LAS NUEVAS TECNOLOGÍAS QUE INVADEN EL DERECHO A LA PRIVACIDAD DE LA INFORMACIÓN

López Alejandro
alejolopezlo@gmail.com
Universidad Piloto de Colombia

Resumen **—**La creación, desarrollo y uso de nuevas tecnologías pueden hacer la vida moderna completamente visible a todos aquellos que la quieran observar. Por tal motivo, en el presente texto, se utilizara el concepto 'privacidad de la información' como una forma abreviada de la capacidad de controlar la adquisición o la liberación de la información acerca de un individuo. Se va a argumentar que tanto el Estado como el sector privado disfrutan de capacidades tecnológicas sin precedentes para recolectar datos de carácter personal, por lo que la invasión al derecho a la privacidad de la información cada vez es más inminente.

Índice de Términos**—**Privacidad, Información, Tecnologías, sector público, sector privado.

Abstract**—**The creation, development and use of the new technologies can make modern life completely visible to all who wish to observe. Therefore, in this text, it will be used the term 'information privacy' as shorthand for the ability to control the acquisition or release of information about oneself. We will argue that both the State and the private sector enjoyed unprecedented technological capabilities to collect personal data, so that the invasion of the right to privacy of information is increasingly imminent.

Index Terms: Information, Privacy, Technologies, Public sector, Private sector.

I. INTRODUCCIÓN

El rápido despliegue de las tecnologías que invaden la privacidad tanto por parte de los gobiernos como por las empresas del sector privado amenaza con hacer, prácticamente, obsoleto el término privacidad de la información. Así las cosas, en este artículo se describen una serie de tecnologías actuales invasoras de la privacidad.

Estas tecnologías incluyen, entre otras: la recolección sistemática de datos nacionales y transaccionales; la creciente vigilancia automatizada en lugares públicos; el seguimiento de los teléfonos móviles y smartphones; el seguimiento por Internet, en especial de las cookies para hacer un 'sendero de clic'; los identificadores de hardware basados en la propiedad intelectual, como las marcas de agua; tecnologías que han ido, y siguen, mejorando con el pasar del tiempo.

El efecto acumulativo y el refuerzo de estas tecnologías pueden hacer la vida moderna completamente visible y permeable a todos aquellos que la quieran observar; no hay ningún lugar donde esconderse. Incluida la autorregulación, las tecnologías de protección de la intimidad, el derecho de protección de datos y los derechos de propiedad han sido varios de los intentos por elaborar una respuesta legal al asalto sobre el derecho a la privacidad de la información que han fracasado en los últimos años frente a estas nuevas tecnologías.

La mayor parte de este artículo se centrará en las cuestiones relacionadas con la recopilación de datos y no con el cotejo de estos. Gran parte de los mejores trabajos sobre la privacidad y su relación con la legislación, ignoran los problemas de recolección de datos, sin embargo, se centran en cuestiones relacionadas con el almacenamiento y la reutilización de estos, en especial en su divulgación maliciosa. Asimismo, este texto se centrará en el momento previo a la recolección de los datos. Debido a que los problemas de uso y reutilización no pueden ser evitados, así sean regulados de manera normativa, por lo que una de las formas de reducir la recolección al imponerle límites al uso de los datos recogidos, es más que incorrecta.

II. LAS NUEVAS TECNOLOGÍAS INVASORAS DE LA PRIVACIDAD DE LA INFORMACIÓN

Las tecnologías que invaden la privacidad se pueden dividir en dos categorías: (i) las que facilitan la adquisición de datos en bruto y (ii) las que permiten procesar y cotejar los datos. Aunque tanto real como útil, la distinción puede ser exagerada porque las mejoras en el procesamiento de la información también hacen posible nuevas formas de recolección de datos. Además, hace posible el seguimiento de cualquier hábito de navegación vía Web, al igual que el almacenamiento de nuevos datos y la organización inteligente de los datos existentes [1].

En el nivel más básico, los observadores iniciales se pueden clasificar en términos generales en: el sector público ―Estado― y el sector privado; aunque también la importancia en esta distinción puede ser exagerada porque las partes privadas, a menudo, tienen acceso a bases de datos gubernamentales y los gobiernos suelen comprar datos recolectados por el sector privado. Hay algunos tipos de recopilación de datos que solo el gobierno puede emprender, por ejemplo, la captura de información en formularios por mandato legal, como los censos y las declaraciones de impuestos. Pero, incluso, estos ejemplos ilustran el peligro de ser demasiado categóricos: muchas declaraciones de impuestos son presentadas por auxiliares comerciales (a través de formularios Web), dando un acceso de los datos a terceros.

En este sentido, grandes cantidades de datos personales se recogen de forma rutinaria hoy en día sin necesidad de un equipo de alta tecnología. Los ejemplos incluyen la recolección de datos personales por parte de los Estados y la enorme cantidad de datos recopilados por el sector privado en el marco de la venta de productos y servicios, entre otros.

Los datos transaccionales

Cualquier operación personal que involucra dinero ya sea de trabajo, compra, venta o inversión, tiende a crear un conjunto de datos relativos a la transacción. A menos que el pago sea en efectivo, el conjunto de datos, por lo general, incluye algunos datos personales sobre el individuo que participa en la operación. La recopilación de datos financieros es un ejemplo interesante de cómo el sector privado recolecta datos por diversos motivos. En muchos casos, los bancos y otros proveedores de servicios financieros recopilan información acerca de sus clientes, ya que los datos tienen un valor comercial. En otros casos, se registran los datos porque el Gobierno los obliga a realizar informes de rutina para ayudar a los esfuerzos de aplicación de la ley tributaria. En efecto, los bancos privados, a menudo, actúan como agentes de los esfuerzos de recolección de datos por parte del Estado, salvo aquellos que tienen sus sedes centrales en los denominados paraísos fiscales.

Incluso, hay máquinas que pueden realizar el seguimiento de las facturas por sus números de serie, algo que es muy común hoy en día, por lo que el pago en efectivo seguirá siendo, relativamente, anónimo. En su afán por recopilar datos personales acerca de los clientes, los comerciantes han recurrido a programas de recompensas de fidelidad, como las tarjetas para clientes frecuentes y las tarjetas de afiliación. Dependiendo de la sofisticación de la tarjeta y del sistema del que forma parte, estos programas de fidelización pueden permitir a los comerciantes acumular información detallada sobre sus clientes. Asimismo, los intermediarios financieros deben recoger los datos personales de sus clientes. Las leyes contra el lavado de dinero (y a veces las leyes tributarias) requieren que los proveedores de servicios financieros presenten informes sobre cada transacción sospechosa [2].

Las alternativas al dinero en efectivo, como son los cheques, tarjetas de débito y tarjetas de crédito, crean un rastro de datos que identifica al comprador, al vendedor, el importe de la venta y en ocasiones los bienes o servicios vendidos. La sustitución del papel por el dinero electrónico crea un rastro de datos digital que une en cada transacción a las partes involucradas. Por tanto, debido a que actualmente no existe un estándar para el dinero electrónico todo sigue siendo posible [2].

Por tal motivo, incluso, sin necesidad de recurrir a sistemas avanzados, grandes cantidades de datos personales se recogen de forma rutinaria alrededor del mundo. La introducción de nuevas tecnologías, sin embargo, promete elevar la cantidad y la naturaleza de la información que se pueda recolectar a niveles insospechados hace diez años.

La vigilancia del espacio público

El movimiento en público no es realmente anónimo, alguien a quien usted conoce puede reconocerle y cualquiera puede anotar el número de matrícula de su vehículo. Sin embargo, al menos en las grandes ciudades, se disfruta de la ilusión, y en gran medida la realidad, de ser capaz de moverse entre el anonimato. No obstante, dicha libertad pronto será

cosa del pasado, ya que los espacios públicos cada vez más se convierten en blanco de las tecnologías que invaden la privacidad. Debido al miedo a la delincuencia, y al bajo costo del hardware, el ancho de banda y el almacenamiento se están combinando para fomentar la rápida difusión de tecnologías de vigilancia rutinaria en los espacios públicos para la identificación de individuos [3].

Las tecnologías de monitorización incluyen cámaras, software de reconocimiento facial y diversos tipos de sistemas de identificación de vehículos. Asimismo, tecnologías relacionadas, algunas de las cuales tienen el efecto de permitir el monitoreo en tiempo real y el seguimiento de los individuos, incluyen la localización de teléfonos celulares y diversos tipos de identificadores biométricos.

Interceptación del teléfono celular

Muchas personas pueden ser rastreadas hoy en día sin la necesidad del uso de cámaras o cualquier otro dispositivo. Los teléfonos celulares deben comunicar su ubicación a una estación base con el fin de realizar o recibir llamadas. Por tanto, cuando un teléfono celular está en uso, es posible identificar de manera efectiva la ubicación de su usuario en pocos minutos (claro está, dentro de un área definida por la tolerancia del teléfono). No obstante, los gobiernos no son los únicos que quieren saber en dónde están y que hacen las personas. Los padres pueden utilizar el seguimiento del teléfono celular para localizar a sus hijos; los esposos pueden monitorear y ubicar a sus esposas, y así sucesivamente.

Las consecuencias de la invasión a la privacidad a través del seguimiento del teléfono celular aumentan dramáticamente cuando el movimiento es almacenado. Una cosa es permitir a la policía utilizar los datos para el seguimiento de un fugitivo en tiempo real; mientras que otra, es archivar los datos, tal vez incluso a perpetuidad, en caso de que la policía u otras personas deseen reconstruir los movimientos de alguien [3].

La vigilancia de las comunicaciones electrónicas y el seguimiento en línea

De acuerdo con un informe elaborado por el Parlamento Europeo, los Estados Unidos y sus aliados mantienen un aparato de espionaje mundial masivo capaz de capturar todas las formas de comunicación electrónica conocido como ‘ECHELON’, esta red puede acceder, interceptar y procesar toda forma moderna e importante de comunicaciones, con pocas excepciones. La red está apoyada por una variedad de tecnologías de procesamiento. A través del reconocimiento de impresión de voz se hace posible determinar si alguno de los participantes en una llamada se encuentra en una lista de vigilancia o negra. Si lo es, la grabación se puede dirigir a un ser humano para su revisión. Del mismo modo, los mensajes de texto, así como los correos electrónicos y faxes se pueden ejecutar a través de los llamados programas ‘diccionario’ que marcan los mensajes con referencias interesantes o patrones de palabras clave [3].

Como la inteligencia artificial mejora, estos programas cada vez son más sofisticados. Mientras tanto, los avances en el reconocimiento de voz (la traducción de voz en texto) prometen transformar el problema del monitoreo telefónico en otro tipo de problema más amplio, el del texto.

La World Wide Web es justamente celebrada como la cúspide de abundancia de la información, la cual está disponible para cualquier persona con una conexión a Internet. Los aspectos de la Web que la convierten en un medio de información tan poderosa (su naturaleza no regulada, la flexibilidad de su navegación por el software y los protocolos subyacentes, al igual que su papel como la biblioteca más grande del mundo, un centro comercial y una sala de chat) se combinan para hacer de la red un terreno fértil para la recolección de datos personales de los internautas. Cuanto más las personas confían en la Web para todos los aspectos de la vida diaria, es más probable que los datos acerca de sus intereses, preferencias y comportamiento económico sean capturados, formando parte de los perfiles personales.

El nivel básico de monitoreo al usuario está incorporado en los navegadores más populares y opera de forma predeterminada. Al hacer clic en un enlace se instruye al navegador a revelar automáticamente la página de referencia para el nuevo sitio. Si una persona ha introducido un nombre o dirección de correo electrónico en el software de comunicación el navegador también lo dará a conocer automáticamente. Estas características no se pueden omitir, ya que son parte del protocolo de transferencia de hipertexto, aunque se pueda eliminar el nombre y la dirección del correo electrónico del software. Los internautas pueden, sin embargo, emplear herramientas de privacidad para mejorar el anonimato y enmascarar

la información personal, no obstante, no son 100 % confiables.

Por su parte, las cookies presentan una serie de problemas potenciales a la privacidad de la información. Los datos de usuario transmitidos, al sitio, como una dirección o número de teléfono, se pueden incrustar en una cookie. Esta información puede ser correlacionada con los números de identificación del usuario fijados por el sitio para crear un perfil. Esto permitirá a un sitio particularmente intrusivo construir un dossier sobre el usuario. Las cookies se pueden compartir entre sitios Web, permitiendo a los diseñadores con experiencia averiguar qué otros sitios son navegados por sus visitantes frecuentes y lo que han revelado a dichos sitios. Al ser reconstruido, este *click trail* puede revelar tranquilamente tanto la información personal como comercial acerca de un usuario sin que este sea consciente de ello. Un visitante frecuente de sitios pornográficos, un comprador regular de medicinas anti-depresión o incluso alguien que tiene una pasión por Mozart, todos, pueden tener suficientes razones para no querer que los demás sepan de sus intereses o acciones en la World Wide Web.

Para complicar más las cosas, lo que aparece como una página en un navegador en realidad puede estar compuesto por múltiples piezas procedentes de varios servidores. Así que es posible incrustar visible, o incluso de manera invisible, contenido en una página Web que proporcione en cualquier momento una ocasión para establecer una cookie.

Las cookies, sin embargo, son solo la punta del iceberg. Lejos encontramos otras características más intrusivas que pueden ser integradas en los navegadores, en el software descargado de Internet y en virus o troyanos. En el peor de los casos, el software podría estar configurado para grabar cada pulsación de una tecla. El examen de las dificultades también surge en el contexto de la gestión automatizada de los derechos de propiedad intelectual. Abundan las propuestas de tecnologías de gestión de derechos de autor (a veces cruelmente apodadas 'herramientas del soplón'), que graban y, en algunos casos, revelan cada vez que un usuario accede a un documento, artículo o incluso a una página de material con licencia, con el fin de evaluar finamente sus descargas. Del mismo modo, los sistemas de filigrana digitales, que insertan etiquetas personalizadas invisibles en documentos electrónicos, como marcas de agua, permiten que dichos documentos sean rastreados [3].

El uso de estas diversas tecnologías permite a los propietarios de datos valiosos vender la información con menos temor. Si la información se vende en forma encriptada, junto con un programa o dispositivo que lo descifre cada vez que un licenciatario desea ver parte del contenido, la carga se puede hacer sobre una base de pago por visión en lugar de exigir una cuota grande por adelantado.

Dejando a un lado la cuestión del efecto sobre el uso justo, la vigilancia con fines de fijación de precios plantea un serio problema de privacidad si la información se registra o es reportado el licenciante. Si solo se indica la cantidad de uso, en lugar de las páginas en particular vistas o consultadas, la privacidad del usuario no se ve afectada. Cuando la medición se realiza en tiempo real, sin embargo, es particularmente difícil que un usuario este seguro acerca de lo que se informa. Si, por ejemplo, un sistema de gestión de derechos de autor conecta a través de Internet al propietario del contenido para asegurar la facturación o incluso el pago antes del acceso, a continuación, tan solo el usuario más sofisticado será capaz de determinar la cantidad de información que se está transmitiendo. La tentación de crear perfiles de usuario para fines de marketing puede ser muy grande. Debido a que los programas que informan en voz baja, es decir, un registro central en tiempo real, por medio de una visita URL, cada vez son más comunes. Hacer clic en lo que está relacionado en la configuración de todas las URL visitadas en una sesión del navegador, informará de nuevo todo el proceso a otro servidor. Esto ayuda a construir una base de datos que puede ser utilizada para guiar navegaciones futuras [1].

Hardware

Por su parte, los fabricantes de hardware también están implementando funciones de privacidad que comprometen una amplia variedad de dispositivos. Los fabricantes de chips de computadoras y adaptadores de tarjeta Ethernet utilizados para la creación de redes y el acceso a Internet de alta velocidad están construyendo de manera rutinaria números de serie únicos que luego son accedidos fácilmente a través de Internet. Cada chip Intel Pentium tiene un número de identificación único. Intel diseñó originalmente el ID chip para funcionar continuamente y ser accesible a programas como los navegadores Web. La intención parece haber sido la de hacer al anonimato electrónico imposible. Los usuarios anónimos pueden, razonó Intel, cometer fraude a la propiedad intelectual digital a través del hackeo. Con un diseño único, el número de identificación indeleble en cada chip, el software

puede ser configurado para trabajar en un solo sistema. Los usuarios solo podrán ocultar sus identidades cuando muchas personas utilizan una sola máquina o cuando una persona utiliza varias máquinas a la vez.

El identificador único también podrá servir como un número de índice para los sitios Web, los mostradores de cookies y otros medios de seguimiento de los usuarios a través de Internet.

De hecho, el nuevo protocolo de Internet, que esta sustituyendo progresivamente el anterior, contempla el uso de una tarjeta Ethernet ID única para crear un identificador único global (GUID). El estándar IPv6 requiere un software para incluir un GUID en la cabecera de todas las comunicaciones de Internet (correo electrónico, navegación Web, chat y otros). Los ordenadores con una tarjeta Ethernet crean un GUID, al combinar el número único de identificación asignado al fabricante de la tarjeta con un número único asignado a la tarjeta en la fábrica.

El hardware con números de identificación incorporados aún no es omnipresente, pero la ampliación de su uso es cada vez más común, en parte, debido a las fuerzas del orden que temen que las actividades anónimas conduzcan a la delincuencia y al comportamiento antisocial.

III. CONCLUSIONES

En la futurista *Sociedad transparente* de David Brin, el autor sostiene que el momento de las leyes de la privacidad pasó mucho antes de que nadie se diera cuenta. Por lo que, quizás anticipando la era del 'polvo inteligente', sugiere que el principal efecto de las leyes de la privacidad será "hacer los insectos más pequeños" [4].

Habiendo concluido que la privacidad ya no es posible, Brin sigue argumentando que la cuestión política fundamental es si los ciudadanos tendrán acceso a los datos recolectados y que son disfrutados inevitablemente por las élites. Tan solo una política de transparencia compartida, en la que todos los datos de carácter personal recolectados tanto por el sector público como el privado sean igualmente accesibles a todos, puede llegar a crear la libertad y la responsabilidad necesaria para vivir en una sociedad libre y privada [4].

La eficacia de las leyes de la privacidad refleja la débil respuesta de la ley ante la realidad del rápido aumento de las nuevas tecnologías invasoras de la privacidad que describimos a lo largo de este artículo. Las leyes de la privacidad actuales alrededor del mundo constituyen en el mejor de los casos un mosaico fino, pero que es claramente inadecuado para afrontar el reto de las nuevas tecnologías de adquisición de datos. Los acuerdos internacionales generales que abordan el tema de la privacidad no son los mejores. Incluso las leyes de privacidad mucho más elaboradas en Europa y Canadá permiten casi cualquier colección y reventa de los datos personales de manera consensual. Lo que es más, la ley, a menudo, tiende a imponer barreras a las tecnologías que mejoran la privacidad.

Ninguna norma legal posiblemente es perfecta. Las leyes se violan todo el tiempo. Pero, aunque suceden cosas ilegales, la regulación también influye en los resultados y a veces el esfuerzo es necesario para lograr resultados serios. Por último, la variedad de usos y usuarios de datos posibles frustran cualquier intento integral para proteger la privacidad de los datos. Cualquiera que sea el derecho de la privacidad de la información, es un derecho que se ve constantemente vulnerado, incluso por tecnologías invasoras patrocinadas por los gobiernos para vigilar nuestra conducta privada.

Así pues, las reglas sobre la adquisición de datos, retención y uso que podrían funcionar para los vecinos entrometidos, comerciantes o agencias de crédito podrían no ser las apropiadas cuando se aplican a las agencias de inteligencia estatales. Por el contrario, muchos gobiernos pueden tener acceso a la información o la tecnología que el sector privado carece, pero que en cualquier momento podría obtener; las normas que se centran demasiado en los usos o en los usuarios específicos están condenadas al fracaso frente a la evolución de la tecnología. La restricción de un aspecto (como lo hemos hecho en esta investigación) para la adquisición de datos, deja de lado cuestiones importantes como la retención y la reutilización de datos, sin embargo, puede hacer que el problema sea más manejable, pero aún así sigue siendo enormemente complejo porque la regulación de una sola tecnología tiende a enmarcarse en diferentes maneras, dependiendo del contexto.

Finalmente, tenemos que considerar si nuestras propias acciones constituyen un agravio invasivo de algún tipo (o tal vez, incluso, una apropiación indebida de información) y si una propuesta normativa que limita la adquisición o publicación de la información puede ir en contra de estas actuaciones. Dicho esto, el cambio tecnológico aún no ha ido tan lejos o ha sido tan rápido como para hacer que los enfoques jurídicos de protección de la privacidad sean irrelevantes. Todavía hay mucho de

lo que la ley puede hacer, solo que aún no se ha intentado.

REFERENCIAS

[1] AGRE, Philip, ROTENBERG, Marc. Technology and Privacy: The New Landscape. Massachusetts: The MIT Press, 2008. 336 p.

[2] BRANSCOMB, Anne W. Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition. En: Vanderbilt Law Review. No. 36. (1983); p. 985-312.

[3] CLARKE, Roger. Information technology and dataveillance. Massachusetts: The MIT Press, 1998. 381 p.

[4] BRIN, David. The Transparent Society: Will Technology Force Us To Choose Between Privacy And Freedom? New York: Basic Books, 1999. 384