Hackeos y Brechas

¿Qué puede hacer la ciudadanía para protegerse y mitigar los daños?

Por Ryan Salaya[1]

Resumen: El futuro llegó hace rato, no es posible concebir un modo de vida que no se proyecte en la digitalización, hoy la identidad digital es un aspecto fundamental de la ciudadanía; en este punto los datos se han transformado el core de gran parte de los negocios y por tanto son el nuevo target de la delincuencia que ha encontrado muchas amenities. En los siguientes párrafos profundizaremos sobre esta temática y propondremos dos herramientas fundamentales con las que cuenta la ciudadanía para resguardarse frente a esta problemática de absoluta coyuntura.

Palabras clave: Era digital – Renaper - ciberseguridad – protección de datos - leaks

Introducción

La era digital tiene una característica intrínsecamente revolucionaria en el sentido latín de la palabra, viene a *"Volver a hacer"* un nuevo mundo y con ello a sepultar un mundo analógico, tangible y físico que habitaba todos los espacios, pero no de forma simultánea como lo hacen hoy las redes digitales.

Desde las ciencias sociales se habla de la era exponencial, por su vertiginosa forma de avanzar, las capacidades de almacenamiento, la reproducción de un virus o la disrupción de una nueva tecnología que tan pronto como se vuelve masiva pasa a su obsolescencia, siendo reemplazada por una nueva que ya tiene fecha de caducidad programada de origen.

En este contexto, donde el dinero virtual, ocupa tanto o más porción que el físico, donde los documentos ya no se imprimen ni se firman con bolígrafo, donde las audiencias se celebran de forma telemática, donde los menús ya no los trae un mesero y hasta los médicos recetan desde un ordenador es el punto en el que nos encontramos hoy.

Con esta realidad conviven generaciones que nacieron antes de que existiera internet o un computador siquiera y tuvieron que hacer su propia alfabetización digital.

El ascenso de los ciberdelitos

Este desarrollo tecnológico también trajo aparejado una nueva modalidad de delito, tomando provecho de la virtualidad y explotando las vulnerabilidades, lograron modelar un nuevo universo de modus operandi conformando un conjunto de prácticas que se aglutinan bajo el término ciberdelitos.

Recuperamos a estos fines la conceptualización de ciberdelitos que ha brindado la Unión Europea que la define

[1] Licenciado en Ciencia Política y Abogado, Magíster en Derecho Penal UPF-UB Barcelona, Especializado en Ciberdelitos, Seguridad de la información y Estrategia en Ciberseguridad. Encargado de Cibercompliance y Delegado de Protección de Datos en la consultora PONDER.

como las *"actividades delictivas realizadas con ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas"*[2]

a) **El impacto del Covid-19**

Es menester explicar que, en este contexto, se trata de un fenómeno global que se vio impulsado aún más con la irrupción de la pandemia Covid-19 donde las medidas de distanciamiento social llevaron al mercado laboral a reinventarse, el teletrabajo, las VPN, los TOKENS, El Cloud, el QR que hace un quinquenio atrás resultaba terminología de expertos informáticos hoy es parte de la jerga cotidiana en muchos ámbitos laborales.

De la misma forma que se produjo este fenómeno ocurrió con los ciberdelitos, que sufrieron una curva significativa a nivel global de 2019 con un aumento constante en el número de investigaciones que se producen cometidas mediante medios digitales, este fenómeno en parte respondió en un primer lugar a la baja circulación de personas -posibles víctimas- y su inversa correlación con el aumento de digitalización de activos[3] y en segundo lugar a las ventajas comparativas que presentan estos medios comisivos: anonimización, extraterritorialidad, sofisticación del ardid, ignorancia e innovación.

b) **Victimas más vulnerables**

Esta situación es aún más grave para dos sectores de la ciudadanía que resultan especialmente vulnerables frente a los posibles ataques, las generaciones analógicas y los niños, niñas y adolescentes quienes, si bien nacieron con estas tecnologías, muchas veces entran en contacto con ellas sin el suficiente grado de madurez que les permita discernir los complejos engaños de quienes cuentan con experiencia para manipularlos para que entreguen información sensible o violar su intimidad.

c) Irrupción de la IA

La sofisticación del *"cuento del tío"* se ve aún más perfeccionada en los últimos dos años con la irrupción de lo que ya se vislumbra como la génesis de una nueva era, la inteligencia artificial, que permite construir ilustraciones a partir de fotos, montar videos a partir de imágenes, replicar voces, duplicar sitios web logrando así muy complejo la distinción entre lo real y lo impostado.

Herramientas de resguardo

Frente a este panorama que parece desolador, existen dos pilares importantes que pueden ayudar a los individuos para evitar ser la próxima víctima, la primera de ellas, es la conciencia digital, ello consiste en formarse continuamente sombre las nuevas tecnologías, y modalidades delictivas y asegurarse de tomar medidas de protección como tener una periodicidad para cambiar las passwords y no compartirlas entre plataformas u optar por autenticadores de passwords, implementar el doble factor es un punto fundamental para el resguardo de las cuentas, de la misma forma que tener sus softwares de antivirus actualizados.

a) **Autodefensa**

Otro de los ejes en la autodefensa implica que cada usuario sea consistente en lo que respecta al manejo de sus datos personales, tomar conciencia a quien le estoy entregando mis datos, si me registro en una web que ésta siga el protocolo https, o borrar los datos de registro de las

[2] https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52007DC0267 Link recuperado el 02/07/24

[3] Se entiende por activos como Datos Personales, Claves, Acciones, Dinero virtual y otros datos sensibles que pueden ser objeto de un ciberataque.

plataformas que ya no utilizo son algunos de estos ejemplos y especialmente resguardar los datos biométricos que son las claves de acceso en un futuro y las mismas son irremplazables, por ello hemos encontrado casos como el de la empresa Worldcoin que entregaba su moneda virtual en contraprestación por permitir a los usuarios el escaneo de su iris, dicha tesitura despertó la preocupación de la Agencia Española de Protección de Datos iniciándose una medida cautelar el pasado mes de marzo para que cesen sus actividades en España[4].

En este punto también es importante leer la política de privacidad de los websites, así como también su regulación en materia de cookies, mientras más información es entregada, más complejo puede ser el engaño pergeñado si esos datos caen en malas manos.

De la misma manera es importante revisar los permisos que se les otorgan a las apps y ejercitar recurrentemente la mente para preguntarse si verdaderamente es necesario permitirle acceso al micrófono de un móvil una aplicación de juegos o acceso a mis contactos a otra de edición de fotos, estas son red flags que nos pueden dar la pauta que estamos frente a un spyware o algún otro tipo de malware.

b) **Protección de Datos Personales**

El segundo pilar fundamental es exigir una política de Protección de Datos y seguridad de la información proactivo, esto implica que las empresas y organismos estatales deben tener un responsable de protección de datos y la creación de una figura de control y revisión como la del Delegado de Protección de Datos, similar a la estipulada por el Reglamento General de Protección de Datos[5] que brinde un tratamiento de datos que resguarde la privacidad de las personas y basándose entre otros en los principios de transparencia, minimización e integridad de los datos de los titulares.

Al respecto resulta interesante traer a colación el trabajo de la Dra. Ann Cavoukian quien fue una de las promotoras del desarrollo del Privacy by Design (PbD), este modelo sostiene siete principios que se pueden resumir como la necesidad y oportunidad de incluir la privacidad desde el momento en que se piensa un tratamiento de datos[6].

Así prefigurando el tratamiento futuro debe tenerse este enfoque atendiendo a siete principios:

i. La proactividad, es decir anticiparse a incidencias futuras y no ser reactivos cuando el problema ya ha acontecido.

ii. La privacidad con configuración determinada, es decir que no dependa de la acción del usuario, sino que ya se encuentre resguardada por diseño.

iii. Que la privacidad este incrustada en los propios sistemas de tecnología de la información, no como una capa que se coloca en la etapa final del desarrollo.

iv. Funcionalidad para lograr un win-win, esto implica dejar de lado falsas dicotomías como optar por privacidad o seguridad, sino generar un ecosistema de suma total.

[4] https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/worldcoin-se-compromete-paralizar-su-actividad-en-espana

[5] Normativa de la Comunidad Europea Ley 2016/679 que crea la figura del Delegado de protección de datos https://www.boe.es/doue/2016/119/L00001-00088.pdf

[6] https://www.edps.europa.eu/sites/default/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf

v. Seguridad en todo el ciclo de vida del dato, es decir asegurarse desde el momento de recolección hasta el de supresión que se hayan brindado las medidas de resguardo de privacidad.

vi. Respetar los principios de lealtad y transparencia, ello implica brindar visibilidad sobre los objetivos del tratamiento y que los mismos sean consistentes con las bases de legitimación al momento de recogida, tanto para usuarios como para proveedores.

vii. Poner en el centro al usuario, ello implica un respeto de su privacidad, notificarlo siempre que se haga un cambio en las políticas y se brinden canales de acceso sencillos para el ejercicio de sus derechos.

De esta forma, la Privacidad desde el diseño busca frenar con la recopilación masiva de datos que se hacen hoy en día, la "Big Data" y de esta forma evitar que las grandes empresas gestionen datos que excedan los fines que se proponen, y en definitiva los mismos sean pasibles de futuras brechas tecnológicas.

Marco Normativo

El Reglamento Europeo sobre Protección de Datos Personales (GDPR) se ha vuelto un cuerpo normativo estandarte en la materia y fija el rumbo a seguir para el resto de los países de la región, Brasil también ha puesto en vigor su propia Ley General de Protección de Datos (2020) lo que faculta a las empresas allí radicadas a establecer acuerdos con empresas dentro de la Comunidad Europea así como también facilita que las empresas originarias de Brasil puedan ofrecer sus servicios a ciudadanos radicados dentro de la zona comunitaria.

a) Avances en la región

La reciente aprobación del convenio 108+ para Latinoamérica incorpora muchos factores importantes para la protección de los datos personales, en primer lugar su aplicación tanto al ámbito público como privado, las categorías especiales para los datos sensibles, el rol del responsable y del encargado de datos en lo que respecta a su seguridad y una responsabilidad comprobada o "Accountability" que establece una obligación proactiva y sistemática del cumplimiento de la normativa en materia de protección de datos, y estipula la obligación de notificar las brechas de datos que puedan interferir gravemente con los derechos y libertades fundamentales de los titulares de los datos, sobre este último punto volveré más adelante.

b) Normativa Local

En Argentina la legislación vigente en materia de protección de datos es la ley nro. 25.326 data del año 2000 la cual incorporó el art. 157 bis a nuestro código penal, que estableció para este tipo de conductas la sanciones que van de un mes a dos años de pena privativa de libertad.

La actualización de esta normativa se vuelve imperante, no solamente para adecuarse a los estándares internacionales, entre ellos el señalado convenio 108 + y facilitar los acuerdos con empresas que brindan un tratamiento de datos conforme a la normativa aludida, sino además para brindar mayor resguardo de la información de la que el ciudadano resulta ser titular.

Brechas o Leaks

Retomando la cuestión de las brechas de datos, en lo que va del presente año se dieron a conocer dos vulneraciones de notoria importancia a bases de datos controladas por organismos nacionales.

El primero de los ciberataques tuvo como víctima la base de datos del Registro

de Licencias de Conducir donde se publicaron 5.7 millones de imágenes en un archivo de 1.25 Tb, y unos días más tarde se dio a conocer un nuevo ataque a la base de datos del Registro Nacional de las Personas Re.Na.Per donde se habían filtrado 59 millones de registros.

a) La versión oficial

Las declaraciones por parte de las autoridades de gobierno negaron la existencia del hackeo, alegando que habían detectado una intrusión a los sistemas pero que lograron neutralizarlo añadiendo que no hubo información sensible comprometida.

b) La versión de los técnicos

Expertos en la materia como Christian Borguello explicaron que sobre este último se detectó que la filtración "leak" se produjo a través del sistema Chutro, software utilizado por el Renaper, y en este punto en lo que respecta a los datos de las personas se filtraron nombre, apellido, fecha de nacimiento, fecha de fallecimiento y número de D.N.I. y en otras también su mail y domicilio.

Además, se puedo advertir la filtración de algunas carpetas con información relativa al Covid-19, una base de datos de extranjeros domiciliados en el país e información personal de las fuerzas Armadas[7].

c) El impacto subyacente

Pero lo que más preocupó a los expertos es el vínculo que tiene el Renaper como Keys de terceros, es decir si por su rol en cadena de suministros, o como validador de identidades en el dialogo entre aplicaciones, "API", esta filtración pueda afectar el registro de bancos, fintech, correos, Ministerios u otros organismos estatales, llegando a contabilizarse cerca de 349 Apis que "hablan" con la base del Renaper.

d) La profundidad del problema

Otro de los datos que exponen el estado de la cuestión es que de los 1610 operadores del sistema interno del Renaper 378 tenían por password 1234; cerca de otros 300 usuarios más 12345 y cerca de otros 100 más 123456 es decir más de la mitad de los usuarios tenían sus accesos a merced del próximo que quisiera ingresar con su usuario poniendo de manifiesto la falta de concienciación en materia de ciberseguridad y sus implicancias sobre los afectados.[8]

El rol del Estado

Es absolutamente lógico que el Estado recolecte datos personales de la ciudadanía, no solo como una cuestión estadística, sino como generador de data para planificar políticas públicas y pensar su implementación.

Ahora bien, la cuestión pasa por hacer que ese tratamiento de datos sea armónico con los derechos constitucionales a la privacidad e intimidad, y cumpla entonces con sus deberes de garante de la seguridad de la información y asegure su confidencialidad.

Entre estas tareas se destaca la de capacitar a su personal sobre la importancia del resguardo de los datos y seguir los protocolos de seguridad para evitar acceso no autorizados y prevenir que se generen brechas de seguridad.

Palabras finales

A modo de conclusión podemos decir que hoy no existe un blanco imposible para los ciberataques en el mundo, sin embargo, existen muchas herramientas en materia de

[7] https://twitter.com/SeguInfo/status/1780713614053412898

[8] https://www.brodersendarknews.com/p/filtraciones-licencias-renaper-argentina-analsis

estrategia en ciberseguridad y protección de datos que pueden mitigar los riesgos.

Por su parte el Estado en su rol de responsable de los datos que trata, debe implementar de forma urgente la figura del Delegado de Protección de Datos para evitar que se recopilen, almacenen y traten datos que no sean estrictamente necesarios es el primer paso para avanzar en el resguardo de los datos personales.

Este cambio debe ser acompañado de una actualización legislativa en la materia que se aggiorne a los estándares internacionales y cree de un organismo de control independiente que pueda dar pautas de Re-acción frente a incidencias de semejante magnitud.

De esta forma, se pone el foco en el ciudadano para la creación de políticas proactivas que capaciten a los más jóvenes sobre los riesgos que se corren en la virtualidad y también a las generaciones mayores para prevenirlos frente a las nuevas modalidades de cibertaques.

Finalmente es fundamental que se tome como una política de estado, que logre generar un nivel de conciencia especialmente a los operadores de las bases de datos públicas que resulte como un primer cortafuegos a los intentos de intrusión en los sistemas estatales.

Bibliografía y citas

- Aboso E. Gustavo, *"Ciberdelitos Análisis doctrinario y jurisprudencial"* ed. El Dial
- AEPD Guia para la Notificación de Brechas
- AEPD *"14 Equívocos com relación a la identificación y autenticación biométrica"* *https://www.aepd.es/guias/nota-equivocos-biometria.pdf*
- APEP *"El futuro de la privacidad difícil equilibro entre derecho objetivo y subjetivo"* https://www.apep.es/el-futuro-de-la-privacidad-dificil-equilibrio-entre-derecho-objetivo-y-subjetivo/
- Cost of a Data Breach Report 2023- IBM
- Incibe- "Como se protege a la ciudadanía frente a los ciberiesgos" 2023 https://www.observaciber.es/sites/observaciber/files/media/documents/Estudios_Como%20se%20protege%20a%20la%20ciudadan%C3%ADa%20de%20los%20ciberriesgos.pdf
- Informe Undoc "informe exhaustivo sobre el delito cibernetico" 2013
- UNQ Material brindado en la Diplomatura de Ciberdelitos.