

LA PANDEMIA COVID-19, DISTANCIAMIENTO SOCIAL, EL USO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN Y LA FALTA DE REGULACIÓN INTERNACIONAL QUE PROTEJA LOS DATOS PERSONALES*

VICTORIA ALVA LUGO**

I. Introducción

La declaratoria de la Organización Mundial de la Salud ante la emergencia sanitaria mundial por el coronavirus que provoca la enfermedad COVID-19 iniciada en Wuhan (China) el 31 de diciembre de 2019, y el establecimiento de las diversas medidas para evitar su propagación entre las que desataca el distanciamiento social, para evitar su contagio tiene como consecuencia que las personas modifiquen el desarrollo de actividades económicas, sociales y culturales para respetar el espacio de metro y medio que es necesario para proteger su salud en todo el mundo.

Las Tecnologías de la Información y la Comunicación tienen la capacidad global para que las actividades de algunas personas se puedan desarrollar de forma ubicua y en cumplimiento de la medida de distanciamiento para proteger su salud. Sin embargo para el teletrabajo, las plataformas audiovisuales y las redes sociales, que son mecanismos para el

* Fecha de recepción: mayo 2020. Aceptado para tu publicación: mayo 2020.

** Catedrática de la Licenciatura en Derecho y en la Maestría en Negocios Internacionales de la Universidad La Salle (México). Correo electrónico: alva_victoria@hotmail.com

desarrollo de las actividades de las personas, requieren una gran cantidad de datos personales de los usuarios para ingresar e interactuar en ellas.

Por lo que los cibernautas se encuentran ante el riesgo de vulneración y accesos no autorizados de sus datos personales, que si los países no cuentan con la legislación adecuada quedan vulnerables los usuarios.

El presente estudio se referirá a la medida de prevención del COVID-19 consistente en el distanciamiento social, para estudiar el fenómeno de la aplicación de las tecnologías de la información y comunicación que emplean las personas para el desarrollo de las actividades económicas, sociales y culturales y los riesgos a vulneración de datos personales que existen ante el uso de aplicaciones, plataformas y compras en línea.

Por lo cual es necesario crear un marco normativo internacional que proteja los datos personales, actualmente el Convenio 108 de la Comunidad Europea, propone un marco normativo de protección de datos personales, que pretende sea aceptado por la comunidad internacional, para alcanzar la protección global de los usuarios de la red.

II. Marco conceptual

La 4ª Revolución Tecnológica reconoce la preponderancia de las Tecnologías de la Información y la Comunicación para el desarrollo de la sociedad, en consecuencia la Constitución Política de los Estados Unidos Mexicanos (CPEUM) reconoce en el Artículo 6 que: “El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet”.

Para garantizar el respeto de los derechos de los usuarios de internet y las tecnologías de la información y comunicación la CPEUM establece en el Artículo 16 segundo párrafo que: “Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros”. Los derechos ARCO (de acceso, ratificación, cancelación u oposición al tratamiento de datos personales) reconocen

que es el titular de los datos personales, quien debe decidir en todo momento, sobre el uso y transmisión de los datos que lo vuelven identificado e identificable.

México se adhirió en 2018 al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del 28 de enero de 1981 (conocido como el Convenio 108), y a su Protocolo Adicional del 8 de noviembre de 2001, relativo a las autoridades de control y a los flujos transfronterizos de datos. No obstante que ya contaba con una ley de protección de datos tanto para entidades públicas como privadas.

El Convenio 108, es reconocido como un importante instrumento que pretende crear un marco legal internacional en materia de protección de datos personales, es considerado el primer instrumento internacional jurídicamente vinculante en el área de la protección de datos, ya que obliga a las partes firmantes a tomar las medidas necesarias a nivel doméstico para adecuar su legislación a los principios establecidos por el Convenio en el ámbito del tratamiento de la información personal.

Los instrumentos globales plantean soluciones a problemas de interés mundial como la declaratoria de emergencia sanitaria de la OMS ante la enfermedad de COVID-19 y la medida de distanciamiento social que solicita implementar para frenar el contagio. La solución tecnológica para continuar con las actividades económicas, sociales y culturales es un aliado para la adecuada implementación de la medida sanitaria del distanciamiento social, a través del uso e implementación de soluciones tecnológicas, en las que se respeten el derecho y la protección de los datos personales de los usuarios.

III. La declaración de la OMS del COVID-19 como pandemia y la recomendación del distanciamiento social como mecanismo de prevención a la propagación

El coronavirus causa infecciones respiratorias en humanos que pueden ir desde el resfriado común hasta enfermedades más graves como el Síndrome Respiratorio de Oriente Medio (MERS) y el síndrome respiratorio

agudo severo (SRAS). El coronavirus que se ha descubierto más recientemente causa la enfermedad COVID-19 con síntomas como la fiebre, la tos seca y el cansancio.

Esta enfermedad denominada COVID-19 inició el 31 de diciembre de 2019 en la ciudad de Wuhan (China), y desde los primeros momentos comenzó a ser monitoreada y estudiada por las autoridades nacionales e internacionales para conocer y establecer medidas de contención y propagación, el 30 de enero de 2020 la OMS emitió entre otras las siguiente recomendación y advertencias:¹

- ✓ Evitar el contacto cercano con personas que sufren infecciones respiratorias agudas.
- ✓ Lavado frecuente de manos, especialmente después del contacto directo con personas enfermas o su entorno.
- ✓ Evitar el contacto sin protección con animales de granja o salvajes.
- ✓ Las personas con síntomas de infección respiratoria aguda deben practicar la etiqueta de la tos (mantener distancia, cubrirse al toser y estornudar con pañuelos desechables o ropa, y lavarse las manos).
- ✓ Dentro de las instalaciones de atención médica, mejorar las prácticas estándar de prevención y control de infecciones en los hospitales, especialmente en los departamentos de emergencias.

El 11 de marzo de 2020 la OMS, profundamente preocupada por los alarmantes niveles de propagación de la enfermedad y por su gravedad, así también por los niveles también alarmantes de inacción, determina en su evaluación que el COVID-19 puede caracterizarse como una pandemia. Así, iniciaron las estrategias que involucraron a autoridades multisectoriales y de todos los niveles locales, regionales e internacionales para frenar el contagio global del COVID-19, estas acciones se centraron en las estrategias principalmente: sanitarias, económicas y sociales, respecto a otras emergencia de salud; con el COVID-19 es necesario el involucramiento de todos los sectores y todas las autoridades para la implementación de las acciones efectivas que frenen los efectos nocivos de la contingencia.

Por cuanto a las estrategias propuestas para controlar la pandemia principalmente se enfocaron en: sanitarias, económicas y sociales; el pre-

¹ OMS, *Novel Coronavirus (2019-nCoV) Situation Report-10*, p. 6.

sente estudio se referirá a las medidas sociales para estudiar el fenómeno del distanciamiento social y la implicación de las tecnologías de la información y comunicación. El distanciamiento social se define como: *“El distanciamiento físico, significa estar físicamente separado. La OMS recomienda mantener una distancia de al menos un metro (3 pies) con los demás. Es una medida general que todas las personas deberían adoptar incluso si se encuentran bien y no han tenido una exposición conocida a la COVID-19.”*²

La adopción del distanciamiento social tiene como objetivo evitar la transmisión de la enfermedad de acuerdo a la OMS *“Una persona puede contraer la COVID19 por contacto con otra que esté infectada por el virus. La enfermedad se propaga principalmente de persona a persona a través de las gotículas que salen despedidas de la nariz o la boca de una persona infectada al toser, estornudar o hablar”*.³ La implementación de esta medida tiene un gran impacto en el desarrollo de las actividades de los ciudadanos, y así también es la medida de prevención más efectiva.

El alcanzar el objetivo del distanciamiento social plantea grandes retos económicos, sociales y culturales; además de que el COVID-19 se encuentra presente en todo el mundo la medida debe alcanzar el cumplimiento global. Por lo cual recomendó a la aplicación de medidas sanitarias adicionales a los Estados que alcancen un nivel igual o mayor de protección sanitaria que las recomendaciones de la OMS y la colaboración y asistencia de los Estados Parte para adopción y aplicación de las mismas.⁴

² OMS, *¿Cuál es la diferencia entre aislamiento, cuarentena y distanciamiento? Distanciamiento Social*.

³ OMS, *¿Cómo se propaga la COVID-19?*

⁴ Reglamento Sanitario Internacional. *Artículo 43 Medidas sanitarias adicionales* 1. El presente Reglamento no impedirá que, en respuesta a riesgos específicos para la salud pública o emergencias de salud pública de importancia internacional, los Estados Partes apliquen medidas sanitarias acordes con su legislación nacional pertinente y las obligaciones dimanantes del derecho internacional: a) que proporcionen un nivel igual o mayor de protección sanitaria que las recomendaciones de la OMS...; *Artículo 44 Colaboración y asistencia* 1. Los Estados Partes se comprometen a colaborar entre sí en la medida de lo posible para: a) la detección y evaluación de eventos, y la respuesta a los mismos, según lo que dispone el presente Reglamento; b) la prestación o facilitación de cooperación técnica y apoyo logístico, en particular para el desarrollo y reforzamiento de las capacidades en la esfera de la salud pública que requiere el presente Reglamento; c) la movilización de recursos financieros para facilitar la aplicación de sus obligaciones dimanantes del presente Reglamento; y d) la formulación de proyectos de ley y otras disposiciones legales y administrativas para la aplicación del presente Reglamento.

IV. Soluciones tecnológicas a la aplicación del distanciamiento social

La implementación del distanciamiento social que propone la OMS para mitigar el COVID-19, tiene serias complicaciones para el desarrollo de actividades sociales, económicas y culturales en la implementación global de la medida y mitigar la pandemia. Para cumplir con el distanciamiento de metro y medio que establece el distanciamiento social, es inminente reducir las actividades de las personas; lo cual podríamos dividir en económicas, sociales y culturales sin embargo también existe la necesidad de continuar con ellas por lo cual las tecnologías de la información y la comunicación ofrecen a las personas una forma alterna al cumplimiento de estas actividades y al tiempo cuidar su salud implementando el distanciamiento social.

La Tecnología de la Información y la Comunicación (TIC's) comparten con el COVID-19 la cualidad de la globalidad, y tienen la capacidad de desarrollar las actividades de las personas cumpliendo con la medida de distanciamiento social que estableció la OMS. Las TIC's ya formaban parte de las actividades que las personas realizaban antes del COVID-19 y tienen la capacidad de adaptarse a las actividades de naturaleza económica, sociales y culturales, además de ser factores decisivos para generar y acceder a la riqueza, el poder y el saber en el Siglo XXI en la 4ª Revolución Tecnológica.

A partir de la creación del Internet a finales de los ochenta se inició el desarrollo tecnológico que evolucionó, hasta formar las TIC's que han revolucionado y se ha adaptado a las actividades y el desarrollo de la humanidad; el fenómeno COVID-19 impulsa aún más la necesidad de crear instrumentos internacionales que regulen el ciber espacio. Ante los retos sanitarios también las TIC's son una herramienta eficiente que se suma al fenómeno de la globalización —termino mezcla de política y economía— que desvaneció las fronteras del comercio, creado una economía global que en fusión con la tecnología y el uso de Internet crea un mercado digital, ideal para el intercambio comercial de gran y pequeña escala otra característica que comparte con la pandemia global.

Manuel Castells⁵ nos dice que “la economía informacional es un sistema socioeconómico distintivo en relación con la economía industrial, pero no debido a que se difieran en la fuente para aumentar su productividad”. La mayor parte del trabajo informático tiene como objetivo el procesamiento rutinario de datos, con poca o nula toma de decisiones asistida por progra-

⁵ Castells, Manuel, *La Sociedad Red*, p. 118.

mas computarizados. Hoy día, cualquier persona tiene a disposición en un celular que se equipara a la tecnología que existía en toda la humanidad hace veinte años, sin embargo en este dispositivo almacenamos todos o casi todos los datos que pueden ser consultados, transmitidos y almacenados.

El COVID-19 ha detonado un sin fin de interacciones en el mundo digital en las que se difunde información, estadísticas, advertencias e incluso se puede ingresar los datos de las personas para tener un pronóstico sobre el riesgo que corre en caso de contraer la enfermedad en la “Calculadora de complicación de salud por COVID-19”,⁶ que desarrolló el Instituto Mexicano del Seguro Social, por mencionar un ejemplo de cómo la tecnología se adapta y desarrolla soluciones que están a disposición inmediata de los usuarios.

Ante el distanciamiento social, nadie piensa en redactar un mensaje en papel para enviarlo a través de la oficina postal, —previo el pago de la estampilla correspondiente— y esperar semanas o tal vez meses, en que ese mensaje llegue a su destinatario y recibir respuesta. La opción tecnológica y lógica, es un *e-mail* que en segundos arriba a su destinatario y en minutos se obtienen múltiples réplicas entre emisor y destinatario. La inmediatez tecnológica se convierte en una solución a la realización de tareas en cumplimiento a la medida de distanciamiento social, que con eficiencia y eficacia cumple con la suspensión de traslados y reuniones presenciales.

La evolución tecnológica, marca una sensible diferencia entre un fenómeno pandémico como la Gripe Española de 1918, en la que una medida como el distanciamiento social resultaría imposible la realización de múltiples actividades. Gracias al avance tecnológico podemos realizar en la pandemia de COVID-19 de forma remota un sin fin de actividades y tareas que hace 20 años sería imposible de realizar como: comprar, vender, trabajar, ejercitarse e incluso celebrar un cumpleaños; todo esto es posible realizarlo en un día y de forma inmediata gracias a los pequeñas y grandes implementaciones tecnológicas.

Sin embargo la OEA ha advertido sobre el riesgo latente que implica la adopción de tecnologías, ante la pandemia COVID-19: “Los cibercriminales han estado entre los más expertos en explotar la pandemia de COVID-19 por las diversas estafas y ataques que llevan a cabo”.⁷ El aislamiento social pone a disposición a millones de víctimas en la red a expuestos a la ser víctimas de ciberdelincuentes listos para explotar vulnerabilidades.

⁶ IMSS, Calculadora de complicación de salud por COVID-19 <http://www.imss.gob.mx/COVID-19/calculadora-complicaciones>

⁷ *Catching The Virus Cybercrime, Disinformation And The COVID-19 Pandemic.*

V. Los dispositivos tecnológicos inteligentes o *Smartthings* y los riesgos a la protección de datos personales

La evolución de la tecnología ha llegado a un grado de adaptación en la vida de las personas que alcanza a auxiliar en tareas como organizar la agenda, optimizando tiempos, sincronizando recorridos y recordatorios diarios. Un ejemplo de ello es el dispositivo de voz “Echo” y “Alexa” de Amazon que ponen a disposición de casi cualquier persona un asistente personal a disposición las veinticuatro horas del día, que no se cansa, no descansa, no olvida nada y que tiene la inteligencia para gestionarse a través del uso de la voz.

El asistente digital activado por voz *Voice Command Device* (VCD)⁸ *Amazon Echo* cuenta con micrófonos omnidireccionales de 360 grados, diseñados para capturar tu voz desde cualquier sitio, incluso si estás escuchando música o viendo el televisor con una amplia gama de estilos a elegir y adaptarse a la decoración de cualquier espacio. El VCD de Amazon tienen integrada a la asistente digital “Alexa” tiene la capacidad de las tecnologías inteligentes para recopilar grandes cantidades de datos que son enviados a través del cómputo de la nube o *Cloud Computing*,⁹ es decir la información no se encuentra alojada en el dispositivo que adquieren las personas, los datos son enviados a almacenamientos remotos donde son concentrados y tratados por la empresa Amazon.

“Alexa” tiene la capacidad de solucionar y mejorar la vida, multiplicando tiempos y logrando una significativa organización del día a día, desde encender y apagar las luces, realizar compras y pagos, hasta leerle las noticias. Sin embargo como todo asistente personal, también requiere acceso a tus datos: cuentas bancarias, identidad, domicilio y hasta lo más íntimo; dependiendo de las tareas que le sean asignadas. ¿Qué tan discreto es este asistente digital activado por voz? ¿Están protegidos los datos de sus usuarios? ¿En dónde y quién garantiza la información que almacena este dispositivo?

⁸ Matthew B. Hoy and Ariel F. Pomputius. *Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants. Voice assistants are software agents that can interpret human speech and respond via synthesized voices.* <https://www.tandfonline.com/doi/abs/10.1080/02763869.2018.1404391>.

⁹ USA. Federal Cloud Computing Strategy. Vwek Kundra U.S. Chief Information Officer. February 8, 2011. Cloud Computing. Permite que los sistemas de TI sean escalables y elásticos. Los usuarios finales no necesitan determinar sus requisitos de recursos informáticos exactos por adelantado. En cambio, proporcionan recursos informáticos según sea necesario, bajo demanda.

Los datos personales son todos los signos e información que vuelven identificado o identificable a una persona. La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPO) menciona que es la: “información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información”. Por lo que toda la información contenida en las cuentas de usuarios de estos dispositivos se considera datos personales, e incluso existen datos personales sensibles que requieren una mayor protección.

Por cuanto a los datos personales sensibles los define la LGPDPPSO como: “Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual”, de lo anterior, podemos observar que también se encuentran registrados datos que pueden ser considerados sensibles, ya que para realizar la compra de un producto es necesario ingresar las cuentas bancarias, NIP de seguridad e incluso con la pandemia COVID-19 algunas aplicaciones solicitan datos personales sensibles como la temperatura del cuerpo.

Internet y los dispositivos digitales necesitan accesos a una gran cantidad de información de los usuarios, para que la tecnología de los “aparatos inteligentes” o *Smartthings* por su nombre en inglés, puedan adaptarse y funcionar adecuadamente a las necesidades de los usuarios, y para ello requieren la transferencia de datos entre dispositivos digitales y hacia el “cerebro” que se encuentra alojado en la nube.

La sinergia entre la conexión a Internet y tecnología informacional de los aparatos inteligentes o “Smartthings” representan un múltiple desafío a la protección de datos. Mike Kuniavsky menciona que: “El Internet de las cosas sugiere un mundo en el que los objetos físicos identificables digitalmente se relacionan entre sí de una manera análoga a cómo se organiza la información puramente digital en Internet (específicamente, la Web)”.¹⁰ Creando un nuevo paradigma para la seguridad de los datos personales en un entorno digital del cual pueden ser sustraídos sin dejar rastro.

El desarrollo tecnológico exponencial y la posibilidad de interconexión e intercambio de información entre dispositivos, nos hace reflexionar: ¿Estamos seguros y protegidos en un entorno digital? ¿Qué sucedería, si toda nuestra información personal contenida en un VCD se diera a conocer? La

¹⁰ Kuniavsky, Mike, *Smart Things, Ubiquitous Computing User Experience Design*, p. 5.

exposición de todo tipo de datos y archivos que revelan nuestra identidad, actividad, familia, ubicación, cuentas bancarias, etcétera es una posibilidad que debemos conocer prevenir y enfrentar.

La experiencia digital, el compartir una foto con un ser querido nos conecta en la distancia, lo que nos ayuda a cumplir con el distanciamiento social y así prevenir el COVID-19, mientras que la posible difusión pública una foto íntima nos confronta con la misma tecnología. Nos hace sentir la fragilidad e incertidumbre respecto a los datos que guardamos en los dispositivos y formularios que nos exigen para su uso y aprovechamiento de las tecnologías que empleamos día con día.

Al respecto Zygmunt Bauman nos dice que:¹¹

Cuando hablo de “inseguridad” pienso en un fenómeno más amplio, que queda mejor definido por el término alemán *Unsicherheit*.

Para traducir el significado de *Unsicherheit* en toda su plenitud son necesarios tres conceptos: incertidumbre, inseguridad y ausencia de protección por lo que considero que no es aceptable el renunciar a la seguridad de los datos, o a la conservación de la salud en cumplimiento al distanciamiento social para frenar el COVID-19.

El Internet de las cosas sugiere un mundo en el que los objetos físicos identificables digitalmente se relacionan entre sí de una manera análoga a la forma en que la información puramente digital se organiza en Internet (específicamente, la Web). De igual forma Zygmunt Bauman¹² afirma que: “La palabra “precariedad” también recoge y plasma la complejidad de nuestros miedos: la sensación de caminar sobre una superficie tambaleante, la fragilidad y la indefinible duración de nuestras condiciones, que se evidencian en casi todos los aspectos de nuestras vidas” y así el COVID-19 ha puesto de manifiesto la fragilidad global de una sola humanidad, que debe establecer en unidad las medidas sanitarias de protección para conservar la salud.

La certidumbre, seguridad y protección corresponden al Derecho, las nuevas tecnologías deben respetar, cumplir y hacer cumplir las medidas que para tal fin se establezcan. Diversas legislaciones en todo el mundo deben su creación a la protección de la privacidad, sin embargo el fenómeno tecnológico se encuentra en pleno desarrollo y no siempre es posible que la legislación se adapte al entorno digital y la intercomunicación de las *Smartthings*; que en segundos tienen la capacidad de coleccionar datos de forma masiva, transmitirlos, procesarlos y almacenarlos, sin que los usua-

¹¹ Bauman, Zygmunt, *Múltiples culturas, una sola humanidad*, p. 19.

¹² *Idem*.

rios se percaten de esta acción aún cuando los datos personales fueran vulnerados no tendrán conocimiento de ello hasta que los efectos nocivos les afecten directamente.

VI. Inteligencia artificial y la era del *Big data*. Análisis de casos “Alexa” y la vulneración a la privacidad y datos personales

Rajat Mehta dice que el: “Big Data ayuda a almacenar todo tipo de datos, ya sea estructurados o no. Por lo tanto, todos los archivos de registro, videos, etcétera pueden almacenarse en el almacenamiento de big data. Dado que casi todo se puede volcar en big data, ya sean archivos de registro o datos recopilados a través de sensores o teléfonos móviles, la cantidad de uso de datos ha explotado en los últimos años. Tres V definen big data y son volumen, variedad y velocidad”.¹³ La posibilidad de recolectar todo tipo de archivos de forma masiva y su posible transferencia e interoperabilidad entre diversas plataformas es un gran reto a enfrentar en la protección de los datos personales.

“Alexa” debe su éxito al desarrollo y popularidad de la computación afectiva —también conocida como inteligencia emocional artificial—. Esta área de estudio busca permitir el desarrollo de sistemas y dispositivos con la capacidad de comprender y replicar los afectos humanos. Y se enfrenta a la protección de los datos personales y el respeto de la vida privada, derechos fundamentales importantes, en razón a que necesita grandes cantidades de información para poder aprender y adaptar su comportamiento “humanizado”. El Parlamento Europeo ha insistido siempre en la necesidad de lograr un equilibrio entre el refuerzo de la seguridad y la tutela de los derechos humanos, incluida la protección de los datos y de la vida privada. Las nuevas normas Europeas en materia de protección de datos, que refuerzan los derechos de los ciudadanos y simplifican las normas para las empresas en la era digital.

La carrera está en desarrollar sistemas de computación inteligentes, que puedan imitar la interacción humana y también emular y convencer a los humanos de que también son humanos, creando un sentido de “confianza”. El caso del asistente personal inteligente, “Alexa” —uno de los disposi-

¹³ Mehta, Rajat, *Big Data Analytics with Java- massive, predictive, social and self-driving*, p. 1.

tivos inteligentes más populares y generalizados— necesita del “Big data” con las 3V *volume*, *variety* and *velocity*, es decir, conocer el desarrollo de todas las actividades de sus usuarios para poder aprender y mejorar su interacción en el menor tiempo posible. Y surge la incógnita “Alexa”: ¿cumple con la protección de los datos personales? ¿Existe un marco jurídico aplicable a sus políticas, incluidas la aplicación de la ley, y la prevención de su uso por la delincuencia?

Para resolver las preguntas planteadas y alcanzar un análisis sobre la inteligencia artificial tomaremos como ejemplo “Alexa” de Amazon y el manejo de funciones a través de la comunicación con el dispositivos en la proximidad del usuario un asistente de este tipo está alimentado por inteligencia artificial, el “cerebro” del asistente está en un lugar virtual, por ejemplo, una nube.

Estos dispositivos se comunican con el *Intelligent Virtual Assistant* (IVA), a veces de forma predeterminada, pero más a menudo sólo cuando están configurados para hacerlo y no tienen inteligencia integrada. Es necesario mencionar que “Alexa” no es el único VCD en el mercado, entre los más populares se encuentran:

Vendedor	IVA	IVA-enabled devices (Endpoints)
Amazon	Alexa	Echo, Dot, Tab, Fire Tablet
Apple	Siri	Phone, Pad, Mac
Google	Google Now & Google	Any phone with Android, Google Home
Microsoft	Assistant Cortana	Any PC with Windows

Los IVA contienen programas del proveedor Amazon Alexa Echo, Dot, Tab y Fire Tablet que los comercializa y que se ejecutan en los dispositivos llamados puntos finales, “Alexa” el IVA de Amazon, plantea una gran cantidad de consideraciones de privacidad estándar importantes. Los servicios e información entregados a través de “Amazon Eco” por “Alexa” están alojados en la nube, lo que significa que todos los datos se almacenan en el servidor de Amazon y luego se entregan a través de “Amazon Echo” cuando se solicitan. Es decir, ninguna información se almacena físicamente.

te en el dispositivo. “Eco” es simplemente un sistema de entrega, funciona conectándose a la red Wi-Fi, sin Wi-Fi no funcionará correctamente.

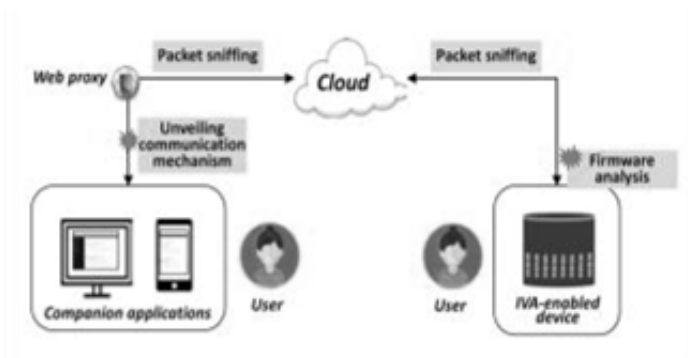
En Apple Siri iPhone, iPad, Mac como iPhone, iPad, Mac, tableta Fire, Echo, Google Home, etcétera la funcionalidad principal, el “cerebro” de un VCD, se aloja como un servicio en la nube que procesa datos de voz (conversión de voz a texto, análisis de contexto lingüístico y respuestas a preguntas) en este lugar es donde se aloja el IVA.

Almacenar datos de voz, hace posible que entidades no autorizadas utilicen los datos para identificar a las personas, obtener acceso de manera malintencionada a los sistemas que implementan el reconocimiento de voz, o simplemente procesar datos y construir artefactos de voz que podrían utilizarse para personificar a los individuos creando escenarios que resultan problemáticos.

Los VCD como toda tecnología tienen el riesgo de que su seguridad sea vulnerada, y como consecuencia la privacidad para los usuarios, ya que los *Intelligent Virtual Assistant* manejan los sonidos de voz reales de las personas, que son información de identificación personal y la privacidad del usuario. Al respecto se realizó un estudio para conocer los alcances e impacto de estos riesgos, titulado: *Alexa can I trust you?*¹⁴ En dicho estudio se identificaron los siguientes riesgos a la seguridad:

Uno de los problemas detectados fueron las escuchas telefónicas de internet. La comunicación de la red de un ecosistema de IVA. Consiste en dos partes: 1. Dispositivo a nube habilitado con IVA o Punto extremo a nube; y 2. aplicación complementaria a la nube o punto final 2 a la nube, como muestra la siguiente ilustración:

Caso 1

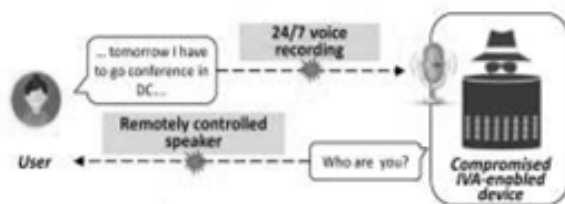


¹⁴ Hyunji Chung, Michaela IORGA, Jeffrey Voas, and Sangjin Lee, *Alexa Can I trust you?*

En el ejemplo, los servicios en la nube pueden usar conexiones cifradas para proteger los datos personales del cliente. Sin embargo, detectar el tráfico de red entre la aplicación complementaria del cliente y la nube puede exponer la seguridad y la privacidad del usuario. Esto se debe a que la identificación de las comunicaciones de red ayuda a los atacantes a comprender las operaciones generales de un ecosistema de IVA. A pesar de que el tráfico está cifrado, se pueden utilizar varios patrones, incluidos el tamaño de la carga útil y las tasas de datos, para identificar el comportamiento del usuario, como encender el dispositivo, el estado inactivo, hablar con el asistente, escuchar música, pedir productos o servicios, etcétera.

En el siguiente caso, es posible detectar la presencia de dispositivos IVA dentro de una red doméstica. Además, si los datos del *firmware*¹⁵ se transfieren a través de paquetes no cifrados, podría tener lugar un ataque de hombre en el medio. Incluso si la imagen no se altera, obtener la imagen del *firmware* es un problema de seguridad importante porque brinda la oportunidad de comprender las operaciones internas de un dispositivo habilitado para IVA. Además, un atacante malicioso puede distribuir imágenes de *firmware* modificadas.

Caso 2



La figura ilustra el escenario de vulnerabilidad de una grabación de voz 24/7. En general, los IVA no siempre están grabando, sino siempre escuchando. Si un dispositivo con IVA escucha la palabra de “activación”, la voz del usuario se graba y se transmite al IVA en la nube. Si el dispositivo habilitado para IVA está comprometido por un atacante malicioso, puede desempeñar el papel de un espía virtual. La grabación de voz “siempre activa” en la ubicación privada de un usuario puede permitir que todos los

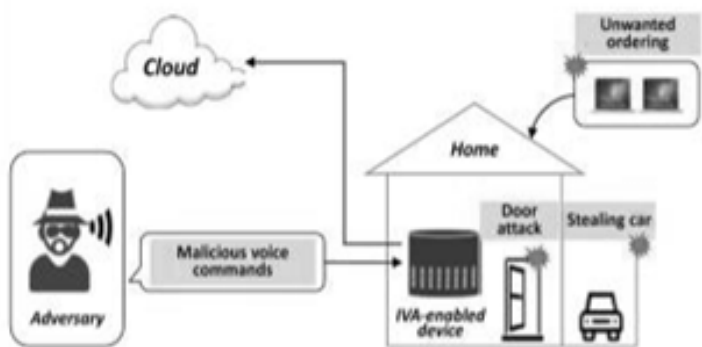
¹⁵ *Firmware* es un sistema que se desarrolla para establecer un “Firme” lazo entre el Hardware y el Software, de ahí proviene su denominación, la cual fue empleada por primera vez en los años 60 para señalar a un conjunto de normas insertando en una tarjeta electrónica para que un aparato más grande ejecutara una función automática.

sonidos o voces se graban y se envían a un atacante en tiempo real. Ésta es una preocupación de privacidad.

Incidentes en “similares, fueron documentados por Andrés Oppenheimer”.¹⁶ ¿Qué pasaría si los robots se vuelven locos? En el que narra que trabajando en su casa a solas escuchó una voz masculina en la sala de estar, sitio en el que se encontraba “Alexa”, que se había encendido sola y estaba transmitiendo la radio. Por lo que solicitó al departamento de atención a clientes de Amazon una explicación al respecto, respondieron que se debía a una “falla técnica”. Explicaron que el programa *National Public Radio* podría haber estado en modalidad de “pausa” y que Alexa podría haber “pensado” que escuchó la palabra reanudar ya sea por medio de la voz o la televisión.

Sin embargo, las explicaciones no le parecieron posibles ni lógicas, así que publicó su experiencia en *The Miami Herald*, obteniendo múltiples réplicas sobre incidentes similares, que no tenían explicaciones lógicas ni posibles. Haciendo una llamada a la necesidad de tomar acciones para proteger la privacidad y la intimidad de las personas frente a estos dispositivos.

Caso 3

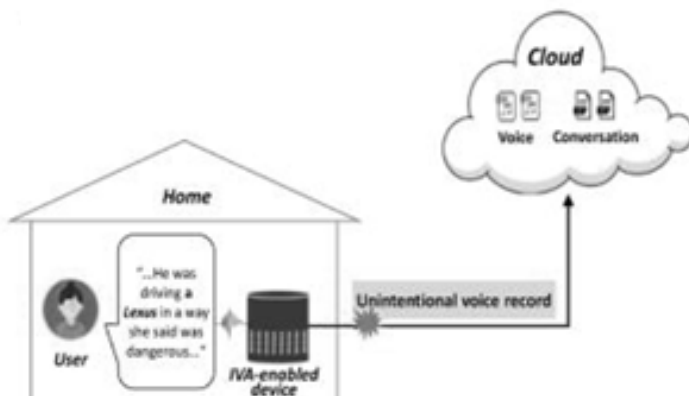


La tercera amenaza incluye comandos de voz maliciosos, en los servicios activados por voz, las voces de los usuarios pueden llevar a resultados peligrosos. Algunos IVA ofrecen una función de entrenamiento de voz, pero es difícil reconocer perfectamente la voz, los tonos y los acentos del usuario. Por lo tanto, un IVA podría procesar solicitudes y responder por otra persona o por una persona maliciosa. Si una persona maliciosa puede acercarse lo suficiente al dispositivo habilitado para IVA, puede ser capaz

¹⁶ Oppenheimer, Andres, *¡Sálvese quien pueda!* pp.68-70.

de engañar al sistema para que piense que el verdadero propietario es la persona que está hablando.

Caso 4



Un dispositivo habilitado para IVA es un altavoz con control remoto. Hubo un caso reciente en el que una familia que vive en Houston¹⁷ habló sobre los horrores que experimentaron al usar un monitor para bebés dentro de la habitación de su hija de 2 años. Los padres descubrieron que un extraño había pirateado el monitor de su bebé y podía espiar a su hija y, a veces, le decía mensajes perturbadores al dispositivo. De manera similar, los IVA pueden ser controlados por personas que pretenden estar cerca del dispositivo habilitado para IVA, mientras que, de hecho, acceden a un altavoz ubicado en la proximidad, en la casa.

Con los ejemplos referidos, queda demostrado que la vulneración en la privacidad y la seguridad de los datos personales y la vida privada de las personas por los IVA es real. Incluso, la información que recolecta Alexa ya ha sido prueba en juicio, el periódico *El País*¹⁸ documenta el caso en el que Amazon se rindió después de meses de litigio con las autoridades, y accedió a aportar los datos recolectados por Echo, su altavoz para el hogar, para dirimir si James Andrew Bates es o no culpable del asesinato de Víctor Collins. Por primera vez, una inteligencia artificial, Alexa, como

¹⁷ CNN en Español, "Un "hacker" agrade a una familia a través del monitor de bebés en EE.UU.

¹⁸ *El País*, "Amazon accede a aportar datos de su sistema de control de voz en un juicio en Arkansas".

se llama su asistente virtual, y sus archivos servirán como prueba en un juicio.

Otro caso documentado sobre el peligro que corren los datos personales y la privacidad de los usuarios de “Alexa”, fue publicado por *El Mundo*¹⁹ en el que un usuario del asistente de voz de Amazon, Alexa, consiguió acceso a más de mil grabaciones ajenas debido a un “error humano” de la compañía. El usuario solicitó poder escuchar grabaciones de sus propias actividades registradas por el asistente de voz pero, en su lugar, pudo acceder a 1,700 archivos de sonido de un desconocido cuando Amazon le envió un enlace de acceso, según ha informado la revista tecnológica alemana.

En las grabaciones registradas y enviadas por Amazon a la persona equivocada, un hombre y una mujer podían ser escuchados hablando, hasta el punto de que los responsables de la revista pudieron identificarlos y contactar con ellos gracias a toda la información registrada. Si bien, hablamos de un factor humano, encontramos que la cantidad que recolecta, almacena y trata Alexa es un gran riesgo para los usuarios y la gran capacidad de almacenamiento en la nube es un riesgo para los datos personales y la privacidad de los usuarios.

Este caso se toma como un ejemplo de la necesidad real que tienen los usuarios en todo el mundo y el riesgo al que se exponen por el aumento del uso de las tecnologías de la información como herramienta para desarrollar las actividades del día a día, en cumplimiento al distanciamiento social para evitar el contagio de la enfermedad COVID-19, por lo que la legislación internacional puede alcanzar la protección para la privacidad y los datos personales de forma global con la implementación y homologación de la protección respecto a ellos.

VII. Reflexiones finales

La enfermedad por coronavirus COVID-19 que inició en Wuhan, China el 31 de diciembre de 2019²⁰ y la declaratoria de pandemia de la OMS, así como la recomendación de medidas sanitarias y la colaboración de asistencia internacional,²¹ para la contención de la propagación de la en-

¹⁹ *El Mundo*, “Un fallo de Alexa permitió a un usuario ‘espiar’ en una casa ajena”.

²⁰ Organización Mundial de la Salud. *Nuevo coronavirus - China*.

²¹ Reglamento Sanitario Internacional. Artículo 43 Medidas sanitarias adicionales. Artículo 44 Colaboración y asistencia.

fermedad a través del aislamiento social, crearon la necesidad de que las personas realizaran sus actividades de forma remota.

La capacidad de las tecnologías inteligentes para recopilar grandes cantidades de datos que son enviados a través del cómputo de la nube o “*Cloud Computing*”²² por su nombre en inglés, en ocasiones sin el consentimiento de los participantes y que están relacionados con el estado emocional de un individuo y los aspectos más íntimos del desarrollo de su vida privada. Visibiliza la urgente y necesaria la aplicación global de legislación como el Convenio 108 del Parlamento Europeo, a los dispositivos IVA y la aplicación de sanciones en caso de vulneración de los datos personales y la privacidad de sus usuarios.

La nueva tecnología debe respetar y procurar un entorno para la protección de los datos y privacidad de los usuarios, el Convenio 108²³ —aprobado 18 de mayo de 2018 y abierto a la firma el 25 de junio en Estrasburgo—, obedece a la necesidad de responder mejor a los retos que como el COVID-19 tienen que ser enfrentados de forma global para asegurar las medidas de protección sanitaria.

Por lo cual, también es necesario generar los mecanismos internacionales que de forma global protejan el derecho fundamental del respeto a la vida privada, la privacidad y los datos personales, que derivado de la pandemia, ha incrementado el uso masivo las tecnologías de la información y comunicación, y de tratamiento de datos y el flujo transfronterizo de datos personales.

A medida que más “cosas” se conectan a Internet, existe una creciente necesidad de comprender mejor las amenazas de seguridad y privacidad de los datos personales y la privacidad. La inteligencia emocional artificial, es tecnología que apenas se está perfeccionando por lo cual es necesario que desde el origen sean regulados aspectos de protección y cumplimiento normativo.

La aplicación más allá de las fronteras en la era de la globalización y de la utilización de Internet, con instrumentos como el Convenio 108 tiene una ventaja esencial: su dimensión transfronteriza y su Protocolo Adicional contienen garantías para proteger el movimiento transfronterizo de datos

²² EUA Federal Cloud Computing Strategy. Cloud Computing. Enables IT systems to be scalable and elastic. End users do not need to determine their exact computing resource requirements upfront. Instead, they provision computing resources as required, on-demand.

²³ La aplicación más allá de las fronteras. En la era de la globalización y de la utilización de Internet, el Convenio 108 tiene una ventaja esencial: su dimensión transfronteriza. El Convenio 108 y su Protocolo Adicional contienen garantías para proteger el movimiento transfronterizo de datos hacia terceros países. En principio, debe asegurarse un nivel de protección adecuado. Al estar abierta la adhesión a los países no europeos, el alcance del Convenio tiene carácter universal.

hacia terceros países. En principio, debe asegurarse un nivel de protección adecuado, al estar abierta la adhesión a los países no europeos, el alcance del Convenio tiene carácter universal en la protección de los datos personales y el respeto a la privacidad que son derechos fundamentales.

El Parlamento Europeo²⁴ siempre ha insistido en la necesidad de lograr un equilibrio entre el fortalecimiento de la seguridad y la protección de los derechos humanos, incluida la protección de datos y la privacidad. Las nuevas reglas sobre protección de datos, que refuerzan los derechos de los ciudadanos y simplifican las reglas para las empresas en la era digital.

El reto consiste en desarrollar sistemas informáticos inteligentes que sean seguros, confiables y que respeten el derecho a los datos personales y datos personales sensibles a favor de la protección de los usuarios. El caso del asistente personal inteligente, “Alexa” plantea muchas consideraciones importantes de privacidad estándar, relacionadas con la capacidad de estos dispositivos para recopilar datos personales, personales sensibles e incluso relacionados con el estado emocional de una persona que pueden ser vulnerados sin que el titular de los mismos lo advierta de forma instantánea.

La computación de la nube o *Cloud Computing* y las implicaciones para la privacidad de la información personal, la confidencialidad de la información comercial y gubernamental. En su análisis y discusión de las leyes relevantes, los organismos gubernamentales y los litigantes privados pueden obtener información de un tercero más fácilmente que del creador de la información. Los términos de servicio, la política de privacidad y la ubicación de un proveedor en la nube pueden afectar significativamente la privacidad y los intereses de confidencialidad de un usuario.

Al respecto Julio Téllez y Ernesto Ibarra²⁵ mencionan la importancia de integrar grupos de trabajo con expertos internacionales —en mi opinión multidisciplinarios— que contribuyan a la elaboración de estudios técnicos y jurídicos para potenciar el *cloud computing*. A lo que agregaría la necesidad de aplicar lo dispuesto por la Ley 108, para su aplicación global en lo referente al cómputo de la nube.

La necesidad de dar continuidad a las actividades económicas, sociales y culturales de las personas en cumplimiento a las medidas sanitarias determinada por la OMS respecto al aislamiento social como método de prevención del contagio por COVID-19, pone de manifiesto que la solución tecnológica hace posible el cumplimiento de ambas a través del teletra-

²⁴ Parlamento Europeo, Personal data protection.

²⁵ Téllez Valdez, Julio e Ibarra, Ernesto, “*LEX Cloud Computing. Estudio Jurídico del Computo de la Nube*”, pp. 140-141.

bajo, la educación en línea, aplicaciones y plataformas de interacción, de forma segura acatando las medidas de seguridad sanitaria.

Sin embargo, también visibilizó la necesidad de desarrollar legislación internacional y homologar la legislación interna como la propuesta por el Convenio 108 de la Consejo de Europa, para que se regulen las protección de datos personales de forma global y se eviten vulneraciones y amenazas ante la falta de seguridad jurídica para la protección de los datos personales, ya que el aislamiento social mundial a causa de la enfermedad del COVID-19 ha detonado el aumento en el uso de estas formas de comunicación, que pone a disposición de la cibercriminalidad que está a la espera de la oportunidad de vulnerar los datos personales de los usuarios, que no en todos los países cuentan con métodos de protección adecuados.

VIII. Bibliografía

Libros

CASTELLS, Manuel, *La Sociedad Red*, Buenos Aires, Argentina, 6ª edición, Siglo Veintiuno Editores, 2005.

BAUMAN, Zygmunt, *Múltiples culturas, una sola humanidad*, Buenos Aires, Argentina, Katz Editores, 2008.

KUNIAVSKY, Mike, *Smart Things. Ubiquitous Computing User Experience Design*, Morgan Kaufman, Esisever, China, 2010.

MEHTA, Rajat, *Big Data Analytics with Java- massive, predictive, social and self-driving*, Birmingham, United Kingdom, Packt Publishing, 2017.

OPPENHEIMER, Andres, *¡Sálvese quien pueda!* México, Penguin Random House, 2018.

TÉLLEZ VALDEZ, Julio e IBARRA, Ernesto, *LEX Cloud Computing. Estudio Jurídico del Computo de la Nube*, Instituto de Investigaciones Jurídicas, México, 2013.

Web

CATCHING THE VIRUS CYBERCRIME, *Disinformation And The COVID-19 Pandemic*. <https://www.oas.org/ext/es/principal/COVID-19/Repositorio/PID/3472/mcat/3474/acad/1/TagID/1838/TagName/Cibercrimen>

CNN EN ESPAÑOL, "Un "hacker" agrede a una familia a través del monitor de bebés en EE.UU." <https://cnnespanol.cnn.com/2013/08/14/un-hacker-agrede-a-una-familia-a-traves-del-monitor-de-bebes-en-ee-uu/>.

EL MUNDO, *Un fallo de Alexa permitió a un usuario 'espiar' en una casa ajena*. <https://www.elmundo.es/tecnologia/2018/12/20/5c1ba926fdddf21998b4598.html>.

EL PAÍS. "Amazon accede a aportar datos de su sistema de control de voz en un juicio en Arkansas", Jiménez Cano, Rosa, San Francisco, https://elpais.com/internacional/2017/03/08/mundo_global/1488935824_982397.html.

HOY, Matthew y POMPUTIUS, Ariel F., *Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants*, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5714311/#R4>

HYUNJI, Chung, LORGA, Michaela, VOAS, Jeffrey y LEE, Sangjin, *Alexa Can I trust you?*. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5714311/#R4>

ORGANIZACIÓN MUNDIAL DE LA SALUD, *Nuevo coronavirus - China* <https://www.who.int/csr/don/12-january-2020-novel-coronavirus-china/es/>.

_____, *¿Cuál es la diferencia entre aislamiento, cuarentena y distanciamiento? Distanciamiento Social*, https://www.who.int/es/emergencias/diseases/novel-coronavirus-2019/advice-for-public/q-a-coronaviruses?gclid=CjwKCAjwte71BRBCEiwAU_V9hxdVID9vUvhVg0vSGCyhlx_Ph4Jhn5_TTnu--PTZUxHwbZbguzZVQxoC5RUQAvD_BwE.

_____, *¿Cómo se propaga la COVID-19?* https://www.who.int/es/emergencias/diseases/novel-coronavirus-2019/advice-for-public/q-a-coronaviruses?gclid=CjwKCAjwte71BRBCEiwAU_V9hxdVID9vUvhVg0vSGCyhlx_Ph4Jhn5_TTnu--PTZUxHwbZbguzZVQxoC5RUQAvD_BwE.

PARLAMENTO EUROPEO, *Personal data protection*, <http://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection>.

Legislación

Constitución Política de los Estados Unidos Mexicanos

Ley General de Protección de Derechos Personales en Posesión de Sujetos Obligados.

Convenio 108 y su Protocolo Adicional. Parlamento Europeo. Mayo 2018.

USA. Federal Cloud Computing Strategy. Vwek Kundra U.S. Chief Information Officer. February 8, 2011.

Reglamento Sanitario Internacional.

Artículo 43 Medidas sanitarias adicionales.

Artículo 44 Colaboración y asistencia