Boletín N° 15.766-03

Proyecto de ley, iniciado en Moción del Honorable Senador señor Bianchi, que regula la obtención y el tratamiento de datos personales mediante la utilización de dispositivos electrónicos.

Idea matriz

Restaurar el imperio del derecho a la vida privada, la inviolabilidad del hogar y las comunicaciones privadas de la ciudadanía.

Fundamentos

¿Tu teléfono sabe exactamente qué quieres, que necesitas, que ofrecerte? ¿la publicidad de tus dispositivos siempre responde a algún deseo cercano, a alguna conversación que hayas tenido, a algo que quieres comprarte?

Según una encuesta telefónica realizada más de 1000 adultos estadounidenses por Consumer Reports en mayo de 2019, el 43% de los estadounidenses que poseen un smartphone, cree que su celular está grabando conversaciones sin su consentimiento.

Aun así, lo que más miedo da, es que según los expertos en ciberseguridad, hay otras formas mucho más eficientes de aprender todo sobre una persona, sin tener que escuchar las conversaciones privadas.

En la actualidad, hay muchas otras formas efectivas a la hora de recopilar datos sobre las personas. Desde los gigantes tecnológicos como Google, Facebook, Uber, etc; hasta el desarrollador de apps más pequeño, registran habitualmente la información personal del usuario (nombre, fechas de nacimiento, información de tarjetas de crédito, etc) simplemente solicitándola en un formulario de registro.

Muchos también rastrean su ubicación en todo momento, utilizando el GPS de su teléfono, IP o redes WiFi a las que se ha conectado. Incluso Facebook monitorea las acciones realizadas más allá de los límites de su propia plataforma

Según los estudios de David Choffnes, profesor de la Universidad de Boston, se encontró que 9000 aplicaciones de Android estaban tomando en secreto capturas de pantalla o grabando videos de la actividad de los teléfonos inteligentes y enviándolas a terceros. Incluso en un caso, una aplicación de entrega de alimentos grabó un video de la actividad del usuario y lo compartió con una empresa de análisis de datos.

En definitiva, medir los datos y la actividad del usuario está bien visto a los ojos del marketing. Por ejemplo, si un individuo realizara una búsqueda en Google de un tipo particular de zapatillas y luego utilice Google Maps para ver el local de zapatillas más cercano y por último use su cuenta de Gmail para registrarse en la lista de correo de esta tienda; es muy probable que dicha persona recibirá anuncios para zapatillas en tu navegador Chrome.

Es por lo anterior que no resulta para nada sorpresivo para quienes utilizamos con frecuencia el teléfono celular que en ocasiones pareciera que éste nos escucha, pues ciertas aplicaciones terminan entregándonos publicidad y ofertas de pasajes cuando hablamos de viajes con algún amigo o familiar, de ciertos productos que mencionamos vagamente o respecto de conversaciones que mantuvimos de forma presencial, telefónica o a través de aplicaciones.

Un alto porcentaje de la población chilena tiene acceso a un dispositivo móvil, a través del cual descargan aplicaciones tales como Facebook, Instagram, Twitter, Amazon, Uber, etc. Esto cobra relevancia porque, son estas aplicaciones las que se encargan de manipular tu dispositivo al punto de servir como un receptor de información.

Estas acciones, que en principio parecieran ser del todo ilícitas, son consentidas por los usuarios, o al menos esa es la principal defensa de las grandes compañías que están por detrás, pues al descargar estas aplicaciones y previo a ser utilizadas, se le exige al usuario aceptar los conocidos “términos y condiciones de uso”, en otras palabras, contratos de adhesión que en la práctica son textos sumamente abultados en cuyo contenido se encuentra la regulación del uso de datos, es decir, los permisos que nosotros como usuarios le concedemos a la aplicación y cómo tratan tu información personal, mensajes, fotos, videos, visualizaciones, contenidos de interés, el cómo accederán a ella y, lo más importante, que pueden hacer con ella.

Lo anterior resulta preocupante ya que existen medios para la obtención de datos que resultan más que gravosos, que superan lo imaginable, como por ejemplo, que se establezca la facultad de ocupar el micrófono de tu celular aun estando cerrada la aplicación, esté bloqueado el teléfono y durante todo el día.

Esto transforma nuestros teléfonos en pequeños aparatos de rastreo, ya que recolectan una gran cantidad de información como donde vamos, horas de sueño, rutinas y toda nuestra información de audio, básicamente nuestra vida y al más puro estilo de James Bond o de películas de espías. Estados Unidos fue el primero en donde la ciudadanía se alzó contra este tipo de situaciones y sentando un precedente con el caso Amazon, oportunidad en que se produjo una avalancha de litigios cuando medios de comunicación informaron sobre la política de recopilación de datos por parte de la empresa, la que permitía que sus dispositivos grabaran audio, conversaciones y cualquier actividad de forma continua, aun sin encontrarse siendo utilizados aquellos dispositivos, es decir, un micrófono escuchándote las 24 horas del día.

¿Para qué? La respuesta es sumamente sencilla, son las empresas las que usan estos datos, porque tal como se señaló con anterioridad, para el Marketing resulta sumamente rentable. El principio básico es que desde una imagen hasta un audio se puede traducir en datos tangibles, una onda que se puede decodificar y transformar en palabras o en códigos binarios, esto para alimentar los motores de publicidad de las aplicaciones, los algoritmos de las propias aplicaciones y creando así bases de datos cuyo valor e impacto en el mercado es incalculable.

Tal es el alcance y la magnitud de la información que estas plataformas recolectas que, en marzo de 2020 año se desveló que Cambridge Analytics en colaboración con Facebook habría utilizado los datos de 87 millones usuarios de Facebook para manipular e influir en las elecciones presidenciales en Estados Unidos el 2016, en otras palabras, al utilizar su posición monopólica y dominante utilizó su aplicación para recopilar millones de datos de internautas de Facebook sin su consentimiento y con fines políticos, y se sirvió de ellos para elaborar perfiles psicológicos de votantes que supuestamente vendieron a la campaña del entonces presidente de EE.UU., Donald Trump, durante las elecciones de 2016, entre otros.

Basta entender que los aparatos electrónicos se han vuelto un indispensable en nuestro diario vivir como para imaginar que, mientras nuestro teléfono está en el bolsillo, va recopilando todas y cada una de las palabras, conversaciones, acciones, movimientos, ubicaciones y recorridos que hacemos, inclusive en dentro de nuestro propio hogar, personas para escuchar clips de audio obtenidos a través de sus dispositivos.

Amazon informó que emplea a miles de trabajadores a tiempo completo y contratistas en varios países, incluidos Estados Unidos, Costa Rica y Rumania, para escuchar clips de audio. No es un misterio entonces que la transgresión a la inviolabilidad del hogar y a las comunicaciones privadas son un hecho más que comprobado.

No se requiere ser un connotado matemático para entender que, de un universo de más de cuatro billones de usuarios, un pequeño porcentaje se traduce en billones de conversaciones de billones de personas a lo largo del mundo.

El año 2022, Meta, la propietaria de Instagram y Facebook, debió alcanzar un acuerdo extrajudicial en una demanda colectiva que se interpuso en su contra por haber "violado la privacidad de los usuarios al compartir sus datos con terceros sin su consentimiento."

Si bien, el tenor de la situación guarda mayor relación con el tratamiento de datos personales que con las escuchas y recopilación de los propios datos, lo cierto es que llegado determinado punto, **a estas empresas monopólicas y propietarias del mundo digital** ya no les interesa la protección del consumidor o sus derechos, sino el redituar a costa de sus usuarios.

Jamás podrá el derecho a la privacidad, a la vida privada y a la inviolabilidad del hogar estar por debajo de la libertad de ejercer una actividad económica. De forma lamentable, pese a los distintos hechos suscitados a lo largo del mundo, el beneficio económico que generan estas prácticas del todo inconstitucionales sigue siendo infinitamente mayor a cualquier tipo de sanción que pueda existir por transgredir las garantías fundamentales de las personas.

Si bien en Chile contamos con una legislación que regula el tratamiento de datos personales, esta está obsoleta en materia digital y no abarca el espectro completo de

posibilidades en la cual se deba proteger al usuario.

Se vuelve necesario que se reestablezca el imperio del derecho, protegiendo a los usuarios, dándole protección a todos aquellos datos e información que ellos estimen compartir, pero además, protegiéndole en todo momento de las obtención ilícita de esta información, de estos datos que, por años, se han utilizado para redituar vulnerando así la vida de todos y cada uno de los ciudadanos que optan por utilizar aplicaciones en su diario vivir. Por todo lo anterior, es que los Senadores firmantes venimos en presentar el siguiente:

PROYECTO DE LEY

ARTÍCULO PRIMERO: La presente Ley tiene por objeto el restablecimiento del imperio del derecho a las comunicaciones privadas, a la protección de los datos personales, regula su obtención y tratamiento en virtud de lo dispuesto en la Ley 21.096.

ARTÍCULO SEGUNDO: Prohíbase a toda empresa, sociedad, persona, software, aplicación móvil u otras análogas la utilización de los micrófonos, cámaras, gps y cualquier componente de dispositivos móviles, electrónicos, altavoces inteligentes u otros análogos para obtener, acceder, almacenar y utilizar información personal de los usuarios, datos de uso, localizaciones, grabaciones, fotos, audios, mensajes, conversaciones y cualquier otro tipo de comunicación sin el consentimiento expreso del usuario.

ARTÍCULO TERCERO: Se prohíbe también el almacenamiento, utilización, venta, cesión, transferencia, entrega a terceros a cualquier título todo dato, foto, audio, grabación, geolocalización, indicador, información financiera, información personal, cédulas de identidad, correos electrónicos, información sobre bienes y cualquier tipo de datos de usuarios a los que la constitución y las leyes den el valor de información personal, a través de softwares, aplicaciones para dispositivos móviles u otros dispositivos análogos, sin el consentimiento expreso del usuario.

ARTÍCULO CUARTO: El consentimiento expreso de los artículo segundo y tercero

precedentes solo podrá darse a través de un formulario electrónico, el cual debe contener, detallada de forma sencilla y expresa, todas y cada una las acciones que el software, aplicación para dispositivos móviles u otros análogos pretenda ejecutar.