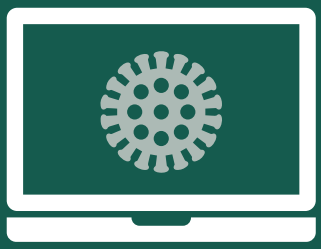

Multidimensionalidad de la pandemia digital

Rodolfo Guerrero Martínez
Vicepresidente de la Academia Mexicana de Derecho Informático, Capítulo Jalisco

Resumen

PALABRAS CLAVE:

Pandemia, TIC, Desconexión, Privacidad, Protección

Sin duda, los efectos ocasionados por el SARS-CoV-2 o la COVID-19, y consecutiva progresividad no solo impactaron la estructura tradicional de las naciones, es decir, todos aquellos entes de naturaleza privada o pública en su labor cotidiana (en un gran porcentaje rudimentaria), sino además, en el aceleramiento en materia de innovación tecnológica, la obligación de las organizaciones a implementar el uso de las tecnólogas de la información y comunicación para el trabajo a distancia, la generación de mejores políticas de salud, educativas y de desarrollo empresarial; así como los efectos negativos por el analfabetismo digital en vulneración de la privacidad a los datos personales, generando así una dependencia tecnológica entre otros fenómenos que crearon una pandemia digital.

I. Introducción

A partir de los efectos causados por la COVID-19, los países tuvieron como objetivo generar bases de datos con el fin de conocer el número de infectados y, de esa manera mejorar protocolos de acción para prevenir la propagación del virus. Precisamente la Organización Mundial de la Salud (OMS) a través de su herramienta *Go.Data* apoyó a los Estados Miembros para facilitar la investigación de los brotes.

En ese sentido, el programa informático contiene entre sus principales características ser de código abierto y libre; proporciona soporte multilingüe y permite agregar y administrar idiomas adicionales a través de la interfaz de usuario; genera una lista de seguimiento de los contactos, permite visualizar las cadenas de transmisión, tiene una aplicación móvil opcional (para Android y iOS) centrada en la recogida de datos de los casos y contactos y en el rastreo y seguimiento de los mismos.

Además de ello, encontramos otras variables en el tema de pandemia, como generar mayor efectividad en la recolección de datos de las estadísticas del trabajo para el proceso de entrevistas de futuros prospectos (OIT, 2020); por ejemplo usando un software experto como CSPro, donde las encuestas vía telefónica, y mensajes SMS, sean analizados por data science, ya que de esto distinguiremos entre sus respuestas, los mejores miembros del equipo, considerando experiencia previa, la tenencia de un teléfono, fluidez de un idioma local, entre otros.

Por lo anterior, queda claro que los datos representan el mayor activo de la pandemia digital que vivimos en cada rubro, ante lo cual el objetivo de este trabajo es generar diferentes reflexiones sobre los temas no resueltos en la pandemia actual, particularmente sobre el ámbito digital en ópticas multidimensionales como: la protección de datos personales, la desconexión digital, la privacidad y la necesaria transversalidad tecnológica.

II. Datos personales y su obligatoria protección

Precisar los principios de protección de datos personales como el de licitud, proporcionalidad y finalidad descritos en el artículo sexto de la Ley Federal de Protección de Datos Personales, resulta un marco preliminar fundamental para apreciar como las bases jurídicas del tratamiento de los datos, durante el marco de la pandemia.

Ahora bien, parte de esa base fundamental se expresa en las recomendaciones (RIPD, 2017) estándares de protección de datos personales para los Estados Iberoamericanos:

- Deberá tener especial cuidado en los datos que han pasado por un tratamiento de seudonimización, debido a que el procedimiento permite identificar a una persona mediante la suma de nuevos datos de forma razonable, por lo cual debe vincularse con las diversas normativas regionales (Numeral 5)

- En caso de que un grupo empresarial realice el tratamiento de datos personales, el establecimiento principal de la empresa que ejerce el control deberá considerarse el principal del grupo empresarial, excepto cuando los fines y medios del tratamiento los determine efectivamente otra de las empresas del grupo (Numeral 5.4)

Lo anterior establece que la irrupción del COVID-19 ha acelerado como nunca la maquinaria de los datos, por ese motivo la Organización Mundial de Salud brindó herramientas digitales y sus usos para el rastreo de contactos COVID-19, motivo por el que expreso en la siguiente tabla algunos aspectos:

Categoría de herramienta	Características y usos	Consideraciones para la implementación, oportunidades y desafíos
Herramientas de respuesta a brotes	• Las herramientas de respuesta a brotes están diseñadas para personal de respuesta de salud pública involucrado en actividades de rastreo de contactos y brote de investigaciones • Optimizar el flujo de datos y los datos proceso de gestión, evitando errores de entrada de datos, empujando la información automáticamente a través del sistema, reduciendo el procesamiento tiempo y mejora de la puntualidad del análisis y monitoreando	• El acceso abierto y el software de código abierto permiten aumentar transparencia y mejora continua de herramientas • Deben incorporarse diferentes roles y responsabilidades en herramientas de respuesta a brotes para reflejar la recopilación de datos y los datos proceso de verificación (como recolectores de datos de campo, líder de equipo para recopiladores de datos y funciones de epi lead que se ocupan de los datos calidad, reduciendo errores de entrada de datos, eliminación de duplicados y aprobación de datos)
Rastreo de proximidad / herramientas de seguimiento	• Usando ubicación GPS o Bluetooth señales, las herramientas de rastreo de proximidad pueden ayudar identificar contactos identificando cuando individuos han estado en estrecho contacto físico proximidad y han tenido contacto prolongado con un estuche.	• Los dispositivos portátiles con GPS o Bluetooth podrían ser desarrollados para personas sin teléfonos inteligentes o para aumentar uso constante

Tabla 1. Herramientas digitales y sus usos para el rastreo de contactos COVID-19. Elaboración y traducción propia a partir de las directrices de la OMS [1]

Cabe resaltar que ante la mal denominada “nueva normalidad”, se pueden establecer cuatro pilares fundamentales, previendo las excepciones para el uso de datos en periodos de emergencia, forjando que el diseño de cualquier intervención debe incluir mecanismos que garanticen su uso de manera segura

1. Generación de datos de calidad por medio de la colaboración.
2. Preservación de Derechos fundamentales a través de la confianza y coordinación.
3. Cierre de brechas implementando la equidad.
4. Agenda de datos sostenible: resiliencia.

[1] Digital tools for COVID-19 contact tracing, World Health Organization. Véase en: https://www.who.int/publications-detail-redirect/WHO-2019-nCoV-Contact_Tracing-Tools_Annex-2020.1

III. Dependencia y desconexión digital

Sufrimos de una gran tecnoadicción, prueba de ello es la duración de una persona en el uso de aplicaciones donde envía mensajes, comparte videos, imágenes e incluso intercambia documentos académicos. En ese sentido, el Digital Report 2021[2] da a conocer que en México existe un aproximado del 71% de usuarios en la Word Wide Web y generando a su vez los siguientes datos:

- 77.2% de la población nacional accede a las redes sociales, lo que representa a 100 millones de personas en México que hace uso de las diversas plataformas de social media.
- Redes Sociales Digitales. Dentro de los lugares de preferencia tenemos:
    1. Youtube con 96.3% de personas que navegaron en la red de videos de Google;
    2. Facebook con el 95.3% de las visitas;
    3. Whatsapp con el 91.3%;
    4. Messenger de Facebook fue usado por 79.4% de los mexicanos en diciembre y;
    5. Instagram con el 76.9% de las personas.

Consecuencia de lo anterior no necesariamente es benéfico, debido a la falta de educación digital en la población, lo que nos obliga el tratar los riegos cibernéticos a partir de una estrategia en ciberseguridad, poniendo como elementos principales a las personas que integran el gobierno, las empresas y la ciudadanía.

Desde la óptica de la CISO[3], en materia de ciberseguridad refiere entre las principales necesidades, el contar con una buena gestión de terceros de la cadena de suministros, la resiliencia y la gestión de la respuesta ante incidentes, muy relacionado con los recursos que tiene el equipo, la orquestación de infraestructuras (donde se prevé la automatización de muchos niveles), la concienciación a todos los grados, incluso en los terceros y desarrollar una cultura de ciberseguridad y riesgos.

Con respecto a la desconexión digital, parte de la base fundamental de un derecho laboral 4.0 al descanso, teniendo como antecedente El *Khomri*, año 2017 en Francia, a su vez España en diciembre de 2018 con la Ley de Protección de Datos Personales y Garantía de los Derechos Digitales, que se reforzó en septiembre de 2020, particularmente en el marco de la pandemia, con un nuevo decreto sobre el trabajo a distancia.

En México se realizaron importantes reformas en el transcurso del 2021 como la hecha en la Ley Federal del Trabajo, donde prevé la relación entre el teletrabajo y el compliance donde el patrón deberá entregar herramientas tecnológicas a sus empleados que trabajen en sus hogares, así como el pago proporcional y total de luz e internet; además establece la integridad como un reto en el trabajo a distancia.

Dicho paquete legislativo entró en vigencia el pasado 11 de enero donde se le adicionó al capítulo 12 bis, 11 artículos que establecen todo lo anterior, no obstante a mi parecer existen puntos imprecisos como el derecho a la desconexión digital.

III. El virus de la privacidad

La privacidad reconocida a mi óptica como fenómeno multidimensional en los ejes: político, social, informático y jurídico, esto explicado a través del estado o condición de toda persona –relacionado con los artículos primero y sexto constitucional-, le permite establecer un contacto especifico, además de dar oportunidad de concentrarse, aislarse, reflexionar y contemplarse en su entorno.

---

[2] El Digital Report 2021 de We Are Social, la agencia creativa especializada en Social Hootsuite. Véase en: https://www.slideshare.net/DataReportal/digital-2021-mexico-january-2021-v01

[3] CISO (Chief Information Security Officer) es el director de seguridad de la información.

Véase en: https://www2.deloitte.com/content/dam/Deloitte/es/Documents/riesgos/Deloitte-ES-informe%20CISOS-ciberseguridad.pdf

Pese a ello, la pandemia aceleró la evolución tecnológica, y la conciencia colectiva, por su parte no tuvo la misma suerte para comprender y anticipar las vulneraciones que podrían darse ante las redes sociales digitales, por ejemplo. De ahí que resulta valioso recordar la pregunta, *¿es la privacidad de los datos el precio que debemos pagar para sobrevivir a una pandemia?* (BID, 2020)

En base a lo anterior, realizar una línea de antecedentes ante los sistemas de rastreo de personas y sus contactos físicos es importante, debido a que uno de los principales desafíos en el despliegue de estas aplicaciones son los límites de privacidad y la gestión del consentimiento informado.

1. Identifica aquellos con los que el paciente infectado tuvo contacto ante los casos confirmados
2. Registra los posibles contactos físicos de los pacientes infectados y los contacta, y
3. Hace seguimiento con el listado de contactos ya sea para hacerles una prueba o para advertirles que estuvieron en contacto con alguien infectado (OMS).

En el caso particular de algunas naciones, apreciamos la aplicación de los sistemas de rastreo

- En Corea del Sur se han utilizado diferentes tecnologías para prevenir y controlar el contagio por medio del rastreo vía GPS de los infectados y en cuarentena para identificar cualquier persona con la que los portadores del virus hayan estado en contacto.
- Singapur lanzó *TraceTogether* el 20 de marzo de 2020, 5 días después había sido descargado por 735.000 personas, aproximadamente el 13% de la población.
- Taiwán hizo un rastreo de los teléfonos de las personas en cuarentena utilizando datos de antenas de teléfonos celulares.

Posterior a las estrategias antes dichas, también debe verse el riesgo de los usuarios en las aplicaciones, ya que ellas son utilizadas para establecer si se han cruzado con un paciente diagnosticado. Dejando claro que el problema es un tercero, como el gobierno al acceder a los datos de ubicación; *Alipay App*, por ejemplo, la cual es una aplicación china usada en más de 200 ciudades para ayudar a los ciudadanos a identificar los síntomas y su riesgo de contagio que se basa en un código QR, donde cada usuario recibe uno de los tres colores: verde, amarillo o rojo, según su ubicación, información básica de salud e historial de viajes.

IV. Transversalidad tecnologica

En la nueva realidad donde la tecnología ya no es un simple utensilio y/o adorno decorativo sino una herramienta de uso obligado para desarrollar el trabajo cotidiano, apela al deber de las personas bajo la filosofía de *"aprender a desaprender"*, particularmente adquiriendo competencias digitales, esto era vislumbrado por (Castells, 1999, pág. 32)

> *"la revolución de la tecnología de la información, de forma medio consciente, difundió en la cultura material de nuestras sociedades el espíritu libertario que floreció en los movimientos de la década de los sesenta. No obstante, tan pronto como se difundieron las nuevas tecnologías de la información y se las apropiaron diferentes países, diferentes culturas, diversas organizaciones y metas heterogéneas, explotaron en toda clase de aplicaciones y usos, que retroalimentaron la innovación tecnológica, acelerando la velocidad y ampliando el alcance del cambio tecnológico, y diversificando sus fuentes".*

Ese proceso de actualización se expresa en el uso seguro de dispositivos inteligentes (IoT), generación de modelos de trabajo colectivo y portátil, y seguridad del teléfono inteligente personal para uso profesional.

En el primer caso, enunciamos que entre las recomendaciones recientemente publicadas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), sobre los riesgos de dispositivos inteligentes, se lean las condiciones de uso y almacenamiento de la información considerando que pueden recoger datos, procesarlos y compartirlos; cambiar contraseñas de fábrica y establecer unas seguras, que contengan más de 8 caracteres en letras minúsculas y mayúsculas, dígitos y caracteres especiales; y evitar vincular el dispositivo inteligente a otros aparatos de los que se desconoce su nivel de seguridad[4].

Lo segundo reflejado en casos de innovación disruptiva en el trabajo como el coworking, donde se facilita el desarrollo de espacios más sostenibles económicamente, pero también incentiva el trabajo colaborativo, en comunidad, generando nuevos modelos relacionales, y virtual offices como ejemplo Microsoft Teams, que cuenta con aproximadamente 115 millones de usuarios activos en todo el mundo. En el año 2020 se consolidó como la oficina virtual para que equipos de trabajo siguieran sus proyectos y tareas desde cualquier lugar.

En tercer lugar, las políticas en materia de protección de datos y seguridad de la información, adecuando correctamente el bring your own device (BYOD), teniendo entre los beneficios, el limitar el uso de aplicaciones y generar perfiles de acceso con restricción de permisos, para evitar la instalación de archivos de origen desconocido, establecer un proceso de destrucción o borrado de información de estos dispositivos cuando el trabajador cesa la relación laboral, actualizar parches de seguridad y del sistema operativo continúo con antivirus y la conexión VPN con firewall que permita activar el sistema de intrusión de amenazas.

V. CONCLUSIÓN

En el mundo las estrategias, protocolos y concepciones se transformaron debido a la pandemia digital, dejando al descubierto el valor de los datos como el petróleo del siglo XXI, a su vez su aprovechamiento se hizo de manera agresiva, en varios casos con una tentadora, pero espeluznante compresión de su uso, con la justificación de disminuir brotes del SARS-CoV-2, olvidando los límites del uso de la geolocalización, el internet de las cosas, entre otros tópicos del bloque exponencial de las TIC, para prevalecer la protección de la privacidad y el debido tratamiento de datos personales.

Adicionalmente en el presente artículo queda clara la necesidad de continuar generando modelos oportunos, para la capacitación de la ciudadanía a través de protocolos, estrategias, e incluso leyes especiales (o reforma) para la tutela de derechos fundamentales de última generación.

[4] INAI, 2021. Recomendaciones sobre privacidad por conexión de aparatos domésticos al internet.

Véase en: https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-261-21.pdf

Rodolfo
Guerrero Martínez

Vicepresidente de la Academia Mexicana de Derecho Informático, Capítulo Jalisco

Abogado por la Benemérita Universidad de Guadalajara, actualmente es estudiante del posgrado en derecho con orientación en materia Constitucional y administrativo por la misma casa de estudios. Es Socio Fundador y Representante Legal de la Sociedad Civil Coffee Law “Dr. Jorge Fernández Ruiz”. Socio fundador de la Academia Mexicana de Derecho “Juan Velásquez” A.C. Miembro de la Junta Menor y encargado de la Comisión de Legaltech del Ilustre y Nacional Colegio de Abogados de México A.C. Capítulo Occidente. Vicepresidente de la Academia Mexicana de Derecho Informático, Capítulo Jalisco. Publicaciones: Derechos humanos de cuarta generación y las tecnologías de la información y la comunicación (Derechos Fundamentales a Debate, CEDHJ 2020), Industria 4.0 Los Derechos de libertad y Consentimiento (INNOVAITESCYT LOS CABOS Publicación N° 7, 2020).

VI. Bibliografía general

CASTELLS, M. (1999). La Era de la Información, Economía Sociedad y Cultura (Vol. Vol 1 La Sociedad Red). México: Siglo XXI, Editores s.a. de c.v.

ESTÁNDARES DE PROTECCIÓN DE DATOS PERSONALES PARA LOS ESTADOS IBEROAMERICANOS. Red Iberoamericana de Protección de Datos Personales, 2017. Véase en: https://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf

DIGITAL TOOLS FOR COVID-19 CONTACT TRACING, World Health Organization. Véase en: https://www.who.int/publications-detail-redirect/WHO-2019-nCoV-Contact_Tracing-Tools_Annex-2020.1

CABROL, MARCEL, atl. ¿Es la privacidad de los datos el precio que debemos pagar para sobrevivir a una pandemia? Banco Interamericano de Desarrollo. (BID). Véase en: https://bit.ly/3pVIK3U

La OMS tiene su propio app, Go.Data (sin IA) para hacer esto – http://socialdigital.iadb.org/en/solutions/go-data-covid-19

El Digital Report 2021 de We Are Social, la agencia creativa especializada en Social Hootsuite. Véase en: https://www.slideshare.net/DataReportal/digital-2021-mexico-january-2021-v01

INAI, 2021. Recomendaciones sobre privacidad por conexión de aparatos domésticos al internet. Véase en: https://bit.ly/3Czt5ti