Observatorio Argentino del ciberespacio

# INFORME N°03


## Protección de datos y de la privacidad en época de dispositivos inteligentes

Comodoro (R) Oscar Mato

# Protección de datos y de la privacidad en época de dispositivos inteligentes

**Autor:** Comodoro (R) Oscar Mato

Somos conscientes del robo de nuestros datos personales y de la continua invasión a nuestra privacidad?

En el mundo actual vivimos nuestra vida a través de distintos dispositivos llamados “inteligentes”, un ejemplo son los “*smartphones*” (o celulares), a ellos se les puede instalar infinidad de aplicaciones (*app*) que se nos ofrecen para vivir conectados a redes sociales, para sacar mejores fotos, para modificar esas imágenes, para ayudarnos a llegar a un lugar, para ver películas, etc., el problema radica en que la mayoría de las personas (usuarios de los dispositivos de telefonía móvil) instala las *app* sin prestar atención a qué cosas realiza esa *app* en su equipo pues sólo le interesa lo que “en teoría” hace esa aplicación.

Quienes estamos en el tema de la ciberseguridad y ciberderecho, antes de instalar un programa o una aplicación en un dispositivo nos fijamos que privilegios va a tomar la aplicación (o software) en cuestión en el equipo, y según nuestro análisis de riesgo (es decir, si vale la pena que la aplicación acceda a nuestros datos para el supuesto servicio que brinda) la instalaremos o la dejaremos de lado. El ejemplo común sobre este tema es la instalación de la aplicación linterna que al verificar que permisos (o privilegios) toma de nuestro dispositivo se verifica que de ser instalada accederá a los contactos, fotos, cámara, micrófono, navegación por internet, datos que nada tienen que ver con tomar control del elemento que se debe encender para iluminar.

Es importante saber que hay organizaciones que se dedican a investigar a las aplicaciones que son ofrecidas en las tiendas de Google y Apple, y han encontrado que gran cantidad de estas app tienen como finalidad instalar malware (software dañino) cuya finalidad es extraer los datos personales de nuestros dispositivos, o permitir que se nos realice el seguimiento por geolocalización, o que se utilice nuestro ancho de banda, etc. (y por supuesto que estas “prestaciones” no están detalladas en las condiciones de aceptación de la instalación).

Existe una normativa que regula la protección de los datos personales (la ley 25326) que en su artículo 4 dispone que “Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y **no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido**. La recolección de datos **no puede hacerse por medios desleales, fraudulentos** o en forma contraria a las disposiciones de la presente ley. Los datos objeto de tratamiento **no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención**.”. Pero de nada sirve la norma si nosotros no cuidamos nuestros datos.

La primer etapa en el proceso de protección de los datos personales es la prevención que el usuario debe tener para evitar que sus datos sean objeto de robo o mal uso, es decir, debemos estar atentos a lo que instalamos en nuestros dispositivos y no caer presa del canto de las sirenas pues el precio a pagar es la entrega de nuestros datos personales. Y si bien el artículo 5 de la ley 25326 dispone: “El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley”, en el problema que nos ocupa, el usuario al hacer “click” aceptando las condiciones para la instalación de la aplicación, es decir está dando su consentimiento. Por eso es necesario que antes de dar “click” y aceptar, se analice si los permisos / privilegios que toma esa app son coherentes con el beneficio que uno obtiene al usarla.

Y como si lo descripto anteriormente fuera poco para nuestros datos personales y para nuestra privacidad, aparecieron nuevos problemas (o desafíos) los dispositivos inteligentes IOT *(Internet of Things*, Internet de las cosas).

Hasta hace un tiempo atrás pensar que una heladera podría ser controlada remotamente desde un teléfono y que esa heladera me avisaría cuando se producibles un corte de energía eléctrica o me quedase sin un alimento, que una cafetera pudiera ser programada a distancia para que al llegar a casa me tuviera el café recién servido, eran cosa de ciencia ficción, pero hoy son una realidad gracias a los IOT. Y así tenemos aire acondicionados inteligentes, cafeteras inteligentes, televisores inteligentes, etc., etc.

Todos esos dispositivos inteligentes que se conectan a Internet y que pueden ser programadas / controlados desde un *smartphone* son la delicia de muchas personas que de manera remota acceden a ellos y al llegar a sus hogares disfrutan de los beneficios de esta tecnología y tiene su ambiente totalmente climatizado sumado a un ahorro de consumo de energía, la serie que no pudo ver por problemas en el tránsito grabada y lista para ser disfrutada, etc.

Ahora bien, no todo es el paraíso en el mundo de las tecnologías IOT, y al igual que ocurre con los *smartphone*, estas computadoras con forma de heladera, cafetera, TV, aire acondicionado, o lo que sea, son un riesgo para nuestra privacidad y la información sobre nuestra vida. Y como la mejor manera de entender algo es a través de ejemplos, les paso a mostrar casos de la vida real

**1)** El robot de cocina marca "*Monsieur Cuisine Connect*" de la empresa LIDL, es un dispositivo inteligente que cuesta 359 euros, ha sido diseñado en Alemania y producido en China. Cuenta con pantalla táctil y se puede conectar al wifi de casa para descargar recetas de cocina. Aunque, claro, todo dispositivo que puede ser conectado a una red también puede ser hackeado, y es esto lo que ha ocurrido. En numerosos medios apareció la noticia que aficionados han hackeado el *Monsieur Cuisine Connect* y han descubierto ciertos problemas de seguridad y privacidad. Lo que más ha sorprendido es que el electrodoméstico cuenta con un micrófono y un altavoz, además de tener la versión Android 6.0, antigua. Si bien la empresa LIDL salió a aclarar que el micrófono está instalado para que en un futuro se lo pueda controlar por medio de la voz, es un tema para tener en cuenta debido a sus vulnerabilidades.

**2)** Muñeco peluche inteligente para chicos: Si bien están pensados para que el chico no se sienta solo nunca, gracias a una aplicación para el *smartphone*, los padres pueden grabar su voz y reproducirla a través del peluche. Como el muñeco no distingue entre las palabras de un adulto y la de un menor, los pequeños también pueden grabarse y escucharse después, como si el animal hablase. Parece divertido pero no lo es tanto si tenemos en cuenta que más de dos millones de estas grabaciones circulan por Internet. A la cantidad de grabaciones hay que sumar 820.000 credenciales, los datos que los padres y madres utilizan para acceder a la app desde su *smartphone* y que incluyen nombre, apellidos, direcciones de correo, número de teléfono o nombre del niño.(https://www.elespanol.com/omicrono/software/20170228/peluche-inteligente-filtrado-millones-grabaciones-padres-hijos/197231095_0.html)

**3)** Barredora de piso inteligente: Estos aparatos crean planos de la casa forma automática durante sus tareas, con el objeto de optimizar el recorrido y ahorrar batería.

Estos planos, según el presidente de la compañía podrían utilizarse para mejorar la calidad de sonido de unos altavoces inteligentes, ajustando la potencia en ciertas direcciones y disminuyéndola en otras para conseguir un sonido más rico y con menos distorsiones y reverberaciones. Con la información recolectada por Roomba este proceso será mucho más sencillo. Pero esas declaraciones han puesto en alerta de quienes buscan la protección de la privacidad de los consumidores, y aunque iRobot ofrece formas de no compartir los datos recolectados por los aspiradores con la empresa, estas opciones no son siempre fáciles de configurar. Aunque en apariencia es limitada, la información que recolectan dispositivos como Roomba puede ser suficiente para saber en qué áreas de la casa suelen estar los ocupantes, cuántos muebles tienen o si han comprado uno nuevo recientemente, si tienen mascotas o cuándo suelen estar fuera del hogar. Los "Acuerdos" y "licencias de uso" que el usuario acepta al poner el funcionamiento el robot por primera vez, están redactados en un lenguaje legal lo

suficientemente ambiguo como para permitir a la empresa compartir estos datos sin temor a demandas.(https://www.elmundo.es/tecnologia/2017/07/25/5977491aca4741db258b45cc.html)

**4)** Televisores inteligentes: Según el New York Times, millones de consumidores de Estados Unidos están siendo monitorizados a través de sus Smart TV y los datos se usan para analizar sus perfiles, descubrir cuántos dispositivos inteligentes hay en sus hogares y lanzar campañas publicitarias (https://www.itdigitalsecurity.es/endpoint/2018/07/las-smart-tv-ponen-en-riesgo-la-privacidad-de-los-usuarios) .

Las investigaciones han mostrado que varios ataques contra smart TVs son posibles y fáciles de ejecutar, generalmente sin necesitar del acceso físico al dispositivo o de la interacción del usuario. También ha sido demostrado en varias ocasiones que, una vez comprometido, un TV con acceso a Internet puede servir como punto de partida para ataques a otros dispositivos en la misma red, apuntando finalmente a la información personal del usuario almacenada en objetivos más atractivos, como PCs o laptops. En 2013, los investigadores demostraron que, explotando agujeros de seguridad en algunos modelos de TV con conexión a Internet de Samsung, era posible encender de manera remota la cámara y el micrófono internos. Y no solo podían convertir a estas TVs en dispositivos capaces de oír y observar, sino que también podían tomar el control de apps de redes sociales embebidas, publicando información en nombre del usuario y accediendo a archivos. Otro investigador destacó un ataque que le permitió insertar noticias falsas en el buscador de un smart TV. (https://www.welivesecurity.com/la-es/2018/02/19/seguro-smart-tv/).

Cualquier usuario de estos dispositivos que lea este artículo puede pensar quién lo va a espiar a él, quién estaría interesado en sus datos o en husmear en su privacidad, pues entre tantos millones de dispositivos que se venden, justo él lo van a espiar? Pero lo que todos debemos tomar conciencia es que en la actualidad todos esa información va a repositorios que a través de técnicas de minería de datos (*data mining*) y de Big Data, junto a plataformas muy potentes, se gestiona y analiza la misma en tiempo real, y el resultado es obtener información acerca de la privacidad de cualquier persona (o de un grupo) sin que esta (o estos) lo sepan.

Con la tecnología ocurre algo similar que con los alimentos que consumimos, muchos de los alimentos que hoy consumimos son tóxicos o dañinos para nuestra salud, otros se nos ofrecen como la panacea para obtener los minerales o vitaminas que debemos ingerir, y el resultado (pese a las advertencias de los médicos y nutricionistas) es que la calidad de vida no es buena por exceso de azúcares, de ingesta de harinas, de bebidas gaseosas, etc, pero es tanto el bombardeo a través de los medios que uno cae en la tentación, y después debe luchar contra las enfermedades (obesidad, diabetes, presión alta, colesterol alto, etc). Pues bien con el uso de los dispositivos tecnológicos (y sus aplicaciones), ocurre lo mismo respecto de la protección de nuestros datos personales y de nuestra privacidad, tanto es el bombardeo, la presión, que se ejerce desde los medios, la moda o el entorno, que uno deja de lado el bien propio a proteger (datos personales o la privacidad) para estar “a la moda”.

Entonces, y ya concluyendo este artículo, la normativa para proteger nuestros datos personales y nuestra privacidad existe, pero el problema es que la tecnología (y los deseos de las personas de usar esa tecnología) avanza mucho más rápido que las normas, por lo tanto somos nosotros, los usuario, quienes debemos ser cuidadosos en el uso de estos dispositivos, pues de nada vale seguir sancionando normas que rápidamente quedarán desactualizadas, si nosotros no ponemos nuestra parte en este tema.