Retos y peligros de vivir sin privacidad en las TIC

Jersain Zadamig Llamas Covarrubias
Co-fundador del movimiento internacional Legal Hackers

Resumen

PALABRAS CLAVES:
Datos Personales, Privacidad, Internet, Acceso No Autorizado, Ciberalfabetización, Ciberhigiene

Con el presente ensayo se pretende abordar una concepción general sobre lo que es la privacidad, así mismo se realiza un análisis de los retos y peligros de vivir sin privacidad y la importancia de la protección de datos ante el rompimiento de paradigmas tradicionales por las nuevas tecnologías disruptivas, concluyendo en que la ciberalfabetización y ciberhigiene son pilares fundamentales para combatir las amenazas, revelaciones, riesgos y vulnerabilidades que pudieran convertirse en incidentes de seguridad que atenten contra la injerencia arbitraria de la vida privada.

Introducción

En las sociedades contemporáneas, las TIC son la espina dorsal del desarrollo. La información se convierte en conocimiento y poder, los datos personales son tan importantes que transmutan la forma en la que percibimos el mundo y se convierten en el petróleo del siglo XXI. Pero esto no termina aquí, ya que con la llegada del Machine Learning, Deep Learning e Inteligencia Artificial en armonía con el Big Data todo se mueve tan deprisa en "Velocidad, Variedad, Volumen, Valor y Veracidad" (Martínez, 2018: 262-263), acorralando al sector público, privado y sociedad civil organizada, a tomar decisiones precipitadas y en ocasiones no del todo estudiadas, pues gracias a la celeridad con la que se mueve el mundo digital, pareciera que es humanamente imposible mitigar los incidentes de seguridad o tomar un breve espacio para hacer conciencia sobre los datos personales y la privacidad.

En el informe del Foro Económico Mundial (2019: 18), titulado The Global Risks Report 2019 14th Edition, específicamente en la encuesta de percepción de riesgos mundiales, coloca los ciberataques: robo de datos/dinero en el cuarto lugar con un 82%. Así mismo en el informe Cost of a Data Breach Report 2019, elaborado por IBM Security y Ponemon Institute (2019: 3), cada registro perdido o robado con información sensible o confidencial tiene un precio de $150 dólares por registro y el promedio mundial de registros expuestos por cada incidente de seguridad es de 25,575.

Por su parte, la empresa internacional LLoyd's (2018a: 20), en su Informe de riesgos emergentes 2018, relacionado con la Tecnología, ha comunicado que a nivel mundial, se estima que el cibercrimen le cuesta a las empresas $400 mil millones al año, lo que significa que los riesgos cibernéticos son uno de los principales problemas que las empresas deben tener en cuenta cuando se trata de su capacidad de recuperación y planificación de continuidad. En el mismo orden de ideas, el "2017 fue uno de los años más costosos para las catástrofes naturales en la última década. Nuevas amenazas como la cibernética plantean diferentes riesgos para el crecimiento económico mundial" (Lloyd's 2018b: 46). Pudiendo deducir que un ataque cibernético es más costoso que un desastre natural.

Privacidad

Definir la privacidad es algo complejo, pues existen diversos enfoques, perspectivas y encuadres epistemológicos, pero lo cierto es que este concepto pese a que se defina directa o indirectamente, todo concluye en que es un pilar insustituible de la dignidad humana y por ende de los derechos humanos.

En la doctrina se encuentran diversos conceptos de privacidad, no obstante, a mi consideración son dos definiciones las que marcan el preámbulo teleológico, la primera que es la más primigenia y posiblemente el arquetipo es el "derecho a que nos dejen en paz" (Warren & Brandeis, 1890). La segunda es el derecho a controlar el uso que otros hacen de las informaciones que nos afectan (Westin, 1968).

Una definición ecléctica de privacidad, es la que define la Comisión Interamericana de Derechos Humanos (2017) donde señala que:

> *El derecho a la privacidad protege al menos cuatro bienes jurídicos, a saber: a) el derecho a contar con una esfera de cada individuo resistente a las injerencias arbitrarias del Estado o de terceras personas; b) el derecho a gobernarse por reglas propias según el proyecto individual de vida de cada uno; c) el derecho al secreto respecto de lo que se produzcan en ese espacio reservado con la consiguiente prohibición de divulgación o circulación de la información capturada, sin consentimiento del titular, en ese espacio de protección reservado a la persona; y d) el derecho a la propia imagen (p. 78).*

En resumen, se ha definido la privacidad desde diversos encuadres epistemológicos, y es necesario demostrar dos enfoques respecto a la privacidad y datos personales. Pues así, como en el mundo existe el lenguaje binario representado en 1 y 0, en verdadero o falso, también podremos encontrar diversos enfoques en la privacidad. Tal es el caso de David Cuartielles (2019), el fundador de Arduino, que dice que la "gente está muy equivoca-

da pensando que sus datos son super valiosos... que la privacidad de los datos personales está sobrevalorada... porque cuanta más gente los tenga menos valen para quienes los quieren para su beneficio", mientras que desde otra perspectiva Bruce Schneier (2006) un reconocido criptógrafo, dice que "la privacidad es un derecho humano inherente y un requisito para mantener la condición humana con dignidad y respeto… la privacidad nos protege de los abusos de quienes están en el poder, incluso si no estamos haciendo nada malo en el momento de la vigilancia".

Aunque hemos abordado conceptos y enfoques de privacidad, sin dejar por un lado la práctica y facticidad, la realidad es que se puede inferir que no hay derechos absolutos, pero a mi percepción esto no es del todo cierto, ya que en un sentido lógico la vida y la libertad son derechos absolutos universales, pero también lo es la intimidad. De manera más puntual, la Real Academia Española (RAE) da luz respecto a una separación entre privacidad e intimidad, donde la intimidad es la "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia" y cómo privacidad al "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión", esto es que no existe ninguna regla, locución sentenciadora o garantía para poder violar la intimidad, incluso ni con excepciones constitucionales o mandamientos escritos, en pocas palabras la intimidad es un derecho inviolable inmutable absoluto universal y la privacidad pese a que es un derecho fundamental, está sujeta a cada caso en concreto.

Además, en este mundo tan hiperconectado y con tantas violaciones de datos, pese a que en un primer plano pudieran colisionar la libertad de expresión y la privacidad, también la privacidad entra en conflicto con la seguridad nacional, y es aquí donde emerge un ciudadano que lucha por su privacidad, con ideologías de Cypherpunk, Lex Cryptographica o Dataísmo, con técnicas de cifrado o anonimato, ya sea utilizando algún seudónimo, software como TOR (The Onion Router), o incluso una VPN Virtual Private Network, en español red privada virtual.

Retos y peligros de privacidad en el siglo XXI

En un primer plano contamos con el Internet; un espacio sin color, nacionalidad, política o religión, que puede ser una herramienta pero a la vez un arma. Un ejemplo es la suplantación o robo de identidad como el riesgo más común, ya que pueden realizarse actos ilícitos con diferentes niveles de dificultad, desde crear un perfil falso y hacerse pasar por alguien más, ingeniería social o hasta utilizar métodos técnicos para lograr un acceso no autorizado. También existen métodos no tan especializados como doxing, acoso, sexting, sextorsion o incluso comentarios de odio, que dañan indirectamente a la privacidad, protegiendo los derechos a la propia imagen, reputación y al honor, creando un menoscabo e injerencia arbitraria en la vida privada.

Otro reto que deberá abatir nuestra sociedad del conocimiento, es el uso de drones, pues pese a que en México y otros países ya exista su regulación especial, requiriendo una licencia para aquellos que dispongan de ciertas características, en la práctica pueden ser utilizados de manera ruin, para vigilar sin el consentimiento de las personas, y es claro que por las características fisonómicas del humano es imposible mitigarlos de manera natural.

Además, otro reto fundamental es el reconocimiento facial, un claro ejemplo es Facebook, donde una Corte Federal de Apelaciones de Estados Unidos dio la razón a un grupo de denunciantes que señalaron que el reconocimiento facial de esta empresa, viola el acta de privacidad de información biométrica (BIPA) del Estado de Illinois (Patel vs Facebook), que prohíbe la recolección de datos biométricos incluida esta tecnología, claramente sin autorización ni consentimiento informado. Es así que Facebook el 03 de Septiembre del 2019 emitió un comunicado donde expresaba que todas las características de reconocimiento facial, incluyendo etiquetado, estarán apagadas por defecto para usuarios nuevos, para los usuarios ya registrados posterior a este comunicado deberían desactivarlo manualmente. (R3D.mx, 2019).

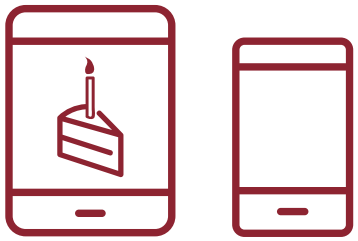
De igual modo, respecto al reconocimiento facial, cuando se une con el Internet de las Cosas, con su comunicación de persona a persona (P2P), persona a máquina (P2M), e inclusive de máquina a máquina (M2M), transforman la manera en la que percibimos el mundo. En primer término, tenemos las cámaras de vigilancia, que su utilización de manera desmedida y no apegada a derecho con la tecnología innovadora de reconocimiento facial, pueden convertir a las naciones en el Gran Hermano de George Orwell. No obstante, ante esta situación desde el ámbito de la moda han diseñado prendas y accesorios personales para evitar ser captados y reconocidos por esta tecnología (Esage, 2019).

Siguiendo con el Internet de las Cosas, que son dispositivos interrelacionados con identificadores únicos y capacidad de transferir datos, llegan los asistentes de voz, que en este pleno año 2019 diversas empresas como Amazon, Google y Apple reconocieron que almacenaban y enviaban las conversaciones a trabajadores que escuchaban lo que dicen los usuarios para mejorar el servicio (elmundo.es, 2019).

Pero esto no concluye aquí, pues si mezclamos Internet, Big Data e Internet de las Cosas, es evidente que tenemos información en dispositivos y sensores conectados que incluso pueden comunicarse de máquina a máquina sin intervención humana, y estos dispositivos son vulnerables a acceso no autorizado u otros ciberdelitos, ya que en ocasiones su software se encuentra desactualizado, vulnerable o desde su fabricación contienen contraseñas genéricas. Si bien podemos encontrarnos con datos identificativos; de origen; ideológicos; sobre la salud; laborales; patrimoniales; sobre procedimientos administrativos y/o jurisdiccionales; académicos y de tránsito y movimiento migratorios, lo cierto es que con las TIC, nacen nuevas formas de información concerniente a personas físicas identificadas o identificables, incluso cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información, aún si se puede "singularizar, vincular o inferir la información relativa a una persona" (Grupo de Trabajo Artículo 29, 2019: 3).

Dicho lo anterior, independientemente de la jurisdicción, pese a que ya se encuentra una homologación a que existen datos personales en identificadores en línea como Cookies; Web Beacons; Metadatos y direcciones IP (en algunos casos), entre otros. A pasos agigantados el mundo virtual trasciende al material, y con todos estos sensores del Internet de las Cosas nacen nuevos retos, pudiendo hacer identificables "la forma de oprimir un teclado y la forma de caminar" (INAI, 2018: 10-11), o también algo que pareciera de ciencia ficción; el pentágono tiene un láser que puede identificar a las personas a distancia, por el latido de su corazón, captando una firma cardiaca única a 200 metros de distancia, incluso a través de la ropa (Hambling, 2019).

En el mismo sentido, si ya se abordó el utilizar la tecnología como un objeto y un medio, ahora surge una nueva forma de vivir la tecnología, utilizándola como fin, y es cuando el ser humano quiere trascender en sus capacidades o suplir déficits, emergiendo nuevas ideologías de transhumanismo y posthumanismo, especialmente con el fenómenos de los cyborgs (ser de materia orgánica y dispositivos tecnológicos). Un caso es Steve Mann (2012), que fue agredido por empleados de Mcdonald's en Francia, por utilizar un EyeTap (pantalla incrustada en la cabeza que se coloca delante del ojo con funciones de cámara y pantalla) con el argumento de proteger el derecho a la privacidad del personal y clientes. Ahora imaginemos a otros cyborgs, como Neil Harbisson con su antena para escuchar los colores, o Rob Spence con su Eyeborg con su ojo biónico con cámara. ¿Esto podría violar la privacidad?



Conclusiones

Después de abordar de manera exhaustiva la definición, riesgos y retos de la privacidad, es necesario concluir que lo más importante y la solución a la mayoría de los problemas de violación de datos son las personas. Ya que sería muy sencillo decir que todo se resolverá gracias a una tecnología disruptiva, por mencionar algunas de la industria 4.0 como: los Sistemas de integración; máquinas y sistemas autónomos (robots); Internet de las cosas (IoT); Manufactura aditiva; Big data y análisis de grandes datos; Computación en la nube; Simulación de entornos virtuales; Inteligencia Artificial; Ciberseguridad; y Realidad Aumentada (Basco, Beliz, Coatz & Garnero, 2018: 26-29), así como Blockchain o conocida como la Cadena de Bloques.

Lo anterior lo sustento con un sencillo ejemplo, que fue el de las elecciones para la presidencia de México del año 2018, donde algunos ciudadanos subieron su foto con el pulgar demostrando que ya habían votado, sin embargo, expertos afirmaron que al realizar esta acción era posible que un ciberdelincuente pudiera extraer la huella dactilar y utilizarla para cometer algún delito, fraude cibernético o acceder a un sistema privado (Meza, 2018). Dicho lo anterior se comprueba que el eslabón más débil y a la vez el más fuerte son las personas, pues todo radica en la educación digital. La Unión Europea en su Reglamento sobre ciberseguridad 2019, menciona dos conceptos clave que deberán forjarse como pilares fundamentales en las sociedades de la información, los cuales son ciberhigiene y ciberalfabetización.

Las formas, métodos y sistemas del pasado fracasaron porque nunca consideraron la privacidad como un pilar fundamental para proteger el futuro. Y es necesario tener presente que “ninguna generación puede atar con sus leyes a las generaciones futuras” (Rodotà, 2014: 30), y si en el pasado la privacidad ha sido derrotada y olvidada, es menester luchar por el derecho de la misma.

Debemos abandonar la idea de que la privacidad ha muerto y que debemos olvidar, que existen otros principios que deben trascender ante nuestros derechos originarios. Pues la privacidad es sinónimo de sociedad libre, es el aliento hacia un plan de prosperidad, aspira a un mundo donde cada quien sea dueño de sus datos. Es necesario entender, que la libertad se basa en la privacidad, que los derechos humanos y su dignidad humana deben encontrar su mejor aliado en este principio.

Debemos recordar y reforzar el asunto del derecho a la propiedad de los datos, donde realmente le pertenezcan a las personas, donde la gente pueda controlar sus propios datos, obtener el derecho de decidir sobre su identidad digital, qué compartir y qué no, respetar y evitar las injerencias arbitrarias a la vida privada, conviviendo con sistemas descentralizados y distribuidos como pilares de una sociedad abierta, libre y anónima, expresandonos de manera respetuosa sin miedo a represalias, pues únicamente de esta manera se construirá una sociedad libre, donde de manera corpórea e incorpórea, individual y colectiva, todos podrán controlar sus propias vidas. Vale la pena forjar un camino donde podamos elegir controlar nuestro destino y lo que somos, a nosotros mismos, somos datos e información. En equilibrio la privacidad y legalidad, se convierten en una lucha por el derecho.

Referencias

Basco A., Beliz G., Coatz D. & Garnero P. (2018). Evolución de las Revoluciones Industriales. Banco Interamericano de Desarrollo. Recuperado de: https://bit.ly/33mYiOy

Comisión Interamericana de Derechos Humanos CIDH. (2017). Estándares para una Internet Libre, Abierta e Incluyente Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. Recuperado de: https://bit.ly/2pOJrOz

Cuartielles, D. (2019, 02 de noviembre). David Cuartielles: "La privacidad de los datos como concepto ético es muy flexible". Elpais España. Recuperada de: https://bit.ly/2Ct1Cfz

Esage, A. (2019). 8 métodos para esquivar cámaras y software de reconocimiento facial. Recuperado de: https://bit.ly/2qpUxtn

Elmundo.es (2019). Apple, Google y Amazon escuchan: ¿es seguro hablar con un asistente de voz?. Recuperado de: https://bit.ly/36GZjU2

Foro Económico Mundial. (2019). The Global Risks Report 2019 14th Edition. Recuperado de: https://bit.ly/33mzjLx

Grupo de Trabajo Artículo 29. (2014). Dictamen 05/2014 sobre técnicas de anonimización. Recuperado de: https://bit.ly/33pEz0Q

Hambling, D. (2019). The Pentagon has a laser that can identify people from a distance—by their heartbeat. Recuperado de: https://bit.ly/2qo5fR0

IBM Security & Ponemon Institute (2019). Cost of a Data Breach Report 2019. Recuperado de: https://ibm.co/2NNMRct

INAI. GUÍA para el Tratamiento de Datos Biométricos. Recuperado de: https://bit.ly/2rapZMn

LLoyd's. (2018a). Emerging Risk Report 2018 Technology. New realities Risks in the virtual world, Recuperado de: https://bit.ly/32mdQB4

LLoyd's. (2018b). A world at risk Closing the insurance gap, Recuperado de: https://bit.ly/32nx8pw

Mann, S. (2012). Augmediated* Reality and "McVeillance". Recuperado de: https://bit.ly/2PMOSrX

Martínez, R. (2018). Capítulo 11 Inteligencia Artificial, Derecho y Derechos Fundamentales. M. Barrios & J. Torregrosa (Ed.), Sociedad Digital y Derecho. (pp. 262-263). Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado. Madrid. Recuperado de: https://bit.ly/2WKmpED

Meza, E. (2018). Compartir fotos del voto con tu huella puede vulnerar tu seguridad. Recuperado de: https://bit.ly/2PXyNiW

R3d.mx (2019). facebook desactiva por defecto el reconocimiento facial para usuarios nuevos. Recuperado de: https://bit.ly/2PXnCqR

Rodotà, S. (2014). El derecho a tener derechos. Editorial Trotta.

Schneier, B. (2006). The Eternal Value of Privacy. Recuperado de: https://bit.ly/2rjDrOf

Warren S., Brandeis L. (1890). The Right to Privacy. Harvard Law Review Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220 (28 pages). Recuperado de: https://bit.ly/36CTneI

Westin, A. (1968). Privacy And Freedom, Washington and Lee Law Review. Recuperado de: https://bit.ly/2Njx3z4

Jersain Zadamig Llamas Covarrubias

Es Abogado por la Universidad de Guadalajara y Maestrante en Derecho Constitucional y Administrativo por la misma. Especialidad en derecho y nuevas tecnologías de la información.

Publicaciones: libro "Internet ¿Arma o Herramienta" (2018) UdG, revista ciencia de la legislación de la Universidad del Salvador en Argentina, Revista Informática Jurídica en España, y en el Congreso del Estado de Oaxaca.

Es un activista y pionero en derecho y nuevas tecnologías de la información en latinoamérica, publicando en diversos medios en Perú, Venezuela, Uruguay y Chile. Es co-fundador del movimiento internacional Legal Hackers en la ciudad de Guadalajara.