IMPLICACIONES ÉTICAS DEL INTERNET DE LAS COSAS María Guadalupe García Martínez 2020

Universidad Autónoma de Querétaro

Facultad de Derecho

IMPLICACIONES ÉTICAS DEL INTERNET DE LAS COSAS

Tesis

Que como parte de los requisitos para obtener el grado de

Maestría en Ética aplicada y Bioética

Presenta

María Guadalupe García Martínez

Centro Universitario, Junio 2020

Universidad Autónoma de Querétaro
Facultad de Derecho
Maestría en Ética aplicada y Bioética

IMPLICACIONES ÉTICAS DEL INTERNET DE LAS COSAS
TESIS

Que como parte de los requisitos para obtener el grado de

Maestría en Ética aplicada y Bioética

Presenta:
María Guadalupe García Martínez

Dirigido por:
Dr. Lutz Alexander Keferstein Caballero

SINODALES

Dr. Lutz Alexander Keferstein Caballero Presidente	_____ Firma
Dra. Hilda Romero Zepeda Secretario	_____ Firma
Dra. Juana Patricia Pérez Munguía Vocal	_____ Firma
Dr. Bernardo García Camino Suplente	_____ Firma
Dr. Víctor Manuel Castaño Meneses Suplente	_____ Firma

_____	_____
M. en A.P. Ricardo Ugalde Ramírez Director de la Facultad	Dra. Ma. Guadalupe Flavia Loarca Piña Director de Investigación y Posgrado

Centro Universitario
Querétaro, Qro.
Junio 2020
México

A mi familia y amigos,

que han caminado este sendero conmigo.

AGRADECIMIENTOS

En primer lugar, me gustaría agradecer a la Universidad Autónoma de Querétaro, que me ha dado cobijo intelectual durante los dos años que dediqué al programa de la Maestría en Ética Aplicada y Bioética. En segundo lugar al Consejo Nacional de Ciencia y Tecnología (CONACYT) de cuyo Programa Nacional de Posgrados de Calidad (PNPC) fui becaria con folio 894851.

Un agradecimiento especial al Dr. Lutz Alexander Keferstein Caballero, que confió en mi tema de investigación y en mis capacidades desde que le solicité fungir como mi director de tesis. A la Dra. Hilda Romero Zepeda, quien fue un apoyo enorme durante la investigación y me animó siempre a seguir adelante, ofreciendome tiempo, conocimiento y apoyo.

Al Dr. Bernardo García Camino, que con sus charlas fomentó siempre mi curiosidad por conocer nuevas cosas. Por último, infinitas gracias a la Dra. Juana Patricia Pérez Munguia quien se convirtió en un modelo docente e intelectual a seguir.

CONTENIDO

RESUMEN

El mundo se encuentra en el apogeo de la cuarta revolución industrial y en la asimilación del mundo físico a la red. Uno de los grandes pilares que sostiene este cambio de paradigma es el internet de las cosas, cuyos dispositivos se han convertido en máquinas activas; por su capacidad de relacionarse con las personas y con otros dispositivos en una continua dinámica de recolección de datos. Esta realidad hace evidente la necesidad del razonamiento ético como elemento primordial para anticipar y/o visibilizar las implicaciones que estos dispositivos tendrán en nuestras vidas. Con una muestra de 94 dispositivos y herramientas de etnografía digital, la presente investigación indaga sobre las implicaciones éticas de esta tecnología disruptiva: privacidad y protección de datos personales; generación de perfiles y manipulación colectiva; algoritmos discriminatorios e e-waste. Finalmente, y como producto de los resultados obtenidos del análisis de los tópicos anteriores, se concluye con una serie de pautas, desde la perspectiva ética, para el diseño de política pública en materia de protección de datos e internet de las cosas.

Palabras Clave: IoT, Bio/Ética, Internet de las Cosas, Política Pública, Protección de Datos

ABSTRACT

El mundo se encuentra en el apogeo de la cuarta revolución industrial y en la asimilación del mundo físico a la red. Uno de los grandes pilares que sostiene este cambio de paradigma es el internet de las cosas, cuyos dispositivos se han convertido en máquinas activas; por su capacidad de relacionarse con las personas y con otros dispositivos en una continua dinámica de recolección de datos. Esta realidad hace evidente la necesidad del razonamiento ético como elemento primordial para anticipar y/o visibilizar las implicaciones que estos dispositivos tendrán en nuestras vidas. Con una muestra de 94 dispositivos y herramientas de etnografía digital, la presente investigación indaga sobre las implicaciones éticas de esta tecnología disruptiva: privacidad y protección de datos personales; generación de perfiles y manipulación colectiva; algoritmos discriminatorios e e-waste. Finalmente, y como producto de los resultados obtenidos del análisis de los tópicos anteriores, se concluye con una serie de pautas, desde la perspectiva ética, para el diseño de política pública en materia de protección de datos e internet de las cosas.

Key words: IoT, Bio/Ethics, Internet of things, Public Policies, Data Protection

I. INTRODUCCIÓN

Hoy, muchas de las narrativas plasmadas por las plumas de Isaac Asimov y Sir Arthur Clarke han sido rebasadas. Asistimos a la cuarta revolución industrial caracterizada por un avance tecnológico que crece a velocidades vertiginosas e innova sistemas enteros, planteando cambios radicales en las formas de ser y estar de la humanidad.

Esta cuarta revolución industrial se cimenta en tres grandes pilares: 1) digital (internet de las cosas, cloud computing, big data, inteligencia artificial y blockchain), 2) físico (nuevos materiales y nuevos dispositivos), y 3) biológico (los cuerpos animales, incluyendo los humanos y la bioingeniería), mismos que encuentran un campo fértil de interconexión y producción de realidad en la sociedad del conocimiento en la que habitamos.

Cuando en 1969 la Advanced Research Projets Agency Network, generó a través del Departamento de Defensa una red que conectaba cuatro computadoras militares y científicas a lo largo del territorio estadounidense[1], la sociedad no alcanzó a dimensionar el alcance operativo de esta red, que hoy supera los cuatro billones de usuarios[2].

En pocas décadas, internet se convirtió en la infraestructura de información por excelencia. La conectividad se ha extendido desde las computadoras, que originalmente eran los enlaces directos del usuario con la red, hasta escenarios y dispositivos más cercanos; electrodomésticos, instrumentos para monitorear y gestionar la salud, sistemas de control de tráfico, y muchos más artículos que adquirieron el calificativo de “smart” y con ello la posibilidad de *“generar,*

[1] Internet Society, *Orígenes de internet*, Suiza, Internet Society, 2017, https://www.internetsociety.org/internet/history-internet/brief-history-internet/ 9 de febrero de 2018.
[2] Internet World Stats. Internet users distribution in the world. Disponible en: https://www.internetworldstats.com/stats.htm 29 de marzo de 2019.

intercambiar y consumir datos con una mínima intervención humana"[3]. A esta interconexión digital, de objetos cotidianos con internet, se le denominó Internet de las cosas (IoT por sus siglas en inglés, Internet of Things), conocido generalmente por su abreviación.

Particularmente, el internet de las cosas (IoT) representa el próximo paso hacia la digitalización de nuestra sociedad; simboliza el puente entre el mundo digital y el físico; unión sólo plasmada, hasta entonces, por la pluma de autores de ciencia ficción o en el plató del séptimo arte.

El IoT se extenderá a casi todos los planos de nuestras vidas. Debido a ello, se ven y verán modificadas las formas en las que nos relacionamos con otros individuos y con las instituciones. La misma dinámica de comunicación con la red cambiará. Actualmente los usuarios son los encargados de generar y descargar contenido a sus dispositivos por lo que ejercen un papel activo en la gestión de la información; con la asimilación del IoT en la vida cotidiana esta interacción será más pasiva. El intercambio de información requerirá muy poca intervención de los usuarios e incluso podrá ejecutarse *"sin que nadie tenga conciencia de lo que está ocurriendo"*[4].

El funcionamiento interno y los flujos de datos del "internet de las cosas" (IoT) son escasamente visibles para las personas por lo que *"un usuario puede creer que un dispositivo está ejecutando ciertas funciones, pero en realidad está realizando funciones no deseadas o recogiendo más información que lo que el usuario desea"*[5]. Es decir, a la información dada por el usuario de manera consciente debe sumársele la información recolectada sin que tenga conocimiento de ello.

[3] ELDRIDGE Scott, Karen Rose y Lyman Chapin. *La internet de las cosas – Una breve reseña*, Internet Society, 2015, p. 5.
[4] Íbid, p.5.
[5] McKinseyCompany. *The internet of things: mapping the value beyond the hype*, 2015, p 2.

Se proyecta que para 2025 habrá 100 mil millones de conexiones al IoT[6] y que el impacto financiero sobre la economía global será aproximadamente de 11.1 mil millones de dólares[7]. La implementación a gran escala de este tipo de dispositivos ofrece la posibilidad de eficientar procesos y maximizar comodidades, en sincronía con el concepto de "ciudades inteligentes".

Una vez que el IoT alcance su apogeo, éste se extenderá a casi todos los planos de nuestras vidas, se verán modificadas las formas en que nos relacionamos con otros individuos y con las instituciones, *"será pues en gran medida en la Red, y a causa de la Red, donde se decidirá el destino de lo que en años venideros deba y pueda entenderse por libertad, por democracia o por igualdad"*[8].

Pista de ello es que comienzan a digitalizarse los servicios públicos. Por ejemplo, la atención en materia de salud se encuentra experimentando con consultas remotas, registros médicos electrónicos, robots quirúrgicos y dispositivos conectados a la red que permiten al médico monitorear y gestionar la salud a distancia. Además, la educación actual está mediada por la tecnología y se ha ido orientando hacia el desarrollo de habilidades para el futuro que nos permitan sumarnos a un mercado laboral compuesto de empleos que aún no existen.

De estos servicios públicos se generan cambios mucho más profundos en las estructuras de gobernabilidad, por lo que nos convertimos en ciudadanos digitales que ejercemos nuestros derechos, participamos y nos desenvolvemos en un entorno preponderantemente digital. Este ecosistema está dejando de ser un pequeño escenario de incursión e innovación para convertirse paulatinamente en

[6]Huawei Technologies Co.,Ltd., *Tendencias y desafíos de la industria*, 2017, http://developer.huawei.com/ict/en/site-iot/article/iot-industry
[7] McKinseyCompany. *The internet of things: mapping the value beyond the hype*, 2015, p 2.
[8] GARCÍA Mexía, Pablo. *Derechos y libertades, internet y Tics*. España, Ed. Tirant lo Blanch, 2014, p.13).

el marco total. Al mismo tiempo, es la única vía a través de la cual se accede a este plano. En este sentido, vía y meta son uno mismo.

Los objetos del IoT, físicos y virtuales al mismo tiempo, por su capacidad de recolección remota, análisis y gestión de datos se perfilan como catalizadores de innovación pero también plantean dilemas y retos para la ética actual, sobre todo en cuanto a privacidad y seguridad se refiere.

II. ANTECEDENTES

El campo del IoT ha despertado gran interés en distintas áreas de conocimiento. Algunas investigaciones están centradas en la arquitectura de la red, marcos de interoperabilidad, diseño y automatización de nuevos dispositivos y servicios. Otras dirigen sus esfuerzos a la exploración de problemas y desafíos que supone la relación de personas con los dispositivos del IoT.

CISRO (por sus siglas de Australia Commonnwealth Scientific and Industrial Research Organisation), ejecuta un programa de investigación en materia de seguridad del IoT. Su premisa principal vincula directamente la seguridad de los dispositivos con diseños de plataformas centrales y la capacitación de usuarios para administrar los múltiples dispositivos que utiliza. A propósito de una aplicación desarrollada para gestionar en cierta medida la seguridad de los dispositivos personales la organización afirma…

> *"está disponible como una aplicación de teléfono inteligente, la plataforma ofrece a los usuarios un centro de comando central desde el cual registrar y autenticar dispositivos para comunicarse entre ellos. Una vez registrado en la plataforma, se monitorea el estado de cada dispositivo para garantizar que su seguridad no se vea comprometida".*[9]

Por otra parte, el Gobierno de la República Popular China ha generado una serie de "Directrices para promover el desarrollo ordenado y saludable de la IoT"[10] que marca como punto prioritario el diseño de mecanismos que brinden seguridad y privacidad a los usuarios y al mismo tiempo permita a los fabricantes continuar la innovación tecnológica.

[9] Australia Commonnwealth Scientific and Industrial Research Organisation, *Una plataforma segura que conecta dispositivos de la IoT*, Data61, 2017, Australia, http://data61.csiro.au/en/Our-Work/Safety-and-Security/Secure-Systems-and-Platforms/Secure-IoT-platform

[10] ELDRIDGE Scott, Karen Rose y Lyman Chapin. *La internet de las cosas – Una breve reseña*, Internet Society, 2015, p. 5., p. 80.

La Unión Europea, que ha mantenido un ritmo positivo en la preparación para la era del IoT, redactó en 2005 el plan llamado *i2010: Una sociedad de la información europea para el crecimiento y el empleo* que establece políticas para el desarrollo del Espacio Único Europeo de Información. Entre sus lineamientos se encuentran los siguientes:

- Hacer que internet sea más seguro frente al fraude, contenidos nocivos y fallos tecnológicos.
- Establecer una estrategia en favor de una sociedad de la información segura, que incluirá la sensibilización sobre la necesidad de autoprotección, la vigilancia y el seguimiento de las amenazas y la respuesta rápida y eficaz a los ataques y a los fallos del sistema.
- Definir y promover acciones centradas en la cuestión de la interoperabilidad, en particular la gestión de derechos digitales.[11]

En 2018, entró en vigor, en la Unión Europea, el Reglamento General de Datos que deroga la Directiva sobre Protección de Datos de 1995. Este nuevo documento permite incorporar pautas para la privacidad, protección y propiedad de datos personales relacionados con dispositivos del IoT; además, incorpora la posibilidad de que existan decisiones automatizadas y sus consecuencias.

En los casos anteriores se muestra ya un interés por la participación activa de los usuarios en la gestión de la información; sin embargo, no hay a nivel nacional investigaciones o publicaciones que den cuenta de las implicaciones de seguridad y privacidad desde la visión de la Ética.

En cuanto a la producción de tesis, se retoman dos por contar con características cercanas a los objetivos de la presente investigación. En primer lugar, se encuentra el trabajo de Miguel Castro Sola, titulado *Internet de las*

[11] Comisión de las Comunidades Europeas, *"i2010 – Una sociedad de la información europea para el crecimiento y el empleo"*, 2005, Bruselas, http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52005DC0229&from=ES.

Cosas. Privacidad y seguridad presentado en el Departamento de Informática de la Escuela Politécnica Superior de Jaén para la obtención de grado en Ingeniería Informática en 2016. El objetivo de dicho trabajo es *"analizar en profundidad todos los cambios que va a suponer la implantación de esta nueva tecnología (IoT) en general, y con ella la sociedad y la manera de hacer las cosas tanto cotidianas como laborales"*.[12]

Como resultado, Castro logró identificar distintas amenazas en materia de seguridad, entre las que figuran: puntos de quiebre o fuga en la transmisión de datos, debilidades en el software de los dispositivos IoT, pautas de seguridad en la configuración por defecto o programable de los aparatos, brecha de seguridad en el hardware, así como los riesgos relacionados con el usuario.

Por otra parte, en el trabajo titulado "El internet de las cosas: antecedentes, conceptualización y riesgos" las autoras buscan "presentar en términos sencillos y claros una compilación de los datos más relevantes acerca del internet de las cosas, considerada como la nueva tendencia del siglo XXI".

Derivado de este análisis, logran generar un panorama enunciativo y descriptivo de los riesgos que representa el IoT para la sociedad actual. Como punto uno, las grandes bases de datos que los proveedores almacenan sobre el historial completo de sus clientes que genera una oferta de información y una amenaza constante de vulneración sobre estos datos. En segundo lugar, la seguridad de los sistemas de estos dispositivos anclados al IoT ya que todo sistema puede ser atacado, comprometiendo la confidencialidad, integridad y disponibilidad de los datos.[13]

[12] CASTRO Sola, M. *Internet de las cosas. Privacidad y seguridad*. Andalucía, Escuela Politécnica de Jaén, 2016. p.2.
[13] ESPINOZA Cecibel, María José PÉREZ, María Beatriz PERALTA. *Internet de las cosas: Antecedentes, conceptualización y riesgos*. Ecuador, Universidad Técnica de Machala, 2017. p.269.

III. FUNDAMENTACIÓN TEÓRICA

3.1. Internet de las Cosas y otros conceptos

Las sociedades que hoy habitamos el planeta asistimos a un acelerado y profundo mecanismo de cambios, casi sin darnos cuenta presenciamos la invención de nuevos materiales, la introducción de dispositivos cada vez más diminutos y la producción masiva de información; “el 90% de los datos actuales del planeta se crearon sólo en los últimos dos años”[14] y estamos duplicando la velocidad con que se producen.

La epidermis del mundo ha cambiado de tal manera que sí hoy Aristóteles pudiera presenciar el encendido de un árbol navideño con diodos emisores de luz (LED), un evento normal e insignificante para nosotros, le resultaría un acontecimiento sumamente impresionante y difícilmente comprensible el fenómeno de electroluminiscencia. Algo similar sucedería con Stanley Kubrick si tuviera enfrente a su Arriflex IIC, con la que filmara *Naranja mecánica* y *El beso del asesino*; y una de las cámaras actuales que permiten, bajo tecnología digital, mayor resolución que los sistemas de video analógico. Mayor, incluso, sería su sorpresa si pudiera presenciar la filmación de alguna de las típicas películas de superhéroes, realizadas en los últimos cinco años, y su posterior proyección.

Un asombro semejante vivieron nuestros padres, y algunos de nosotros, cuando ante sus ojos las computadoras fueron cambiando en capacidad, tamaño y forma. La computadora empleada en 1965 para enviar el primer mensaje de un equipo a otro era más alta y ancha que una persona adulta, dentro de un gabinete se contenían los múltiples circuitos y componentes físicos. Hoy existen computadoras cuyo tamaño apenas alcanza unos cuantos milímetros y su potencia (velocidad, memoria y rendimiento) excede a sus antecesoras de grandes tamaños.

[14] The Software Alliance. *¿Por qué son tan importantes los datos?*. Washington, DC, 2018, p.6.

Sin embargo, tanto Aristóteles y Kubrick (en sentido hipotético) como nuestros padres y nosotros mismos (en sentido real), además de preguntarnos sobre las posibilidades y características del funcionamiento de estos aparatos nos preguntaríamos sobre los efectos de ellos en la sociedad, las implicaciones que esto supone y los nuevos cambios que generarían. Un ejemplo de este ejercicio de análisis lo muestra Arthur Koestler en su novela Darkness at Noon:

> *"Los simios sumamente civilizados, se balanceaban con elegancia entre las ramas: el neandertal era basto y estaba atado a la tierra. Los simios, satisfechos y juguetones, pasaban la vida sumidos en sofisticados entretenimientos o cazando pulgas con contemplación filosófica; el neandertal se movía oscuramente dando pisotadas por el mundo, repartiendo porrazos aquí y allá. Los simios lo miraban divertidos desde las copas de los árboles y le tiraban nueces. A veces el terror los sobrecogía: mientras que ellos comían frutas y plantas tiernas con delicado refinamiento, el neandertal devoraba carne cruda y mataba a otros animales y a sus semejantes. El neandertal cortaba árboles que siempre habían estado en pie, movían rocas de los lugares que el tiempo había consagrado para ellas y transgredía todas las leyes y tradiciones de la selva. Era basto y cruel, y no tenía dignidad animal: desde el punto de vista de los sumamente civilizados simios, no era más que un paso atrás en la historia"*.[15]

En este fragmento el autor describe la forma en como los simios veían con desagrado los "avances" y el "progreso" evolutivo del neandertal, calificándolo incluso como un retroceso en la historia. Lo mismo pasa en ocasiones con nosotros, el pasado y los avances tecnológicos. Sin embargo, este texto no pretende, en ningún sentido, satanizar a la tecnología sino analizar un sector específico de la misma, bajo parámetros objetivos para identificar elementos de

[15] KOESTLER Arthur. *Darkness at noon*, Londres, 2005 pp. 183-184.

análisis desde la Ética. Para tal ejercicio es necesario comenzar por explicar y delimitar algunos conceptos como internet, internet de las cosas, etc.

3.1.1. Internet

De manera casi tradicional suele definirse a internet como la *red de redes*, sin embargo, esta concepción aporta pocas luces en la compresión de lo que es internet. Muchas interpretaciones podrían darse de esta frase y casi ninguna nos llevaría a la comprensión cabal. En un esfuerzo más lúcido Rodríguez Ávila aclara que "internet no es una simple red de ordenadores, sino una red de redes, es decir, un conjunto de redes interconectadas a escala mundial con la particularidad de que cada una de ellas es independiente y autónoma"[16]. En esta definición puede entenderse de manera clara y contextualizada la expresión red de redes al tiempo que pone sobre la mesa una visión clara de lo que es internet.

Por otra parte, García Mexía encuentra una explicación mucho más ilustrativa que permite apreciar los distintos elementos que componen internet:

> *"internet se compone de tres principales facetas o estratos: el del código, es decir, los estándares y protocolos que programan su funcionamiento y que obedece desde su nacimiento a pautas única y exclusivamente tecnológicas; el de los contenidos, tan variados como se pueda imaginar (desde un periódico en línea hasta una compraventa o un servicio administrativo); y el de la infraestructura o soporte físico, desde la fibra óptica a cable coaxial telefónico, hasta el propio espectro radioeléctrico, en cuanto actúa como medio de transmisión de internet sin hilos"*.[17]

[16] RODRÍGUEZ Ávila Abel. *Iniciación a la red de internet. Concepto, funcionamiento, servicios y aplicaciones de internet*, España, ideas propias editorial, 2007, p. 1.
[17] GARCÍA Mexía, Pablo. Derechos y libertades, internet y Tics. España, Ed. Tirant lo Blanch, 2014, p.13).

Empero, las definiciones no son suficientes para comprender la facilidad con que hoy enviamos un correo electrónico, compramos la edición especial de algún libro en Amazon o consultamos el tráfico, para ello es necesario conocer los eventos históricos que lo permitieron. En este sentido, la red precursora de internet nació en Estados Unidos de América derivada del objetivo de conectar diversos centros gubernamentales de manera tal que, en caso de ataque o eliminación de algún nodo, la comunicación no se interrumpiera. Esto en el contexto de la guerra fría y la carrera tecnológica emprendida por las dos potencias hegemónicas de ese periodo histórico.

En esta campaña, iniciada por la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA) se logró conectar en 1965 a la Universidad de California Los Angeles (UCLA) con el Stanford Research Institute (SRI). Para 1969 ya se encontraban conectadas cuatro universidades americanas, a las dos ya mencionadas se sumaron la Universidad de California Santa Barbara (UCBS) y la Universidad de Utha. El 29 de octubre de ese mismo año se logró transmitir el primer mensaje de un servidor a otro. Desde una computadora localizada en la UCLA a otra situada a 644km en el SRI, en esta comunicación se pretendía enviar de un dispositivo al otro la palabra LOG que en términos anglosajones e informáticos indica “Iniciar sesión”. Sin embargo la computadora localizada en el Instituto de Stanford falló antes de recibir el mensaje completo, por lo que el primer mensaje enviado a través de esta conexión fue “LO”.[18]

Con la interconexión de estas cuatro instituciones se consolidó la primera red de internet, conocida como ARPANET, que cumpliría el objetivo buscado: mantener las comunicaciones en caso de fallo de alguno de los nodos. En sentido básico la información generada por el equipo emisor era dividida en paquetes

[18] Saville Productions, Werner Herzog. *Lo and Behold: Reveries of the connected world*. Documental, Estados Unidos, 2016.

(unidades menores de información), circulada por diferentes rutas existentes en la red y finalmente reordenada en el equipo receptor. [19]

En un inicio la red aún no resultaba atractiva para la población y el uso no se había democratizado. No fue hasta la aparición de dos herramientas singulares que comenzó el uso masivo de la red, estas herramientas son:

a) Correo electrónico y,
b) World Wide Web

En marzo de 1972 Ray Tomlinson, de BBN Technologies, escribió el software básico de envío y lectura de mensajes de correo electrónico y eligió el signo de arroba "@" para dividir la dirección del usuario de la del servidor, por ello es identificado como uno de los padres del internet y se reconoce que su programa significó un engranaje importante en la revolución de la comunicación. La elección del signo arroba no fue aleatoria, cuando la máquina de escribir se creo se incluyó este símbolo ya que se trataba de una unidad de medida empleado en el sistema europeo. El diseño del teclado de las primeras computadoras retomó la composición del teclado de la máquina mecánica de escribir por lo que se agregó este signo, sin embargo, para el siglo XX, el arroba se encontraba en desuso. Tomlinson, decidió retomarlo y con ello le dio un significado diametralmente distinto.

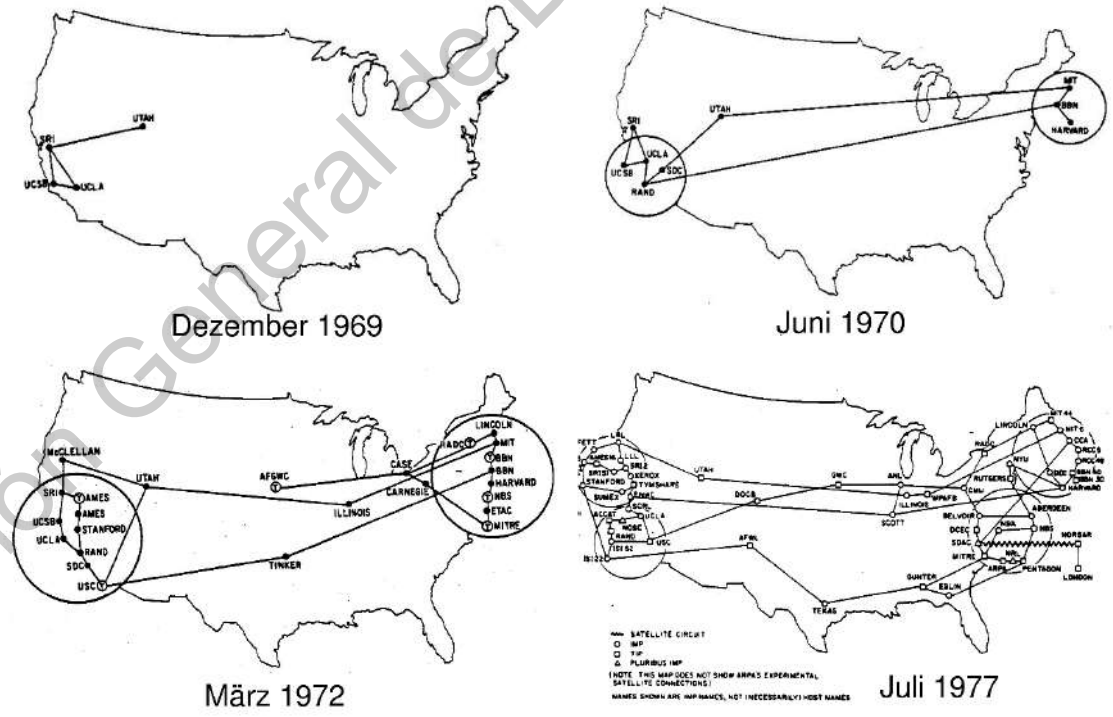
Cuatro meses después, en julio de 1972, Roberts amplió la utilidad del naciente correo electrónico habilitando algunas opciones como listas de mensajes, lectura selectiva, archivar, reenviar y responder; alternativas que permitían gestionar los mensajes de forma más sencilla y comprensible para los usuarios.[20]

[19] LÓPEZ i Seuba, Manel. *Internet de las Cosas, la transformación digital de la sociedad*, España, Editorial Ra-Ma, 2019, p.32.
[20] Internet Society. *Breve historia de internet*. Disponible en: https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/

Este desarrollo permitió desde el intercambio de mensajes personales hasta la gestión de operaciones bancarias y comerciales entre empresas, sin importar los kilómetros de tierra firme u océano que separaran a los dos puntos. De esta forma, el uso de la red se intensificó y generó un crecimiento en el número de nodos que la conformaban.

Ese mismo año, 1972, la red ya estaba formada por 50 universidades y centros de investigación norteamericanos y en 1973 se establecieron las primeras interconexiones con otros países. Finalmente, en 1981 se adoptó el nombre de internet, por lo que podría decirse que se cierra el primer bloque histórico de internet; el de su nacimiento.

Imagen 1. Computadoras conectadas en ARPANET (1969-1977).



Fuente: Defense Advanced Research Projects Agency.[21]

[21] Defense Advanced Research Projects Agency. *A History of the ARPANET: The First Decade*, Virginia, 1981, pp.119-129.

Para 1984 se llegó a los 1000 equipos conectados y en 1989 la cifra ascendía a 100,000. Este crecimiento sostenido, y después exponencial, fue impulsado por elementos como la mejora en velocidad y acceso a la conexión de la red, pero *"sin duda alguna, uno de los que más contribuyó a ello fue la aparición en 1991, de la World Wide Web"*[22].

También conocida como WWW, por sus iniciales, se trata de un sistema de distribución de documentos diseñado por Tim Berners-Lee que permite visualizar las páginas web alojadas en un servidor que está conectado a la WWW. Para ello se requiere de tres supuestos esenciales.

1. La existencia de un documento HTML (HyperText Markup Language) con el contenido de la página web.
2. La conexión del servidor (donde se aloja el documento HTML) con la WWW.
3. Contar con un programa que pueda leer el código HTML, ejecutarlo y mostrar la página web en términos gráficos. Estos programas son conocidos como navegadores de internet o browser, por ejemplo Internet Explorer, Google Chrome, o el más popular en los primeros años de los 90: Navigator Netscape.

El incumplimiento de alguno de estos supuestos frustra la visualización de la página. Por ejemplo, si no existiera el documento HTML sería similar a la falta de materia prima para la elaboración de algún dispositivo por lo que no se podría llevar a la realidad. Si el servidor que aloja el documento HTML no se encontrara conectado con la WWW sería imposible encontrarlo y acceder a él. Por último, si nuestro equipo no contara con un browser sólo veríamos el código HTML y no los

[22] LÓPEZ i Seuba, Manel. *Internet de las Cosas, la transformación digital de la sociedad*, España, Editorial Ra-Ma, 2019, p.33.

diseños de las páginas web a los que estamos acostumbrados, no podríamos interpretarlo a menos que conociéramos bien este lenguaje.

En estricto sentido, esta aportación de Berners-Lee hizo posible el uso de enlaces de hipertexto para conducir a una parte específica de la Web generando un acceso simple y a voluntad. Este sistema facilitó el uso de la red y aceleró tanto su expansión que actualmente suele confundirse o tomarse como sinónimo a internet (la red de nodos) y web (World Wide Web).

Sin embargo, la web se refiere sólo a un sistema de documentos conectados y disponibles a través de internet sin abarcar todo el contenido, código y soporte físico de este. Podría decirse que la Web es apenas una muestra del potencial de internet.

Con el nacimiento de la web se potencializó el crecimiento de internet, tan sólo un año después, en 1992, el número de ordenadores conectados ascendía a un millón y para 1996 superó la barrera de los 10 millones. El crecimiento de la Web siguió un camino similar, en 1993 existían tan sólo 100 sitios web que podríamos haber visitado en un solo día y para 1997 ya eran más de 200,000. En 2019 se registraron más de 1900 millones de sitios web activos[23].

Por tanto, la introducción, desarrollo y penetración de la Web abraza lo que podría constituirse como un segundo bloque histórico del internet: el de su expansión.

El siguiente paso evolutivo del internet fue la aparición del concepto Web 2.0, novedosa porque rompe con lo estática de la Web clásica y ofrece al usuario experiencias compartidas e interactivas. Dicho término fue empleado por primera vez en la empresa O'Reilly Media en 2004, esta empresa fue responsable también de crear la primera página web comercial del mundo en 1993.

[23] Íbid p.34.

Podría decirse que la Web 2.0 “significa hacer más inmediatas las acciones de los individuos”[24], es por ello que estuvo acompañada del surgimiento de redes sociales y de teléfonos inteligentes.

Para este momento, la penetración de la red era considerablemente importante, su uso se había democratizado en la población y comenzaba a percibirse como indispensable para el desarrollo de las actividades productivas, económicas y sociales. Ante ello, se hizo cada vez más evidente la necesidad de reconocer derechos y principios en torno de internet.

En 2008, la Internet Rights & Principles Coalition (IRP) comenzó la promoción activa de principios basados en la gobernanza de internet en el Internet Governance Forum (IGF) de la Organización de Naciones Unidas y en otros espacios formales, esto bajo el objetivo de adaptar los Derechos Humanos existentes al entorno de internet.

En este sentido, la Coalición IRP ha emitido dos importantes documentos. En primer lugar, la Carta de Derechos Humanos y Principios para internet, misma que fue publicada en la reunión del IGF de 2010 en Vilnius, Lituania. El contenido de la Carta *“intenta interpretar y explicar cómo afectan internet y las nuevas tecnologías a los Derechos Fundamentales recogidos en la Declaración Universal”*[25]. Entre los temas que trata, destacan los siguientes:

- **Derecho al acceso a internet:** afirma que toda persona tiene derecho a acceder a internet e incluye la calidad del servicio, libertad en la elección de sistema y software, garantizar la inclusión digital, así como neutralidad e igualdad de la red.

[24] PÉREZ Salazar, Gabriel. La Web 2.0 y la sociedad de la información. Revista mexicana de ciencias políticas y sociales. Vol. 56, N1. 212. Mayo/agosto 2011. ISSN 0185-1918.
[25] Internet Rights & Princiles Colition. *Carta de Derechos Humanos y Principios para Internet*. Internet Governance Forum, 2015, p. 9.

- **No discriminación en el acceso, uso y gobernanza de internet:** prevé la igualdad en el acceso, necesidades específicas de grupos marginados, e igualdad de género.
- **Libertad y seguridad en internet:** platea que todas las medidas de seguridad deben estar en concordancia con el derecho y las normas internacionales, por lo que las medidas de seguridad serán ilegales en la medida que restrinjan otro derecho humano, por ejemplo; el derecho a privacidad o a la libertad de expresión.
- **Libertad de expresión información en internet:** comprende la libertad de protesta en línea, libertad ante la censura, el derecho a la información y pautas ante los discursos de odio.
- **Privacidad en Internet:** incluye el derecho al anonimato y a utilizar cifrado, libertad ante la vigilancia y la difamación, la protección de la personalidad virtual, además prevé el diseño de legislaciones nacionales sobre privacidad, normas de confidencialidad e integración de los sistemas TIC, así como políticas de configuración de la privacidad.
- **Protección de datos digitales:** incorpora la protección de datos personales, obligaciones de los colectores de datos, monitorización la protección y normas mínimas sobre el uso de datos personales.
- **Apropiación de un orden internacional y social en internet**: en este apartado se insertan la gobernanza de internet, así como la participación efectiva en esta.
- **Obligaciones y responsabilidades en internet:** implica el respeto de los derechos de los demás y la responsabilidad de quienes ejercen el poder.

El segundo documento se titula “Ten Puncy Principles” o Diez poderosos principios publicado en 2011. Este instrumento es resultado del trabajo emprendido para generar un documento que rescatara el contenido de la Carta de

Derechos Humanos y Principios para internet, y al mismo tiempo permitiera su difusión, educación y promoción, por lo que se formuló en un formato más libre que su predecesora. Este documento propone los siguientes puntos: universalidad e igualdad; derechos y justicia social; accesibilidad; expresión y asociación; confidencialidad y protección de datos; vida, libertad y seguridad; diversidad; igualdad; normas y reglamento, así como gobierno.

Con el abanderamiento de estos documentos y posterior adopción por los países miembros, se configura un tercer bloque histórico del internet: el de los derechos y la regulación. Es en esta etapa donde nos encontramos ahora, sin embargo, no es una etapa estática que pueda ser narrada en sentido lineal, se trata de una etapa viva y en desarrollo que presenta múltiples significados y proyecciones de acuerdo con el territorio del que se trate.

3.1.2. Internet de las cosas

Una vez comprendido el concepto de internet, resulta más sencillo o por lo menos más claro entender a qué nos referimos cuando hablamos del internet de las cosas (IoT). Dicho término fue introducido por Kevin Ashton, del Instituto Tecnológico de Massachusetts (MIT), en 1999, a manera de hipótesis sobre un sistema en el cual los objetos en el mundo físico podrían conectarse a internet a través de sensores para automatizar la recogida de datos.

Actualmente, se ha definido a internet de las cosas como *"la tecnología basada en la conexión de objetos cotidianos a internet que intercambian, agregan y procesan información sobre su entorno físico para proporcionar servicios de valor añadido a los usuarios finales"*.[26] O como una *"red de objetos físicos que se conectan a internet usando diversas tecnologías y que tienen capacidad de*

[26] BARRIO, Moisés. *Internet de las cosas*. España, Ed. Reus, 2018.

conexión e interacción con el entorno, capacidades que les permiten tomar decisiones y comunicarse con el mundo"[27] .

Por su parte el International Telecommunication Union ha conceptualizado a la IoT, en la Recomendación UIT-T Y.2060(06/2012), como:

> *"una infraestructura global para la sociedad de la información, que permite la ejecución de servicios avanzados mediante la interconexión física y/o virtual de cosas mediante tecnologías de información y comunicación interoperativas que existen actualmente pero que evolucionan a lo largo del tiempo".*[28]

En general, las definiciones presentadas destacan del internet de las cosas: 1) la interconexión de objetos cotidianos a internet, 2) la capacidad de estos objetos de levantar, intercambiar, y procesar información de su entorno físico, 3) la posibilidad que tienen los dispositivos para tomar decisiones sin intervención humana, así como 4) el carácter dinámico del IoT, dada su evolución constante y el puente trazado entre lo físico, lo digital y lo virtual.

Para comprender esta tecnología, es necesario contar la historia de internet no desde la sucesión de eventos, como se hizo en la sección pasada, sino desde las características de los dispositivos, pero sobre todo desde los usos de internet. En este sentido es necesario reconocer que existen cuatro fases[29]:

1. Científico-académica: comenzó con el nacimiento de internet y se potencializó tras la democratización de la red a principios de los años 90. En esta fase los usuarios comunes eran investigadores, docentes y estudiantes

[27] EVANS, Dave. Internet de las cosas: cómo la próxima evolución de internet lo cambia todo, Cisco Internet Business Solutions Group, 2011
[28] International Telecommunication Union. Recomendación UIT-TY.2060 (06/2012), 201, p.2.
[29] EVANS, Dave. Internet de las cosas: cómo la próxima evolución de internet lo cambia todo, Cisco Internet Business Solutions Group, 2011

de distintos niveles académicos, principalmente universitarios; las funciones estaban concentradas en el uso de correo electrónico, navegación web y empleo de motores de búsqueda. El único dispositivo conectado a la red era la computadora y el usuario tenía un papel dinámico en la gestión de datos; eran los individuos quienes nutrían de información a la red y al mismo tiempo disponían de ella partiendo de necesidades particulares.

2. Económica: se caracteriza por la transformación de los procesos empresariales y significó la conexión digital de los sistemas logísticos a finales de los años 90. Esto posibilitó el inicio del comercio electrónico y cambió radicalmente la forma en que las empresas acceden a los mercados. Además, implicó la asimilación de la banca al ecosistema digital, prácticamente todos los bancos migraron sus datos y algunas de sus acciones a la red. La computadora tradicional dejó de ser el único dispositivo conectado y se sumó la computadora portátil, el usuario promedio perdió un poco de protagonismo en la gestión de datos ya que los agentes económicos y empresariales cobraron un papel relevante en la dinámica de la información.

3. Social: comenzó a principios de los 2000 y se caracterizó por la asimilación de la vida social a la red; el uso de redes sociales y servicios de comunicación se convirtieron en los usos más destacados de la red. Significó el paso de una Web de datos estáticos a la información transaccional. Con esto el usuario perdió casi por completo el protagonismo en la gestión de sus datos. De hecho, se dio por sentado que todo lo publicado en una red social dejaba de ser propiedad del usuario y pasaba a ser del dominio público, gestionable por cualquier otro usuario o empresa. A la computadora y la laptop se sumaron el celular y la Tablet como dispositivos conectados.

4. Internet de las cosas: comienza entre 2008 y 2009 cuando más dispositivos que personas se conectaron a la red. A los dispositivos tradicionales de conexión se sumaron autos inteligentes, bombillas, termostatos, semáforos, cámaras, marcapasos, televisores, aviones, refrigeradores y un largo etcétera que cubre casi cualquier tipo de dispositivo

en áreas tan diversas como el hogar, la medicina, los deportes, la milicia y el transporte. Se ampliaron los servicios de video y audio en línea, el cloud computing (use de nube en base de datos???) y los datos se convirtieron en el activo más importante de usuarios y empresas. Sin embargo, los dispositivos arrebataron todo protagonismo a los usuarios en cuanto a la gestión de datos, al pasar de dispositivos simplemente conectados a dispositivos inteligentes con la capacidad de recoger información, procesarla y tomar decisiones al respecto. Hoy no es necesario que los usuarios nutran de datos a la web, los dispositivos del Internet de las cosas (Internet of things; IoT) han tomado ese papel protagónico.

Es en esta cuarta etapa, la de los objetos conectados, donde nos encontramos actualmente. No quiere decir esto que los usos y dispositivos anteriores se hayan superado, sino que se ha generado una especie de acumulación o sumatoria. A las características, dispositivos y retos de las etapas anteriores deben sumarse los de Internet de las cosas.

Hay que mencionar además que, esta cuarta fase se encuentra en constante evolución y que hasta el momento presenta tres etapas evolutivas, propuestas por Doug Davis de Intel Corporation[30]:

1. Tecnología incrustada: es conocida también como tecnología embebida e incluye a los dispositivos que cuentan con una computadora incrustada y cuyo acceso es factible gracias al uso de controladores. Ejemplo de esto son los automóviles que incorporan microprocesadores para realizar distintas funciones, a ellos se conectan los técnicos del taller, a través de un controlador para tener acceso a los datos del automóvil.
2. Masificación de la conectividad: comprende a todos los dispositivos que poseen capacidades de conexión, es decir, envían y reciben datos de la nube. Ejemplo de ello son los automóviles capaces de

[30] LÓPEZ i Seuba, Manel. *Internet de las Cosas, la transformación digital de la sociedad*, España, Editorial Ra-Ma, 2019, p.40.

notificar al conductor sobre accidentes terrestres, tiempos de llegada al lugar de destino, mapas en línea, etc.

3. Inteligencia: podría decirse que es la fase actual y se centra en el análisis de datos a través de Big Data, Inteligencia Artificial y machine Learning. En este caso el ejemplo podría ser un automóvil capaz de conducirse de manera autónoma, analizando los datos recabados del contexto y bases de datos, en comunicación dinámica con la nube y dotado de capacidades para decidir acelerar, frenar, cambiar de ruta, activar seguros, modificar la temperatura, etc.

En este sentido, algunas definiciones más adelantadas describen al IoT como *"una infraestructura de red dinámica global capaz de auto configurarse basada en protocolos de comunicación estándar e inter operativos donde tanto las cosas físicas como virtuales tienen identidad propia, atributos físicos, personalidad virtual, e interaccionan de forma inteligente, y se integran de forma transparente, es decir, pasando desapercibidos, en la red de información"*[31]. Esta definición, además de descartar la intervención humana en la toma de decisiones, dota a los elementos físicos y virtuales del IoT de capacidades como identidad y personalidad, propios, hasta hora, de los humanos. Ante esta dimensión, es factible pensar a Internet de las Cosas como uno de los agentes que revolucionarán al mundo en el futuro cercano.

El propio Kevin Ashton, creador del concepto, declaró que:

> *"Si los libros, termostatos, refrigeradores, paquetería, lámparas, botiquines, partes automotrices, entre otros, estuvieran conectados a internet y equipados con dispositivos de identificación, no existirían, en teoría, artículos fuera de stock o medicinas caducas: sabríamos exactamente su ubicación, cómo se consumen en el mundo: el extravío*

[31] VAN Kranenburg, Rob. *The Internet of Things: A critique of ambient technology and the all-seeing network of RFID*. Institute of Network Cultures, Amsterdam, 2018.

sería cosa del pasado, y sabríamos qué está encendido y qué está apagado en todo momento. Internet de las cosas tiene el potencial de cambiar el mundo, como lo hizo Internet en su momento. Tal vez aún más".[32]

De ahí que internet de las cosas se configure como el próximo paso hacia la digitalización de nuestra sociedad y represente el puente entre el mundo digital y el físico; unión sólo plasmada, hasta entonces, por la pluma de autores de ciencia ficción o en el plató del séptimo arte, caracterizada cada vez más por la conexión máquina-máquina y la disminución de la comunicación máquina-persona.

En este sentido, los elementos que permiten que internet de las cosas sea posible en nuestra realidad pueden dividirse en cuatro, a saber: objetos, datos, procesos y personas.

En primer lugar, los **objetos o cosas** son todos los dispositivos que están conectados a internet y entre ellos. Recopilan datos de sí mismos y de su entorno, los gestionan y comunican a su proveedor e incluso a otros dispositivos. Estos dispositivos atraviesan prácticamente todas las áreas de desarrollo e intervención humana. Por ejemplo, en el área de la salud, existen dispositivos implantados en los pacientes para ayudar a los médicos a diagnosticar enfermedades, monitorear la salud e incluso posibilitan la aplicación de tratamiento. Tal es el caso de marcapasos conectados a la red que dan aviso a los médicos cuando se presentan anomalías en el ritmo cardiaco, el médico puede controlar de manera remota un impulso eléctrico que reajuste el ritmo cardiaco, incluso el dispositivo puede tomar la decisión, de acuerdo con las funciones programadas, de aplicar él mismo el impulso eléctrico necesario.

En el sector industrial, los objetos del IoT se aprecian como sensores de energía, tecnologías de seguimiento de paquetes y vehículos, además de la

[32] LÓPEZ i Seuba, Manel. *Internet de las Cosas, la transformación digital de la sociedad*, España, Editorial Ra-Ma, 2019, p.28.

interconexión digital en infraestructura crítica. Hoy centrales nucleares, bases de defensa e instalaciones petroleras se hallan conectadas a la red. Múltiples ciudades y administraciones locales han conectado a la red edificios, alumbrado público, sistemas de transporte, estructuras de semaforización y control de tráfico. Además, hay otras aplicaciones que interconectan a humanos y animales con otros dispositivos del IoT.

Dispositivos aún más cercanos a la vida cotidiana los encontramos en termostatos inteligentes que modulan la temperatura de acuerdo con información que recolectan del exterior y con proyecciones que ejecutan de acuerdo a información del internet. A este ejemplo debemos sumar televisores, refrigeradores, luces inteligentes, consolas de videojuegos, automóviles, centros de acceso, impresoras, sistemas de sonido, medidores de energía, cámaras inteligentes y casi cualquier objeto que tengamos en mente.

En segundo plano, los **datos** que, generados por los objetos se transforman en información útil para la toma de decisiones y la mejora de resultados del propio dispositivo, de otros dispositivos de la misma familia e incluso de dispositivos ajenos. Actualmente, los datos generados por el IoT son recursos renovables y prácticamente inagotables, además de ser factores clave de impulso económico. Es por ello que se han generado de manera persistente mejoras en su velocidad (rapidez con que se crean), volumen (cantidad de datos), variedad (tipos de datos) y veracidad (precisión). En este sentido, la gestión de datos por los dispositivos del IoT permiten un crecimiento circular, es decir, el perfeccionamiento de los objetos y sus sistemas, a partir de los datos recopilados, almacenados y analizados por los propios dispositivos.

En tercer lugar, los **procesos lógicos** orientados a conseguir los resultados esperados, es decir la ejecución de instrucciones dictadas por un programa. En este sector podríamos resaltar, por ejemplo, el IPv6 (Internet protocol version 6) que es la versión más reciente del IP.

Por último, las **personas**, que se convierten en productores de datos y receptores de servicios. Esto aun cuando no hayan adquirido de manera directa un dispositivo del IoT. Por ejemplo, una ciudad que cuenta con sistemas de video vigilancia recopila a través de sus cámaras información de sujetos que no adquirieron de manera directa dichos dispositivos. En este sentido, todas las personas dejan un rastro digital a través de su interacción con la red.

Es así como el ciberespacio se conecta con el mundo físico, como internet se vuelve sensorial ante fenómenos reales e interactúa con ellos; dotando de capacidades inteligentes a objetos tradicionalmente pasivos convirtiéndolos en objetos activos y participes de los procesos de conexión y comunicación.

Al respecto, se reconocen tres tipos principales de conexión y comunicación:

- Persona a persona (PP) donde el origen y el destino de la comunicación son personas, por ejemplo; una reunión de teletrabajo por medio de una plataforma de videoconferencia.
- Máquina a persona (MP) cuyo origen de la comunicación es una máquina y el destino una persona, por ejemplo; interpretación de la información arrojada por el rastreador GPS de un vehículo de carga.
- Máquina a máquina (MM) donde el origen y destino de la comunicación son máquinas, por ejemplo; un edificio inteligente donde los sistemas de iluminación, climatización y control de puertas intercambian información para la toma de decisiones.

Estos tipos de conexión son distintos en entornos tradicionales y en entornos digitales del IoT. En los primeros, predominan las conexiones PP, en tanto que en los segundos priman las MM. Esto no quiere decir que las conexiones PP y MP desaparezcan, sino que el protagonismo lo ha adquirido la

comunicación máquina a máquina, sin embargo la intervención humana sigue siendo indispensable en cuanto a programación, interpretación y fundamentalmente auditoría.

Por otra parte, para entender cabalmente la relevancia del IoT, es necesario comprender otros conceptos, y tecnologías, así como la relación que guarda con ellos, tal es el caso del cloud computing (en español por favor también), big data (metadatos) e inteligencia artificial, mismos que se exponen en las páginas siguientes.

3.**1.3 IoT y Cloud Computing**

La computación en la nube o cloud computing se ha definido como "un modelo para hacer posible el acceso a red adecuado y bajo demanda a un conjunto de recursos de computación configurables y compartidos cuyo aprovisionamiento y liberación puede realizarse con rapidez y un mínimo de esfuerzo de gestión e interacción por parte del proveedor del cloud"[33]. En un sentido muy simple, podría decirse que es un sistema que permite que cualquier elemento informático puede ser gestionado en la nube, es decir en la red. Estos recursos de gestión son ofrecidos por proveedores que prestan servicio a través de centros de datos remotos a múltiples clientes, quienes pueden tener acceso a sus recursos desde cualquier dispositivo conectado a internet.

De hecho, el término "cloud" hace referencia, en este caso, a la descolocación y diseminación geográfica de los sistemas y terminales; da a entender que *"hay algo, que está allí, aunque no se sabe muy bien dónde"*[34]. Por ejemplo, si escuchamos el álbum London Calling, de The Clash, en Spotify o algún

[33] INTECO. *Riesgos y amenazas en Cloud Computing.* 2011, p. 6. https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

[34] LÓPEZ i Seuba, Manel. *Internet de las Cosas, la transformación digital de la sociedad*, España, Editorial Ra-Ma, 2019, p.333.

otro servicio de streaming musical, seremos conscientes de que ni “Spanish bombs”, ni el resto de canciones que lo componen se encuentran alojadas en nuestro dispositivo, pero tampoco sabemos bien a bien dónde es que se ubican. Sin embargo, tenemos claro que podemos acceder al material cada vez que lo deseemos.

Existen cuatro tipos de infraestructuras cloud: privada, pública, comunitaria e híbrida así como tres tipos de servicio, mismos que pueden identificarse según se ofrezca software, plataformas o infraestructura como servicio:

- *Software as a Service (SaaS)*: consiste en un software que ha sido creado como un servicio, los usuarios generalmente acceden a través de la Web sin identificar el servicio como un software propiamente. Es decir, es la sustitución de aplicaciones instaladas en los equipos por opciones situadas en la nube. Todo el mantenimiento es responsabilidad del proveedor, quien se encarga totalmente del funcionamiento. Ejemplos de esto son: Dropbox, Gmail y Google Docs.
- *Platform as a Service (PaaS)*: Los clientes hacen uso de la plataforma para generar desarrollos, por lo tanto tienen control parcial sobre las aplicaciones y la configuración del entorno, en este sentido la seguridad y la gestión es compartida entre ambas partes pero la mayor proporción está a cargo del proveedor. Ejemplos de este tipo de servicio son: Google App Engine y Heroku (que permiten desarrollar y alojar aplicaciones web).
- *Infrastructure as a Service (IaaS)*: consiste en el alquilamiento del entorno físico (procesadores, disco duro, memoria RAM, routers, sistemas de seguridad) para ser usados por el cliente, quien se encarga de desarrollar la plataforma y el software propiamente. En este sentido, el proveedor se encarga de la instalación y funcionamiento del hardware, mientras el usuario se encarga de la gestión y seguridad del entorno lógico. Ejemplos de este tipo de servicio son: Amazon Web Service y vCloud.

La descripción de estos servicios permite visibilizar la tendencia actual de alojarlo todo en la nube e internet de las cosas no escapa a esta inclinación global. El software y los datos que permiten gestionar a los dispositivos del IoT residen en la nube, es decir, las plataformas y aplicaciones diseñadas para el funcionamiento de los dispositivos, así como los datos que estos recolectan de manera local están "almacenadas" fuera del dispositivo (en la nube), lejos de donde se generaron.

3.1.4 IoT y Big Data

Habitualmente, se piensa en los metadatos o big data como una gran masa de datos, sin embargo esta concepción, si bien es cierta, resulta simplista y limitativa al mom.ento de comprender la importancia y realidad del concepto. De acuerdo con Rob Kitchin, big data se encuentra dotado de siete características generales[35]:

- **Enorme volumen** de datos (terabytes o petabytes por lo menos), recolectados por archivado automático en la web o por maquinas en el caso del IoT. Este volumen de datos cobra valor por su integridad (veracidad) o precisión más que por su tamaño.
- **Alta velocidad** con que se crean y recolectan, habitualmente en tiempo real y en flujo continuo, lo que permite la toma de decisiones de manera rápida y automática.
- **Variedad** en la fuente y tipo de dados, lo que quiere decir que un solo dato puede tener varias fuentes y que se están recopilando al mismo tiempo una gran cantidad de datos distintos entre sí. Además, estos pueden recibirse de manera estructurada (bases de datos) o no estructurada (si organización inicial, por ejemplo videos de una cámara de seguridad).

[35] KITCHIN, Rob. *"Big data, new epistemologies and paradigm shift"*, en Big Data & Society, núm. I, 2014, p.1.

- **Alcance exhaustivo** que captura datos de poblaciones o sistemas enteros.
- **Resolución fina** y **naturaleza relacional**, es decir, que contiene campos comunes que permiten la unión de diferentes conjuntos de datos con el objetivo de generar conclusiones.
- **Flexible**, ya que puede agregar campos nuevos de manera eficiente y permite expandir rápidamente su tamaño.

Además, el *big data* puede describirse como un proceso que consta de tres fases: generación, evaluación y distribución. En la primera, tanto personas como máquinas proveen de datos al sistema, mismos que serán analizados durante la segunda fase. Ya en la etapa de evaluación, especialistas de datos o algoritmos dan tratamiento a los datos para transformarlos en información útil a través de métodos estadísticos tradicionales hasta los más novedosos de aprendizaje automático. Por último, las conclusiones son distribuidas a máquinas y personas para la toma de decisiones.

Un ejemplo claro de la relación entre *IoT* y *Big Data* lo encontramos en la analítica sanitaria: Zhao T, Ni H, Zhou X, Qiang L, Zhang D y Yu Z presentaron en 2014 un sistema automatizado capaz de detectar patrones anormales en actividades diarias, signos y síntomas de adultos mayores que viven solos, esto a través de dispositivos de la IoT empleados en su hogar y de sensores médicos IoT desplegados en sus cuerpos. A través de arquitecturas de big data y algoritmos de aprendizaje automático son analizados todos los datos arrojados por los dispositivos con la finalidad de robustecer a diario un sistema de respuesta de emergencia médica en tiempo real[36].

[36] ABDERRAHMANE Ed-daoudy y Khalil Maalmi. *"A new Internet of Things architecture for real-time prediction of various diseases using machine learning on big data environment"*, en Journal of Big Data. Núm. 6, noviembre 2019. Disponible en https://doi.org/10.1186/s40537-019-0271-7

3.1.5 IoT e Inteligencia Artificial

El tema de la Inteligencia Artificial (IA) es tan complejo y amplio en sí mismo, que difícilmente se lograría abarcar en estas líneas. Por tanto, el objetivo de esta sección no es explicarla a profundidad, sino dejar claro por qué es una impulsora del internet de las cosas.

En sentido amplio, la IA es la rama de las ciencias computacionales que se encarga del diseño y construcción de sistemas capaces de realizar tareas asociadas con las funciones de la cognición humana, tales como: creatividad, sensibilidad, aprendizaje, entendimiento, percepción del ambiente y uso de lenguaje[37].

De estas funciones, la más relevante para los ambientes del *IoT* es el aprendizaje, de ahí que el sub campo de la *IA* denominado *Machine Learning*, aprendizaje de las máquinas o aprendizaje automático, haya tomado tanta relevancia en los últimos años. El objetivo de esta área es lograr que las máquinas aprendan a base de ejemplos, por lo que son nutridos constantemente por big data para aumentar su efectividad al contar con un mayor número de patrones, de los que aprende constantemente.

Por ejemplo, un sistema de semaforización inteligente compuesta por dispositivos IoT conectados a la red, que recopilan un gran número de datos sobre flujos vehiculares y peatonales, accidentes terrestres, así como información climática, distribución de comercios y oficinas gubernamentales: puede aprender de los patrones de movimiento y configurar los tiempos de alto y siga para generar una movilidad más dinámica y efectiva.

De acuerdo con López i Seuba la *IA* en general, y *Machine Learning* en particular, pueden colaborar con IoT de las siguientes formas:

[37] INCyTU. *"Inteligencia artificial"*. En Foro consultivo de ciencia y tecnología. Núm. 012, Marzo 2018. Disponible en https://www.foroconsultivo.org.mx/INCyTU/documentos/Completa/INCYTU_18-012.pdf

- Calibración automática de sensores.
- Mantenimiento de dispositivos, basándose en líneas históricas para predecir cuándo se generará una falla.
- Optimización de sistemas de seguridad, analizando situaciones de riesgo pasadas.
- Mejora de servicios basados en el contexto, tal es el caso de la regulación de temperatura e iluminación en relación a los patrones de los usuarios.
- Control de acceso de usuarios, en relación con los conocimientos previos.
- Reorganización de cadenas de producción interrumpidas por factores externos.
- Discriminación de datos incorrectos o no relevantes, dentro de grandes flujos y volúmenes de información.
- Supervisión en búsquedas de patrones anómalos o incorrectos.
- Clasificación y extracción en cadenas de producción.
- Diagnosis médica.
- Reacción empática ante seres humanos, en relación al análisis de sus rasgos a través del reconocimiento facial[38].

Es pertinente mencionar que estos puntos son sólo enunciativos y de ninguna forma limitativos. Actualmente, y como ya se mencionó con anterioridad, el IoT se encuentra en la fase evolutiva de "inteligencia" lo que supone un uso frecuente de los procesos de aprendizaje, *big data* y *cloud computing*.

En general, la incorporación del IoT a la vida diaria implica por un lado: mayor productividad, eficiencia y eficacia; nuevas y mejores oportunidades de

[38] LÓPEZ i Seuba, Manel. *Internet de las Cosas, la transformación digital de la sociedad*, España, Editorial Ra-Ma, 2019, p.350.

desarrollo, aumento en los niveles de confort en ámbitos urbanos y rurales, además de una larga lista de beneficios. Sin embargo, en el otro extremo de este escenario se colocan preguntas relacionadas con los riesgos probables alrededor de estos dispositivos: ¿Cómo se gestionan los datos recolectados? ¿Quién tiene acceso a ellos? ¿Qué problemas de seguridad son probables? ¿El IoT representa un riesgo para la privacidad? ¿Qué efectos tiene la incorporación de los dispositivos a nuestra vida? ¿Qué medidas deben tomarse para proteger a los usuarios?, entre muchas otras preguntas que son discutidas en los siguientes capítulos de la presente.

IV. HIPÓTESIS O SUPUESTOS

La intervención del internet de las cosas en la vida de los individuos genera violaciones a su privacidad y seguridad, además de problemas ambientales. Un tratamiento ético de los dispositivos puede generar mejores condiciones de justicia entre los usuarios.

V. OBJETIVOS

5.1. General

Analizar los problemas de seguridad con perspectiva ética, que pueden surgir en el marco del internet de las cosas y su operatividad con la noción de privacidad, a través de una metodología mixta, que permita plantear formulaciones éticas tendientes a paliar daños potenciales a la seguridad de los usuarios.

5.2. Específicos

- Analizar las implicaciones éticas que tiene el internet de las cosas en la seguridad y la privacidad de los usuarios, así como los derechos que pueden verse comprometidos.
- Examinar qué otras implicaciones éticas supone la incorporación de los dispositivos del internet de las cosas en nuestras vidas.
- Identificar planteamientos ético-jurídicos que puedan emplearse para generar políticas públicas benéficas para usuarios y proveedores.

VI. METODOLOGÍA

La comprensión de un tema como el que se trata en este documento exige el diálogo con distintas disciplinas, por ello se emplea un modelo metodológico mixto compuesto por tres núcleos que permiten observar al fenómeno con distintos focos y desde distintos lugares.

En **primer lugar**, se realiza un análisis estadístico de empresas que comercializan dispositivos de IoT en México, para lo cual se elaboró la siguiente ruta:

1. Cálculo muestral: de acuerdo con la fórmula estadística determinada para muestras en poblaciones finitas o conocidas, cuyos datos se describen en la Tabla 1.

Tabla 1. Datos para cálculo muestral	
Fórmula: $n=\frac{N Z^2 \ pq}{d^2 \ (N-1)+Z^2 \ pq}$	
Donde:	
n= **Tamaño de la muestra**.	**94**
N= **Tamaño de la población.**	4,000 (Estimado de la AMITI).[39]
Z^2= **Nivel de confianza.**	(1.96 que equivale a 95% recomendado).
p= **Prevalencia esperada.**	(recomendada de 0.5 cuando no se conoce).
q= 1 – p	(1 – 0.5).
d^2= **Error que se prevé cometer.**	(0.1 que equivale a 10% máximo recomendado para investigaciones científicas).

Fuente: Elaboración propia.

[39] Asociación Mexicana de la Industria de Tecnologías de la Información. *Foro AMITI Cybersecurity: en un entorno digital, mejora tu seguridad.* México, 4 de abril de 2019.

2. Muestreo: la selección de las empresas analizadas responde a criterios de muestreo estratificado. 70 por ciento del total de la muestra corresponde a empresas internacionales y 30 por ciento a empresas nacionales, tal como se puede observar en la Tabla 2. Esta distribución está definida dada la amplitud considerablemente mayor del mercado internacional de dispositivos IoT.

Tabla 2. Muestreo estratificado

Estrato	**Equivalencia**
Internacional (70%)	**66**
Nacional (30%)	**28**
Total	**94** empresas

Fuente: Elaboración propia.

3. Definición de unidad de análisis: Un dispositivo por cada empresa, seleccionado bajo criterios de ventas y publicidad.
4. Definición de variables: Se establecen ocho rubros de variables a partir de la revisión de antecedentes y del marco teórico (ver tabla 3). La información relaciona con cada variable es recolectada por medio de etnografía digital que se describe en párrafos subsecuentes.

Tabla 3. Muestreo estratificado

Rubro	Variable	Descripción
1 Sector de aplicación	1.1 Sector de aplicación	Área (s) donde se inserta (n) las funciones del dispositivo: Hogar, salud, ciudad, milicia, transporte, etc.
2 Datos personales	2.1 Datos solicitados	Lista de todos los datos solicitados o recolectados por el dispositivo.
	2.2 Tipología del dato	Los datos recolectados son convencionales o sensibles.
	2.3 Proporcionalidad	Datos recolectados de acuerdo con las funciones del dispositivo.
	2.4 Uso	Empleo que se le da a los datos.
	3.1 Existencia 3.2 Contenido	El dispositivo cuenta o no con aviso de privacidad. Áreas que abarca el aviso de privacidad.

3 Aviso de privacidad	3.3 Lenguaje	Empleo de lenguaje técnico y legal de difícil comprensión, comprensible con pocos conocimientos informáticos y/o legales, comprensible sin conocimientos informáticos y/o legales.
	3.4 Modalidad	Física o digital.
	3.5 Accesibilidad	Facilidad del usuario para disponer del aviso de privacidad
4 Consentimiento	4.1 Tipo	Consentimiento tácito o expreso.
	4.2 Mecanismo	Forma de obtener el consentimiento: firma, voz, casilla.
	4.3 Revocación	Mecanismos de revocación del consentimiento.
5 Medidas de seguridad	5.1 Tipo	Administrativas, técnicas o físicas.
	5.2 Características	Descripción de las medidas de seguridad.
6 Comunicación con el usuario	6.1 Vías	Formas que el usuario tiene de contactar al proveedor: teléfono, correo electrónico, buzón de quejas, alerta desde el dispositivo.
	6.2 Accesibilidad	Facilidad para el usuario de comunicarse con el proveedor.
7 Antecedentes de vulneración	7.1 Descripción	Registro de eventos de vulneración y sus características.
	7.2 Compromiso de datos personales	Posibilidad de que datos personales de los usuarios fueran comprometidos.
	7.3 Notificación	Aviso a usuarios sobre el evento de vulneración.

Fuente: Elaboración propia.

5. Procesamiento de la información: Una vez reunida la información será procesada en bases de datos con software de visualización de datos.

En **segundo lugar**, y como complemento del análisis estadístico, se aplica etnografía digital para la recolección e interpretación de los datos. En sentido estricto la etnografía es "investigación inductiva-iterativa basada en una serie de métodos (…) que reconoce la función de la teoría y la del propio investigador, y que considera que los seres humanos son en parte objetos y en parte sujetos". [40]

En la etnografía digital, las principales herramientas de la etnografía tradicional se transforman para atender a las características naturales de los medios digitales. En ésta se posibilita el estudio de experiencias, eventos,

[40] O´REILLY, Karen. *Ethnographic methods*. Londres, Ed. Routledge, 2005, p.3.

prácticas, relaciones, localidades y cosas a través de “un contacto mediado, más que a través de la presencia directa”.[41] Por ello, se emplean tres herramientas etnográficas habilitadas a lo digital:

- Exploración y observación: de sitios web de las empresas, información publicitaria de los dispositivos, blogs de comunidades digitales.
- Diario de Campo: en plataforma Evernote que permite almacenar contenido audiovisual.
- Entrevistas: a expertos en la materia, presenciales y con opción a emplear un medio digital.

En **tercer lugar** se realiza un análisis histórico de la evolución occidental del concepto de privacidad a través de la legislación, los avances tecnológicos y el discurso público con la intención de encontrar patrones que permitan generar formulaciones a futuro sobre dicho concepto. En todo momento, la información derivada de los tres núcleos metodológicos será analizada bajo los enfoques teóricos de Byung-Chul Han, y los preceptos de autonomía, justicia, no maleficencia y beneficencia.

[41] PINK, Sara et al. *Etnografía digital: principios y práctica*. España, Ed. Morata, 2019, p. 19.

VII. RESULTADOS Y DISCUSIÓN

7.1. Privacidad y protección de datos.

Desde la perspectiva principialista la irrupción a la privacidad y a la protección de los datos personales constituye una violación directa a los principios de autonomía y justicia. Además, en casos concretos puede serlo también de los principios de no maleficencia y beneficencia.

Esta perspectiva fue introducida por Tom Beauchamp y James Childress, primero en las reuniones de la Comisión Nacional para la Protección de Sujetos Humanos de Investigación Biomédica y de Comportamiento en Estados Unidos de Norteamérica (1974), y después en "principios de ética biomédica" (1979) y se sustenta en los cuatro principios ya mencionados:

- Autonomía: alude a la libertad de elección y se sustenta en la libertad de la influencia controladora y la capacidad de acción intencional. Es decir, no influir en la elección de otros y asegurar las condiciones necesarias para su ejercicio libre.
- Justicia: puede interpretarse también como la distribución equitativa.
- No maleficencia: se trata, ante todo, de no hacer daño intencional al otro, respetando la integridad física y psicológica.
- Beneficencia: se refiere al "bienestar" como fin último de las acciones.[42]

Así, en los siguientes apartados del capítulo analiza la privacidad y la protección de datos desde esta perspectiva, señalando los conflictos que surgen con los principios enunciados. Primero desde las concepciones teóricas de los

[42] ARELLANO Rodríguez, José Salvador. Teoría ética para una ética aplicada. México, Universidad Autónoma de Querétaro, 2012, pp. 145-149.

mismos conceptos, y después desde la exploración de una muestra de dispositivos del internet de las cosas.

7.2. Privacidad, intimidad, confidencialidad y protección de datos

En las últimas décadas, la dicotomía de lo público y lo privado se ha empleado para definir los espacios de interacción económica, política y cultural a través de formulaciones normativas que dibujan mapas concretos de la actividad humana. Lo privado se vincula con el aislamiento y la autonomía en escenarios domésticos, familiares y sexuales; el hogar, se erige, por tanto, como la estructura principal de la vida privada y dota a los individuos de herramientas para proteger parte de sus vidas de la intervención y el escrutinio públicos.

La primera vez que se utilizó el término “privacidad” como pretensión jurídica, fue en la sentencia de un tribunal norteamericano en 1873, misma que sentó un precedente importante para que en 1890 los abogados Warren y Brandeis escribieran el artículo The Right to Privacy.

En el escrito se defendía la necesidad de proteger al individuo de la injerencia de “numerosos ingenios mecánicos” (refiriéndose al teléfono, la cámara fotográfica y la producción a gran escala de materiales impresos), que amenazaban al sujeto en un plano distinto al físico:

> *“La intensidad y complejidad de la vida, que acompañan a los avances de la civilización, han hecho necesario un cierto distanciamiento del mundo, y el hombre, bajo la refinada influencia de la cultura, se ha hecho más vulnerable a la publicidad, de modo que la soledad y la intimidad se han convertido en algo esencial para la persona; por ello, los nuevos modos e inventos, al invadir su intimidad, le producen un sufrimiento espiritual y una*

angustia mucho mayor que le pueden causar los meros daños personales".[43]

Hoy, las amenazas que suponen los aparatos que inspiraron el artículo de Warren y Brandeis son mínimas en comparación con la inmensidad de riesgos que acompañan a los sofisticados dispositivos con los que interactuamos día a día.

Para 1994, Morales Prats afirmaba que *"la preocupación por la autonomía individual, enmarcada en la escala de valores del liberalismo individualista, hace florecer en el ciudadano un sentimiento de defensa frente a las violaciones e injerencias en su vida privada"*.[44]

Las palabras de Morales Prats describen a la privacidad como un aspecto a defender en la vida de las personas, en sintonía con la definición de privacidad contenida en el Diccionario de la Real Academia Española que la describe como *"el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión"*[45]. Por otra parte, el Oxford English Dictionary define privacy como *"a state in which one is not observed or disturbed by other people"*[46] (estado de quien no es observado o molestado por otras personas).

Para la Real Academia Española el concepto contiene un carácter prescriptivo ("se tiene derecho a") y para el caso inglés es meramente descriptivo ("un estado"). Sin embargo, en ambos casos las definiciones conducen a una misma idea: la privacidad implica, necesariamente, una parte de la vida de las

[43] WARREN, Samuel. y Brandeis, Louis. The right to privacy, en Harvard law review, 1890, p.193-200.

[44] MORALES Prats, Fermin. *La tutela penal de la intimidad: privacy e informática*. Barcelona, Editorial Destino, 1994, p.17.

[45] Real Academia Española. Diccionario de la lengua española, Privacidad. Disponible en: https://www.rae.es/dpd/privacidad 10 de septiembre de 2019

[46] Oxford English Dictionary, Privacy. Disponible en: https://www.oxfordlearnersdictionaries.com/definition/american_english/privacy#:~:text=noun,I%20value%20my%20privacy. 10 de septiembre de 2019

personas libre de intromisiones, observaciones o molestias, sean estas devenidas de personas o dispositivos.

Además, de acuerdo con la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, así como la Convención Europea sobre Derechos Humanos; la privacidad es un derecho importante ya que se constituye como un facilitador fundamental de la autonomía personal, la dignidad y la libertad de expresión. En este sentido, la definición de la Real Academia Española cobra relevancia, pues se describe a la privacidad desde el lente de lo prescriptivo y no sólo de lo descriptivo.

Desde esta perspectiva, se supera la idea de privacidad como "un estado" para incorporarse a una esfera de protección positiva que aspira a:

> *"garantizar el control de la información que nos concierne y que otros conocen de nosotros, no se trata de reaccionar cuando nuestra intimidad se ha visto vulnerada, sino de exigir positivamente al Estado, deberes de tutela del derecho, y en todo caso, de garantizar facultades para la tutela y defensa de las libertades de la persona*"[47].

El derecho a la privacidad contempla al ser humano desde su perspectiva más profunda, misma que lo define y diferencia de los demás, así mismo, posibilita que el individuo decida en qué medida comparte con otros, pensamientos, sucesos, sentimientos e información, asegura una calidad mínima de vida social. De ahí que la violación a este derecho generaría una perturbación en la dignidad humana y el desarrollo individual de quien vea vulnerada su privacidad.

En palabras de Herrán Ortiz: *"el derecho a la privacidad no asienta sobre la ocultación de determinados aspectos de la personalidad del individuo al*

[47] HERRÁN Ortiz, Ana Isabel. *El derecho a la protección de datos personales en la sociedad de la información*, Cuadernos Deusto de Derechos Humanos. Bilbao, Universidad de Deusto, 2003, p.11.

conocimiento ajeno, sino sobre la necesidad de un ámbito de libertad interior, como instrumento imprescindible para el pleno desarrollo de la personalidad individual y como garantía de respeto a la dignidad personal"[48].

Es por ello que en el entorno digital en general, y el universo del IoT en particular, el derecho a la privacidad ocupa un lugar central al ser muchas las fuentes de levantamiento de datos y observación de los individuos. Para comprender este contexto, muy diferente ya al planteado por Warren y Brandeis, es necesario acompañar a la noción de privacidad con una serie de conceptos adyacentes.

Uno de estos conceptos es el de la intimidad que se refiere a un ámbito personal más restringido. La intimidad forma parte de nuestra privacidad, al tratarse de un sub-campo de la misma, por ejemplo, una cuenta bancaria contiene información personal y valiosa para el titular, pero no incluye información íntima; mientras que las relaciones afectivas y sexuales, a la vez que personales, son también íntimas.

En el caso de la intimidad el objetivo es excluir a terceros del conocimiento de estos datos, en tanto que el objetivo de la privacidad es la protección, pero también el control, en cierta forma es un proceso mucho más dinámico.

> *"las cosas privadas, al igual que las cosas íntimas, son reservadas, pero de distinta forma. Nuestra intimidad puede ser desconocida incluso para las personas más próximas, mientras que la vida privada es compartida con ellas y pretendemos que esté protegida de la mirada de quien no forma parte de nuestro entorno personal"*.[49]

[48] HERRÁN Ortiz, Ana Isabel. *La violación de la intimidad en la protección de datos personales*. Madrid, Ed. Dykinson, 1999, p.11-12.

[49] DÍAZ Rojo, José Antonio. *La privacidad: ¿Neologismo o barbarismo?*, en Espéculo Revista de Estudios Literarios. Madrid, Universidad Complutense de Madrid, 2002, p. 6. Disponible en: https://digital.csic.es/bitstream/10261/3662/1/privacidad.pdf

En segundo lugar, otro concepto aledaño al de privacidad es el de confidencialidad, mismo que *"designa la cualidad de los datos e informaciones reservados o secretos"*[50]. Implica que no pueden ser revelados sin el consentimiento del titular, pero no necesariamente competen al terreno de lo privado. Por ejemplo, la fórmula de un producto de limpieza puede ser confidencial, por interés de la empresa fabricante, pero no pertenece al plano de lo privado; por el contrario, el historial de enfermedades mentales que una clínica pueda tener de una persona, además de pertenecer al campo de lo privado (incluso íntimo), pueden configurarse como confidenciales.

Así, la confidencialidad implica un acuerdo o compromiso para no revelar la información, mientras que los datos privados pueden ser tratados en tanto no se revele la identidad del o los titulares.

En tercer lugar, el concepto de protección de datos, encuentra nexos directos y necesarios con la privacidad en una relación medio-fin. El derecho a la protección de datos tiene un carácter eminentemente procedimental ya que articula una serie de medidas que sirven como medios para garantizar privacidad al individuo.

La importancia de la protección de datos resulta irrebatible en entornos automatizados como en los que nos desarrollamos actualmente, rodeados de sensores que recogen información las 24 horas del día, con infinidad de posibilidades de tratamiento, sucesión a terceros y entrecruzamiento de datos que escapan al conocimiento de los usuarios. Por ello, "el grado de sensibilidad de las informaciones ya no depende únicamente de si afectan o no a procesos de intimidad. Hace falta más bien conocer la relación de utilización de un dato para poder determinar sus implicaciones"[51].

[50] Ídem, p. 8.
[51] DARANAS, M. (Tr). Jurisprudencia constitucional extranjera. Tribunal Constitucional Alemán. Boletín de jurisprudencia constitucional, núm. 33. España, 1984, p. 155.

Es decir, el derecho a la protección de los datos no se centra en la naturaleza íntima o no del dato, sino en la utilización, finalidad de tratamiento o posible interconexión de datos personales tratados, permitiendo así la autodeterminación informativa, al generar mecanismos que facultan al individuo para ejercer control sobre su información personal.

7.3. Sociedad transparente: el desdibujamiento de la privacidad

Definitivamente el escenario en el que hoy nos desenvolvemos, dista mucho de aquel observado por Warren y Brandeis en 1890, cuando comenzaron a cuestionarse sobre la injerencia de los nuevos aparatos en la vida de las personas. No sólo los aparatos han mutado en dispositivos más inteligentes e intrusivos, sino que también ha cambiado la forma en que nos relacionamos con ellos y el grado de aceptación de la permeabilidad de estos dispositivos en nuestras vidas. Todo parece indicar que desde 1890, a la fecha, se han seguido dos caminos distintos, cada uno con velocidades y características particulares:

El primero en el ámbito de la regulación, el derecho y recientemente la ética, que explota las incertidumbres sobre el tratamiento que dan empresas y otros particulares a los datos personales que recolectan. Dando como resultado la consolidación de la privacidad y la protección de datos personales como derechos; la incorporación de nuevos derechos como la autodeterminación informativa, los derechos ARCO y el derecho al olvido; así como el diseño y ejecución de normas legales.

La velocidad de desarrollo de esta vía ha sido relativamente lenta, además de desigual en los distintos puntos del globo. Por una parte, la Unión Europea y Estados Unidos han construido sólidas normativas en materia de privacidad y proyección de datos, y por la otra; zonas como América Latina han retrasado el diseño de sus instrumentos. En México, por ejemplo, apenas en 2010 se publicó en el Diario Oficial de la Federación la Ley Federal de Protección de Datos

Personales en Posesión de los Particulares y en 2017 la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lo anterior, frente al segundo ámbito, el del avance tecnológico acelerado y la normalización de la recogida y procesamiento de datos por parte de dispositivos en todas las áreas de nuestra vida.

En este punto, los dispositivos del IoT se han convertido en objetos de consumo altamente deseados, por sus características "inteligentes" ofrecen al usuario una vista al futuro y cierto status frente a sus pares. A cambio, el individuo ofrece grandes cantidades de información privada a través de las múltiples conexiones que estos dispositivos mantienen con la red. Sin embargo, parece contradecirse la conducta que el individuo mantiene "online" con aquella que manifiesta en el discurso y en las relaciones cotidianas "offline". No daríamos dirección y fotografías de nuestra casa a un desconocido en la calle, por ejemplo, pero sí lo hacemos de manera consciente en redes sociales y en aplicaciones estándar; y de manera un poco más inconsciente en dispositivos del IoT.

Al respecto de este segundo punto, Byung –Chul Han ha desarrollado el concepto de "sociedad de la transparencia" donde expone que se ha instalado en el discurso público una consigna de transparencia, vista ésta tradicionalmente como la rendición de cuentas que se exige a los gobiernos para que se mantengan abiertos.

Sin embargo, para el autor este no es el único aspecto de la vida social en el que se exige transparencia, es apenas la punta del iceberg. Se revelan como transparentes cosas, acciones, tiempo e imágenes, siendo quizá más evidentes estas últimas que *"se hacen transparentes cuando, liberadas de toda dramaturgia, coreografía y escenografía, de toda profundidad hermenéutica, de todo sentido, se vuelven pornográficas"*, es decir cuando existe un *"contacto inmediato entre la imagen y el ojo"*[52].

[52] HAN, Byung-Chul. *La sociedad de la transparencia*. Barcelona, Ed. Herder, 2012, p. 12.

Este contacto inmediato exige aceleración en la comunicación y procesos operacionales que aseguren la máxima velocidad, los dispositivos del IoT trabajan bajo esta premisa de inmediatez, levantan información y la procesan de manera automática para generar entornos adecuados a la medida de sus usuarios; generan imágenes para ellos.

Para el autor, la transparencia es violenta en el sentido de que "la coacción de la transparencia nivela al hombre hasta convertirlo en un elemento funcional de un sistema"[53] cuyo valor se mide "tan solo en la cantidad y la velocidad del intercambio de información"[54]. En este sentido, se aprecia a los sujetos únicamente por su valor de exposición.

Según Benjamín, para las cosas que están "a servicio del culto (…) el que existan es más importante que el hecho de ser vistas"[55], es decir, su valor depende de su existencia y no de su exposición, es así que algunos objetos culturales importantes permanecen resguardados, lejos de la vista de otros para poder preservar su existencia. Sin embargo, como ya se mencionó, en la sociedad transparente tanto personas como imágenes y experiencias son convertidas en mercancía, "han de exponerse para ser, desaparece su valor cultural a favor del valor de exposición (…), la mera existencia es por completo insignificante"[56].

El ciudadano digital se expone diariamente ante internet en su más amplio sentido, desde redes sociales, hasta sensores de IoT cuyos reflectores se encuentran siempre iluminando el andar del sujeto, contando sus pasos, midiendo su ritmo cardiaco, siguiendo los clics que da en las páginas web, escuchando su voz para predecir tendencias de consumo. Bajo este mecanismo de exposición es también explotado sistemáticamente como productor de datos y como mercancía en sí mismo.

---

[53] Ídem, p. 14.
[54] Ibídem, p. 23.
[55] BENJAMIN, Walter. La obra de arte en la era de su reproducción técnica, en Discursos interrumpidos. Madrid, Ed. Taurus, 1982, p. 20.
[56] HAN, Byung-Chul. *La sociedad de la transparencia*. Barcelona, Ed. Herder, 2012, p. 26.

Parece difícil pensar que exista la privacidad en unas sociedad cuyo imperativo hace sospechoso todo lo que no se somete a la visibilidad, que desnuda al sujeto más allá de los límites del cuerpo y "no permite lagunas de información ni de visión"[57], que insiste en verlo todo, en consumir intimidades.

Lo privado es considerado como un enemigo a erradicar, para ello se erigen discursos que legitiman la colonización de estos territorios. La seguridad, por ejemplo, ha sido utilizada ampliamente como excusa para aceptar de buena gana la invasión a la vida privada de los ciudadanos mediante la instalación de circuitos de videovigilancia, reconocimiento facial y otros dispositivos de control.

Es justo en esta aceptación, incluso deseo, incuestionable de la exposición que la sociedad de la transparencia y el control se consuman "allí donde el sujeto se desnuda no por coacción externa, sino por la necesidad engendrada en sí mismo, es decir, allí donde el miedo de tener que renunciar a su esfera privada e íntima cede a la necesidad de exhibirse sin vergüenza". Hoy por ejemplo, países como China, Corea del Sur y Japón someten su vida cotidiana a la observación de los proveedores y fabricantes de dispositivos, pero también al escrutinio de las autoridades locales y federales.

Como ejemplo, se encuentra el sistema de 'rating' con el que Pekín ha comenzado a evaluar a sus ciudadanos en este 2020. El gobierno verifica información de distintas bases de datos para generar un perfil de cada ciudadano y asignarle una calificación que podrá determinar si se tiene derecho a un crédito hipotecario, ser contratado en un empleo o si sus hijos son admitidos o no en la escuela de su elección. Todo esto soportado en información que proveen redes sociales como contactos, opinión sobre el régimen, preferencias personales; datos emanados de la navegación online tal como poder adquisitivo, compras, páginas web visitadas y clics; así como información proporcionada por dispositivos del IoT como ubicación, rutas y horarios, incluso si es que se ha pasado un semáforo en rojo.

[57] Ídem, p. 17

De acuerdo con un artículo publicado por el periódico El País, en China hay 200 millones de cámaras provistas de técnicas sofisticadas de reconocimiento facial que captan detalles pequeños como lunares, “estas cámaras dotadas de inteligencia artificial pueden observar y evaluar a todo ciudadano en los espacios públicos, en las tiendas, en las calles, en las estaciones y en los aeropuertos”[58]. Todo con la aceptación de los ciudadanos, quienes ceden su esfera privada a cambio de seguridad y bajo una normalización que no cuestiona la injerencia de terceros, al punto de que “en el vocabulario de los chinos no aparece el término esfera privada”[59].

Esto no exime a occidente, donde los procesos de observación son quizá más discretos (hasta el momento) pero existentes; donde los ciudadanos se resisten a la observación gubernamental, pero se abren y exponen a ser observados por sus dispositivos y en consecuencia por las empresas fabricantes; donde las leyes se han quedado rezagadas, minimizadas ante el rápido desarrollo de la tecnología.

Así, el globo entero habita en lo que Byung –Chul Han ha denominado ‘panóptico digital’. Para comprender mejor el concepto, es necesario rememorar el modelo tradicional de panóptico, diseñado por Jeremy Bentham a finales del Siglo XVIII como estructura carcelaria. El elemento principal de esta estructura panóptica era una torre central que permitía al vigilante observar a los prisioneros que se encontraban en celdas individuales alrededor de la torre. Este elemento arquitectónico permitía que la identidad del guardián permaneciera velada y que los prisioneros no pudieran cuando se le vigila y cuando no.

En cambio, el panóptico digital no se restringe a una estructura arquitectónica, sino que se constituye como dispositivo social, omnipresente, la

[58] HAN, Byung-Chul. La emergencia viral y el mundo de mañana. Periódico El País, 2020, Disponible en: https://elpais.com/ideas/2020-03-21/la-emergencia-viral-y-el-mundo-de-manana-byung-chul-han-el-filosofo-surcoreano-que-piensa-desde-berlin.html 21 de marzo de 2020

[59] Ídem.

vigilancia no viene desde una torre sino de todas partes, desde cada dispositivo conectado, pero también desde cada individuo de la sociedad transparente. Mientras los moradores del panóptico tradicional se sabían vigilados, quienes habitamos el panóptico digital creemos que nos encontramos en libertad, muchos años se creyó que internet era un medio de total anonimato, donde podíamos actuar sin ser vistos, hoy hemos visto pruebas de que no es así, pero de alguna manera seguimos fieles a esta vieja idea.

Mientras en el modelo de Bentham, las personas se encuentran aislados e incomunicados unos de otros, en el panóptico de Byung –Chul Han los habitantes se conectan e hipercomunican, garantizando la transparencia y colaborando de manera activa en la supervivencia del sistema, esto en la medida que ellos mismos se exhiben y desnudan como moneda de cambio para observar a otros.

En consecuencia, la sociedad de la transparencia, el panóptico digital y la exhibición pornográfica del ciudadano digital se configuran como negativas en sentido ético ya que restringen la autonomía del sujeto y aniquilan la confianza en el camino de vigilarlo todo:

> *"La confianza hace posibles acciones a pesar de la falta de saber. Si lo sé todo de antemano, sobra la confianza. La transparencia es un estado en el que se elimina todo no saber. Donde domina la transparencia, no se da ningún espacio para la confianza. (…) En una sociedad que descansa en la confianza no surge ninguna exigencia penetrante de transparencia. La sociedad de la transparencia es una sociedad de la desconfianza y la sospecha, que, a causa de la desaparición de la confianza, se apoya en el control"*[60].

[60] HAN, Byung-Chul. *La sociedad de la transparencia*. Barcelona, Ed. Herder, 2012, p. 91-92.

Además, *"la sociedad de la transparencia se despide tanto de la dialéctica como de la hermenéutica"*[61], dejando quizá toda interpretación a las máquinas, quienes construyen información a partir de la inmensidad de datos que recolectan. Sin embargo, suponer que esta masa monstruosa de datos suple la reflexión y la teoría es un camino peligroso en el que la sociedad de la transparencia se ha estado deslizando lentamente.

Por último, y aunque Byung –Chul Han no cree completamente en una era Post Privacy (desaparición completa de la privacidad), presenta un argumento poderoso y preocupante:

> *"la potente exigencia de transparencia indica precisamente que el fundamento moral de la sociedad se ha hecho frágil, que los valores morales (…) pierden cada vez más su significación. En lugar de la resquebrajadiza instancia moral se introduce la transparencia como nuevo imperativo social"*[62].

Este argumento, introduce la urgencia, no de frenar el avance tecnológico, sino de reflexionar sobre la normalización de la violación a la privacidad y de buscar mecanismos que frenen el impacto que esto tendrá en nuestras vidas y en la de generaciones venideras, donde las máquinas pueden conocernos mejor de lo que nosotros mismos nos conocemos.

Para ello, no es suficiente la formulación de leyes que se ven rebasadas rápidamente, sino que se requieren formulaciones éticas que permitan a los particulares tomar decisiones correctas en el tratamiento de los datos personales, aún cuando las leyes no se lo exijan.

[61] Ídem, p. 18.
[62] Ibídem, p. 92.

7.4. Protección de datos de dispositivos IoT en México

Los parámetros de transparencia, descritos por Byung –Chul Han son aplicables también para el territorio mexicano. En sentido amplio, son aplicables para casi cualquier rincón del planeta, en el sentido de que los dispositivos de la IoT igual recolectan información de personas que de ecosistemas (y con ello plantas, animales, cualidades del suelo, el clima y un largo etcétera de datos). Sin embargo, para fines de la presente investigación y dado que la privacidad es un derecho atribuible a los humanos, es que nos centraremos en las amenazas que los dispositivos inteligentes representan para la privacidad, en el territorio mexicano específicamente.

En primer lugar, es importante remarcar que se emplea el derecho a la protección de datos como el medio para proteger el derecho a la privacidad. Esto tiene dos implicaciones:

I. Que el término de protección de datos ha tomado un papel mucho más central en el diseño de normativas jurídicas. De tal suerte que la mayoría de legislaciones que pretenden proteger la privacidad alrededor del mundo incluyen este concepto en su título y no el de privacidad.

II. Que el término privacidad ha sido desplazado poco a poco en el marco de la sociedad de la transparencia. Así la protección de datos es quizá el último vestigio de una sociedad que, totalmente expuesta, no goza ya de una esfera privada y se ha tenido que contentar con que esos datos que han sido arrancados de sí cuenten por lo menos con parámetros mínimos de cuidado.

En este sentido, la protección de datos personales cobra un papel relevante al ser al mismo tiempo el vestigio de la privacidad y el mecanismo para resguardarla. Por ello es que más que considerarla un mecanismo jurídico, debe considerarse una herramienta ética.

En México, y en el resto del mundo, uno de los instrumentos más importantes para alcanzar la protección de los datos personales en el aviso de privacidad. Este ha sido conceptualizado por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), en su artículo 3 y 15, como un "documento físico, electrónico o de cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales" con la intención de "informar de los datos, la información que se recaba de ellos y con qué fines"[63].

El mismo documento jurídico, en su artículo 16, señala que dicho instrumento debe contener, al menos la siguiente información:

a. Identidad y domicilio del responsable que los recaba.

b. Las finalidades del tratamiento de datos.

c. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos.

d. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición (Derechos ARCO).

e. En su caso, las transferencias de datos que se efectúen.

f. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad.

g. Señalamiento expreso en caso de que se traten datos personales sensibles.

Es así que el aviso de privacidad es concebido como un documento jurídico y su configuración depende de los ordenamientos legales. Sin embargo, desde una perspectiva ética este instrumento debería ser tratado, además, como una

[63] Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Diario Oficial de la Federación. Estados Unidos Mexicanos, 2010. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

variación del consentimiento informado con los principios y aspectos que lo caracterizan.

Para la Comisión Nacional de Bioética (CONBIOÉTICA), el consentimiento informado es *"la expresión tangible del respeto a la autonomía de las personas en el ámbito de la atención médica y de la investigación en salud. El consentimiento informado no es un documento, es un proceso continuo y gradual que se da entre el personal de salud y el paciente y que se consolida en un documento"*[64] que *"más allá de ser un acto jurídico o normativo, es simplemente, un acto humano, de comunicación entre el médico y el paciente que legitima el acto médico y otorga obligaciones y derechos recíprocos"*[65].

En este sentido, el aviso de privacidad debe ser concebido también como una expresión del respeto a la autonomía de los usuarios y como un proceso que trasciende al acto jurídico para convertirse en una acción de comunicación y confianza entre el titular y el responsable de los datos.

A continuación se analizan algunas variables de los datos recogidos por 94 dispositivos IoT que se comercializan en México, así como de sus avisos de privacidad. En cada rubro se analiza el contenido del aviso de privacidad y su contraste con la legislación mexicana y los principios de la figura de consentimiento informado.

[64] CONBIOÉTICA. Consentimiento informado. Disponible en: http://www.conbioetica-mexico.salud.gob.mx/interior/temasgeneral/consentimiento_informado.html 18 de septiembre 2019

[65] LEE, Gabriel. *El consentimiento válidamente informado en la práctica médica*, en Revista CONAMED, Vol. 9, Nº 3. México, Comisión de Arbitraje Médico, 2004, p. 3.

7.4.1. Datos recolectados

Uno de los objetivos principales del consentimiento informado es que el personal de salud brinde al paciente información, de calidad y cantidad suficientes, respecto de la naturaleza de su enfermedad, el procedimiento diagnóstico y terapéutico que se planea utilizar, los riesgos y beneficios de estos, así como las posibles alternativas.

Por tanto, el aviso de privacidad deberá seguir la misma lógica y explicar en primer plano qué datos, no solo personales, recolecta el dispositivo. Esto en respeto a la autonomía del sujeto, que implica la facultad de gobernarse a si mismo y de tomar las decisiones que lo involucran, pero también de negarse a determinadas acciones si es que no le parecen convenientes[66].

En la exploración de dispositivos IoT comercializados en México se encontró (Ver Gráfico 1) que el dato personal más recopilado es el correo electrónico, seguido del teléfono, el nombre y la dirección. Sin embargo, también se detecta la recopilación de datos más sensibles, de carácter biométrico (la voz, huellas dactilares, rasgos faciales), médico (datos de ciclo menstrual, hábitos de sueño, enfermedades mentales, uso de medicamentos, médico tratante), sociales (religión, preferencia sexual, número de personas en la familia -particularmente número de hijos-, estados de ánimo) y sobre le lugar de residencia (planos del hogar o lugar donde se encuentre el dispositivo, así como el nivel y tipo de actividad en la misma).

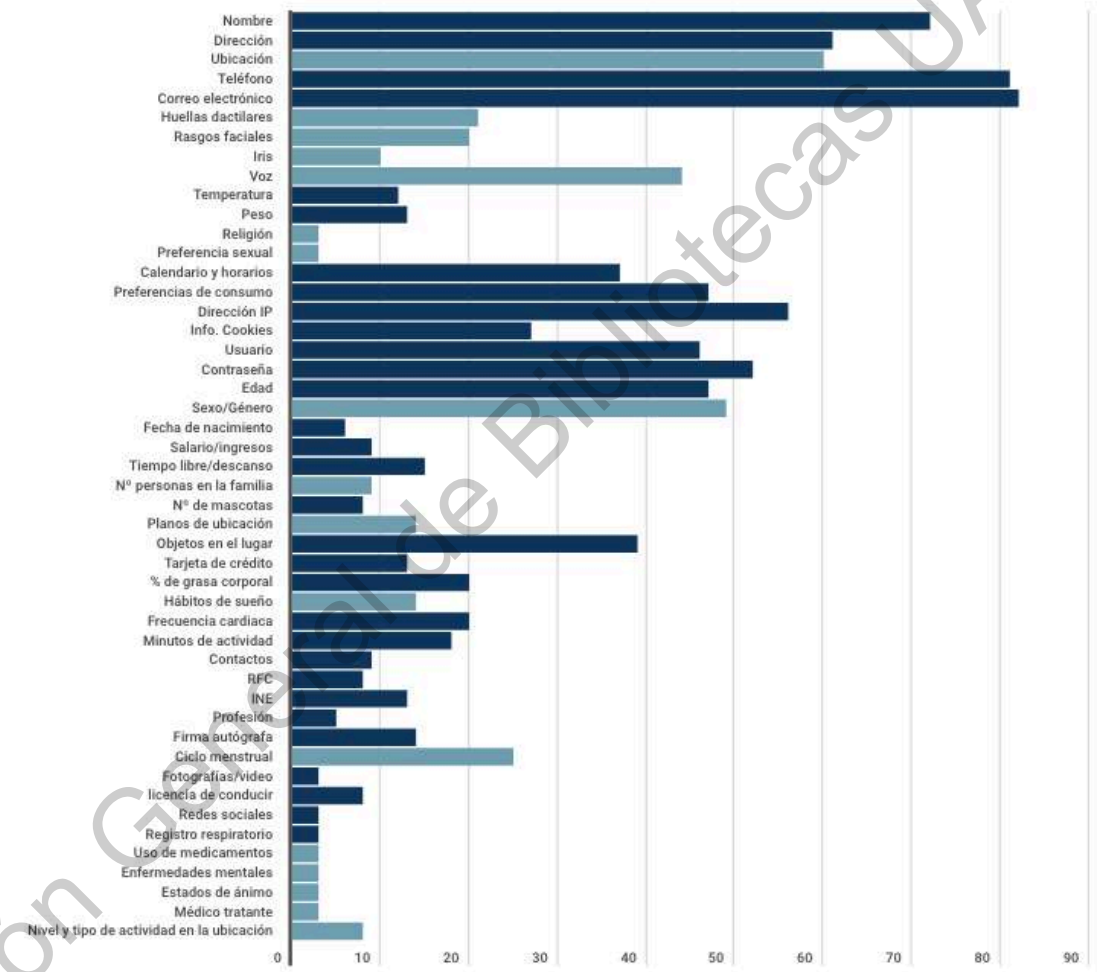
Derivado de este análisis se detectan las siguientes observaciones:

a) La LFPDPPP, en su artículo 16, donde se enuncian los aspectos mínimos que debe contener el aviso de privacidad no incluye como elemento básico la lista de datos personales recolectados.

[66] BEAUCHAMP, Tom. y James Childress. *Principles of Biomedical Ethics*, 5ta edición. Nueva York, Ed. Oxford University Press, 2001, p. 57-112.

b) El 100 por ciento de las empresas cuentan con un aviso de privacidad genérico, que incorpora sus dispositivos, sucursales y página web.

Gráfico 1. Datos recolectados por dispositivos IoT en México.



Fuente: Elaboración propia.

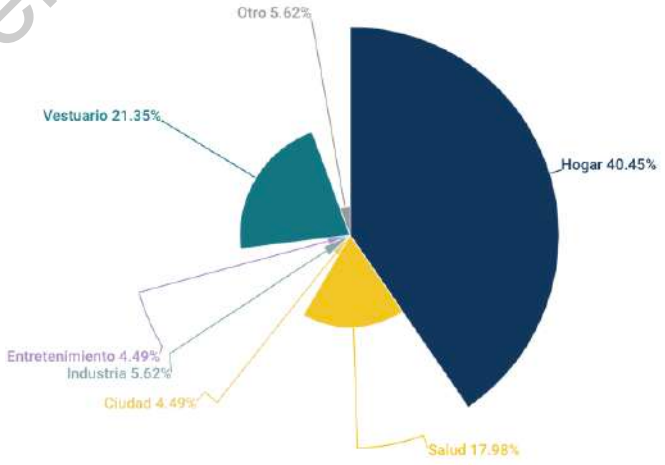
c) Esto genera confusión e imprecisión en el usuario, ya que resulta difícil identificar cuáles son los datos recolectados sólo por el dispositivo. Esta

situación se agrava cuando se trata de empresas que manejan una gran diversidad de dispositivos, que recogen variedades muy dispares de datos unos de otros.

d) Por lo menos 43 por ciento de las empresas analizadas no enuncian la totalidad de datos recolectados por el dispositivo en su aviso de privacidad. Suele usar frases como “los datos personales recolectados”, sin especificar cuáles son; o mencionar los grupos de datos “demográficos, biométricos, financieros”, sin aclarar cuales se están tratando particularmente.

Esto implica el incumplimiento a uno de los elementos más importantes del consentimiento informado, el de brindar información clara, veraz, suficiente, oportuna y objetiva, lo que resulta preocupante, ya que por lo menos el 40 por ciento de estos dispositivos se encuentran en el hogar (Ver Gráfico 2).

Gráfico 2. Sector de aplicación de los dispositivos IoT en México.



Fuente: Elaboración propia.

7.4.2. Tipología y proporcionalidad de los datos.

La definición más difundida de datos personales es “cualquier información concerniente a una persona física identificada o identificable”, es esta misma definición la que se recupera en el Art. 3 de la LFPDPPP. Los elementos que componen esta definición son reiterativos en los distintos cuerpos normativos de protección de datos alrededor del mundo, por ejemplo:

Los Estándares de Protección de Datos Personales para los estados Iberoamericanos indican, en el inciso c) del artículo 2.1 que el dato personal es “cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo”.

El Convenio 108 del Consejo de Europa para la Protección de Personas con respecto del Tratamiento Automatizado de Datos de Carácter Personal lo define como “cualquier información relativa a una persona física identificada o identificable”.

Es así, que el concepto se compone de cuatro elementos esenciales:

- Cualquier información: es decir, que puede esta expresada en cualquier formato (numérica, acústica, gráfica o cualquier otro tipo) y ser de carácter objetivo o subjetivo.
- Concerniente: la información concierne a una persona cuando se refiere a ella. Para cumplir con este criterio el GAT29 (Grupo de Trabajo del Artículo 29), considera que debe haber un elemento de contenido, finalidad o resultado. El elemento de contenido describe la relación directa entre el dato y la persona; la información se refiere a esa persona. El elemento de finalidad surge cuando es probable que el dato se utiliza, o es probable que se utilice, para evaluar, tratar de determinada manera o influir en la situación o comportamiento. El elemento resultado se materializa cuando es probable que su uso repercuta en los derechos e intereses de la

persona[67]. En este sentido, hay datos que fácilmente se pueden identificar como personales, pero habrá otros cuya identificación dependa de las circunstancias.

- Persona física: excluye a las personas morales y se limita a personas individuales, humanas, esto al tratarse de derechos humanos (derecho a la privacidad y a la protección de datos personales).
- Identificada o identificable: es decir cuando la identidad de una persona "pueda determinarse, directa o indirectamente, mediante cualquier información. No se considera persona física identificable cuando para lograr la identidad de ésta se requieran plazos o actividades desproporcionadas".

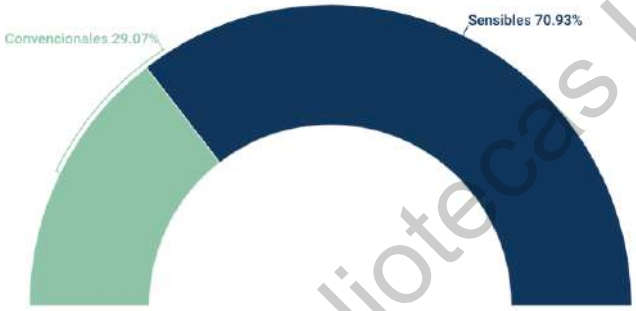
Ahora bien, los datos personales pueden clasificarse de acuerdo al área personal a la que pertenecen, por ejemplo; datos biomédicos, biométricos, demográficos, fiscales, etc. Pero también pueden clasificarse de acuerdo al grado de intimidad y especificidad, en este sentido, se dividen en datos personales convencionales y datos personales sensibles. Estos últimos son conceptualizados por la LFPDPPP como "aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida, pueda dar origen a discriminación o conlleve a un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual"[68].

En el análisis realizado a dispositivos IoT comercializados en México, se identificó que el 71 por ciento de las empresas recolectan datos sensibles (Ver

[67] INAI. *Diccionario de protección de datos personales, conceptos fundamentales.* México, Instituto Nacional de Acceso a la información, 2019, p. 214.
[68] Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Diario Oficial de la Federación. Estados Unidos Mexicanos, 2010. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Gráfico 3). De ellas, ninguna incluyó en su aviso de privacidad un señalamiento expreso manifestando que sus dispositivos levantan este tipo de datos.

Gráfico 3. Tipo de datos personales recolectados.

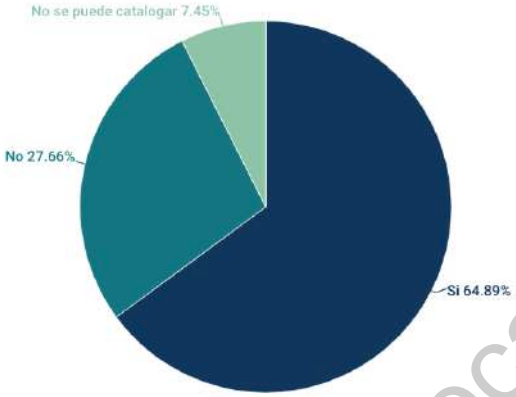


Fuente: Elaboración propia.

Además, tres empresas incluyeron un enunciado exponiendo que no recogían datos sensibles, aún cuando las propias descripciones del producto (contenidas en documentos distintos al aviso de privacidad) dejaban ver que sí lo hacían.

Por otra parte, respecto de la proporcionalidad entre los datos recolectados por el dispositivo y las funciones del mismo, se encontró que 30 por ciento de las empresas recogen información desproporcionada (ver Gráfico 4). Es decir, la información que registran y gestionan los dispositivos, misma que es compartida con la empresa proveedora excede la necesaria para la correcta operación del dispositivo.

Gráfico 4. Proporcionalidad de datos recolectados.

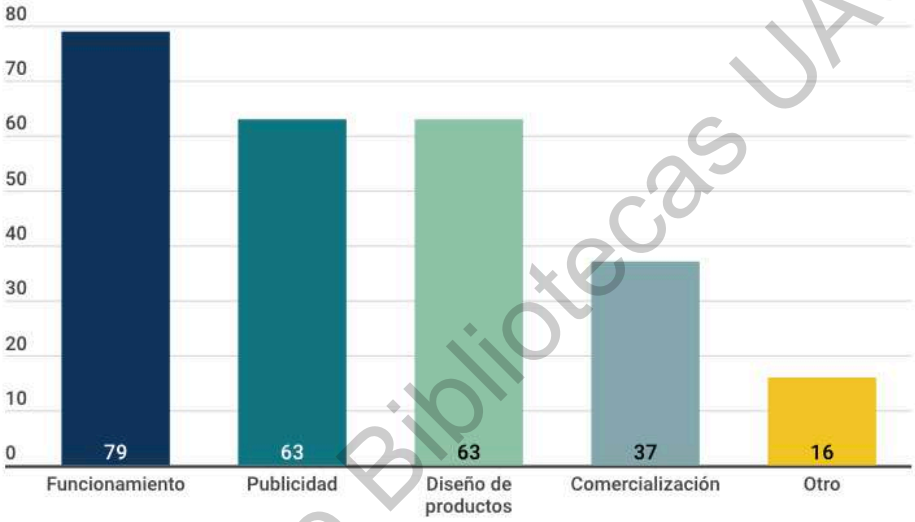


Fuente: Elaboración propia.

Por ejemplo, el robot limpiador N recoge información como planos de la casa y mapeo de objetos en el espacio, datos que aunque sensibles son necesarios para el funcionamiento operativo del producto. Sin embargo, excede los límites de la proporcionalidad al recoger datos relativos a la profesión del usuario, personas en el núcleo familiar y patrones de voz, al no ser necesarios para su funcionamiento.

La información del usuario, además de ser empleada para el funcionamiento y operación del dispositivo, también es tratada con otros fines particulares de las empresas (ver Gráfico 5), particularmente para fines de publicidad y diseño de nuevos productos.

Gráfico 5. Aplicaciones del tratamiento de datos personales.



Fuente: Elaboración propia.

Derivado de este análisis se detectan las siguientes observaciones:

a) La definición de datos personales sensibles que ofrece la LFPDPPP resulta ambigua al no dejar claro el concepto. Además, la enunciación de ejemplos, en lugar de ser descriptiva, resulta limitativa. Es pertinente aclarar, como lo hace la Ley General de Protección de datos Personales en Posesión de Sujetos Obligados, que la lista de ejemplos "no es limitativa".

b) Es importante considerar, tal como se hace para el consentimiento informado, una lista de casos obligatorios (en este caso de datos sensibles) donde se tenga que señalar, en el aviso de privacidad, de manera expresa que se están tratando este tipo de datos.

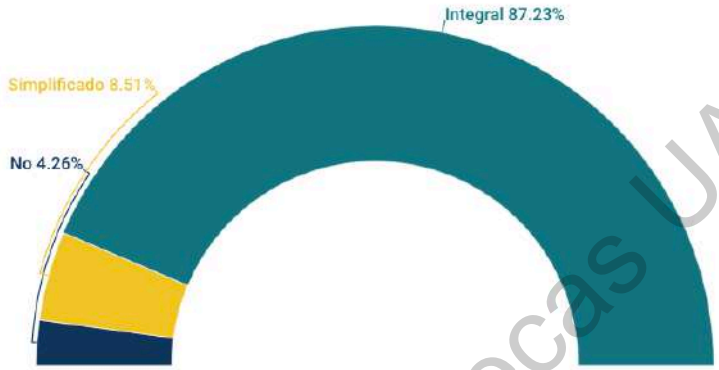
c) Se detectó un número significativo de dispositivos diseñados para niños y que por lo tanto recaban información principalmente de ellos. Aun cuando estos dispositivos especifican en su aviso de privacidad que se recolecta la información sólo con el consentimiento de un padre o tutor, resulta imperante que todo dato relacionado con un menor sea catalogado y tratado como dato sensible.

d) Se registraron 27 casos donde el responsable de la información manifiesta frases ambiguas o abiertas respecto del uso de los datos y el tiempo que los empleará, por ejemplo: "y para otros fines internos", "tanto tiempo como sea necesaria para nuestros intereses comerciales". Este tipo de frases facilitan la opacidad, entorpecen la rendición de cuentas y pueden ser obstáculos para el ejercicio del derecho a la protección de datos, ya que generan lagunas que pueden ser aprovechadas por las empresas para lucrar con los datos personales. Dicha situación contraviene el objetivo del consentimiento informado de brindar información clara, veraz y objetiva.

7.4.3. Contenido del aviso de privacidad.

A pesar de que, el aviso de privacidad es un requerimiento legal que marca la LFPDPPP para todos aquellos particulares que recojan y gestiones datos personales, se detectaron cuatro empresas que no cuentan con él, mismas que representan poco más del cuatro por ciento de total (Ver Gráfico 6). Adicionalmente, 8.5 por ciento de los particulares cuentan sólo con aviso de privacidad simplificado, que resume pero no suple al aviso de privacidad integral. Esto quiere decir, que 12 por ciento de los particulares se encuentra violando, de manera directa, el derecho a la protección de datos de sus usuarios al no poner a su disposición el aviso integral de privacidad, herramienta principal para el ejercicio de dicho derecho.

Gráfico 6. Existencia de aviso de privacidad.



Fuente: Elaboración propia.

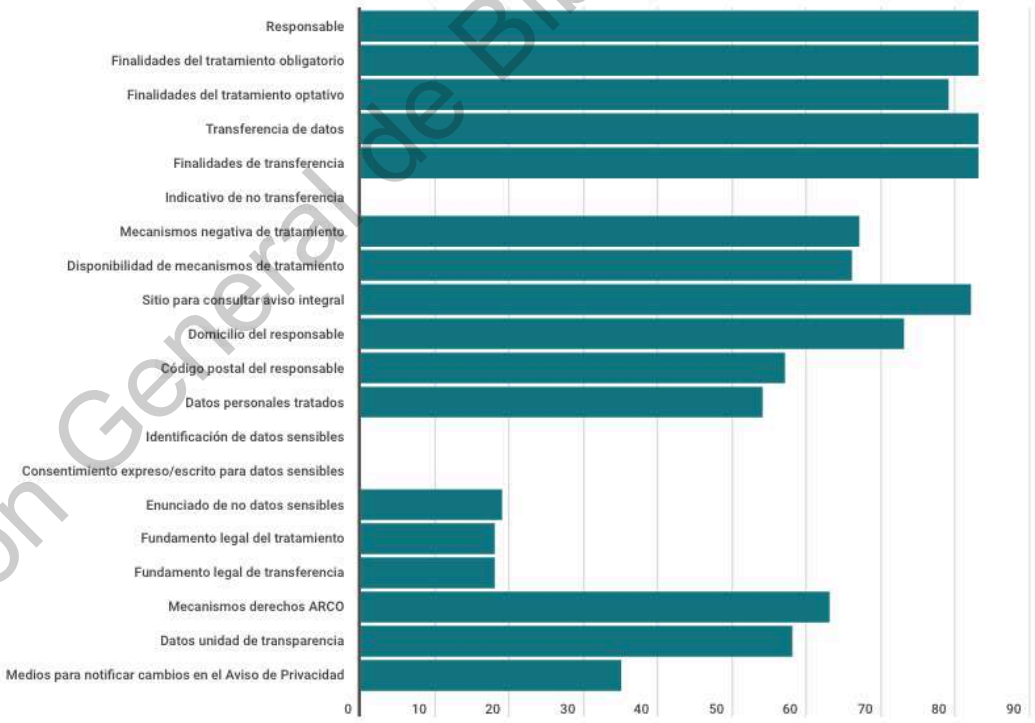
En cuanto a las secciones o elementos que componen un aviso integral de privacidad, se retoman los expuestos por el Instituto Veracruzano de Acceso a la Información y Protección de Datos Personales:

- Responsable.
- Finalidades de tratamiento obligatorio.
- Finalidades de tratamiento optativo.
- Transferencia de datos.
- Finalidades de las transferencias.
- En su caso, indicativo de no transferencia.
- Mecanismos para la negativa de tratamiento.
- Disponibilidad de los mecanismos de negativa de tratamiento.
- Sitio para consultar el aviso de privacidad integral.
- Domicilio del responsable.
- Código postal del responsable.
- Datos personales que serán sometidos a tratamiento.
- Identificación de datos sensibles.
- Consentimiento expreso y escrito para datos sensibles.

- Fundamento legal del tratamiento de datos personales.
- Fundamento legal de la transferencia de datos personales.
- Mecanismos, medios y procedimientos para el ejercicio de los de derechos de acceso, rectificación, cancelación y oposición (ARCO).
- Datos de la unidad de transparencia.
- Medios a través de los cuales el responsable comunicará a los titulares los cambios en el aviso de privacidad[69].

En el Gráfico 7 se puede observar la medida en que los particulares que comercializan productos de la IoT, en México, cumplen con estos criterios.

Gráfico 7. Contenido de avisos de privacidad.



Fuente: Elaboración propia.

[69] IVAI (2018). Guía para elaborar avisos de privacidad. México, Instituto Veracruzano de Acceso a la información y Protección de Datos Personales, 2018, pp. 3-6.

Puede observarse que no todas las empresas cumplen con criterios tan básicos como lo es la enunciación del responsable. Sin embargo, en la mayoría de los criterios de observa un cumplimiento arriba del 60%, tal es el caso de; responsable, finalidades de tratamiento obligatorio y optativo, transferencia y sus finalidades, mecanismos de tratamiento y su disponibilidad, sitio del aviso de privacidad integral, domicilio del responsable y mecanismos para el ejercicio de derechos ARCO.

Por el contrario, se identifica una baja incidencia en la identificación de datos sensibles, o en su caso la enunciación de no tratamiento de estos datos que, como se explicó con anterioridad, representa un grave problema ya que la mayoría de dispositivos sí recolectan datos sensibles sin embargo estos no son mencionados o identificados en los avisos de privacidad.

Además, se presenta una baja recurrencia en los fundamentos legales de tratamiento y transferencia que puede deberse a que la gran proporción de dispositivos analizados pertenecen a empresas extranjeras que cuentan con avisos de privacidad generales para toda la empresa sin importar el país en que se venda el producto

Derivado de este análisis se detectan los siguientes puntos:

a) Es necesario que las Entidades Federativas y la Federación homologuen los criterios mínimos que debe contener un aviso de privacidad, ya que la ley federal establece un número menor de elementos.

b) El aviso de privacidad es la herramienta principal para el ejercicio del derecho a la protección de datos, por lo que el Estado debe incentivar su existencia más allá de la publicación de leyes. No debe ser aceptable que operación de empresas que recolectan información personal sin contar con un aviso de privacidad que permita informar a sus usuarios y generar un compromiso con ellos.

c) El medio más utilizado para notificar sobre las actualizaciones al aviso de privacidad, es la propia actualización del aviso en la página

oficial del producto. Este mecanismo resulta infértil ya que los usuarios difícilmente verificarán las páginas web tras adquirir su producto. Es por ello que las empresas deben optar por mecanismos más cercanos como el envío de un correo electrónico al usuario o una notificación el dispositivo, esto con la intención de mantener informado al titular de los derechos.

7.4.4. Lenguaje, modalidad y accesibilidad del aviso de privacidad.

De acuerdo con Simón-Lorda, el consentimiento informado se sustenta en la voluntariedad y por ello los planteamientos deben ser hechos con claridad, con información transmitida en cantidad suficiente y comprensible[70]. Por ello la forma en cómo se presenta el aviso de privacidad puede influir en la comprensión que el usuario tenga, influyendo en sus decisiones e incluso coartando su autonomía.

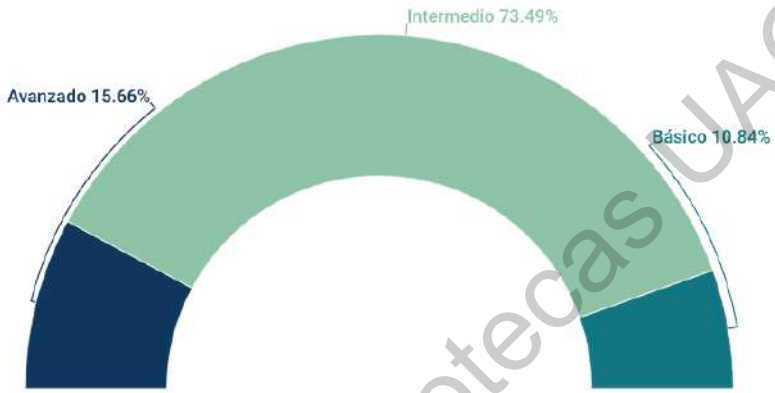
En este sentido, el 96% de los avisos de privacidad revisados se encuentran disponibles en formato digital y 4% en físico. En general, estos formatos no representan mayor dificultad para el usuario, sin embargo, se detectaron algunos casos en que la extensión del documento superaba las 25 páginas, situación que puede desincentivar su revisión y comprensión.

Además, se analizó el lenguaje de los avisos de privacidad, catalogándolo de la siguiente forma:

- Avanzado: se constituye en su mayoría por conceptos técnicos y legales de difícil comprensión.
- Intermedio: comprensible con conocimientos técnicos y legales básicos.
- Básico: comprensible sin conocimientos técnicos ni legales.

[70] SIMÓN-LORDA, Pablo. *El consentimiento informado y la participación del enfermo en las relaciones sanitarias*. Madrid, ed. Triastela, 1999.

Gráfico 8. Lenguaje de avisos de privacidad.



Fuente: Elaboración propia.

Tal como se observa en el Gráfico 8, sólo el 10.8 por ciento cuenta con avisos de privacidad comprensibles para cualquier individuo, sin necesidad de contar con conocimientos técnicos y legales. La mayor proporción (73.4%), ha formulado estos documentos con un lenguaje intermedio que requiere del manejo de algunos conceptos técnicos y legales básicos, es decir, no comprensible por todos, pero con cierto grado de dominio para las generaciones recientes o quienes cuenten con educación media superior o superior sin importar el área.

Sin embargo, existe también un 15.6 por ciento que ha formulado sus avisos de privacidad con una gran carga de elementos jurídicos y técnicos, además de ser documentos por lo general extensos. Estos documentos son comprensibles solo para un pequeño sector especializado que cuenta con estos conocimientos de manera previa, habitualmente por el sector laboral en el que desarrollan.

Sumado a lo anterior, la facilidad o dificultad con que el usuario pueda acceder al aviso de privacidad marca un hito importante. Por una parta, la LFPDPPP en su artículo 17, marca que *"el aviso de privacidad deberá ser facilitado en el momento en que se recaba el dato"*[71]. Y por otro lado, la CONBIOÉTICA dice a propósito del consentimiento informado, que este debe ser otorgado con las condiciones necesarias para que se ejerza el derecho a decidir[72].

En el caso de la recolección de datos personales por página web, formularios, encuestas y otras modalidades convencionales resulta oportuno que el aviso de privacidad se emita cuando el dato está por ser recolectado, sin embargo, en el caso de los dispositivos de la IoT, no es para nada pertinente pues el individuo se encontrará ya con el producto en su hogar, oficina, cuerpo o cualquier otro escenario. En este sentido, el aviso de privacidad debe ser facilitado en el momento en que el usuario se encuentra decidiendo si adquirirá o no el producto, de tal forma que esta información pueda ser de utilidad en el proceso de toma de decisiones.

Es por ello que se catalogó la accesibilidad del aviso de privacidad de la siguiente manera:

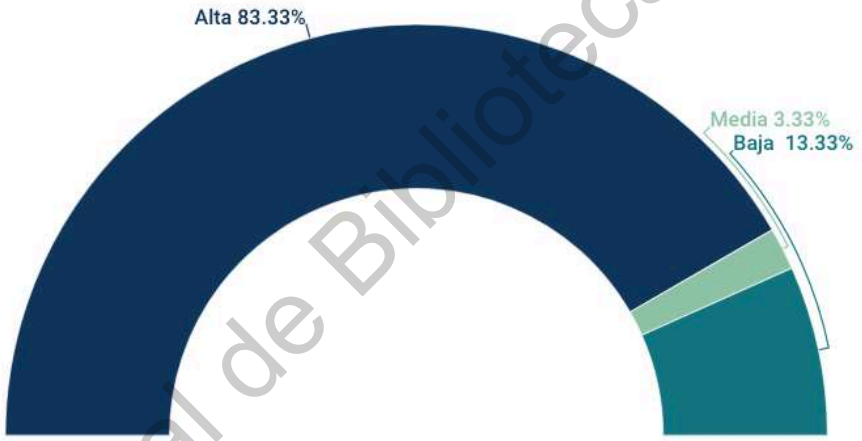
- Alta: Disponible y visible antes de adquirir el producto, es decir, se encuentra en la página principal del producto.
- Media: Disponible pero poco visible antes de adquirir el producto, es decir, no se encuentra en la página principal del producto y requiere una búsqueda más exhaustiva.
- Baja: Disponible hasta adquirir el producto.

[71] Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Diario Oficial de la Federación. Estados Unidos Mexicanos, 2010. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

[72] CONBIOÉTICA. Consentimiento informado. Disponible en: http://www.conbioetica-mexico.salud.gob.mx/interior/temasgeneral/consentimiento_informado.html 18 de septiembre 2019

Respecto a ello, se identificó que más del 80 por ciento de las empresas de IoT en México cuentan con accesibilidad alta, sin embargo 13.3 por ciento del total solo tienen disponible el aviso de privacidad hasta que el usuario adquiere el producto. Situación que no contraviene la ley pero que entorpece la toma de decisiones y por tanto el espíritu del consentimiento informado.

Gráfico 9. Accesibilidad de avisos de privacidad.



Fuente: Elaboración propia.

Como producto de este análisis se proponen las siguientes observaciones:

a) Como práctica de compromiso con la privacidad de los usuarios, las empresas pueden fomentar la producción de avisos de privacidad audiovisuales que favorezcan la comprensión. Por ejemplo, Google ha generado versiones animadas de algunas secciones de su aviso de privacidad que contienen conceptos más complejos y difíciles de comprender.

b) La legislación actual se encuentra desactualizada frente a la irrupción de los dispositivos de la IoT en la vida cotidiana, es evidente que deben modificarse aspectos que impiden el pleno ejercicio del derecho a la

protección de datos, tal es el caso del momento previsto para facilitar el aviso de privacidad.

7.4.5. Consentimiento

El consentimiento se sustenta en la libertad de elección y la autonomía del sujeto. De acuerdo con la CONBIOÉTICA, el consentimiento en el Consentimiento informado debe ser expresado y comprobado por escrito, además de dar la posibilidad de no otorgarlo[73].

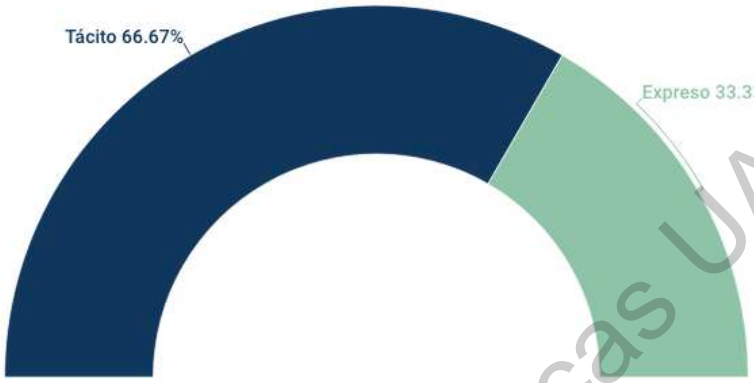
La LFPDPPP establece que el tratamiento de datos personales está sujeto al consentimiento de su titular, para ello contempla dos tipos de consentimiento: expreso y tácito. Respecto del primero expresa que se configura "cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos". En cuanto al segundo, será entendido "cuando el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición"[74].

En este sentido se encontró que el 66.6 por ciento de los particulares (ver Gráfico 10), que cuentan con aviso de privacidad, optan por el consentimiento tácito, es decir se restringen a su publicación, dejando toda la responsabilidad al sujeto. Esto propicia que algunos usuarios, sobre todo los más alejados de estos temas, no conozcan los avisos de privacidad y se considere su consentimiento sin haberlo ejecutado realmente.

[73] CONBIOÉTICA. Consentimiento informado. Disponible en: http://www.conbioetica-mexico.salud.gob.mx/interior/temasgeneral/consentimiento_informado.html 18 de septiembre 2019

[74] Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Diario Oficial de la Federación. Estados Unidos Mexicanos, 2010. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Gráfico 10. Modalidades del aviso de privacidad.



Fuente: Elaboración propia.

De 33.3 por ciento que contempla un consentimiento expreso, 20 por ciento lo realiza por medio de firma autógrafa y 80 por ciento a través de una verificación de casilla. En el primer caso, se encuentran dispositivos de salud que recogen información altamente sensible del sujeto, por ejemplo pastillas inteligentes que monitorean niveles de medicamento y enfermedades mentales, por lo que resulta lógico que busque que sus usuarios comprendan de manera cabal los términos de privacidad.

Por otro lado, en el segundo caso donde se expresa el consentimiento a través de la verificación o marcaje de una casilla, se encuentran algunos dispositivos que requieren instalar una aplicación en el celular y una vez instalada muestran al usuario el mismo aviso de privacidad disponible online, para que el usuario pueda consultarlo de nuevo y expresar su consentimiento.

Por último, el 96 por ciento de los avisos examinados incluyen la opción de revocar el consentimiento, así como los términos y mecanismos para realizar el proceso. Sin embargo, un 4 por ciento no incluye de manera clara la opción de revocación y un 26 por ciento que no menciona los mecanismos por los que el usuario se puede negar al tratamiento de sus datos.

Como producto de este análisis se proponen las siguientes observaciones:

a) Considerando que el consentimiento debe ser informado no debe tomarse la simple disponibilidad o publicidad del aviso de privacidad como consentimiento tácito, sobre todo tomando en cuenta que el usuario puede no conocerlo o no entenderlo.

b) La suma de los factores 'consentimiento tácito' más 'falta de mecanismos para revocación' constituyen un peligroso bache para los usuarios, ya que si de manera inicial no se encontraba informado de que estaba dando su consentimiento con el simple hecho de adquirir el producto y además carece de vías para lograr que sus datos no sean tratados, el usuario se encontrará en un camino sin salida que le impide ejercer el derecho a la protección sus datos personales.

c) Si al punto anterior se le suma que la empresa que provee el dispositivo se encuentra en otro país, el escenario se torna aún más complicado, la como se explora en la siguiente sección.

7.4.6. Comunicación con el usuario

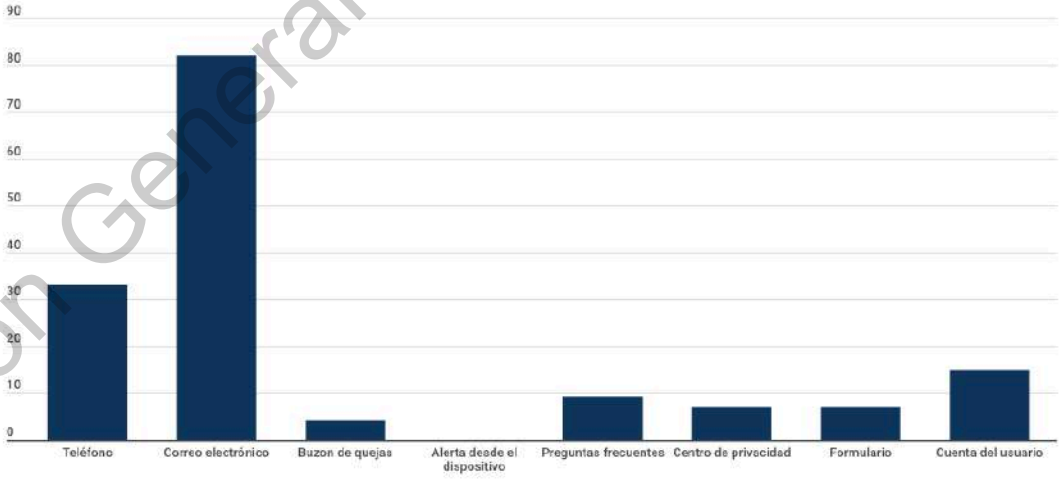
Un elemento sumamente importante para el consentimiento informado es la comunicación entre médico y paciente, por lo que, aplicado al terreno de la privacidad, podríamos decir que resulta imperante una comunicación efectiva, fluida y de confianza entre el titular de los derechos y el responsable de los mismos. Por esta razón es significativo analizar los mecanismos que las empresas proveedoras de IoT establecen para formar y fomentar el lazo de comunicación con sus usuarios.

En este sentido, y como puede observarse en el gráfico 11, el mecanismo que más empresas han habilitado es el correo electrónico. En segundo lugar, aunque con una diferencia significativa respecto del primero, se encuentra el teléfono. Ambos mecanismos tradicionales de comunicación no solo en este

campo, sino en la vida social en general. Sin embargo, en las pruebas realizadas, un 19 por ciento de particulares no respondieron los correos electrónicos y un 8 por ciento de los teléfonos no se encontraban habilitados o pertenecían a otro titular.

En todos los casos anteriores, la dirección del proveedor pertenecía a otro país, por lo que sus usuarios radicados en México tendrían complicaciones para comunicarse con ellos y probablemente verían limitado también su derecho a la protección de sus datos personales, al no contar con mecanismos confiables que les permitan mantenerse en contacto con la empresa, exponer dudas o tratar asuntos relacionados con su privacidad.

Gráfico 11. Mecanismos de comunicación entre titular y responsable.



Fuente: Elaboración propia.

Además, se hace uso de otros mecanismos de comunicación que pueden resultar más efectivos para el usuario, por ejemplo bancos de preguntas frecuentes donde el titular puede resolver dudas comunes y generales; o el formulario, donde a través de preguntas simples se envían formatos de dudas que son devueltas en espacios cortos de tiempo.

Sin embargo, quizá dos de las herramientas más flexibles y sofisticadas sean el centro de privacidad destinado a resolver dudas especializadas y la cuenta del usuario, donde el titular de los datos puede hacer modificaciones directas de acuerdo con sus preferencias de privacidad y en algunos casos puede interactuar vía chat con los asesores del centro de privacidad.

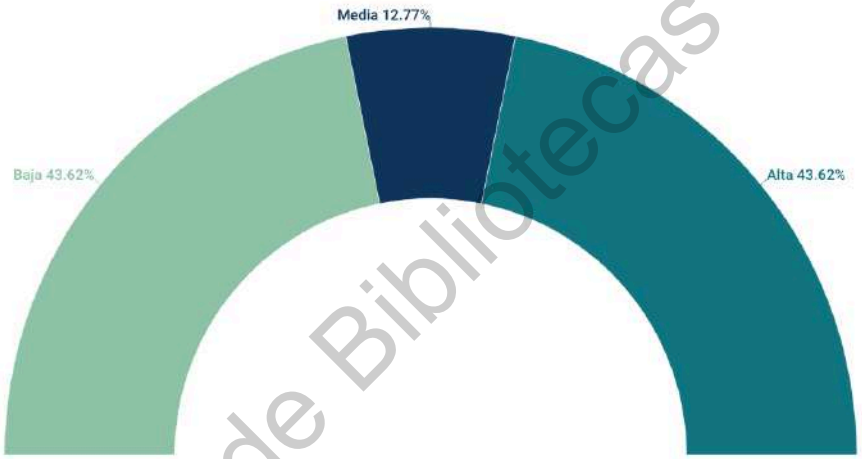
A pesar de la puesta en marcha de mecanismos efectivos por algunas empresas, no todas se encuentran en la misma sintonía, ni cuentan con los mismos recursos humanos y tecnológicos para poder brindar los mismos servicios en esta materia. Es por ello que se generó la siguiente categorización para catalogar la accesibilidad y respuesta de los medios de comunicación:

- Baja: con sólo una vía de contacto, cuya gestión depende del proveedor.
- Media: más de una vía de contacto con gestión dependiente del proveedor.
- Alta: una o más vías de contacto dependientes del titular de los datos personales.

Respecto a este nivel de accesibilidad y respuesta, el 43. 6 por ciento se encuentra en un nivel alto (Ver Gráfico 12), lo que quiere decir que cuentan con más de una vía de contacto que depende absolutamente de la iniciativa y gestión del titular, tal es el caso del banco de preguntas frecuentes y el perfil de la cuenta de usuario. Sin embargo, en la misma proporción (43.6%) se presenta un grupo de proveedores de IoT cuyo nivel de comunicación es bajo, es decir, sus usuarios

cuentan con recursos limitados para comunicar dudas o resolver procedimientos relacionados con su privacidad.

Gráfico 12. Mecanismos de comunicación entre titular y responsable.



Fuente: Elaboración propia.

7.4.7. Antecedentes de vulneración y medidas de seguridad

Por último, se registró que 38 de los 94 dispositivos analizados, es decir el 40 por ciento, se han visto involucrado en algún evento de vulneración cibernética, principalmente del tipo Zero Day (Ver tabla 4) que explota vulneraciones, no conocidas públicamente, de los sistemas o dispositivos. De ellos, en 35 se vieron comprometidos los datos y solo en 6 se notificó a los usuarios acerca del evento de vulneración, los riesgos para sus datos personales y los mecanismos para acceder a más información.

Tabla 4. Eventos de vulneración registrados.

Tipo	Descripción	Eventos
Spear-phishing	Envío de correos electrónicos a individuos específicos que contengan un archivo malicioso.	2
Zero day	Explotación de vulnerabilidades no conocidas públicamente a sistemas de empresas específicas.	30
Subversión de cadena de suministro	Atacar un equipo de software antes de que sea entregado a una organización.	0
Phising	Envío de correos electrónicos a un gran número de individuos pidiendo información sensible o alentándolos a entrar a una página con código malicioso.	3
Ransomware	Diseminación de malware enfocado a extorsionar empresas e individuos.	0
Denial of service	Utilización de código malicioso para dirigir a computadoras infectadas a abrumar un sitio o servicio de red, afectando su funcionamiento.	0
Ciber hactivismo	Utilización de bots que simulan medios legítimos, redes sociales y otras herramientas para manipular la opinión pública e influir sobre la toma de decisiones de grupos. [75]	3

Fuente: Elaboración propia.

[75] McKinsey&Company. *Perspectiva de ciberseguridad en México*. México, Consejo Mexicano de Asuntos Internacionales, 2018, p. 17.

Esto quiere decir que sólo el 17 por ciento de las empresas que sufrieron ataques de vulneración a los datos personales respetaron el derecho a la información en que se sustenta el consentimiento informado. El otro 83 por ciento, además de violar este derecho limitaron la libertad de elección y por lo tanto la autonomía del sujeto al impedirle al usuario conocer información que pudiera influir en sus elecciones.

Al tener información sobre eventos de vulneración, el titular de los datos personales puede decidir sobre su configuración de privacidad, el ejercicio de alguno de los derechos ARCO o incluso puede resolver anular su relación con la empresa o dejar de usar el dispositivo.

Al respecto, la LFPDPPP en su artículo 20 menciona que:

> *"las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos"*[76].

Esta disposición, formulada para garantizar el derecho a la privacidad y a la protección de datos personales es incapaz de llegar a sus objetivos en el sentido de que deja a discrecionalidad del responsable del tratamiento determinar la gravedad del evento, y de acuerdo con esa valoración decidir si se notifica o no al titular.

Por otro lado, la mayoría de ordenamientos internacionales para la protección de datos, entre ellos la LFPDPPP, el Convenio 108 del Consejo de

[76] Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Diario Oficial de la Federación. Estados Unidos Mexicanos, 2010. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Europa para la Protección de Personas con respecto del Tratamiento Automatizado de Datos de Carácter Personal y los Estándares de Protección de Datos Personales para los estados Iberoamericanos, consideran que deben existir medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra tratamientos no autorizados, así como pérdida, daño o alteración.

Las medidas administrativas son elementos o acciones enfocados principalmente en los roles y responsabilidades del personal que interviene en algún punto del ciclo de tratamiento de datos personales[77]. Algunos ejemplos pueden ser: contratos y acuerdos de confidencialidad; programas de concientización y capacitación sobre la relevancia de la privacidad y la protección de datos; así como la generación de códigos éticos.

Por otro lado, las medidas de seguridad tecnológicas se conforman por soluciones de hardware y software, por ejemplo: programas de detección de malware, spam e intrusos que detectan y eliminan código malicioso; canales de cifrado para protección de redes y comunicaciones; así como uso de algoritmos hash que obtienen un resumen o huella de datos y los revisan periódicamente para verificar que los datos no han sufrido alteraciones[78].

Por último, las medidas físicas se refieren al conjunto de normas, controles y procesos que tienen como objetivo garantizar la seguridad del entorno físico en donde se alojan los datos[79]. Por ejemplo: control de acceso con gafete autorizado, acceso con introducción de clave, alojamiento de la información el ubicaciones distintas a la planta matriz, etc.

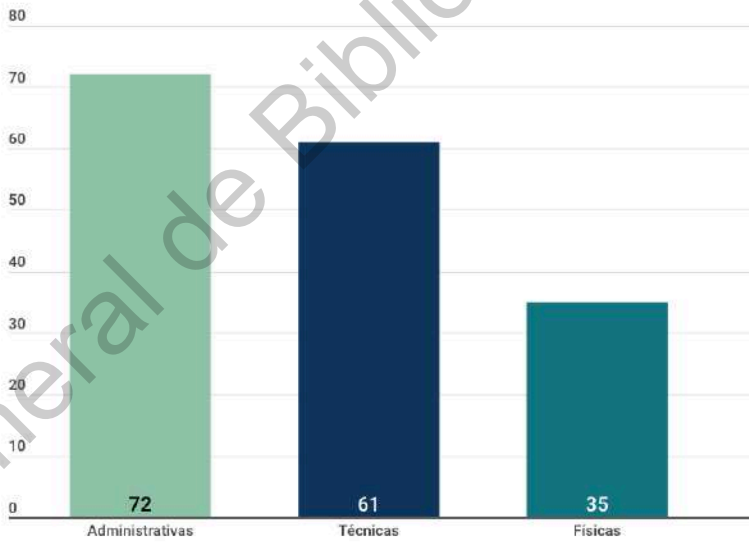
Respecto a estas medidas de seguridad, las empresas analizadas reportan el empleo de medidas administrativas en mayor medida, seguidas de medidas

[77] IN INAI. *Diccionario de protección de datos personales, conceptos fundamentales.* México, Instituto Nacional de Acceso a la información, 2019, p. 555.
[78] Ídem, p. 557.
[79] Ibídem, p. 562.

técnicas (Ver Gráfico 12). Sin embargo, menos del 40 por ciento manifestó el empleo de medidas físicas para procurar la protección de los datos.

Sumado a esto, se identifican 8 empresas que no disponen de esta información. Si bien la legislación mexicana no demanda que las empresas agreguen de manera explícita esta información, sí sería un factor de gran utilidad para los usuarios al momento de decidir adquirir un producto, por lo que sería un elemento de gran importancia para el consentimiento informado.

Gráfico 13. Tipos de medidas de seguridad adoptadas.



Fuente: Elaboración propia.

Sin embargo, ninguna medida o sistema de seguridad es 100 por ciento seguro y las empresas se encuentran en una brecha de inseguridad. De acuerdo con un reporte sobre el estado de la ciberseguridad en el mundo, realizado por la Asociación de Auditoría y Control de Sistemas Informáticos (ISACA), cuatro de cada cinco empresas consideran como probable o muy probable experimentar un

ciber ataque. Además, en el reporte realizado en 2017, 50% de las empresas manifestaron haber sido blanco de más ataques que el año anterior[80].

Derivado de este análisis se plantean las siguientes observaciones:

a) La información a los usuarios sobre las vulneraciones a datos personales no debe estar determinada por "el impacto significativo" de estos sino que, basados en el derecho a la información, a la protección de datos y a la privacidad, debe notificarse al titular de los derechos en todos los casos donde exista la mínima sospecha de compromiso o vulneración.

b) Las empresas suelen incluir en su aviso de privacidad que "protegen la información con medidas administrativas, tecnológicas y físicas", sin embargo, al ser la información uno de los activos más importantes para las empresas y en el caso de los datos personales, un elemento importantísimo de la vida de las personas, resulta necesario que los usuarios gocen de mayor certeza en cuanto a las medidas empleadas para proteger sus datos. Tal es el caso de auditorías y sellos de seguridad emitidos por la autoridad competente (el Instituto Federal de Acceso a la Información y Protección de Datos Personales, para el caso de México).

7.5. Otras implicaciones éticas.

También desde la perspectiva principialista se identifican otras consecuencias de los dispositivos IoT que vulneran los principios propuestos por Beauchamp y Childress. En este sentido, el objetivo de este apartado es explorar la huella digital y la formulación de perfiles como violaciones a los principios de autonomía y no maleficencia; el uso de algoritmos discriminatorios como

[80] ISACA. State of Cyber Security. 2017. Disponible en: https://www.cybersecobservatory.com/wp-content/uploads/2017/06/state-of-cybersecurity-2017-part-2_res_eng_0517-1.pdf

transgresión a los principios de autonomía, justicia y no maleficencia; y la producción de basura electrónica como vulneración a los principios de justicia y no maleficencia.

7.5.1. Huella digital, formulación de perfiles y manipulación colectiva.

Además de los dispositivos del IoT, nuestros nexos con internet en general son bastante amplios; algunos sectores en materia de salud se encuentran experimentando con consultas remotas, registros médicos electrónicos y robots quirúrgicos. Además, la educación actual está mediada por la tecnología y se ha ido orientando hacia el desarrollo de habilidades para el futuro que nos permitan sumarnos a un mercado laboral compuesto de empleos que aún ni siquiera existen.

Además, se generan cambios profundos en las estructuras de gobernabilidad, nos hemos convertimos en ciudadanos digitales que ejercemos derechos, participamos y nos desenvolvemos en un entorno preponderantemente digital. Este ecosistema está dejado de ser un pequeño escenario de incursión e innovación para convertirse paulatinamente en el marco total. Al mismo tiempo, es la única vía a través de la cual se accede a este plano. En este sentido, vía y meta son uno mismo.

Todos estos cambios modifican la realidad y dejan la puerta abierta a una nueva concepción de la naturaleza humana, una que nos conceptualiza como usuarios y nos exige determinadas características para pertenecer al ecosistema digital y desarrollarnos con el resto de la “humanidad”. Entre los requisitos que califican a los individuos como usuarios y por lo tanto como miembros de la humanidad están:

- Habilidad de utilizar la tecnología y los medios digitales.
- Construir y gestionar una identidad en línea paralela al mundo real.

- Administrar de manera eficiente el tiempo de pantalla, realizando distintas funciones a la vez.
- Inclinación por la transparencia; abandono de la privacidad.

Aquellos que logren cumplir con los requerimientos podrán gozar de los beneficios que brinda el entorno digital (que pronto gobernará y cubrirá todo), ganarán la oportunidad de ser considerados como miembros del grupo humano ahora proyectado en lo digital.

Quienes no logren adherirse a este entorno, no cuenten con las habilidades necesarias o no puedan asimilarse al ecosistema digital quedarán fuera de juego, rezagados y en calidad de excluidos. Tal como en la época de la conquista se consideraba neófitos a los naturales de américa y se negaba la naturaleza humana de las personas africanas, así en nuestra actualidad se considera neófitos a quienes no tienen los medios para adherirse a la red, pero tienen posibilidad de adquirir las habilidades necesarias. En el mismo sentido, existe el peligro de negar la naturaleza humana a aquellos que queden atrapados por la brecha digital, imposibilitándoles su participación en la construcción del mundo, el ejercicio de sus derechos y el propio reconocimiento con los otros.

Así como Colón encontraba tres móviles en la conquista: lo humano (riqueza), lo divino y el disfrute de la naturaleza[81], también se pueden localizar estos tres móviles en la digitalización del mundo. En primer lugar, lo humano (la riqueza) se despliega en el crecimiento económico que generan los pilares de la cuarta revolución industrial; en segundo lugar, lo divino cuyo espacio a dejado de ser trono de Dios para serlo de los datos y la información; y tercero, el disfrute de la naturaleza que se equipara al goce de las comodidades, la simplificación de la vida y la automatización de los procesos.

En 1552, Fray Bartolomé de las Casas decía de los naturales de América:

[81] TODOROV, Tzvetan. La conquista de América, el problema del otro. México, Ed. Siglo XXI editores, 2010, pp. 23-24.

> *"Son eso mesmo de limpios y desocupados y vivos entendimentos; muy capaces y dóciles para toda buena doctrina, aptísimos para recebir nuestra santa fe católica y ser dotados de virtuosas costumbres, y las que menos impedimentos tienen para esto que Dios creo en el mundo. Y son tan importunas desque una vez comienzan a tener noticia de las cosas de la fe, para saberlas, y en ejercitar los sacramentos de la iglesia y el culto divino, que digo verdad que han menester los religiosos para ufrillos ser dotados por Dios don muy señalado de paciencia… cierto, estas gentes eran lo más bienaventuradas del mundo si solamente conocieran a Dios"* [82](p. 14).

Hoy, se hace un reconocimiento similar de aquellos que están dispuestos, y tienen el entendimiento necesario, para recibir la fe de un dios que ya no es el católico sino la información, la interconexión y la tecnología. Aquellos con actitudes dóciles para la doctrina, que aceptan la digitalización del mundo, son bien recibidos. De igual manera se preparan sistemas completos para evangelizar y dotar de herramientas a aquellos que acepten y califiquen como usuarios de la red.

Existe esta misma relación entre los esclavos negros traídos a América y aquellos rezagados por la brecha digital. A las poblaciones africanas se les consideraba incapaces de acercarse a Dios, sin habilidades para comprender sus mandatos y herejes por negar su existencia y preferir otras prácticas entendidas como demoníacas por los católicos.

Asimismo, quienes se pierden en la brecha digital por no poder o querer acceder a los medios y dispositivos de contacto con la red; quienes no cuenten con los requerimientos necesarios para convertirse en usuarios; y quienes decidan

[82] Fray Bartolomé de las Casas. Brevísima relación de la destrucción de las Indias. Editorial Universidad de Antioquía, 1552, p. 14.

no acoplarse a esta digitalización, corren el peligro de ser negados como parte de la humanidad. De manera general, será prácticamente imposible que puedan participar, ejercer sus derechos y construir mundo. En cierta forma es negar su categoría de humanos.

En este sentido los neófitos nos hemos sometido al proceso de asimilación con la intención de no quedar rezagados, ser considerados ciudadanos digitales, y humanos funcionales. Sin embargo, se termina pagando el precio de la transparencia, debemos exponernos para poder ver la exposición de los demás. Esta suerte de vigilancia constante afecta en primer lugar a la privacidad y en segundo lugar, a la personalidad misma.

La primera, sobre privacidad y protección de datos, ha sido explorada en el capítulo anterior. Sin embargo, la segunda consecuencia, sobre la personalidad, es aún más nociva.

De acuerdo con la Real Academia Española, la personalidad es un "Diferencia individual que constituye a cada persona y la distingue de otra"[83], es decir el conjunto de elementos que nos hacen ser nosotros mismos y no otros, que nos diferencian. En este sentido, para entender cómo es que la vigilancia ejercida a través de internet impacta y lesiona la personalidad de los individuos, es necesario ilustrar el siguiente caso:

En 2016, la empresa de asesoría política Cambridge Analytic, participó en la campaña electoral de Donald Trump a la presidencia de Estados Unidos de América empleando técnicas psicográficas basadas en datos obtenidos de Facebok, ello en aparente colaboración. Esta no era su primera intervención política, ni tampoco la primera vez que empleaban estas técnicas. Se ha vinculado a la empresa con el proceso del Brexit, así como con procesos electorales en Trinidad y Tobago, esto por mencionar alguno de los casos más sonado y para los

[83] Real Academia Española. Diccionario de la lengua española, Privacidad. Disponible en: https://dle.rae.es/personalidad 17 de octubre de 2019

cuales se ha logrado reunir evidencia por parte de periodistas de The New York Times y The Guardian.

Sin embargo, fue el caso de las elecciones estadounidenses el que permitió construir una radiografía más clara sobre la forma de operar de Cambridge Analytic, misma que puede resumirse en los siguientes pasos:

1) Se difundió en Facebook un cuestionario sobre gustos y personalidad, basado en un cuestionario de personalidad diseñado por psicólogos de la Universidad de Cambridge.

2) Una vez que un usuario accedía a este cuestionario en línea, la aplicación extraía *"no sólo datos de su perfil, sino también de los de 205 de sus amigos en Facebook: sin su consentimiento y sin que lo supieran, se descargaron sus nombres, fechas de nacimiento y datos de ubicación, así como listas de cada página de Facebook a la que había dado me gusta"*[84].

3) Esta información se gestionaba en bases de datos donde se catalogaba a los sujetos indecisos como blancos de la siguiente fase.

4) Una vez identificados los blancos, Cambridge Analytic generaba y enviaba contenido personalizado (muchas veces falso) para activar la opinión deseada. En palabras de Brittany Kaiser (ex directora de desarrollo de negocios de Cambridge Analytica); *"los bombardeabamos con blogs, notas de sitios web, videos, anuncios, todas las plataformas imaginables hasta que vieran el mundo como nosotros queríamos. Hasta que votaran por nuestro candidato"*[85].

De este modo, información privada de más de 50 millones de usuarios estadounidenses fue tratada para manipular su opinión. En algún momento, como

[84] ROSENBERG, Matthew y Gabriel J.X. Dance. Así funcionaba la recolección de datos de Cambridge Analytica. The New York Times, 2018. Disponible en: https://www.nytimes.com/es/2018/04/10/espanol/facebook-cambridge-analytica.html 10 de abril de 2018

[85] Netflix Productions, Jehane Noujaim. *The great hack*, Estados Unidos, 2016. Min. 42.16.

parte de una charla sobre los servicios de la compañía Alexander Nix (ex director general y fundador de Cambridge Analytic afirmaba que poseían *"cerca de cuatro mil o cinco mil puntos de datos que podemos usar para predecir la personalidad de cada adulto del país en Estados Unidos. La personalidad condiciona la conducta y la conducta influye en nuestro voto. Podríamos dirigirnos a la gente con contenido digital muy concreto"*[86].

Esto, representa una amenaza clara a la autonomía de los sujetos, a su derecho a decidir de manera libre, atentando contra su personalidad misma, en el sentido de que sus elecciones se han derivado de la manipulación de esos rasgos que lo hacen único y diferenciable. Además, es una afrenta contra el principio de no maleficencia y justicia ya que pone en riesgo la democracia y el estado de derecho.

Cambridge Analytic es el claro ejemplo de cómo las empresas tecnológicas han convertido al sujeto en un simple proveedor de datos, en fuente de recurso inagotable y explotable, valioso sólo en medida de la monetización de sus datos. Sin embargo, como se ha dicho con anterioridad, estas empresas no siempre nos arrancan los datos a nuestras espaldas, en una gran proporción hemos decidido exponernos sin saber bien a bien las implicaciones de esto.

Todos generamos registros y rastros al utilizar internet que eventualmente terminan constituyendo nuestra huella digital. Tal como la huella dactilar, la huella digital contiene información específica e irrepetible de quienes somos.

El gran riesgo de los dispositivos del IoT, en este apartado, se debe principalmente a tres características:

1) Por su ubicación e injerencia en nuestra vida, los dispositivos del internet de las cosas pueden tener acceso a datos incluso más sensibles que los recolectados por redes sociales.

[86] Ídem. Min. 14.25.

2) El nivel de opacidad de estos dispositivos es aún mayor. Esto debido a la fácil ejecución de funciones en segundo plano, sin necesidad incluso de que el usuario de un clic.

3) En algunos casos los dispositivos del IoT no recolecta información únicamente del usuario (persona que adquirió el producto), sino de más personas con las que tienen contacto y que no han dado su consentimiento para ser vigilados.

En conclusión, un manejo inadecuado de los datos recolectados por dispositivos del internet de las cosas y el ejercicio de prácticas no éticas en esta materia podrían potencializar un mecanismo, que en palabras de Brittany Kaiser es considerado como un arma: "la herramienta de selección era controlada por el gobierno británico, lo cual significaría que la metodología se consideraba un arma"[87].

7.5.2. Algoritmos discriminatorios

Cuando hablamos de un algoritmo nos referimos al conjunto de instrucciones para solucionar un problema, dichas instrucciones tienen la particularidad de estar expresadas en lenguaje de programación. Para Ricardo Peña, son *"un conjunto de reglas que, aplicadas sistemáticamente a datos de entrada apropiados resuelven un problema en un número finito de pasos elementales"*[88]. Son, por tanto, mancuerna inseparable de la inteligencia artificial (IA).

[87] Guardian News. Brittany Kaiser testifies before MPs – watch live (video), 2018. Disponible en: https://www.youtube.com/watch?v=xZAvQzRhJ0I 10 de enero de 2020

[88] PEÑA Marí, Ricardo. *De Euclides a Java, historia de los algoritmos y de los lenguajes de programación*. España, NivolaLibros y ediciones, 20016, p. 26.

José Ignacio Latorre argumenta que, pese al gran conocimiento que ha amasado el ser humano, aún se intenta analizar la esencia del alma humana. Sin embargo, esta tarea no ha logrado llegar a su fin, pese a ello, el ser humano se plantea una nueva idea "¿tal vez no comprendamos el alma humana, pero podemos simularla artificialmente?"[89]. Esto a través de dotar de inteligencia artificial a las máquinas (dispositivos IoT). En este sentido, el autor expresa:

> *"Es más que probable que una generación de sofisticados algoritmos penetrará en nuestra intimidad. Esos algoritmos se convertirán en los compañeros más fieles de personas solitarias o de avanzada edad. De forma casi involuntaria, los humanos empezaremos a hablar con las inteligencias artificiales como si se tratase de personas. Las insultaremos (¿quién no ha insultado a su ordenador?), suplicaremos que nos hagan caso (¿quién no ha suplicado a su ordenador?), serán nuestras confidentes. Si no nos placen, nos divorciaremos de ellas"*[90].

Hasta antes de la irrupción de los dispositivos inteligentes en nuestras vidas, las máquinas se encontraban al margen de la ética. Los dilemas éticos se desarrollaban en la mente de los científicos que diseñaban las tecnologías o en aquellos que las utilizaban con determinados fines. Por el contrario, ahora que las máquinas han comenzado a ejecutar algunas funciones mentales superiores (aprendizaje, memoria, lenguaje, etc.), la situación se ha movido de lugar; las decisiones morales pueden ser tomadas también por máquinas.

Dos de los eventos que han abierto interrogantes en este tema son 1) la muerte de Joshua Brown, dueño de un Tesla Model S, quien falleciera al impactarse con el remolque de un camión en una carretera de Florida, Estados

[89] LATORRE Sentís, José Ignacio. *Ética para máquinas*. Barcelona, Ed. Ariel,2019, p. 24.
[90] Íbid, p. 25.

Unidos, mientras el automóvil era conducido por el piloto automático[91]. 2) La muerte de Elaine Herzberg, en Tempe, Arizona, al ser atropellada por un vehículo sin conductor operado por Uber. Esto mientras se encontraba cruzando la carretera, caminando fuera del paso de peatones y con su bicicleta[92].

De acuerdo con Azim Shariff y Díaz Limón

> *"la paradoja en la construcción de automóviles cada vez más inteligentes, radica en que el algoritmo de programación implica la reducción del número de muertes ante un inminente accidente de tránsito, por lo que, indefectiblemente la IA 'tomaría la decisión autónoma' de salvar la mayor cantidad de vidas, aunque esto cueste aquella del propietario del vehículo"*[93].

Sin embargo, no se ha determinado a quién correspondería la compleja tarea de delimitar los parámetros morales que deberán tener estos dispositivos: consumidores, fabricantes, gobiernos u organismos independientes y colegiados. Hasta el momento

> *"la IA de cada unidad, permite que estas aprendan de forma autónoma, lo que invariablemente puede llevar a que cada vehículo construya su propia moral. Es decir, si bien los vehículos saldrán de la fábrica con exactamente las mismas características, el comportamiento, las rutas y las instrucciones*

[91] JIMÉNEZ Cano, Rosa. *El dueño de un Tesla, primer muerto en un coche con piloto automático*. El País, 2016. Disponible en: https://elpais.com/tecnologia/2016/07/01/actualidad/1467337732_779288.html 2 de julio de 2018

[92] JIMÉNEZ Cano, Rosa. *Primer atropello mortal de un coche sin conductor*. El País, 2018. Disponible en: https://elpais.com/tecnologia/2018/03/19/actualidad/1521479089_032894.html 20 de marzo de 2018

[93] DÍAZ Limón, Jaime. *Abogado digital: estudios sobre derecho cibernético, informático y digital*. México, ed. VLex, 2019, p. 55.

de la interfaz humana comenzarán a redactar su moral conforme al algoritmo de repetición y aprendizaje que poseen, lo que generará tantos tipos de comportamiento como vehículos de IA en las calles"[94].

Para tratar de comprender esta situación, el Massachusetts Institute of Technology creó la plataforma Moral Machine[95], donde plantea diversos dilemas morales, el usuario debe elegir el menor de los males en situaciones que involucran autos inteligentes, conductores y peatones. En el experimento, realizado en 2014 se reunieron 40 millones de decisiones de usuarios de distintos países que reflejaron claras diferencias en las elecciones tomadas por diversos clusters culturales.

Sumando los argumentos anteriores es posible ver un problema aún mayor. Si actualmente cada dispositivo dotado de inteligencia artificial es capaz de generar su propios preceptos morales a través del aprendizaje derivado de los datos por los que se alimenta y al mismo tiempo, estos parámetros difieren de un cluster cultural a otro, entonces es razonable pensar que los dispositivos reflejaran las percepciones, ideas y prejuicios del lugar donde se insertan, en general; y del usuario, en particular.

Sin embargo, esto no quiere decir que el dispositivo será un reflejo de la moral de sus usuarios. El Model S de Tesla, por ejemplo, aprende también de los demás autos conectados y de sus usuarios, es de esperarse entonces que nuestro auto pueda actuar de formas no aceptables para nosotros.

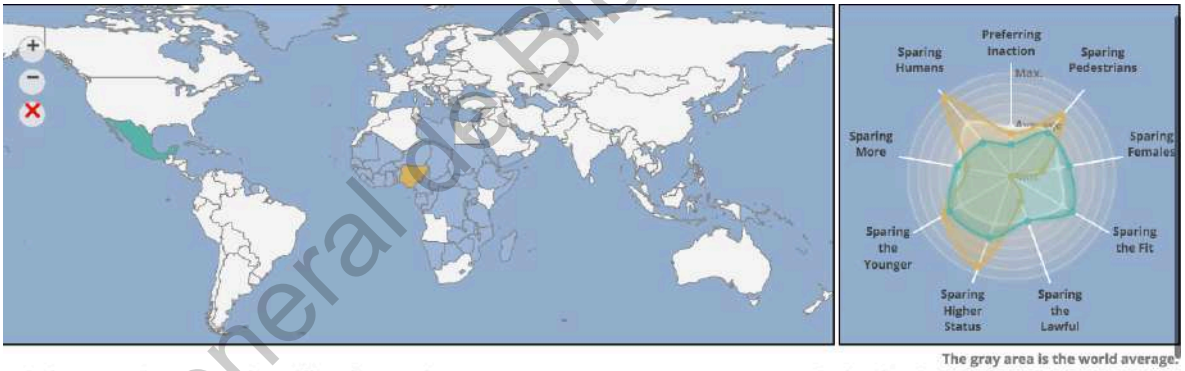
[94] Íbid, p. 56.

[95] Mit Media Lab. Moral Machine. Massachusetts Institute of Technology. Disponible en: http://moralmachine.mit.edu/ 9 de enero de 2020

En este aprendizaje automático, los algoritmos incluso pueden generar tratos diferentes a los usuarios, y que generen perjuicios por motivos de raza, sexo, religión, profesión, reputación digital o cualquier otra característica personal.

Pensemos en un caso hipotético, sobre dispositivo que ha aprendido de las ideas, percepciones, representaciones e información que circula en un cluster cultural eminentemente machista y que utiliza esa información para la toma de decisiones. Es posible que el dispositivo replique parámetros de violencia en distinta medida según sus funciones, en el caso de los autos inteligentes, esta decisión puede ser la de valorar la vida de un hombre por sobre la de una mujer.

Imagen 2. Resultados Moral Machine de México y Nigeria.



World Ranking (out of 117 Countries)	Preferring Inaction	Sparing Pedestrians	Sparing Females	Sparing the Fit	Sparing the Lawful	Sparing Higher Status	Sparing the Younger	Sparing More	Sparing Humans
Nigeria	62nd	12th	103rd	117th	102nd	3rd	19th	82nd	1st
Mexico	94th	69th	30th	34th	60th	23rd	33rd	56th	102nd

Fuente: Massachusetts Institute of Technology[96].

[96] Massachusetts Institute of Technology. Moral Machine Results. Disponible en: http://moralmachineresults.scalablecoop.org/ 9 de enero de 2020

Por ejemplo, en la imagen 2 puede observarse una comparación de los resultados de la Moral Machine de México y Nigeria, donde existen claras diferencias en la apreciación de ciertos sectores. Por ejemplo, en México se prioriza salvar a mujeres y personas que respetan la ley, en mayor proporción que en Nigeria. Contrariamente, en este segundo país se decide salvar prioritariamente a humanos (frente a los animales) y personas de clases altas.

Por último, es importante mencionar que, si bien la discusión de los dilemas morales resulta de gran importancia, y ejercicios como el del MIT permiten conocer los parámetros morales de las distintas regiones del mundo frente a casos hipotéticos; estos no dejan de ser ejercicios mentales que deben ser transformados en productos reales para la toma de decisiones. Ello con el cuidado de no reproducir preceptos violentos, discriminatorios o que atenten contra la justicia.

7.5.3. E-waste

En las sociedades actuales los datos cobran una importancia enorme, también lo hacen aquellos dispositivos electrónicos que levantan, almacenan, procesan e interpretan la información. Como se ha explicado, en la era del internet de las cosas el número de estos dispositivos aumentan de manera exponencial, se estima que para 2020 habrá por lo menos 50,000 millones de dispositivos conectados, cifra que se duplicará en 2025 con 100,000 millones de conexiones a la IoT[97].

Además de los riesgos para la privacidad y la protección de datos, esto implica una grave amenaza para el medio ambiente. Es necesario tener en cuenta que los 100,000 millones de dispositivos conectados para 2025 se convertirán en algún momento en basura electrónica (*e-waste*) generando impactos sociales y ambientales difíciles de afrontar.

[97] Huawei Technologies Co.,Ltd. *Tendencias y desafíos de la industria,* 2017. Disponible en: http://developer.huawei.com/ict/en/site-iot/article/iot-industry

En este sentido, define a la *e-waste* o desechos electrónicos como "Todos aquellos elementos de aparatos eléctricos y electrónicos o de sus componentes, que hayan sido desechados por sus propietarios como desperdicios sin ánimo de reutilizarlos[98].

En 2014, a nivel global se producía 41.9 millones de toneladas de *e-waste*, de la cual: 12.8 millones de toneladas eran de equipos pequeños (microondas, aspiradoras, cámaras de video), 11.8 millones de toneladas de equipos grandes (lavadoras, secadoras, paneles), 7 millones de toneladas de equipos de intercambio de calor (refrigeradores, calentadores), 6.3 millones de toneladas de pantallas, 3 millones de toneladas de dispositivos pequeños de tecnologías de la información y la comunicación (laptops, celulares, tabletas) así como un millón de toneladas de lámparas[99].

Esta cantidad de residuos aumenta significativamente su riesgo si consideramos que contienen elementos tóxicos, potencialmente dañinos una vez que estos han llegado al final de su vida útil y se convierten en *e-waste*.

En un estudio realizado por GreenPeace en emplazamientos de reciclaje de residuos electrónicos en Ghana, se encontraron distintos elementos tóxicos en contacto con suelo, plantas y humanos:

- **Cadmio:** se encuentra presente en los aparatos electrónicos y en pilas recargables, Puede acumularse en el cuerpo a lo largo del tiempo, por lo que la exposición causa a largo plazo daños a los riñones y a la estructura ósea. Se sabe que el cadmio y sus compuestos son cancerígenos para el ser humano, principalmente mediante la inhalación de vapores y partículas de polvo contaminadas.
- **Plomo:** se usa extensamente en los productos electrónicos como componente principal de soldaduras y en el cristal de los tubos de

[98] BALDÉ, C., Forti, V., Gray, V. Kuehr, R. & Stegmann, P. *Observatorio mundial de los residuos electrónicos 2017*; cantidades, flujos y recursos. United Nations University, 2017, p. 11.
[99] International Telecommunication Union. *RAEE: desde el reto-e hasta la oportunidad-e*, 2015, p. 2.

rayos catódicos en televisiones y monitores, así como en baterías de plomo. Se puede acumular en el organismo mediante la exposición reiterada y tener efectos irreversibles sobre el sistema nervioso, en particular durante su desarrollo en la infancia.

- **Antimonio:** es un metal usado en varias aplicaciones industriales, entre ellas como retardante de llama y como trazador en soldaduras metálicas. La exposición a altos niveles, presentes en partículas de polvo o vapores, en el lugar de trabajo, puede conllevar severos problemas de piel y otros efectos negativos sobre la salud. El trióxido de antimonio está reconocido como posible cancerígeno en humanos.
- **Bifenilos y policlorados:** Son sustancias químicas sumamente persistentes y bioacumulativas, que se dispersan con rapidez en el medio ambiente y se acumulan en concentraciones elevadas en el cuerpo de los animales. Se les asocia con un amplio rango de efectos tóxicos que incluyen la supresión del sistema inmunológico, afecciones en el hígado, desarrollo del cáncer, daños al sistema nervioso, cambios conductuales y daño al sistema reproductor masculino y femenino.
- **Clorobencenos:** Sustancias químicas relativamente persistentes y bioacumulativas. Los efectos por exposición dependen del tipo de clorobenceno, pero los más comunes incluyen efectos sobre el hígado, la tiroides y el sistema nervioso central.
- **Polibromodifenil éteres:** son un tipo de retardante de flama que se utilizan para prevenir la propagación del fuego en gran variedad de materiales, incluyendo las fundas y los componentes de muchos productos electrónicos. Son sustancias químicas persistentes en el medio ambiente y algunas son sumamente bioacumulativas, capaces de afectar el desarrollo cerebral normal en los animales. Se sospecha que ciertos PBDEs son disruptores endocrinos, capaces de interferir con las hormonas del crecimiento y el desarrollo sexual. También se han documentado efectos sobre el sistema inmunológico.

- **El trifenilfosfato (TPP)** es un tipo de retardante de llama organofiosforado que se utiliza en los aparatos electrónicos, por ejemplo, en las carcasas de los monitores de ordenador. El TPP es muy tóxico para la vida acuática y un inhibidor importante de un sistema enzimático clave de la sangre humana. También se sabe que en algunos individuos provoca dermatitis por contacto y es un posible disruptor endocrino[100].

La vida de los dispositivos electrónicos lleva consigo una silenciosa carga ecológica desde el momento de su creación, por ejemplo; el físico Eric Williams, en un estudio elaborado junto con Ruediger Kuehr para las Naciones Unidas, afirma que la fabricación de una computadora de escritorio requiere al menos 240 kg de combustibles fósiles, 22 kg de productos químicos y 1,5 toneladas de agua. Es decir, el peso en combustibles fósiles utilizados supera las cien veces el peso de la propia computadora[101].

Aún los microdispositivos tienen un costo ecológico demasiado alto en comparación con su tamaño. En el mismo estudio, de Eric Williams y Ruediger Kuehr, se mostró que un microchip de 2 gr requiere, para su fabricación, 72 gr de productos químicos, 20 litros de agua, y el equivalente a 1,2 kg de combustibles fósiles en consumo energético, además de generar 17 kg de aguas residuales y 7,8 kg de desechos sólidos, junto a toda una serie de emisiones tóxicas a la atmósfera.

Esto deja de manifiesto que, mientras la tecnología da pasos agigantados en la reducción del tamaño de los dispositivos electrónico, el impacto ambiental aumenta sus riesgos y sus efectos se acumulan, esto en clara vulneración al principio de no maleficencia.

[100] GreenPeace. *Envenenando la Pobreza: residuos electrónicos e Ghana*, 2008, pp. 12-15.
[101] KUEHR Ruediger, y Eric Williams, (2003), *Computers and the Environment. Understanding and Managing Their Impacts*, Kluwer Academic Publishers, Dordrecht, 2003.

Además, el ciclo de vida de los dispositivos electrónicos, se encuentra marcada por dos términos producto de nuestra sociedad de consumo: en primer lugar, la obsolescencia programada, es decir la determinación *a priori* del periodo de funcionamiento del producto, misma que el fabricante determina desde la fase de diseño. Bajo este criterio se determina la temporalidad en que el aparato será considerado obsoleto, inservible o disfuncional.

En segundo lugar, la obsolescencia percibida, generada por el mercado, donde el usuario realiza una valoración subjetiva de su dispositivo y lo califica como disfuncional e inoperante a pesar de contar con la funcionalidad técnica. Generalmente sucede una vez que el usuario genera un deseo por adquirir un nuevo producto, más compatible con la tendencia social, destinado a cubrir necesidades simbólicas y pocas veces reales.

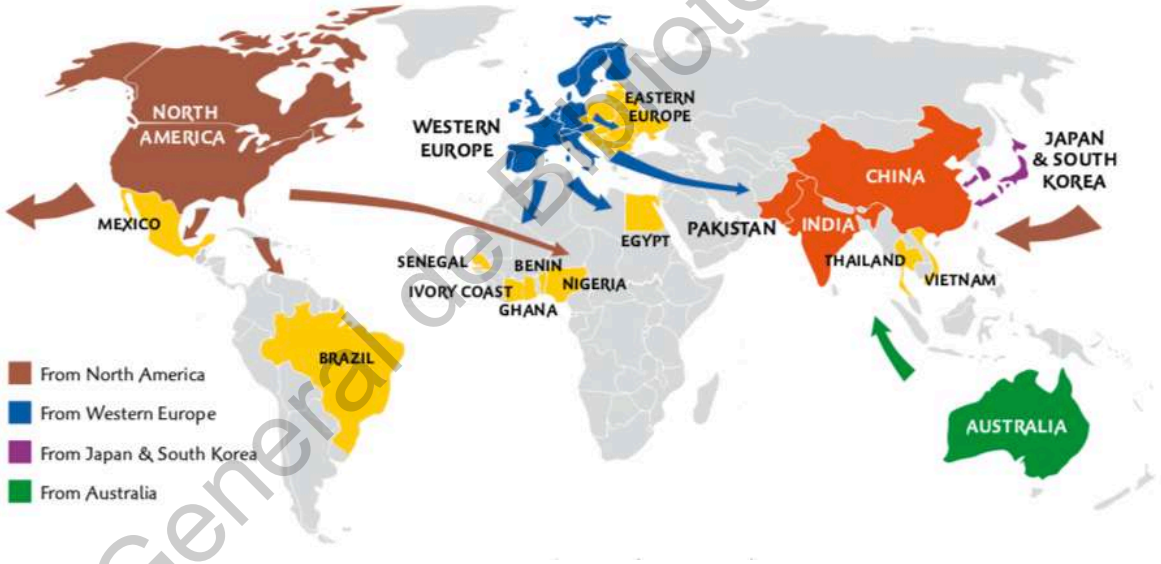
Ambos procesos han aumentado la cantidad de productos desechados, por una parte, los aparatos se encuentran programados para durar poco y, por lo tanto, comprar más, por el otro; desechamos productos que aún son operables y pueden cubrir las funciones para las cuales fueron creados. Así, estas implicaciones ambientales violentan el principio de justicia ecológica propuesto por Lecaros en tres vertientes: justicia global, justicia intergeneracional y justicia interespecífica[102].

En primer lugar, el mal manejo de los residuos electrónicos y la toxicidad que los acompaña, se contrapone a la justicia global ya que tiene daños potenciales a nivel planetario. Sobre todo, causa daños en sectores empobrecidos y genera aún más desigualdad. Zonas geográficas como Ghana, India y México se han convertido en los vertederos privados de países de la Unión Europea Y Estados Unidos (Ver Imagen 3), quienes envían los dispositivos caducos a través de rutas de tráfico o falsas donaciones.

[102] LECAROS Urzúa, Juan Alberto. *La ética medio ambiental: principios y valores para una ciudadanía responsable en la sociedad global*, en Acta Bioethica; 19 (2), 2013, pp. 177-188.

Mientras los habitantes de Estados Unidos, Canadá, la Unión Europea, Oceanía y Japón producen en promedio más de 15 kilogramos de basura electrónica al año, pobladores de Asia generan 3.7 kg y habitantes de África producen sólo 1.7 kg. Sin embargo, son territorios de estos dos últimos los que se han convertido en vertederos y blancos del tráfico ilegal de residuos[103].

Imagen 3. Rutas de exportación de e-waste.



Fuente: International Labour Office, 2012[104].

[103] International Telecommunication Union. *RAEE: desde el reto-e hasta la oportunidad-e*, 2015, p. 3.
[104] International Labour Office. (2012). *The global impact of e-waste, addressing the challenge*. Ginebra, 2012, p. 15.

Esta situación resulta evidentemente abusiva, violatoria de los principios de autonomía, justicia, no maleficencia y beneficencia ya que los traslados se realizan por la vía de la ilegalidad, cubriendo los cargamentos como donaciones de tecnología para países menos avanzados bajo el conocimiento del daño que se está trasladando a estos lugares.

En segundo lugar, la e-waste, vulnera la justicia intergeneracional ya que causa daños irreversibles para generaciones futuras, quienes recibirán de nuestras manos un mundo en pedazos. Fenómenos como la contaminación del aire, agua y suelo, así como el efecto invernadero, intensificados por la basura electrónica, deterioran las condiciones de un mundo habitable y ponen en peligro la salud y supervivencia de generaciones venideras.

En tercer lugar, esta realidad atenta contra la justicia inter específica ya que no afecta únicamente a la especie humana, sino que desencadena efectos negativos para otras especies de animales y plantas.

En ejercicio de una ciudadanía ecológica responsable y del principio de justicia ecológica debemos buscar mecanismos que atiendan el problema actual que está generando la excesiva cantidad de residuos electrónicos derivados de la asimilación del internet de las cosas a nuestras vidas. Dichos mecanismos deberán estar pensados

Entre otras cosas, las políticas públicas deben considerar las siguientes características:

- Gestionarse de manera global o regional con la intención de generar impactos globales y en medida de lo posible responsabilidades colectivas.
- Economía circular como eje estratégico con la finalidad de reincorporar materiales y generar la menor cantidad de desechos.

- Prácticas de fabricación sostenibles que prioricen el ecodiseño, ciclos de vida más largos, la utilización de materiales no tóxicos y reutilizables.
- Concientizar a los ciudadanos sobre la obsolescencia real de sus dispositivos y generar pautas de autocuidado.
- Desarrollar normas internacionales en la gestión del ciclo de vida de los dispositivos electrónicos.

VIII. CONCLUSIONES

8.1. Aportes para una política en materia de protección de datos e IoT.

Estamos transitando de la era industrial a la era de la información, como especie debemos tomar conciencia de las consecuencias inherentes a la tecnología disruptiva que estamos creando. Tener presente que los dispositivos del internet de las cosas son más que dadores de confort, que han dejado de ser máquinas pasivas para convertirse en objetos activos, es ineludible para enfrentar los retos que se han presentado y quizá otros más sofisticados que están por venir.

Las consideraciones para enfrentar los problemas de un futuro que ya está aquí descansan definitivamente en la ética, no en la tecnología que trabaja bajo el imperativo de *"todo lo que es factible y puede ser hecho, debe ser llevado a cabo"*[105], ni del derecho que lo hace con "todo lo que no está expresamente prohibido por la ley está permitido"[106], sino de la ética que plantea la construcción de un mundo donde la acción de todos sea deseable.

Esto es importante ya que dependiendo el discurso imperante es que se marcarán los límites de la conducta humana (y no humana aparentemente). En este sentido, y de acuerdo con lo expuesto en el párrafo anterior, los límites tecnológicos están dados por la capacidad de saber y crear, es decir, todo lo que sea factible de ser creado y conocido, lo será sin importar las consecuencias negativas que pueda traer. En el campo del derecho estos límites están fijados por la ley, el conjunto de normas dispuestas por los órganos legislativos que dispone procedimiento vinculatorios para quienes no acaten estos límites, y que no siempre se encuentra actualizada. Y por último, la ética que fija los límites en el

[105] GONZÁLEZ Graciano. *El imperativo tecnológico, una alternativa desde el humanismo*, España, Asociación Española de bioética y ética médica, 2004, p. 38.

[106] *El principio de legalidad*. Anónimo, disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/1/22/9.pdf p. 124.

propio sujeto, en su capacidad de auto limitarse para procurar el bienestar de otros.

Así es que las más poderosas herramientas para enfrentar los problemas éticos derivados del internet de las cosas se encuentran en:

a) Esquemas robustos de autorregulación para empresas e individuos.

b) Ética por diseño, es decir incorporar a la ética desde el nacimiento de la idea de una nueva máquina hasta su implementación. Recordando siempre que "las armas son las máquinas sin ética por excelencia"[107].

c) Generación de estudios que permitan comprender con mayor profundidad las consecuencias que tendrán estos dispositivos en nuestras vidas.

d) Diseñar estrategias en materia de política pública que atiendan las consecuencias generadas por dispositivos del IoT en dos bloques:

I. Relacionados con la privacidad y protección de datos,

II. Relacionados con la creación de perfiles, manipulación colectiva y algoritmos discriminatorios.

III. Relacionados con el medio ambiente.

En este sentido, es objeto de este capítulo atender el último punto d, sección I, de los mencionados anteriormente, es decir, proponer algunos elementos para el diseño de política pública y el tratamiento ético de los dispositivos del internet de las cosas en su relación con la privacidad y la protección de datos personales.

[107] LATORRE Sentís, José Ignacio. *Ética para máquinas*. Barcelona, Ed. Ariel, 2019, p. 41.

8.2. Pautas de diseño

Pese a que apenas en 2010 se promulgó en México la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP). Con la intención de proteger los datos personales tratados por personas físicas o morales de carácter privado la ley pretende *"regular el tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas"*.

Este ejercicio, aunque retrasado en comparación con otros países que mucho antes comenzaron a legislar al respecto, resultaba urgente para el país en 2010. A través de esta ley se sienta el primer precedente de la protección de datos personales en México y se generan aportes importantes, tal es el caso de los siguientes:

- Conceptualización de datos personales como *"cualquier información concerniente a una persona física identificada o identificable"* (Art. 3).
- Conceptualización de los datos personales sensibles como *"aquellos datos personales que afectan a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este"* (Art. 3).
- Contenido mínimo de avisos de privacidad que, entre otros elementos, contempla las especificaciones sobre el tratamiento que se le dará a los datos (Art. 16).
- Enunciación y descripción de los derechos de los usuarios, particularmente de los llamados derechos ARCO: Acceso, Ratificación, Cancelación y Oposición (Arts. 22-35)."

A esta Ley, se sumó en 2017 la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), misma que retoma los parámetros de la LFPDPPP pero aplicados a sujetos obligados, es decir,

aquellos que disponen de recursos públicos, subsidios o estímulos fiscales, tal es el caso de: universidades públicas, partidos políticos, organismos de los poderes ejecutivo, legislativo o judicial, etc.

Mediante ambas leyes se habilita al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) que a su vez coordina el Programa Nacional de Protección de Datos Personales, mismo que busca la correcta aplicación de las dos legislaciones vigentes. Sin embargo, y pese a los esfuerzos hasta ahora desarrollados, la política actual resulta insuficiente y presenta deficiencias importantes.

En este sentido, la Ley General de Protección de Datos Personales en Posesión de Particulares presenta conceptos demasiado abiertos que facilitan lagunas legales y entorpecen los procedimientos, tal es el caso de la conceptualización de “datos personales sensibles”, donde cualquier y ningún dato pueden caber.

Además, en los requerimientos del aviso de privacidad no se contempla un elemento sumamente importante: los datos recogidos y gestionados. En este mismo rubro, cuando se presume la existencia de un aviso de privacidad, la ley entiende que el titular consciente tácitamente el tratamiento de los datos, sin importar realmente que el usuario conozca y entienda las implicaciones del mismo. Por otro lado, sólo se exige consentimiento expreso para datos financieros o patrimoniales y no para datos relacionados con el IoT como horarios, rutinas, enfermedades mentales, patrones de voz, reconocimiento facial y perfiles creados por los dispositivos.

En el caso de Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, no se contemplan sanciones penales para aquellos que incurran en malas prácticas, es decir, aquellos funcionarios públicos que cometan faltas podrán recibir una sanción civil o administrativa pero nunca penal.

Por último, en ambas legislaciones se considera que las investigaciones sólo podrán ser iniciadas por el titular de los derechos por lo que se descartan procedimientos de oficio detectados por algún otro medio, situación problemática ya que muchas veces el usuario es el último en conocer los vicios del manejo de sus datos personales o incluso puede que nunca se enteren de tal caso. En esta línea el INAI ejecuta auditorias sólo a petición de usuarios y deja un vasto campo de instituciones, empresas y personas sin ser supervisadas. Sumado a esto, en ambos documentos solo se prevén consecuencias para los responsables de la gestión de datos que incurran en faltas, pero no para la parte complementaria que compra o emplea los datos para fines particulares, muchas veces violatorios de derechos.

Sin embargo, estas no son las únicas problemáticas que se presentan. Existen por lo menos una decena de puntos más que dejan ver el débil estado en el que se encuentra la protección de datos en México.

Primero: No existen pautas marcadas desde el Plan Nacional de Desarrollo 2019-2024 en materia de protección de datos personales, situación que denota poca preocupación y atención por el tema, deja sin estrategia clara a la federación y limita el acceso presupuestal para acciones en este terreno.

Segundo: Los particulares y sujetos obligados desconocen el contenido de la LFPDPPP y la LGPDPPSO. Aun cuando nos encontramos a 9 años de la entrada en vigor de la primera y a dos de la segunda. Situación grave ya que quienes gestionan datos personales no comprenden lo sensible de la actividad y los alcances de sus actividades.

Tercero: Poca profesionalización en materia de protección de datos tanto en medios físicos, administrativos y técnicos, lo que supone no solo la formación de ingenieros sino de otros perfiles, así como diálogo interdisciplinar, que permita contar con capital humano capaz de atender los retos de protección de datos al interior de empresas e instituciones públicas.

Cuarto: Poca cultura de protección de datos personales en la sociedad mexicana, principalmente en grupos vulnerables que afectados por la brecha digital tienen acceso a las tecnologías, pero no a la información, formación y desarrollo de habilidades que la sociedad digital exige. Condición que facilita el ejercicio de malas prácticas, desconocimiento de normas y una pobre gestión de medidas protectoras en el entorno individual y familiar.

Quinto: Heterogeneidad excesiva de los mecanismos de ejercicio de derechos ARCO ya que cada empresa decide los procedimientos a seguir dentro de su propia organización. Esto representa que las personas que deciden hacer valer alguno de sus derechos de acceso, rectificación, cancelación u oposición del tratamiento de sus datos personales deben enfrentarse a sistemas siempre diferentes de atención, según sea la empresa. Una estandarización de estos procesos permitiría a los usuarios conocer la ruta base para poder aplicarla en cada institución sin importar si es pública o privada. Además, facilitaría la transmisión de conocimiento en cuanto a estos derechos y la forma de ejercerlos.

Sexto: La LFPDPPP y la LGPDPPSO no estipulan ningún tipo de protección o medidas preventivas para datos públicos al concebirlos como dominio general. Situación que por sí misma amerita un análisis exhaustivo pues enfrenta dos conceptos aparentemente contrarios.

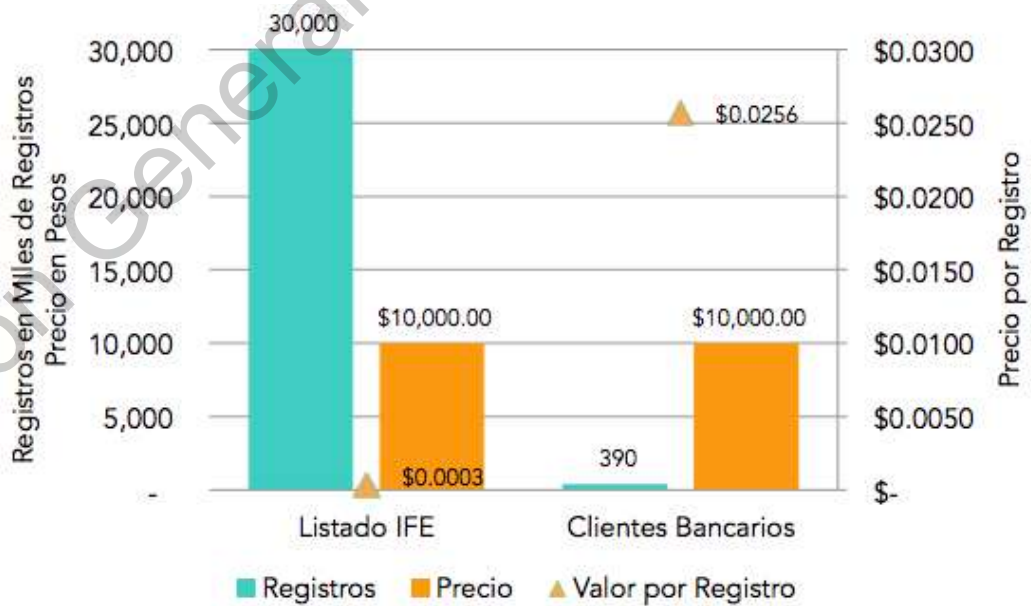
Séptimo: Poca regularización de empresas dedicadas a la venta y comercialización de bases de datos generada por una laguna legal. Ya que "las empresas dedicadas a la venta y comercialización de datos personales generan transacciones utilizando datos de terceros, sean registros públicos o datos que son autorizados por los titulares para su comercialización"[108]. En ambos casos, y aun cuando son prácticas permitidas por la legislación

[108] Asociación Mexicana de Internet A.C (AMIPCI). (2016). Estudio sobre el valor económico de los datos personales. México, AMIPCI, p.40. Disponible en: https://clustertic.org/wpcontent/uploads/2016/06/valor_eco_Datospersonales_FINAL.pdf

vigente, se puede comprometer la seguridad y privacidad de los usuarios, además de representar un campo fértil para el mercado negro de datos personales.

Octavo: El creciente mercado negro de datos personales generado "tanto por dependencias del sector público como por empresas privadas, especialmente del sector financiero"[109]. Por ejemplo, se ha detectado que un listado de 30,000 registros del Instituto Nacional Electoral (antes Instituto Federal Electoral) es vendido en el mercado negro en tan solo $10,000 pesos mexicanos (Tal como se observa en el Gráfico 12). Esto quiere decir que por tan solo 33 centavos de peso mexicano se estaría exponiendo nombre, dirección, fecha de nacimiento, ocupación y clave electoral de una persona.

Gráfico 12. Estimado de precios de datos personales en mercados ilegales en México.



Fuente: AMIPCI, 2016. p.44

[109] Ídem, p.44.

Noveno: El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales no cuenta con mecanismos eficientes que permitan auditar o dar seguimiento a las empresas mexicanas que no reciben quejas. Esto derivado de la multiplicidad de funciones que el instituto tiene que atender en sus tres áreas de desarrollo (transparencia, acceso a la información, protección de datos) y al presupuesto asignado[110] que resulta limitativo para tres áreas tan amplias como las atendidas por el instituto.

Décimo: Empresas e instituciones no ejecutan buenas prácticas ya que no existe una cultura empresarial y gubernamental en materia de protección de datos personales. Hasta ahora, solo se aplican algunas pautas en el sector público y privado con la intención de cumplir la reglamentación oficial pero aún no ha permeado como una cuestión ética y de responsabilidad social.

Ante la detección de estos problemas, se propone una serie de adiciones y modificaciones a la política pública actual para atender los graves riesgos que entrañan las malas prácticas en la gestión de datos personales.

De acuerdo con Santander y Torres-Melo, idealmente *"las políticas públicas son reflejo de los ideales y anhelos de la sociedad, expresan los objetivos de bienestar colectivo y permiten entender hacia dónde se quiere orientar el desarrollo y cómo hacerlo"*[111]. Este argumento nos permite romper con el mito de que la política pública es un diseño exclusivo de los órganos gubernamentales, por el contrario, plantea el deber de involucrarnos en la toma de decisiones.

[110] De acuerdo con el Proyecto de Egresos de la Federación 2019, en este año se asignó al INAI un monto de 900 millones 435 mil pesos.
[111] SANTANDER, Jairo y Jaime Torres-Melo. *Introducción a las Políticas Públicas. Conceptos y herramientas desde la relación entre Estado y Ciudadanía. Bogotá*: IEMP Ediciones, 2013, p.15.

En este sentido, se plantean algunas ideas en el marco de la protección de datos en México; urgente dado el sistema arcaico que tenemos y a la ya importante penetración del IoT, que como se ha visto tiene implicaciones importantes en esta materia.

Como bien sabemos, el diseño de una política pública se compone de una parte estable que contiene los objetivos, ejes rectores y el esqueleto jurídico que dan sostén a la misma; y de otra esencialmente dinámica que se compone de programas, proyectos y acciones que pueden modificarse para atender las condiciones cambiantes del entorno, es decir, se compone de un núcleo y una periferia[112].

En cuanto al núcleo que dará personalidad, fijará los ejes rectores y dibujará el campo de acción de los actores clave en este diseño germinal están: la actualización del Plan Nacional de desarrollo para incluir el tema de protección de datos ya que hasta ahora es un tema obviado por el gobierno federal; Generar una Estrategia General Nacional; Reformar la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, así como la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y; generar tipos penales dentro del Código Penal Federal en materia de violaciones de datos personales (Ver Tabla 5).

[112] MAJONE, Giandomenico. *Evidencia, argumentación y persuasión en la formulación de políticas*. México: Fondo de Cultura Económica, 1989.

Tabla 5. Elementos Núcleo de la Política Pública

Elemento	Objetivo	Temp.	Indicadores de Gestión	Indicadores de Impacto
Actualización del Plan Nacional de Desarrollo.	Contar con un instrumento de PP que marque tendencia en la protección de datos personales a nivel nacional y permita el acceso a presupuesto estandarizado.	1 año	- Número de expertos en colaboración. - Número de actividades realizadas para la formulación.	- Presupuesto contemplado para la Estrategia Digital Nacional (específicamente la PDP).
Estrategia Digital Nacional	Diseñar documento rector alineado con el PND que contenga los ejes rectores de la política en materia de protección de datos personales.	1 año	- Número de expertos en colaboración. - Número de actividades realizadas para la formulación. - Tipo de instrumentos empleados para el diseño.	- Porcentaje de programas eficientes en evaluación PRE (Tiempo, objetivo, actor, tipo de apoyo, monto de apoyo, frecuencia de apoyo, formalidad, monitoreo, sanción y elegibilidad).
Reforma de LFPDPPP y LGPDPPSO.	Actualizar la normativa mexicana para incorporar el tratamiento remoto y autónomo, así como categorías de datos según su riesgo, además de otros requerimientos actuales y derivados del IoT.	2 años	- Número de expertos en colaboración. - Número de actividades realizadas para la formulación. Tipo de instrumentos empleados para el diseño.	- Porcentaje de materias de PDP cubiertas por la normatividad.
Tipos penales en materia de violaciones en materia de PDP.	Contar con instrumentos que contemplen sanciones penales para actores que compran y venden datos personales o no cuenten con mecanismos de seguridad para tratamiento remoto y/o autónomo de DP.	2 años	- Número de expertos en colaboración. - Número de actividades realizadas para la formulación. Tipo de instrumentos empleados para el diseño.	- Número de tipos penales eficientes. - Número de carpetas de investigación iniciadas en un año. - Número de sentencias positivas anuales.

Fuente: Elaboración propia.

En cuanto a la parte dinámica (periferia), se proponen las siguientes acciones, divididas en tres de acuerdo a los sectores que atiende. En Primer lugar, las dirigidas al sector empresarial (Ver Tabla 6): un Programa Nacional de Incentivos Fiscales a Empresas que resulte atractivo para los particulares que gestionan datos personales y permita generar mejores prácticas y apego a la ley; Proyecto de homologación y mejora de procedimientos para ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los usuarios sin importar la empresa con la que se estén relacionando y; un Programa Rector de Profesionalización que permita generar recurso humano especializado bajo un estándar nacional de conocimientos y permita cubrir la deficiencia de personal capacitado en el país.

Tabla 6. Elementos Periféricos de la Política Pública

(Relacionados con el sector empresarial).

Elemento	Objetivo	Temp.	Indicadores de Gestión	Indicadores de Impacto
Programa Nacional de Incentivos Fiscales a Empresas	Generar un mecanismo de difusión de la normativa vigente, así como un interés del sector privado por dar cumplimiento a la misma.	2 años	- Número de estrategias de difusión. - Número de incentivos otorgados a empresas.	- Porcentaje de empresas que cuentan con conocimientos avanzados de la legislación vigente. - Porcentaje de empresas que cuentan con mecanismos efectivos de PDP.
Proyecto de homologación y mejoramiento de procedimientos ARCO	Trazar una ruta efectiva para el ejercicio de los derechos ARCO fundamentado en la autogestión.	1 año	- Número de procedimientos modificados. - Número empresas con procedimientos autogestivos.	- Porcentaje de homologación nacional. - Variación porcentual de resoluciones positivas. - Índice de efectividad de procedimientos establecidos.
Programa Rector de Profesionalización	Formar recursos humanos con conocimientos técnicos, físicos y administrativos en materia de protección de datos personales con aval del INAI e instituciones de educación superior.	2 años	- Número de programas de formación inicial. - Número de programas de actualización. - Número de programas de especialización. - Número de instituciones que ofertan programas.	- Porcentaje de empresas que cuentan con personal cualificado y certificado por el INAI. - Porcentaje de Encargados de Datos que se encuentran certificados.

Fuente: Elaboración propia.

En segundo lugar, aquellas acciones orientadas a la sociedad y grupos vulnerables: Programa de difusión de derechos digitales, Proyecto de visibilización de malas prácticas personales y Proyecto de visibilización de deficiencias de protección de datos personales de los dispositivos de IoT (Ver tabla 7).

Tabla 7. Elementos Periféricos de la Política Pública

(Relacionados con la sociedad).

Elemento	Objetivo	Temp.	Indicadores de Gestión	Indicadores de Impacto
Programa de difusión de derechos digitales	Fomentar el conocimiento generalizado de ciudadanía digital y derechos digitales con énfasis en derechos ARCO. - Primarias y secundarias. - Grupos de mujeres. - Adultos mayores. - Periodistas. - Defensores sociales y activistas. - Comunidades indígenas. - Comunidad LGBTTTIQ	1 año	- Número de beneficiarios directos e indirectos. - Presupuesto asignado a instituciones públicas para su ejecución. - Índice de actividades de sensibilización, socialización y promoción de los derechos digitales.	- Porcentaje de entidades federativas que aplican alguna estrategia. - Variación porcentual en nivel de conocimiento social sobre derechos digitales. - Variación porcentual de quejas y procedimientos iniciados por mal uso de datos personales presentadas ante instituciones públicas.
Proyecto de visibilización de malas practicas personales en materia de protección de datos.	Generar mecanismos que permitan a grupos vulnerables visibilizar malas prácticas en materia de protección de datos personales.	1 año	- Número de beneficiarios directos e indirectos. - Índice de actividades de sensibilización, socialización y promoción de los derechos digitales.	- Índice de detección personal de malas prácticas. - Variación porcentual de malas practicas personales en PDP. - Índice de malas prácticas por grupo vulnerable.
Proyecto de visibilización de deficiencias de protección de DP en dispositivos IoT.	Evidenciar a las empresas y dispositivos IoT que presentan deficiencias en PDP.	1 año	- Número de dispositivos analizados. - Número de informes negativos.	- Número de quejas y procedimientos iniciados a las marcas y dispositivos. - Porcentaje de quejas y procedimientos resueltos. - Porcentaje de empresas que ejecutan procedimientos de mejora.

Fuente: Elaboración propia.

Por último, las acciones pensadas para atender el mercado negro y mejorar las pautas administrativas de respuesta: La creación de un nuevo Instituto Nacional de Protección de Datos independiente del actual INAI con la finalidad de mejorar los flujos administrativos sobrecargados actualmente; Proyecto de auditorías aleatorias a empresas que operan en México que permitirá supervisar empresas que no han recibido quejas pero que podrían estar incurriendo en malas prácticas e incluso faltas, y; un Proyecto de seguimiento a empresas que comercializan datos (Ver Tabla 8).

Tabla 8. Elementos Periféricos de la Política Pública

(Relacionados los procesos administrativos).

Elemento	Objetivo	Temp	Indicadores de Gestión	Indicadores de Impacto
Instituto Nacional de Protección de Datos	Crear un órgano independiente del INAI que atienda específicamente los temas de protección de datos, verifique el cumplimiento de la ley, cuente con elementos vinculantes, realice investigación e incida de manera activa en la PP en materia de PD.	2 años	- Presupuesto asignado al INPD. - Índice de acciones ejercidas por el INP.	- Variación porcentual de quejas y procedimientos iniciados por mal uso de datos personales presentadas ante instituciones públicas. - Porcentaje de quejas y procedimientos resueltos.
Proyecto auditoras aleatorias a empresas que operan en México	Generar un mecanismo eficiente que permita auditar a las empresas internacionales y nacionales que operan en territorio mexicano.	1 año	- Número de auditorias anuales.	- Índice de eficiencia de la auditoria. - Índice de riesgos y malas practicas detectadas. - Variación porcentual de violaciones a la norma. - Número de carpetas de investigación penal y civil iniciadas. - Porcentaje de procedimientos concluido positivamente.
Proyecto de seguimiento a empresas que comercializan datos	Establecer pautas de acción y monitoreo continuo a empresas de comercialización legal de datos.	1 año	- Número de empresas monitoreadas. - Número de auditorias. - Número de informes emitidos.	- Índice de eficiencia de la auditoria. - Índice de riesgos y malas practicas detectadas. - Variación porcentual de violaciones a la norma. - Número de carpetas de investigación penal y civil iniciadas. - Porcentaje de procedimientos concluido positivamente.

Fuente: Elaboración propia.

En general, la propuesta pretende dar solución a todos los problemas detectados hasta ahora en materia de protección de datos personales y el vínculo de esto con el internet de las cosas. Esto bajo el entendido de que se debe robustecer la política pública de protección de datos personales en general para poder pensar en un ecosistema que proteja los datos gestionados por dispositivos de la Iot. Además, resulta necesario recalcar que lo aquí presentado apenas son las bases para el diseño de una efectiva política pública y que se requiere diseñar cada uno de los tópicos con estrictos niveles técnicos y con participación de distintos sectores de la sociedad.

En este sentido, se identifican como actores clave a Gobierno Federal, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, así como al Centro de Cultura Digital como entes directores,

encargados de la formalización de la política pública y de la posterior conducción y administración de la misma. A las asociaciones civiles como Internet Society, Red en Defensa de los Derechos Digitales y Asociación de Internet Mx, así como las instituciones de educación superior como aliados, expertos y promotores. Además, la indispensable participación de empresas transnacionales que operan en México, empresas mexicanas y la sociedad en general.

El diseño goza de factibilidad técnica alta ya que las organizaciones civiles que se han mencionado como actores clave poseen conocimientos amplios sobre el tema y pueden generar gran aporte para el diseño desplegado, la operación y el monitoreo; factibilidad legal alta dado que se cuenta ya con un marco jurídico que, si bien requiere actualización, dota de legalidad a las acciones propuestas; factibilidad social media dado que la población en general desconoce aún estos temas y no se cuenta con una preocupación generalizada sobre la protección de datos; factibilidad política alta dado que recientes eventos de fallas en la seguridad digital de instituciones gubernamentales que han comprometido los datos personales de miles de mexicanos generaron la apertura de una ventana política donde se plasma la preocupación de este sector; por último y el grave problema de este diseño es la factibilidad económica baja ya que se requiere de una inversión fuerte y por ahora gobierno federal no se muestra con disposición de flexibilizar el gasto público.

Aunque existen ciertas dificultades en su aplicación, puede comenzarse con trabajos provenientes de las organizaciones civiles y las empresas comprometidas con la sociedad para mejorar un mejor ecosistema de protección de datos personales.

“La responsabilidad de nuestros actos no se transfiere a los objetos inanimados. La ética sigue en manos de los humanos, de momento”.

José Ignacio Latorre.

IX. REFERENCIAS

ABDERRAHMANE Ed-daoudy y Khalil Maalmi. “A new Internet of Things architecture for real-time prediction of various diseases using machine learning on big data environment”, en Journal of Big Data. Núm. 6, noviembre 2019. Disponible en https://doi.org/10.1186/s40537-019-0271-7

ARELLANO Rodríguez, José Salvador. Teoría ética para una ética aplicada. México, Universidad Autónoma de Querétaro, 2012.

Asociación Mexicana de la Industria de Tecnologías de la Información. *Foro AMITI Cybersecurity: en un entorno digital, mejora tu seguridad.* México, 4 de abril de 2019.

Australia Commonnwealth Scientific and Industrial Research Organisation, *Una plataforma segura que conecta dispositivos de la IoT*, Data61, 2017, Australia, http://data61.csiro.au/en/Our-Work/Safety-and-Security/Secure-Systems-and-Platforms/Secure-IoT-platform

BALDÉ, C., Forti, V., Gray, V. Kuehr, R. & Stegmann, P. *Observatorio mundial de los residuos electrónicos 2017*; cantidades, flujos y recursos. United Nations University, 2017.

Banco Interamericano de Desarrollo. *La ruta hacia las smart cities: migrando de una gestión tradicional a la ciudad inteligente.* BID, 2016.

BARRIO, Moisés. *Internet de las cosas*. España, Ed. Reus, 2018.

BEAUCHAMP, Tom. y James Childress. *Principles of Biomedical Ethics*, 5ta edición. Nueva York, Ed. Oxford University Press, 2001.

BENJAMIN, Walter. La obra de arte en la era de su reproducción técnica, en Discursos interrumpidos. Madrid, Ed. Taurus.

BANKINTER. *El internet de las cosas: en un mundo conectado de objetos inteligentes*. Fundación de la innovación Bankinter, Portugal, 2011.

CASTRO Sola, M. *Internet de las cosas. Privacidad y seguridad*. Andalucía, Escuela Politécnica de Jaén, 2016.

Comisión de las Comunidades Europeas, *"i2010 – Una sociedad de la información europea para el crecimiento y el empleo"*, 2005, Bruselas, http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52005DC0229&from=ES.

DARANAS, M. (Tr). Jurisprudencia constitucional extranjera. Tribunal Constitucional Alemán. Boletín de jurisprudencia constitucional, núm. 33. España, 1984.

Defense Advanced Research Projects Agency. *A History of the ARPANET: The First Decade*, Virginia, 1981.

DÍAZ Limón, Jaime. *Abogado digital: estudios sobre derecho cibernético, informático y digital*. México, ed. VLex, 2019.

DÍAZ Rojo, José Antonio. *La privacidad: ¿Neologismo o barbarismo?*, en Espéculo Revista de Estudios Literarios. Madrid, Universidad Complutense de Madrid, 2002, p. 6. Disponible en: https://digital.csic.es/bitstream/10261/3662/1/privacidad.pdf

ELDRIDGE Scott, Karen Rose y Lyman Chapin. *La internet de las cosas – Una breve reseña*, Internet Society, 2015.

ESPINOZA Cecibel, María José PÉREZ, María Beatriz PERALTA. *Internet de las cosas: Antecedentes, conceptualización y riesgos*. Ecuador, Universidad Técnica de Machala, 2017.

EVANS, Dave. Internet de las cosas: cómo la próxima evolución de internet lo cambia todo, Cisco Internet Business Solutions Group, 2011.

Fray Bartolomé de las Casas. Brevísima relación de la destrucción de las Indias. Editorial Universidad de Antioquía, 1552.

GARCÍA Mexía, Pablo. *Derechos y libertades, internet y Tics*. España, Ed. Tirant lo Blanch, 2014.

GONZÁLEZ Graciano. *El imperativo tecnológico, una alternativa desde el humanismo*, España, Asociación Española de bioética y ética médica, 2004.

GreenPeace. Envenenando la Pobreza: residuos electrónicos e Ghana, 2008.

HAN, Byung-Chul. *La sociedad de la transparencia*. Barcelona, Ed. Herder, 2012.

HERRÁN Ortiz, Ana Isabel. El derecho a la protección de datos personales en la sociedad de la información, Cuadernos Deusto de Derechos Humanos. Bilbao, Universidad de Deusto, 2003.

HERRÁN Ortiz, Ana Isabel. *La violación de la intimidad en la protección de datos personales*. Madrid, Ed. Dykinson, 1999.

Huawei Technologies Co.,Ltd., *Tendencias y desafíos de la industria*, 2017, http://developer.huawei.com/ict/en/site-iot/article/iot-industry

INAI. *Diccionario de protección de datos personales, conceptos fundamentales.* México, Instituto Nacional de Acceso a la información, 2019.

INCyTU. “Inteligencia artificial”. En Foro consultivo de ciencia y tecnología. Núm. 012, Marzo 2018. Disponible en https://www.foroconsultivo.org.mx/INCyTU/documentos/Completa/INCYTU_18-012.pdf

INTECO. *Riesgos y amenazas en Cloud Computing.* 2011, p. 6. https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

International Telecommunication Union. Recomendación UIT-TY.2060 (06/2012), 2012.

International Telecommunication Union. *RAEE: desde el reto-e hasta la oportunidad-e*, 2015.

International Labour Office. (2012). *The global impact of e-waste, addressing the challenge*. Ginebra, 2012.

Internet Rights & Princiles Colition. *Carta de Derechos Humanos y Principios para Internet*. Internet Governance Forum, 2015.

Internet Society. *Breve historia de internet*. Disponible en: https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/

Internet Society, *Orígenes de internet*, Suiza, Internet Society, 2017, https://www.internetsociety.org/internet/history-internet/brief-history-internet/

ISACA. State of Cyber Security. 2017. Disponible en: https://www.cybersecobservatory.com/wp-content/uploads/2017/06/state-of-cybersecurity-2017-part-2_res_eng_0517-1.pdf

IVAI (2018). Guía para elaborar avisos de privacidad. México, Instituto Veracruzano de Acceso a la información y Protección de Datos Personales, 2018.

KITCHIN, Rob. *"Big data, new epistemologies and paradigm shift"*, en Big Data & Society, núm. I, 2014.

KOESTLER Arthur. *Darkness at noon*, Londres, 2005.

KUEHR Ruediger, y Eric Williams, (2003), Computers and the Environment. Understanding and Managing Their Impacts, Kluwer Academic Publishers, Dordrecht, 2003.

LATORRE Sentís, José Ignacio. *Ética para máquinas*. Barcelona, Ed. Ariel,2019.

LECAROS Urzúa, Juan Alberto. *La ética medio ambiental: principios y valores para una ciudadanía responsable en la sociedad global*, en Acta Bioethica; 19 (2), 2013.

LEE, Gabriel. *El consentimiento válidamente informado en la práctica médica*, en Revista CONAMED, Vol. 9, Nº 3. México, Comisión de Arbitraje Médico, 2004.

LÓPEZ i Seuba, Manel. *Internet de las Cosas, la transformación digital de la sociedad*, España, Editorial Ra-Ma, 2019.

MAJONE, Giandomenico. *Evidencia, argumentación y persuasión en la formulación de políticas*. México: Fondo de Cultura Económica, 1989.

McKinsey&Company. *Perspectiva de ciberseguridad en México*. México, Consejo Mexicano de Asuntos Internacionales, 2018.

McKinseyCompany, *The internet of things: mapping the value beyond the hype*, 2015.

MORALES Prats, Fermin. *La tutela penal de la intimidad: privacy e informática*. Barcelona, Editorial Destino, 1994.

O´REILLY, Karen. *Ethnographic methods*. Londres, Ed. Routledge, 2005.

PEÑA Marí, Ricardo. *De Euclides a Java, historia de los algoritmos y de los lenguajes de programación*. España, NivolaLibros y ediciones, 20016.

PÉREZ Salazar, Gabriel. La Web 2.0 y la sociedad de la información. Revista mexicana de ciencias políticas y sociales. Vol. 56, N1. 212. Mayo/agosto 2011. ISSN 0185-1918.

PINK, Sara et al. *Etnografía digital: principios y práctica*. España, Ed. Morata, 2019.

RODRÍGUEZ Ávila Abel. *Iniciación a la red de internet. Concepto, funcionamiento, servicios y aplicaciones de internet*, España, ideas propias editorial, 2007.

SANTANDER, Jairo y Jaime Torres-Melo. *Introducción a las Políticas Públicas. Conceptos y herramientas desde la relación entre Estado y Ciudadanía. Bogotá*: IEMP Ediciones.

SIMÓN-LORDA, Pablo. *El consentimiento informado y la participación del enfermo en las relaciones sanitarias*. Madrid, ed. Triastela, 1999.

The Software Alliance. *¿Por qué son tan importantes los datos?*. Washington, DC, 2018.

TODOROV, Tzvetan. La conquista de América, el problema del otro. México, Ed. Siglo XXI editores, 2010.

WARREN, Samuel. y Brandeis, Louis. The right to privacy, en Harvard law review, 1890.

Jurídicas

Cámara de Diputados del H. Congreso de la Unión, *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, Diario Oficial de la Federación, 2017, México, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Cámara de Diputados del H. Congreso de la Unión, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, Diario Oficial de la Federación, 2010, México, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Secretaría de Salud, Norma Oficial Mexicana NOM-012-SSA3-2012, Diario Oficial de la Federación, México, 2012, http://dof.gob.mx/nota_detalle.php?codigo=5284148&fecha=04/01/2013

Mesográficas

CONBIOÉTICA. Consentimiento informado. Disponible en: http://www.conbioetica-mexico.salud.gob.mx/interior/temasgeneral/consentimiento_informado.html

HAN, Byung-Chul. La emergencia viral y el mundo de mañana. Periódico El País, 2020, Disponible en: https://elpais.com/ideas/2020-03-21/la-emergencia-viral-y-el-mundo-de-manana-byung-chul-han-el-filosofo-surcoreano-que-piensa-desde-berlin.html

Internet World Stats. *Internet users distribution in the world*. Disponible en: https://www.internetworldstats.com/stats.htm

JIMÉNEZ Cano, Rosa. *El dueño de un Tesla, primer muerto en un coche con piloto automático*. El País, 2016. Disponible en: https://elpais.com/tecnologia/2016/07/01/actualidad/1467337732_779288.html

JIMÉNEZ Cano, Rosa. *Primer atropello mortal de un coche sin conductor*. El País, 2018. Disponible en: https://elpais.com/tecnologia/2018/03/19/actualidad/1521479089_032894.html

Mit Media Lab. Moral Machine. Massachusetts Institute of Technology. Disponible en: http://moralmachine.mit.edu/

Oxford English Dictionary. Disponible en: https://www.oed.com/

Real Academia Española. Diccionario de la lengua española. https://www.rae.es/

ROSENBERG, Matthew y Gabriel J.X. Dance. Así funcionaba la recolección de datos de Cambridge Analytica. The New York Times, 2018. Disponible en: https://www.nytimes.com/es/2018/04/10/espanol/facebook-cambridge-analytica.html

Producción audiovisual

Guardian News. Brittany Kaiser testifies before MPs – watch live (video), 2018. Disponible en: https://www.youtube.com/watch?v=xZAvQzRhJ0I

Netflix Productions, Jehane Noujaim. *The great hack*, Estados Unidos, 2016. Min. 42.16.

Saville Productions, Werner Herzog. *Lo and Behold: Reveries of the connected world*. Documental, Estados Unidos, 2016.