticos, microfilmes, películas u elementos similares. También hay se aplican distintas normas Iso-Iram, como la 17.799 de Tecnología de la Información, que establece un Código de Práctica para la administración de la seguridad de la información, que trae distintas medidas de protección lógica y física. Aún así, se debería acentuar la aplicación de Códigos de Conducta, enfatizando las reglas éticas y de comportamiento que se espera cumplan los empleados, gerentes y ejecutivos. Ya que las principales causas de fuga de información desde la propia empresa es por ingeniería social o por maniobras de fraude corporativo.