Derechos de la SOBERANÍA DIGITAL

Jesús Armando
López Velarde Campa

UNIVERSIDAD AUTÓNOMA DE AGUASCALIENTES
LA BIBLIOTECA

DERECHOS DE LA SOBERANÍA DIGITAL

DERECHOS DE LA SOBERANÍA DIGITAL

Jesús Armando López Velarde Campa

LA BIBLIOTECA

Derechos de la soberanía digital
Jesús Armando López Velarde Campa

Primera edición: agosto, 2021

D.R. © Ediciones La Biblioteca, S.A. de C.V.
Azcapotzalco la Villa No. 1151
Colonia San Bartolo Atepehuacán
C.P. 07730, México, CDMX.
Tel. 55-6235-0157 y 55-3233-6910
Email: contacto@labiblioteca.com.mx

ISBN UAA: 978-607-8782-66-6
ISBN La Biblioteca: 978-607-8733-39-2

Diseño: Fernando Bouzas Suárez

Impreso y encuadernado en México
Printed and bound in México

Índice

Índice de tablas

Índice de figuras

Índice de gráficas

Prólogo

El mundo se encuentra profundamente interconectado. La vida cotidiana de las personas ya no sólo se delimita por su apego a normas jurídicas o determinaciones de autoridades políticas, sino también, por las acciones y decisiones de grandes empresas internacionales, así como por individuos, grupos y comunidades organizados más allá de las fronteras del estado-nación. La revolución tecnológica que impera ha ocasionado que "ciber" deje de ser un simple elemento compositivo de la lengua para ser una realidad aplicable a prácticamente cualquier ámbito de la actividad humana.

De acuerdo con Bauman[1], en el contexto actual de "modernidad líquida" y derivado de las globalizaciones, del desarrollo científico y tecnológico, se ha propiciado un alejamiento de aquello que en antaño otorgaba unidad y certeza a las personas. Lo anterior resulta palpable para gran parte de las culturas, y en especial, para las occidentalizadas. A decir de Picciotto, como efecto de la globalización los Estados se han fragmentado y se han reorganizado las estructuras de poder;[2] en éste proceso histórico, se ha dado paso a un sistema global, que como apunta Castells[3], se configura en redes de intercambios y flujos acelerados de comunicación, que además, tiene la ambivalencia de ser profundamente incluyente para lo que estima valioso y excluyente de aquello que resulta ajeno.

En este dinámico escenario, conceptos tradicionalmente pétreos como Estado, soberanía, autonomía, seguridad, adquieren una connotación diferenciada en un contexto de fluidez, flexibilidad e interdependencia de los intercambios sociales. Cabe señalar que, como postula Peters[4], la evolución en la interpretación de conceptos como los anteriores bien pudiera hacerse en favor de la persona humana.

---

[1] Bauman, Z., Modernidad líquida, FCE, México, 2009.

[2] Picciotto, S., Fragmented States and International Rules of Law, SLS, 1997, Vol. 6, N° 2, pp. 259-279.

[3] Castells, M., Globalización, identidad y estado en América Latina, PNUD, Santiago de Chile, 1999.

[4] Peters, A., Humanity as the (Alpha) and (Omega) of sovereignty, EJIL, 2009, Vol. 20, N° 3, pp. 513-544.

El ágora gradualmente ha mutado hacia el ámbito virtual. Ahí, la discusión sobre los valores converge con los riesgos, ambos de naturaleza global e impacto local, (glocal); entre otros, se entremezclan: lo público con lo privado, Estado y empresa, individuo y colectividad, razones locales e impactos internacionales.

En esta tesitura, por citar algunos problemas glocales que requieren una adecuada gobernanza, pensemos en cómo en época de confinamiento por medidas sanitarias, los usuarios de medios electrónicos hemos estado expuestos a los ataques (con *Malware* o *Phising*) en contra de la privacidad y las finanzas; o bien, el reto que ha supuesto reconducir los procesos educativos hacia un contexto de mediación tecnológica, o bien, los retos en la operación del gobierno a través de medios electrónicos (e-gobierno). Además, los problemas anteriores han puesto en evidencia uno de naturaleza horizontal, la brecha digital.

De igual manera, es palpable la controversia que han tenido los gobiernos, principalmente de estados de desarrollo económico avanzado, por controlar el surgimiento de actores, como empresas tecnológicas, que le compiten por la gestión de la información (como Google o Facebook) o bien, de particulares que facilitan información clasificada.

También, en ésta gama de retos impacta en el ámbito de lo comercial y lo financiero, con las luchas políticas de las grandes potencias por el control económico, o bien, la emergencia de nuevos valores (criptomonedas), que si bien no son dinero en sí, sirven como activos virtuales con los cuales se generan transacciones fuera del control efectivo de algún banco central.

Acorde a lo hasta ahora comentado, se destaca que para comprender el contexto actual se requiere de información y herramientas que faciliten el conocer el origen y trazar el destino. Y es precisamente ahí donde radica una de las fortalezas de la obra en estudio, ya que, desde un punto de vista crítico, multidisciplinar e incluyente, el Dr. López Velarde Campa nos ofrece, por un lado, el análisis de la institucionalidad que ha regido a la sociedad, y por otro, posibilidades en la (re) interpretación creativa con el objeto de afrontar los nuevos retos derivados de los derechos de la soberanía digital.

En el libro, se analiza una serie de problemas que surgen de la revolución tecnológica y su impacto tanto en las estructuras sociales (jurídicas, políticas y económicas) como en la esfera jurídico-política de las personas.

El trabajo es novedoso, por la actualidad de los temas que aborda, y pertinente, por el desarrollo expositivo que se logra. A lo largo del libro, se va dejando evidencia de la experiencia de nuestro autor en el ámbito de la academia y el oficio del quehacer público. Así, el Dr. López Velarde Campa ofrece claves para entender de manera amplia problemas complejos, con una visión global, con perspectiva jurídica y de impacto político.

Concretamente, en el libro se analiza un nuevo concepto de la soberanía digital y el papel que juega el Estado y el ciudadano en el escenario de la revolución tecnológica. Posteriormente, aborda la ciberdelincuencia así como la ciberseguridad, presentando casos concretos y retos específicos para América Latina. En la obra, se indaga sobre la cuestión ineludible de la brecha digital, con especial atención al vínculo virtuoso que debe generarse entre conocimiento, economía y desarrollo. Así mismo, en el trabajo se describe el papel que desempeñan actores en la escena internacional, como las grandes compañías tecnológicas estadunidenses en la monetización y gestión de los datos (*Big Data*). Finalmente, presenta un análisis sobre el reto que para el proceso europeo de integración económico y financiero supone la regulación de las criptomonedas y el euro digital.

Es importante reconocer que el resultado del esfuerzo del autor, el libro que nos ofrece, es un texto valioso para fines académicos, pero también, es relevante como obra de consulta para los operadores jurídicos, políticos o cualquier persona interesada en entender de mejor manera los retos que las nuevas tecnologías suponen a la sociedad.

José Manuel López Libreros
Doctor en Derecho Internacional por la Univesidad Complutense
Profesor Investigador del Departamento de Derecho
Universidad Autónoma de Aguascalientes

Capítulo 1. Soberanía digital

Introducción

Con la globalización, los productos y servicios digitales se encuentran presentes en todos los aspectos de la vida, convirtiéndose en el sistema central de la economía, de la información, de la investigación, de la política, de la organización de la sociedad y de las relaciones interpersonales.

En los últimos años, las tecnologías de la información y de la comunicación, penetraron en todos los aspectos de la vida de las personas, convirtiéndose en un desafío para los Estados.

De acuerdo con datos de la Unión Internacional de Telecomunicaciones (UIT), a finales de 2019, el 53,6% de la población mundial o 4,1 mil millones de personas, utilizaban Internet.[5] Tan sólo en América Latina "más del 50% del tráfico que consumimos por Internet es canalizado por compañías de Estados Unidos como Google, Facebook y Netflix".[6]

Así pues, en la "medida de que los medios de comunicación masiva se implementaron en el mundo, los gobiernos comenzaron a regular estos servicios, dada su importancia estratégica y su capacidad de influir en las masas".[7]

En América Latina, "la amenaza a la soberanía se puede identificar en tres grandes frentes: proveedores de tecnología, proveedores de red y proveedores de contenidos, los cuales dominan el 100% de nuestros mercados, tienen la capacidad de influir en las decisiones de los ciudadanos y, si en algún momento lo desean, pueden desconectarnos de Internet".[8]

[5] Unión Internacional de Telecomunicaciones (UIT), Estadísticas. Disponible en: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx, consultado el: 05/03/2021.

[6] ¿Estamos perdiendo la soberanía digital?, Disponible en: http://www.andinalinkvirtual/, consultado el 05/03/2021

[7] Idem.

[8] Idem.

Dada la complejidad del fenómeno a estudiar, en un primer apartado abordamos la conceptualización de la soberanía digital, posteriormente profundizamos en el rol que tienen los Estados en la regulación del espacio digital y por último nos acercamos a la soberanía digital desde la postura del ciudadano.

1.1 Concepto de soberanía digital

A los debates tradicionales sobre la soberanía nacional, se han sumado la llamada soberanía digital, entendida ésta como:

> La capacidad de actuar y la libertad de decidir de los consumidores a la hora de desempeñar papeles diferentes en el mundo digital, es decir como operadores en el mercado, en calidad de ciudadanos consumidores de una sociedad, así como en carácter de "consumidores" en las redes. El concepto hace referencia, además, a los derechos y obligaciones de los ciudadanos en el marco normativo estatal y subraya las condiciones marco en las que un individuo puede utilizar medios y servicios digitales libremente, de forma competente y responsable y, de esa forma, estar en condiciones de participar activamente en calidad de ciudadano en una sociedad digital.[9]

En este sentido, de acuerdo con Carlos Rivera, si la soberanía es un derecho exclusivo que ejerce el Estado sobre determinado territorio, la soberanía digital, también debe ser interpretada como:

> El derecho exclusivo de ejercer la autoridad del Estado sobre el ciberespacio y tecnología existente en el territorio sometido a tal soberanía. El Estado nacional dispone en su territorio de un conjunto de bienes y recursos naturales que constituyen un patrimonio inalienable e imprescriptible sobre el cual ejerce soberanía plena. Al concepto de soberanía digital, subyace la idea que un Estado de la autonomía, para determinar su tecnología digital (*hardware* y *software*) ya que al no hacerlo dependiente de otro para generar tecnología digital, no es totalmente soberano, de donde se desprende, que ser soberanos es poder gobernar el Ciberespacio que cada país tiene, con el mayor grado posible de libertad y de autonomía. Sin embargo, el Estado debe mantener el control y la gestión del Ciberespacio, permitiendo que todas las perso-

[9] Sachverständigenrat Für Verbraucherfragen, Soberanía Digital. Estudios científicos del Consejo de Expertos en materia de Asuntos del Consumidor, Alemania, 2017, p. 5.

> nas tengan derecho al acceso a las tecnologías en condiciones dignas y en cantidad suficiente y equitativa. Entendiendo al Ciberespacio como (ente abstracto, homogéneo y especulable) por medio de una relación vertical jerárquica y unidireccional, obteniendo una realidad compleja, multidimensional y dependiente.[10]

En este sentido, la soberanía digital abarca dos caras de la misma moneda, por un lado los derechos y obligaciones de los Estados para regular el ciberespacio, ya sea de manera autónoma o dependiendo de terceros Estados y, por el otro, los derechos y obligaciones de los ciudadanos frente a las tecnologías. Veámos este primer aspecto.

1.2 Soberanía digital: el rol del Estado

Con el avance de los medios electrónicos, la gran mayoría de los países en vías de desarrollo se han visto obligados a importar tecnología, no obstante hay un pequeño grupo de países en el mundo que se encuentran en una carrera sin precedentes por convertirse en una "ciberpotencia" o en una "potencia nacional en el ciberespacio", ahora es tan fundamental como la propia sobrevivencia de los Estados.

En este sentido, "las tecnologías de la información y la comunicación (TIC), la innovación en inteligencia artificial y la capacidad de desplegar sistemas e infraestructura rápidamente en mercados emergentes, están concentradas en algunos pocos países, que ahora han entrado en una carrera por ser el número uno".[11]

Por lo que, diversos Estados, liderados por las grandes potencias, como China, Rusia, Estados Unidos y Francia, han implementado políticas de conectividad global y de manejo de las tecnologías, estos temas son parte de las agendas políticas, económicas y legislativas de las grandes potencias.

El presidente francés, Macron, en un discurso sobre inteligencia artificial (IA) en el College de France, planteó la necesidad de hablar ya

[10] Rivera España, Calos Alberto, Elaboración de un concepto de soberanía digital en base al estudio de los casos de Julian Assange y Edward Snowden, Instituto de Altos Estudios Nacionales, Ecuador, 2017, p. 70.

[11] Ávila Pinto, Renata, ¿Soberanía digital o colonialismo digital?, Sur 27, V. 15, No. 27, 2018, p. 16.

de una soberanía digital europea, señaló que: "¿Quién puede pretender ser soberano, solo, frente a los gigantes digitales?".[12]

Por otro lado, en los EUA, el expresidente Obama, enfocó algunos de sus discursos a la ciberseguridad en referencia a la soberanía nacional, pero vinculado a la idea del Internet abierto, de la libertad de Internet, en contraposición con China, con la instrumentación de políticas restrictivas de acceso y de contenido de Internet a su población.

Vladimir Putin, patrocina el Programa Nacional de Economía Digital que entró en vigor en noviembre de 2019, por el cual llama a los proveedores de servicios de Internet a tener los recursos y herramientas necesarias para seguir operando en el país en caso de ser desconectados del Internet.

En el marco de este programa, en mayo de 2019, se aprobó en dicho país, la Ley Rusa de "desconexión de Internet", que prevé el funcionamiento de la red rusa (RUNET) en caso de la desconexión de las redes internacionales, para protegerse de ciberataques.[13] Al igual que China, Rusia aplica muchas restricciones a sus ciudadanos, como el bloqueo de páginas y la prohibición de usar el VPN para cifrar comunicaciones. En el marco de esta censura, el líder opositor ruso Alexei Navalny fue detenido, en enero de 2021, al aterrizar en el aeropuerto de Moscú, luego de 5 meses de exilio y después de ser envenenado con un agente nervioso.[14]

No obstante, su postura interna de regulación de contenidos y de no permitir intromisiones de carácter cibernético, al exterior, existen acusaciones de su injerencia en las elecciones presidenciales de 2016 en los EUA a favor de Donald Trump, mediante el hackeo de miles

[12] Ministerio de Perú, Embajada de Francia en Lima, Discurso de Emmanuel Macron, Por un renacimiento Europeo. Disponible en: https://pe.ambafrance.org/Discurso-de-Emmanuel-Macron-Por-un-Renacimiento-Europeo, consultado el: 05/03/2021.

[13] ED Economía Digital, Rusia aprueba su ley de "desconexión" de Internet. Disponible en: https://www.economiadigital.es/tecnologia-y-tendencias/rusia-aprueba-su-ley-de-desconexion-de-Internet_622796_102.html, consultado el: 05/03/2021.

[14] BBC News Mundo, Alexei Navalny: líder opositor ruso es detenido tras aterrizar en Moscú, 5 meses después de su envenenamiento. Disponible en: https://www.bbc.com/mundo/noticias-internacional-55698266, consultado el: 05/03/2021.

de correos electrónicos referentes a la campaña de Hillary Clinton, candidata del Partido Demócrata.[15]

Ya siendo presidente Donald Trump, en el año 2018, aceptó las conclusiones de las agencias de inteligencia estadounidenses que afirmaban que Rusia sí había interferido en los comicios, pero matizando, al señalar que la intromisión rusa no tuvo ningún impacto en los resultados.[16]

Para el 2021, la relación entre ambos países sigue siendo complicada, el presidente Joe Biden, dijo que el presidente Putin era un "asesino" y advirtió que "pagaría las consecuencias" por tratar de socavar su candidatura en las elecciones del año 2020.[17]

De acuerdo con Renata Ávila, existen tres elementos con los que cuentan los países en la carrera por la soberanía digital:

- Los recursos, tanto capitales como intelectuales, los primeros se refieren al control de cables y servidores, los segundos a técnicos e instituciones de investigación;
- La arquitectura legal, tanto internacional como nacional que les permita innovar, y
- El capital financiero necesario para invertir en investigación y desarrollo, no solo para expandirse a todos los mercados que sea posible sino exportar formas innovadoras de incorporar las TIC en todos los aspectos de la administración pública, el sector privado, defensa, seguridad y en la aplicación de los derechos de los ciudadanos.[18]

En este sentido, observamos esfuerzos importantes de regulación. Los Estados están consagrando en sus leyes nacionales términos como:

---

[15] BBC News Mundo, Rusia intervino en las elecciones para promover la victoria de Donald Trump. Disponible en: https://www.bbc.com/mundo/noticias-internacional-38274334, consultado el: 05/03/2021.

[16] BBC News Mundo, Trump rectifica: ahora acepta que Rusia sí interfirió en las elecciones presidenciales de los Estados Unidos en 2016. Disponible en: https://www.bbc.com/mundo/noticias-internacional-44867589, consultado el: 05/03/2021.

[17] Expansión, Revista digital, Biden llama "asesino" a Putin y sube la tensión entre EU y Rusia. Disponible en: https://expansion.mx/mundo/2021/03/17/biden-llama-asesino-a-putin-y-sube-la-tension-entre-eu-y-rusia, consultado el: 05/03/2021.

[18] Ávila Pinto, Renata, op. cit., p. 17.

cifrado, servicios nacionales de correo electrónico, localización de centros de datos, enrutamiento nacional del tráfico de Internet e infraestructura nacional de comunicaciones.[19]

Muchos gobiernos han promulgado leyes para proteger al propio Estado y a sus nacionales. En Brasil, el presidente Rousseff, propuso un plan para eliminar el Internet brasileño de las influencias de los EUA y otros países más avanzados tecnológicamente, como una medida para afirmar su soberanía digital.

Alemania, creó correos electrónicos nacionales, cables submarinos y almacenamiento de datos localizados a fin de contrarrestar la vigilancia de los EUA.

Francia adoptó el chat encriptado de código abierto gubernamental después del hackeo de sus datos durante las elecciones de 2017, para reafirmar su soberanía digital. Canadá mejoró su infraestructura para disminuir el enrutamiento de sus datos a través de los EUA.[20]

En este sentido, existen 4 elementos fundamentales que deben atender los Estados:

- La toma de acciones sobre el ciberespacio es parte de la soberanía tradicional del Estado.
- Atañe al ámbito nacional su regulación.
- El Estado, a través de su política tecnológica y digital expresa un alto grado de soberanía.
- El Estado que ejerce su soberanía digital: a) tendrá independencia en su política tecnológica y digital, b) generará ingresos al exportarla, c) puede ser prestamista de ancho de banda, d) la tecnología puede convertirse en expresión de su identidad.[21]

No obstante, son los propios Estados y saben y reconocen que el regular las redes digitales se extienden más allá de la soberanía nacional, ya que la infraestructura del ciberespacio se desarrolla a escala planetaria, rompiendo así con la figura del Estado Nación, por lo que a nivel internacional, también se están llevando a cabo grandes esfuerzos como por ejemplo los Foros de Gobernanza de Internet.[22]

[19] Sabiguero, Ariel, et al., Relaciones entre soberanía y tecnología en los tiempos de Internet, Revista de la Facultad de Derecho, No. 41, Jul-Dic, Uruguay, 2016.
[20] Idem.
[21] Rivera España, Calos Alberto, op. cit., p. 69.
[22] Sabiguero, Ariel, et al, op. cit.

1.3 La soberanía digital y los ciudadanos

En cuanto al tercer aspecto, podemos afirmar que la soberanía digital impacta directamente sobre:

> El derecho de los pueblos a acceso tecnológico, navegar por Internet, recibir, transmitir y almacenar información de forma segura, así como la potestad de cada estado para detallar sus propias políticas tecnológicas y digitales de acuerdo a objetivos de desarrollo permanente y seguridad del ciberespacio, capacidad para solventar y controlar lo relacionado con el ciberespacio, incluido el ancho de banda que hay en circulación, los equipos tecnológicos, los tipos de *software*, sistemas operativos, seguridad, etc.[23]

En este sentido la soberanía digital "es la capacidad del pueblo de gestionar la producción y distribución tecnológica y digital",[24] vinculada a la libertad de elección, autodeterminación, autocontrol y seguridad para los ciudadanos.[25]

Bajo esta perspectiva, la soberanía digital se encuentra vinculada también a la participación ciudadana en países democráticos, en términos del gobierno abierto, la gobernanza global del Internet, la transparencia, la protección de datos personales y de marcas y patentes, donde interactúen ciudadanos, y otros actores sociales, económicos y políticos de manera cotidiana.[26]

Por lo que el concepto de soberanía digital se entiende relacionado al derecho de decidir y disponer de medios para ello y al empoderamiento de los ciudadanos a través de las nuevas tecnologías, como herramientas de la vida diaria, por ejemplo las telecomunicaciones, la informática de usuario, las plataformas móviles y las redes sociales.

Así pues, la soberanía digital abarca aspectos sociales, económicos y políticos fundamentales para la ciudadanía cuando se vincula a los gobiernos abiertos en países altamente democráticos, en donde se utilizan mecanismos de participación ciudadana, tales como las iniciativas

[23] Rivera España, Carlos Alberto, op. cit., p. 68.
[24] Ibidem, p.69
[25] Sachverständigenrat Für Verbraucherfragen, op. cit.
[26] López Velarde Campa, Jesús Armando (Coord.), La Gobernanza en la Ciudad de México. Visiones multidisciplinaria, Instituto de Investigaciones Jurídicas, UNAM, Asamblea Legislativa del Distrito Federal, VII Legislativa, México, 2018, p. 124.

populares o los presupuestos participativos, por ejemplo, en Suiza, los referendos, el presupuesto participativo en Brasil o México, en los que la soberanía digital viene a sumarse a la apertura de espacios para los ciudadanos.

En este sentido, "la implementación de las nuevas tecnologías en el modelo de participación y gestión provoca que la consulta suponga un engranaje más de las instituciones, pasan a ser herramientas auxiliares (presupuestos participativos) o procesos de especial importancia (*referendums* vinculantes), a mecanismos útiles para la gestión pública y la toma de decisiones políticas".[27]

Adicionalmente, la utilización de las tecnología en el ejercicio de los derechos de los ciudadanos vuelve fundamental su utilidad en los procesos democráticos, ello sin desconocer, que el solo hecho de contar con las tecnologías no garantiza el ejercicio de los derechos ciudadanos.

En el estudio científico del Consejo de Experto en materia de Asuntos del Consumidor sobre la Soberanía digital, señalan diferentes medidas que se deben adoptar para hacer realidad este derecho ciudadano:

[27] Martínez Cabezudo, Fernando, Soberanía tecnológica y gobierno abierto. Profundizando en las necesidades democráticas de la participación desde la tecnopolítica, Revista Internacional de Pensamiento Político, I Época, vol. 10, 2015, p. 50.

Tabla 1. Soberanía digital. Vertientes y propuestas

Vertiente	Propuestas
Tecnología	- Crear un portal de datos centrado en el consumidor: el SVRV recomienda el desarrollo de un portal de datos centrado en el consumidor (tablero de mandos) para materializar la soberanía individual de datos. - Introducir principios de privacidad desde el diseño y de privacidad por defecto: el SVRV reafirma la exigencia de una configuración predefinida de los sistemas de comunicación (privacidad / seguridad desde el diseño y privacidad / seguridad por defecto como directrices) que sea accesible para el usuario, consuma menos datos y, al mismo tiempo, esté orientada a la seguridad. Los proyectos fomentados de forma estatal deberán regirse por estas directrices. - Aumentar la seguridad en el Internet de las cosas: de cara a los problemas de seguridad cada vez más graves en el segmento del Internet de las cosas, el SVRV recomienda verificar cómo se puede garantizar que, a imagen de los procedimientos en el sector sanitario, se puedan asegurar de forma continua y comprometida los productos y servicios puestos en circulación a través del ciclo vital completo por medio de actualizaciones de seguridad. Será necesario desarrollar estándares tecnológicos y depositar de forma duradera códigos fuente (de forma análoga a la „fórmula" utilizada en el sector alimenticio). - Ampliar la oferta de productos que consuman menos datos: el SVRV recomienda verificar si se puede conceder a los consumidores un derecho a la utilización de productos digitales que recopilen menos datos y que les permita tener la posibilidad de poder escoger una variante digital que recoja menos datos.
Competencia Digital	- Cerrar un pacto de cualificación para la „competencia digital en la formación de docentes": el SVRV recomienda realizar un pacto de cualificación para la „competencia digital en la formación de docentes" (de forma análoga al pacto de calidad de la enseñanza o a la ofensiva de calidad en la formación de docentes). - Apoyar las ofertas para fomentar la competencia digital: el SVRV recomienda financiar de forma permanente y afianzar estructuralmente las ofertas ya existentes para fomentar la competencia digital o las (institucionales) que puedan establecerse en el futuro. Para lograrlo se deberán ampliar sistemáticamente las ofertas que sirvan de hilo conductor, las ofertas para multiplicadores y las ofertas para los consumidores. - Desarrollar medidas de autocontrol al utilizar medios y servicios digitales: el SVRV recomienda a los ministerios de cultura desarrollar medidas para fomentar el autocontrol al utilizar los medios y servicios digitales. - Estudiar los efectos de la digitalización en la cognición, la emoción y la vida social: el SVRV recomienda el fomento específico de la investigación interdisciplinaria sobre los efectos de la digitalización en la cognición, la emoción y la vida social de los consumidores. Esto afecta tanto a los „aborígenes digitales", como así también a los „migrantes digitales".

Vertiente	Propuestas
Regulación	- Formular CGC (Condiciones Generales de Contratación) y declaraciones en materia de protección de datos de forma breve en una sola página (one-pager): el SVRV reafirma la recomendación de que antes de concluir un contrato las empresas informen al consumidor en una sola página (500 palabras) sobre las normas relevantes respecto al derecho en materia de protección de datos, así como las disposiciones de las CGC. El SVRV recomienda que esa idea de „una sola página" se implemente por medio de un proyecto piloto organizado por el Ministerio Federal Alemán de Justicia y Protección al Consumidor (BMJV) con sectores interesados importantes. - Revelar algoritmos y permitir que sean verificables: el SVRV reafirma la recomendación de asegurar mediante normas legales (a) que los algoritmos tengan en cuenta las normas de los derechos del consumidor, del derecho en materia de protección de datos, del derecho en materia de antidiscriminación y de la seguridad digital, así como hacer transparentes los parámetros en los que se basan los algoritmos que estén en contacto directo con los consumidores y (b) que mediante la obligación estandarizada de revelar informaciones se revelen estos algoritmos a un círculo de expertos que mediante la toma de pruebas al azar verifique la seguridad legal. El SVRV recomienda desarrollar estándares legales y depositar de forma duradera los códigos fuente. - Mejorar el derecho a la información gratuita: el Consejo de Expertos recomienda garantizar el derecho a la información gratuita (artículo 34 de la BDSG [Ley Alemana sobre Protección de Datos]) sin limitaciones, así como obligar a las empresas a informar a los consumidores de forma transparente, entendible y fácilmente reconocible sobre el derecho que los consumidores tienen a la información y a la posibilidad de rectificar datos erróneos al ofrecer sus productos (es decir rectificación, eliminación y bloqueo). - Seguir desarrollando estándares mínimos para la interoperabilidad: el SVRV recomienda desarrollar estándares mínimos que garanticen una cierta compatibilidad entre los servicios digitales de forma tal que sea posible una comunicación entre las cuentas de usuario independientemente de los oferentes (interoperabilidad – de forma análoga a la telefonía móvil). - Concretizar el derecho a la portabilidad de los datos: el SVRV reafirma la recomendación de entender el derecho a la portabilidad de los datos como el derecho a rescisión de contrato y recomienda fijar un marco para poder cambiar entre los diversos oferentes (de forma análoga a las transacciones de pago digital).

Fuente: Sachverständigenrat Für Verbraucherfragen, Soberanía Digital. Estudios científicos del Consejo de Expertos en materia de Asuntos del Consumidor, Alemania, 2017.

Capítulo 2. Ciberdelincuencia

Introducción

El cibercrimen es un delito transnacional de rápido crecimiento en el mundo actual, derivado de las TIC. El uso de las TIC ha generado beneficios para la población y los países, pero también riesgos, ya que han abierto nuevas posibilidades a los delincuentes para cometer delitos en el ciberespacio.

De acuerdo con datos de *The Boston Consulting Group* de 2017, el cibercrimen se ha vuelto un negocio global, que a nivel mundial cuesta 575,000 millones al año, en América Latina tiene un costo de 90 mil millones, lo cual constituye aproximadamente la mitad el PIB de Perú.[28]

Respecto a cifras de ciberataques de 2016 y 2017, estadísticas de *Kaspersky Lab*, revelaron que los usuarios de Internet en América Latina recibieron un total de ataques de 677,216,773 ataques de *malware* en 2017, 59% mayor a los recibidos en el año anterior.[29]

En la misma región, de 2018 a 2020, se registraron 97 millones de ataques de *phishing*, encaminados a engañar con premios, historias y relatos a los usuarios con la finalidad de obtener acceso a sus cuentas y tan solo en 2020, se presentaron 42 ataques de *software* malicioso o *malware* por segundo en América Latina.[30]

Adicionalmente, la propia naturaleza de estos ataques implican complicaciones operativas y jurisdiccionales para poder llevar ante la justicia a los delincuentes, que implican la aplicación de la ley correspondiente, los retos en las investigaciones transfronterizas, problemas

[28] E&N, Centroamérica y Mundo, Los ciberataques (en el mundo) cuestan US$575.000 millones anuales. Disponible en: https://www.estrategiaynegocios.net/centroamericaymundo/1111615-330/los-ciberataques-en-el-mundo-cuestan-us575000-m-anuales, consultado el: 05/03/2021.

[29] Idem.

[30] El Tiempo, El cibercrimen no descansa, éstas son las proyecciones para el 2020. Disponible en: https://www.eltiempo.com/tecnosfera/dispositivos/cifras-de-ciberataques-de-2019-y-tendencias-para-el-2020-435508, consultado el: 05/03/2021.

jurídicos y las capacidades de cooperación y tipificación de delitos en todo el mundo.

En este sentido, este capítulo lo reservamos al estudio de la ciberdelincuencia, fundamentalmente el Tratado de Budapest de 2001, como uno de los mayores esfuerzos en el ámbito internacional por contar con marcos normativos de cooperación y armonización de las legislaciones nacionales para la persecución de ciberdelitos y finalmente abordamos dos casos paradigmáticos que prendieron las alertas sobre la vulnerabilidad de los gobiernos ante este tipo de delitos.

2.1 Ciberdelincuencia y el Convenio Sobre Ciberdelincuencia de 2001 (Convenio de Budapest)

En las últimas décadas, se ha tratado de definir al ciberdelito desde diversas perspectivas. Asimismo, se le ha diferenciado de términos como delito informático, que se refiere a "cualquier comportamiento ilícito realizado mediante operaciones electrónicas que atentan contra la seguridad de sistemas informáticos y de los datos que éstos procesan".[31] En cambio el ciberdelito se conceptualiza como:

> Cualquier comportamiento ilícito cometido por medio de un sistema informático o una red de computadores, o relacionado con éstos, incluidos delitos tales como la posesión ilícita y la puesta a disposición o distribución de información mediante sistemas informáticos o redes de computadores".[32]

Esta definición es muy amplia, abarca tanto delitos tradicionales como es el homicidio, en caso de que se haya utilizado una computadora, como objeto físico, para lesionar y matar a alguien, hasta la distribución de pornografía, fraude informático, robo, falsificación, espionaje, extorsión, piratería, crímenes contra la propiedad intelectual, entre otros.

Es decir, los ciberdelitos, implican "cualquier infracción punible, ya sea delito o falta, en el que se involucre un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de

[31] ITU, Ciberseguridad. Comprensión del Ciberdelito: Fenómenos, Dificultades y Respuesta Jurídica, Informe. 2014, p. 11.
[32] Idem.

audio o video o dispositivo electrónico, en general, puede ser usado para la comisión de un delito o pueda ser objeto del mismo delito".[33]

Por su propia naturaleza internacional se requiere un esfuerzo internacional para su persecución y sanción. Por ejemplo, la INTERPOL cuenta con una estrategia mundial contra la ciberdelincuencia que abarca las siguientes acciones:

- Evaluación y análisis de amenazas y seguimiento de tendencias. Ésta es una medida preventiva que busca identificar posibles ataques, ciberdelincuentes y grupos de ciberdelincuencia.
- Acceso a datos digitales brutos. Una vez realizado el ataque, facilitar, por parte de las autoridades correspondientes, acceso a todos los datos relacionados con el ciberataque, herramientas y mecanismos que permitan su persecución.
- Procesos de gestión de pruebas. Se refiere a la recopilación legal de pruebas informáticas y conservación de las mismas para poder llevar a cabo el proceso judicial.
- Correlación de información digital y física. Se entiende la labor de realizar una correlación entre las huellas digitales y la identificación física, es decir, la ubicación real de los posibles perpetradores.
- Armonización e interoperación. Mejorar la cooperación en la persecución de estos delitos e impulsar la armonización legislativa.[34]

Como se observa, existe una gran dificultad para determinar y perseguir estos delitos, adicionalmente, no existe un criterio único que comprenda todos los diferentes enfoques jurídicos nacionales, regionales e internacionales sobre cómo deben tipificarse.[35] En este sentido, su naturaleza internacional se ve como un reto para su tipificación, persecución y la consecuente sanción a los ciberdelincuentes.

Un importante esfuerzo para la armonización del marco jurídico aplicable a estos delitos es el realizado por el Consejo de Europa,

[33] Rayón Ballesteros, María Concepción y Gómez Hernández, José Antonio, Cibercrimen: particularidades en su investigación y enjuiciamiento, Anuario Jurídico y Económico, XLVII (2014) pp. 209-234.
[34] INTERPOL. Estrategia mundial contra la ciberdelincuencia. Secretaría General de INTERPOL. 2017.
[35] ITU, Ciberseguridad, op. cit,. p. 12.

que en el año 2001, se reunió con la intención de crear un tratado internacional de vocación universal que estableciera un frente común y protegiera a toda la comunidad internacional de los ataques de la ciberdelincuencia a través de una legislación adecuada y mecanismos de cooperación eficientes.[36]

El resultado fue la adopción, el 23 de noviembre de 2001, en Budapest, Hungría, del Convenio sobre la Ciberdelincuencia, en vigor desde 2004. Siendo éste el único tratado internacional sobre la materia, constituye una "ley modelo"[37] o en ejemplo para las legislaciones nacionales a fin de armonizar sus marcos jurídicos internos y políticas para prevenir y sancionar los ciberdelitos.

Este instrumento internacional se divide en 4 grandes apartados: derecho penal sustancial, en el que se establecen los tipos penales de los delitos cibernéticos; el derecho procesal penal, en esta parte se establecen los procedimientos para la conservación de datos que sirvan para la investigación penal, cooperación judicial; formalidades para la firma, ratificación o adhesión al tratado, entrada en vigor, entre otros.[38]

Este tratado requiere que los Estados parte del mismo, se obliguen a incluir en sus marcos jurídicos dos cuestiones fundamentales:

- Tipificar 4 categorías de delitos: delitos cometidos contra la confidencialidad, integridad y disponibilidad de sistemas y datos informáticos; delitos cometidos mediante el uso de las TIC; delitos por su contenido (por ejemplo, pornografía infantil); y delitos contra derechos de autor.
- Dotar a las autoridades penales de facultades y herramientas procedimentales para investigar y sancionar los delitos cibernéticos; que incluyen: capacidades de inteligencia y vigilancia, cateo e incautación de bienes, monitoreo de contenidos en línea, retención y transferencia de datos e intervención de comunicaciones privadas.

Como se observa, este instrumento internacional establece una categorización de los tipos de ciberdelitos, no obstante ésta no es del

[36] Fundación Karisma, Convenio de Budapest: Aplicación en Colombia frente a derechos humanos, 2018, p. 3.
[37] Centeno Danya, México y el Convenio de Budapest: Posibles incompatibilidades, 2018, p. 3.
[38] Fundación Karisma, op. cit. p. 3.

todo clarificadora, ya que se utiliza un solo criterio para realizar estas categorías. Las primeras 3, se refieren al objeto de protección, es decir la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos, el contenido, y los derechos de autor, pero incluye otra categoría denominada delitos informáticos, que no se refieren al objeto tutelado sino a los medios de comisión. Ello aunado a que varios de los delitos cibernéticos pueden inscribirse en más de una de las categorías causando confusión.[39]

Los delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos, son de los delitos más antiguos en la materia pero que tienen una vigencia importantísima aún en el año 2020. Éstos se inscriben de manera genérica en lo que se ha denominado piratería, que es la incursión de manera ilícita a un sistema informático protegidos en páginas web protegidas por contraseñas.[40]

Algunos de los objetivos más recurrentes de este delito son: la NASA, el Pentágono, las fuerzas aéreas de los EUA, Yahoo, Google, entre otros.[41] Es un delito muy popular entre los ciberdelincuentes y de los que han generado mayor expectativa en la población mundial, dada la información que es expuesta y difundida después de los ciberataques. Algunos lo hacen por burlar las medidas de seguridad, por probar sus capacidades, por motivos políticos o por represalias ante algún acontecimiento.

Para 2019, los ataques más comunes son a través de *malware, phishing* y en contra de la web, el 77.6% de todos los ataques se realizan contra empresas y 22,4% son hacia particulares.[42] Véase Gráfica 1.

[39] ITU, Ciberseguridad, op. cit,. p. 12.
[40] Ibidem. p. 17.
[41] Idem.
[42] El País, Economía, Nube de cifras. Ciberseguridad: las cifras de los ataques informáticos, Revista Retina. Disponible en: https://retina.elpais.com/retina/2020/07/17/tendencias /1594958904_685745.html, consultado el: 05/03/2021.

Gráfica 1. Ciberseguridad. Cifras (2019)

Fuente: https://retina.elpais.com/retina/2020/07/17/tendencias/1594958904_685745.html

En México, en 2020 y en el contexto de pandemia por COVID 19, los ciberataques a particulares son un imperativo constante, por lo cual nuestro país se encuentra en el top 10 de los países con más *phishing* en el mundo. Es decir, los mexicanos son atacados de manera reiterada a través de correos electrónicos anzuelo para el robo de datos personales.[43]

No obstante, la existencia de este tratado, son pocos los países que lo han firmado, ratificado o adherido. Para 2020, sólo 60 Estados, incluyendo países miembros de la UE, Estados Unidos, Canadá, Australia y Japón;[44] no obstante, los ataques cibernéticos siguen ocu-

[43] Expansión, México está entre el top 10 de países con más *phishing* por el COVID-19. Disponible en: https://expansion.mx/tecnologia/2020/04/16/mexico-esta-entre-el-top-10-de-paises-mas-*phishing*-covid-19, consultado el: 05/03/2021.

[44] Biblioteca del Congreso Nacional de Chile, Convenio sobre Ciberdelincuencias: Convenio de Budapest. Disponible en: https://obtienearchivo.bcn.cl/obtie-

rriendo, acometiendo a empresas, ciudadanos y gobiernos, que no se encuentran exentos de éstos.

Ejemplo de anterior, son dos casos paradigmáticos de ataques contra gobiernos que fueron los realizados por Julian Assage, programador, periodista y activista australiano, fundador del sitio web Wikileaks; y Edward Snowden, consultor tecnológico estadounidense, informante y ex empleado de la Agencia Central de Inteligencia (CIA) y de la Agencia de Seguridad Nacional Estadounidenses. En ambos casos, se realizaron incursiones a sistemas gubernamentales y sacaron a la luz información fundamental que afectó a los Estados Unidos.

2.2 El caso de Julian Assange

Julian Paul Assange nació el 3 de julio de 1971 en Australia, Townsville, Estado de Queensland. Desde su adolescencia se interesó por la programación, y en 1991 fue detenido por hackear las computadoras de una Universidad australiana y de otras instituciones, en ese momento se declaró culpable de 24 delitos informáticos.[45]

Ya desde joven notaba su interés por la libertad de expresión y del *software* libre, así como sus dotes en el manejo de las computadoras pero fue hasta el año 2006, que fundó Wikileaks.org, como "un servicio público cuyo objetivo es proteger a informantes, periodistas y activistas" que quisieran publicar material sensible. Sitio que funcionaba con base en donaciones independientes.[46] Aunque cabe señalar que años más tarde, colaboradores del sitio denunciaron la opacidad del manejo de los recursos.[47]

Este sitio, sin fines de lucro, se encarga de difundir documentos de interés público, que provocan el enojo de gobiernos y el asombro de los ciudadanos,[48] por lo que con el objetivo de que no cierren su

nearchivo?id=repositorio/10221/26882/1/Convenio_de_Budapest_y_Ciberdelincuencia_en_Chile.pdf, consultado el: 05/03/2021.

[45] El Comercio, Política, Conozca quién es Julian Assange y la cronología del caso, 2012. Disponible en: https://www.elcomercio.com/actualidad/politica/conozca-julian-assange-y-cronologia.html, consultado el: 05/03/2021.

[46] Rivera España, Carlos Alberto, op. cit., p. 69.

[47] El Comercio, Política, op. cit.

[48] Idem.

sitio, los servidores donde alojaba la información se repartían en varios países.[49]

Wikileaks es la "versión no censurable de Wikipedia para el *leaking* (publicar información secreta sin autorización oficial) y análisis masivo de documentos de manera no rastreable, combina la protección y anonimidad que proporciona la tecnología criptográfica *cutting-edge* con la transparencia y simplicidad del interfaz wiki".[50]

En una declaración de 2006, Assange señaló que el propósito de Wikileaks es: "El objetivo es la justicia, el método la transparencia".[51] En 2007, había publicado el saqueo económico realizado a Kenia por parte del Presidente Daniel Arap Moi; y en 2008, difundió extractos de correos electrónicos de la Gobernadora de Alaska y candidata a la Vicepresidencia de los EUA, Sarah Palin.[52]

En marzo de 2008, tras la publicación de comunicaciones de la Embajada de EUA, el Pentágono sostuvo que planeaba destruir la confianza de Wikileaks y amenazó a Assange con exponerlo y criminalizarlo.[53]

Más adelante, en 2010, Assange publicó más de 700 mil documentos clasificados, donde se documentan crímenes cometidos por el ejército estadounidense durante las guerras de Irak y Afganistán, cables diplomáticos del Departamento de Estado de las comunicaciones de las embajadas estadounidense en todo el mundo.[54] En ese momento, Assange declaró que lo hizo por "traer a la luz las políticas de gobiernos de conspiración y miedo".[55]

---

[49] Rivera España, Carlos Alberto, op. cit., p. 70.

[50] Idem.

[51] Rees, Stuart, Julian Assange and Wikileaks: a case study in the criminalization of dissent, University of Sydney, Australia, 2019.

[52] El Mundo, Wikileaks: cronología de un escándalo, 2011. Disponible en: https://www.elmundo.es/elmundo/2011/11/02/internacional/1320232744.html, consultado el: 05/03/2021.

[53] Rees, Stuart, op. cit.

[54] Página 12, Diario del juicio a Julian Assange, 2020. Disponible en: https://www.pagina12.com.ar/293866-diario-del-juicio-a-julian-assange, consultado el: 05/03/2021.

[55] France 24, La historia por la que Julian Asange lleva una década en la mira de EE.UU. 2020. Disponible en: https://www.france24.com/es/historia/20200227-historia-julian-assange-wikileaks-extradicion-juicio, consultado el: 05/03/2021.

Después de la publicación por parte de Wikileaks de un cuarto de millón de documentos sobre las guerras en Irak y Afganistán, así como de un video de cómo el ejército estadounidense mató a 11 iraquíes en julio de 2007,[56] donde se mostraban imágenes de la guerra, que presentaban a soldados estadounidenses asesinando, desde un helicóptero a civiles, entre ellos adultos y niños heridos en las calles de Bagdad.[57]

Ocho días después de la publicación del video, el Secretario de Defensa, Robert Gates, aseguró que el video había sido publicado sin proporcionar el contexto de la operación.[58]

Ese mismo año, en agosto de 2010, en Suecia, se inicia una investigación en su contra por presunto acoso sexual. Esto no desalentó a Assange, que en octubre de 2010 publicó en su plataforma 391,000 documentos del Pentágono sobre la inactividad de los EUA respecto a presuntos abusos contra presos en Irak de 2004 a 2009, o fallecidos durante la invasión.[59]

Fue hasta el 7 de diciembre de ese año, que el periodista fue arrestado por la policía británica, que en colaboración con la policía europea, hizo cumplir una orden de arresto emitida por la Fiscalía Sueca. No obstante, el 16 del mismo mes queda libre luego de pagar su fianza, cabe señalar que fueron sus seguidores quienes lo apoyaron recaudando 240,000 libras esterlinas.[60] Ese mismo día, Visa y Mastercard suspende los pagos a Wikileaks y hackers bloquean la página de la Fiscalía de Suecia y de Mastercard.[61]

El 7 de febrero de 2011, se anunció el inicio del juicio para el proceso de extradición del periodista a Suecia y el 24 de ese mismo mes, el Juez Howard Riddle del Tribunal de Belmarsh, aprueba la extradición. Paralelamente, Wikileaks filtró 251,287 documentos de comunicaciones estadounidenses con sus diplomáticos con la instrucción de espiar a políticos extranjeros y altos funcionarios de la ONU.[62]

A principios de ese año, Wikileaks denunció que las grandes corporaciones estaban vendiendo a los gobiernos sus sistemas de datos,

[56] El Mundo, op. cit.
[57] Rees, Stuart, op. cit.
[58] El Mundo, op. cit.
[59] Idem.
[60] France 24, op. cit.
[61] El mundo, op. cit.
[62] Idem.

para desarrollar mecanismos de vigilancia y control de la información de cada persona, a través de sus celulares, correos electrónicos y redes sociales,[63] y para agosto y septiembre de 2011, Wikileaks publicó 230,000 cables de la diplomacia estadounidense, y en octubre de ese mismo año, esta empresa anunció que dejaría de publicar documentos oficiales por falta de financiamiento.

El 19 de junio de 2012, Assange, transgrediendo su fianza, ingreso a la Embajada Ecuatoriana en Londres para huir de su inminente extradición a Suecia y ser juzgado por cuatro acusaciones de acoso sexual y violación planteadas por dos mujeres con las que tuvo contacto en agosto de 2010,[64] cuando viajo a Suecia con la intención de poner una sucursal de Wikileaks en dicho país.

Meses después le fue concedido el asilo político por parte de la Embajada Ecuatoriana, donde estuvo refugiado durante 7 años, no obstante, en abril de 2019, la policía del gobierno de Reino Unido lo detuvo, por lo cual se encuentra en una cárcel de máxima seguridad.

Reino Unido lo condenó a 50 semanas de prisión por incumplir su fianza y Suecia reabrió las investigaciones por abuso sexual, aunque pocos meses después desestimo uno de los casos por falta de evidencia.[65] No obstante, enfrenta un juicio en el que se determinará si es extraditado o no a los EUA, acusado por 18 cargos por la infiltración de miles de documentos secretos,[66] espionaje, reclutamiento, conspiración, piratería informática, así como exponer la vida de algunos de sus informantes en el extranjero.[67]

El 7 de septiembre de 2020 se inició la segunda fase del juicio de extradición de Assange, había comenzado en febrero pero se pospuso por la pandemia de COVID 2019. Semanas antes del reinicio del juicio, los EUA, presentaron nuevas denuncias, en las que también acusaron a dos socios de Wikileaks y un empleado por conspirar contra la seguridad estadounidense, además de sostener que no solo recibió

[63] France 24, op. cit.
[64] Rivera España, Carlos Alberto, op. cit., p. 71.
[65] France 24, op. cit.
[66] Proceso, Assange presenta depresión severa y comportamientos suicidas, 2020. Disponible en: https://www.proceso.com.mx/649615/assange-presenta-depresion-severa-y-comportamientos-suicidas, consultado el: 05/03/2021.
[67] Página 12, op. cit.

información del ex soldado estadounidense Chelsea Manning sino de otros hackers.[68]

Sus abogados señalaron que no se les brindó suficiente tiempo para preparar la defensa sobre las nuevas acusaciones. Asimismo, sostuvieron que la extradición a los EUA sería ilegal, ya que existen razones para sospechar que el juicio será injusto, ya que los delitos por los que se le llevará juicio están políticamente motivados y adicionalmente, Assange se encuentra gravemente deprimido y en alto riesgo de suicidio.[69] Por los cargos pudiera ser condenado a 175 años de cárcel.

La importancia de los sucesos antes narrados, radica en el hecho de dar a conocer lo que los gobiernos han tratado de ocultar a los ciudadanos, que se sospechaba pero no se tenía certeza de los hechos.

2.3 El caso de Edward Snowden

Edward Joseph Snowden, nació el 21 de junio de 1983, en Carolina del Norte, en su juventud, siguiendo los pasos de su papá, Oficial de la Guardia Costera de los Estados Unidos (EUA), decidió ser marine. No obstante, su estatura media y su bajo peso, no le permitieron prosperar en ese ámbito.

Más tarde ingresaría a la Agencia Nacional de Seguridad (NSA) y posteriormente a la Agencia Central de Inteligencia (CIA),[70] en donde su conocimiento de Internet y su talento en programación le permitió llevar una carrera en rápido ascenso.[71]

Ahí fue donde descubrió los programas de vigilancia masiva PRISM y Keyscore, capaces de llevar a cabo operaciones de espionaje y acciones globales ilimitadas, en donde ningún ciudadano de los EUA y del mundo está libre de vigilancia.[72] Éstos incluían la recopilación de datos masivos de teléfonos móviles e Internet de las personas, tanto el

[68] Idem.
[69] Proceso, op. cit.
[70] INFOBAE, El caso de Snowden: historia del genio cyber que traicionó a su patria y huyo a Rusia protegido por Putin, 2019. Disponible en: https://www.infobae.com/america/mundo/2019/04/20/el-caso-snowden-historia-del-genio-cyber-que-traiciono-a-su-patria-y-huyo-a-rusia-protegido-por-putin/, consultado el: 05/03/2021.
[71] Rivera España, Carlos Alberto, op. cit., p. 72.
[72] INFOBAE, op. cit.

contenido de las comunicaciones como los metadatos de poblaciones enteras. Ello a través de PRISM, en funciones desde 2007, que utilizaba datos de las principales empresas de Internet y telefónicas.[73]

Se habló de que el Tribunal de Vigilancia de Inteligencia había otorgado una orden secreta que obligaba a *Verizon*, una de las empresas de telecomunicaciones más grandes de EUA, a dar acceso a la NSA a los registros telefónicos de millones de estadounidenses, que incluía llamadas desde teléfonos fijos, como celulares, dentro del territorio estadounidense y llamadas desde los EUA a otros países.[74] Por lo cual, el gobierno obtenía información de los ciudadanos, sospechosos o no de actos terroristas.

También, se reveló que dicho espionaje abarcaba las comunicaciones de 80 Embajadas y Consulados, así como a diferentes líderes del mundo, como Angela Merkel, Dilma Rousseff, Enrique Peña Nieto, funcionarios de la ONU, incluso al Secretario General Ban Ki-moon, empresas como Google, Petrobras,[75] funcionarios de la Unión Europea, Organismo Internacional de la Energía Atómica.[76]

Esta información fue filtrada por Snowden, basado en la idea de que estas acciones eran un abuso a la privacidad y a la libertad de los ciudadanos, consagrada en la Constitución estadounidense.[77]

Fue el 5 de junio de 2013, que se publicó la existencia de esta red infinita de espionaje a través de *The Guardian*, *The New York Times* y otros medios de comunicación, donde explican a detalle las actividades de vigilancia de la NSA y otras agencias de inteligencia.[78]

El 6 de junio de 2013, *The Washington Post*, informó la existencia del programa PRISM, bajo el cual la NSA recopila correos electrónicos, teléfonos de Internet, llamadas, fotos, videos, transferencias de archivos y datos de redes sociales.[79]

---

[73] Karin Wahl, Jorgensen, et al, The Normalization of Surveillance and the Invisibility of Digital Citizenship: Media Debates After the Snowden Revelations, International Journal of Communication 11(2017), pp. 740–762.

[74] Wright, David, European responses to the Snowden Revelations, Increasing Resilience in Surveillance Societies, December 2013.

[75] Idem.

[76] Idem.

[77] INFOBAE, op. cit.

[78] Wright, David, op. cit.

[79] Idem.

El 8 de junio, el Director de Inteligencia Nacional de los EUA, James Clapper, reconoció la existencia del PRISM, señalando que era legal y bajo la autorización del Tribunal de Vigilancia de Inteligencia.[80]

Un día después, el 9 de junio, Snowden reveló que había filtrado los documentos, señalando que "él no quería vivir en un mundo donde todo lo que hago y digo es grabado".[81]

Como consecuencia, el 11 de junio, es despedido por violar la política y código de ética de la empresa donde trabajaba, Booz Allen Hamilton, empresa contratada por la NSA.

El 16 de junio, se refugia en Hong Kong, antigua colonia del Reino Unido y provincia autónoma de China, pero se equivocó en la búsqueda de un país seguro, ya que China fue presionada por EUA para entregarlo.[82] Él escapa de Hong Kong a través de un salvoconducto emitido por el Cónsul de Ecuador en Londres.

El 21 de junio, *The Guardian* publicó que el Gobierno de Reino Unido tenía acceso a las redes de cable que transportaban llamadas telefónicas y tráfico de Internet y que había estado procesando grandes cantidades de información que compartía con la NSA.[83]

El 23 de ese mismo mes Snowden llegó a Moscú en un vuelo comercial y este país le otorgó asilo por un año. La respuesta de los EUA no se hizo esperar, pero no fue tan contundente con Rusia que con los países latinoamericanos y el 27 junio, en ese entonces el presidente Barack Obama, se limitó a señalar que: "No voy a enviar un avión a reacción para detener a un hacker de 29 años..., pero haremos todo lo posible para detenerlo y juzgarlo".[84] Cabe señalar que en EUA la sentencia por traición a la patria y espionaje, puede llegar a la pena de muerte o cadena perpetua.

A la declaración de EUA el Estado Ruso respondió que se había visto obligado a dar el asilo a Snowden, debido a que EUA había atemorizado al resto de los Estados y que nadie lo quería recibir.[85]

En julio de 2013, países latinoamericanos como Ecuador, Venezuela y Bolivia, ofrecieron a Snowden asilo en sus territorios, lo cual

[80] Idem.
[81] Idem.
[82] Rivera España, Carlos Alberto, op. cit., p. 72.
[83] Wright, David, op. cit.
[84] INFOBAE, op. cit.
[85] Rivera España, Calos Alberto, op. cit., p. 72.

provocó la ira de los EUA. El descontento se evidencio a través de la diplomacia.

- En el caso de Ecuador los chantajes económicos fueron las preferencias arancelarias (ATPDEA), beneficios recibidos de los convenios por la lucha contra el narcotráfico; para sorpresa de todos, Ecuador renunció a las preferencias arancelarias e indicó que ese dinero se lo regalaba a EUA para que lo utilizara en beneficio de su población.
- En el caso de Venezuela, EUA reaccionó enviando portaaviones con la intención de atacar al Estado suramericano, situación que no se ejecutó por el inmediato pronunciamiento internacional de diferentes organismos como UNASUR.
- En el caso de Bolivia, Portugal, España y Francia negaron el aterrizaje al avión presidencial boliviano que viajaba con el presidente Evo Morales a Bolivia luego de una gira en Rusia.[86] Se sospechaba que Snowden estaba a bordo del avión, pero no estaba ahí. Ello surgió ya que en una entrevista en Moscú, el Presidente Evo Morales sostuvo que consideraría favorable una solicitud de asilo de Snowden.[87]

El 30 de octubre, *The Washington Post*, publicó que la NSA había entrado en los cables de fibra óptica sin cifrar de Google y Yahoo en todo el mundo, sin permiso de las empresas.[88]

Snowden continúa en Rusia hasta la actualidad, el 16 de abril de 2020 solicitó nuevamente prórroga de 3 años, según comentó su abogado Anatoli Kucherena: "Entregamos a migración los documentos para solicitar la prórroga del permiso de residencia de Snowden, que caduca en abril de este año".[89]

Asimismo, en 2020 Snowden publicó un libro "Vigilancia Permanente", una autobiografía en la que explica cómo llegó a trabajar en estas dos grandes agencias de seguridad estadounidenses, cómo descubrió el espionaje masivo y se decidió a difundir la información.[90]

[86] Idem.
[87] Wright, David, op. cit.
[88] Idem.
[89] El Comercio, op. cit.
[90] Idem.

Pero más allá de los hechos, las revelaciones de Snowden cristalizaron los debates sobre vigilancia, seguridad, ciudadanía digital, privacidad, derechos digitales y sociedad de vigilancia.

Así mismo, se observó una dicotomía en los medios de comunicación, por un lado, los medios conservadores tradicionales que minimizaron el hecho de la vigilancia masiva a millones de ciudadanos, que se centraron en el escándalo de la vigilancia a líderes y grandes personalidades; y por el otro, los blogs que crearon un espacio de mayor libertad y crítica respecto a la vigilancia masiva.

Con las revelaciones de Snowden, los ciudadanos ahora saben que las agencias estadounidenses están violando gravemente su privacidad justificando dicha violación en aras de prevenir ataques terroristas, pero no es solo eso, la vigilancia masiva también va dirigida a dar servicio a las empresas nacionales de los EUA generando una ventaja sobre sus competidores, alterando el orden económico, pero también el social, ya que vigilan también a disidentes y organizaciones civiles.[91]

Así también tensaron las relaciones entre los EUA y los presidentes de otros Estados los cuales habían sido objeto de espionaje, adicionalmente con las empresas que dieron sus bases de datos a la NSA, como Verizon, AT&T, Google y Facebook. Por ejemplo, la Presidenta Dilma Rousseff canceló su viaje los EUA y condenó el espionaje en su discurso en la Asamblea General de la ONU.[92]

La noticia fue impactante, no porque no se hubiera realizado antes, se sabía del espionaje, sino por la magnitud de la vigilancia, parece que la NSA, con ayuda del gobierno de Reino Unido, prácticamente vigila las llamadas y uso de Internet de todos los ciudadanos estadounidenses.[93]

Ambos casos, Assange y Snowden, son famosos por revelar información secreta del funcionamiento del gobierno estadounidense, hallaron fama a nivel mundial por cooperar con diarios muy importantes, han sido objeto de libros, películas e innumerables artículos de periódicos.[94]

---

[91] Wright, David, op. cit.

[92] Idem.

[93] Idem.

[94] El Diario, Assange contra Snowden: parecidos y diferencias. 2014. Disponible en: https://www.eldiario.es/turing/vigilancia_y_privacidad/assange-snowden-parecidos-diferencias_1_5089118.html, consultado el: 05/03/2021.

Los dos tuvieron como motivación la justicia, la transparencia, la libertad de expresión, por lo que pensaron en coadyuvar a hacer público lo que consideraban un abuso, una gran trama de corrupción y violación de los derechos de los ciudadanos,[95] y por su convicción de que "la acumulación masiva de información por parte de un gobierno, es riesgosa para la conservación del sistema democrático".[96]

En este sentido, por un lado, podemos observar las conductas delictivas y abusivas por parte de los EUA, a través de las revelaciones de Assange, que muestran el engranaje de la política interna e internacional estadounidense y las violaciones al Derecho Internacional Humanitario cometidas en las guerras en Afganistán e Irak; por el otro, en las de Snowden se visibiliza la violación masiva a los derechos de los ciudadanos a la privacidad.

No obstante la similitudes, el tratamiento que han tenido ha sido diferente. Snowden es una fuente primaria, tuvo acceso a la información, en cambio Assange, es una fuente secundaría, alguien le transfirió la información para que él la pudiera difundir. En este sentido, las actividades de Assange se encuentran reguladas por las leyes de prensa, aunque los EUA lo acusen de espionaje al igual que a Snowden.[97]

Los medios estadounidenses defienden a Snowden por destapar los abusos de la NSA, en cambio a Assange lo repudian criticando lo poco transparente de su fuente de información.[98]

Snowden ha evitado tener enfrentamientos, malentendidos o choques con los periódicos con los que trabajo, a diferencia de Assange que los medios periodísticos le han denominado con diferentes calificativos despectivos, por ejemplo: "*The New York Times* cuenta que una fuente huele mal y es arrogante en un reportaje firmado por su director, o que publique en portada un perfil muy poco favorecedor

[95] Notimérica, Papeles de Panamá, Snowden y Wikileaks: similitudes y diferencias de las 3 filtraciones. 2016. Disponible en: https://www.notimerica.com/sociedad/noticia-papeles-panama-snowden-wikileaks-similitudes-diferencias-tres-mayores-20160412160516.html, consultado el: 05/03/2021.

[96] Código Frontera, Snowden y Assange: héroes y villanos. 2017. Disponible en: http://www.codigoyfrontera.space/2017/05/24/snowden-y-assange-heroes-y-villanos/, consultado el: 05/03/2021.

[97] El Diario, op. cit.

[98] Código Frontera, op. cit

que tacha su estilo de "dictatorial, excéntrico y caprichoso", ni que *The Guardian* publique en un libro que "se disfrazó de viejecita".[99]

Con el periódico *The Guardian* tuvo problemas cuando David Leigh, periodista de dicho diario, publicó en un libro la contraseña que daba acceso a los cables originales completos con los nombres de informantes. Hecho que posteriormente el gobierno de los EUA denunció contra Assange, ya que consideraba que se había puesto en riesgo la vida de sus informantes.

En términos de cantidad de información, Assange publicó un aproximado de 11.5 millones de documentos confidenciales, en cambio Snowden publicó aproximadamente 1.7 millones.

[99] El Diario, op. cit.

Capítulo 3. Ciberseguridad

Introducción

Los estudios sobre ciberseguridad se iniciaron a mediados de los años 90's, cuando los EUA comenzaron a preocuparse por los hackers o piratas informáticos, que pudieran tener acceso a información gubernamental sobre plantas nucleares, hidroeléctricas, transporte, salud, defensa y otros servicios de infraestructura básica cuya difusión pudiera dejarlos en estado de vulnerabilidad.[100]

En el ámbito internacional, tres sucesos levantaron las alertas sobre la seguridad en el ciberespacio. Por un lado, en 2007, se realizó el primer ciberataque conocido en contra de un país, un ciberataque contra Estonia. Se cree que fue ejecutado desde direcciones rusas, derivado de la remoción de un monumento dedicado a los soldados soviéticos caídos en la Segunda Guerra Mundial. Se trata de la escultura del "soldado de bronce" colocada en el año 2000 en un cementerio a las afueras de Tallin.[101]

El gobierno determinó su traslado del centro de Tallin al cementerio a las afueras de la ciudad, ello causó muchas protestas por parte de medios rusos y muchos ruso parlantes salieron a las calles a protestar. Los ciberataques no se hicieron esperar, en algunos casos, las páginas del gobierno estuvieron bloqueadas durante semanas, pero no solo el gobierno sino también empresas privadas como las páginas web de bancos y medios de prensa fueron saturados con *spam* (correos basura).[102]

Estos hechos iniciaron el debate de si estos ataques podrían ser atribuidos a los gobiernos o si pudieran ser considerados *causa belli*, ya que no constituían un ataque físico convencional, como lo establece la

[100] Espinosa, Edgar Iván, Hacia una estrategia nacional de ciberseguridad en México, Revista de Administración Pública, , vol. L, no. 136, p. 116.
[101] BBC NEWS, Mundo, Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país. Disponible en: https://www.bbc.com/mundo/noticias-39800133, consultado el: 05/03/2021.
[102] Idem.

Carta de las Naciones Unidas o si se aplicaría el Derecho Internacional Humanitario en caso de que se interpretará como una agresión.[103]

Por otro lado, en 2010, otro foco rojo, fue el ciberataque contra una planta nuclear. Inspectores de la Agencia Internacional de Energía Atómica que visitaban una planta nuclear en Irán, observaron que las centrifugadoras que enriquecían el uranio estaban fallando. 5 meses después se observó la misma falla, pero en esa ocasión los técnicos de la planta pudieron detectar el origen del fallo de la misma, un virus informático, denominado *Stuxnet*.

Este gusano había tomado el control de las máquinas, dando la instrucción a las mismas de autodestruirse. Fue el primer ataque que "logró dañar la infraestructura del mundo real"[104] y es considerado como la primer ciber arma.[105] La creación del virus y del ciberataque, fueron atribuidas a Estados Unidos e Israel.

Estos ataques también pusieron sobre la mesa, la posibilidad de que el mundo virtual pudiera tener implicaciones en el mundo físico; la generación de virus *ad hoc*; la probable participación de un Estado, lo que pudiera implicar una nueva manera de hacer la guerra, la ciberguerra, que en cualquier momento puede estallar.[106]

El tercer suceso que puso en alerta a todo el mundo fue el caso de las revelaciones realizadas por Edward Snowden, ex analista de seguridad informática de la Agencia de Seguridad Nacional (ASN) de los Estados Unidos, que alertó a la comunidad internacional sobre los mecanismos de espionaje y las capacidades estadounidenses para intervenir de manera masiva correos electrónicos, servicios de voz, video, chat, foros y redes sociales de cualquier persona, incluidos los grandes líderes mundiales.[107]

Con ello, la tecnología demostró que no estábamos preparados para hacer frente a estas nuevas maneras de atacar las estructuras esta-

[103] Espinosa, Edgar Iván, op. cit. p. 117.
[104] BBC NEWS, Mundo, El virus que tomó control de mil máquinas y les ordenó autodestruirse. Disponible en: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet, consultado el: 05/03/2021.
[105] Espinosa, Edgar Iván, op. cit. p. 117.
[106] Idem.
[107] Ibidem. p. 117.

tales y personales, así como la facilidad con que los ciberdelincuentes podrían acceder a la información gubernamental y/o privada.

En este contexto, considero fundamental abordar el estudio de la ciberseguridad en el presente capítulo. En el primer apartado se abordan las características generales de la ciberseguridad, como son la amenaza, su definición y sus fases, posteriormente en un segundo apartado profundizamos en el fenómeno de la ciberseguridad en América Latina.

3.1 La seguridad en el ciberespacio

Desde el inicio de las computadoras y ahora con los nuevos desarrollos, estas herramientas han traído consigo tanto bondades como amenazas dentro de las cuales podemos mencionar desde gusanos y virus computacionales hasta instrumentos de espionaje sofisticados.

Los ataques se han vuelto cada vez más frecuentes, teniendo un crecimiento exponencial. En este sentido, las amenazas más usuales a las que se enfrentan empresas, gobiernos, organismos internacionales y la ciudadanía en general son:

- Ciberguerra: se trata de un ataque, en el que los ciberdelincuentes intentan recopilar la mayor cantidad de información para comprometer a un gobierno o partido político. De acuerdo con el "Concepto Estratégico de la Alianza" de la OTAN, en las que define sus políticas de ciberdefensa, señala que las ciber amenazas pueden ser causa de legítima defensa colectiva.[108]
- Ciberterrorismo: es un ataque que tiene por objeto recopilar el mayor número de información con la finalidad de generar un ambiente de terror en los ciudadanos.
- Cibercrimen: es el ataque realizado por hackers que acceden a sistemas informáticos protegidos para ser publicados y, en algunos casos, intentan obtener ganancias con los mismos. Estos se llevan a cabo en contra de gobiernos como de ciudadanos

[108] OTAN, Nuevas amenazas: el ciberespacio, Revista de la OTAN. Disponible en: https://www.nato.int/docu/review/2011/11-september/cyber-threads/es/index.htm, consultado el: 05/03/2021.

a quienes pueden extorsionar.[109] Se pueden realizar a través de *malware* (código malicioso), es un programa informático que se coloca en un dispositivo con la intención de atacar la confidencialidad de datos, las aplicaciones o sistemas operativos, estos pueden ser: virus, gusanos, troyanos, *rootkits* (permite instalar herramientas para acceso remoto del ordenador) y *spyware* (rastrea y registra la actividad de equipos y dispositivos móviles), y pueden infectar el dispositivo a través de correos electrónicos, sitios web, descargas, el uso compartido de archivos y la mensajería instantánea.[110]

- Ingeniería social: los atacantes intentan engañar a las personas a fin de obtener información, mediante el *phishing*, *smishing* y el *vishing*. El primero se refiere al método por el cual el delincuente envía un correo electrónico a una persona, fingiendo ser una compañía o sitio de confianza para robar su contraseña o información sensible; el segundo, es el ataque mediante un mensaje de texto (MSM) al celular, por el cual se solicita a la persona llamar a un número de teléfono o ir a un sitio web; el tercero, se realiza a través de llamadas telefónicas en las que se pretende engañar suplantando la identidad de otra persona o compañía para solicitar información privada.[111]

En el mismo sentido, la empresa Kaspersky, realizo un estudio respecto a los riesgos percibidos en el ciberespacio, donde la ciberamenaza ocupa el primer lugar con un porcentaje del 46%, el espionaje industrial y el robo de propiedad intelectual el 18% y el terrorismo el 10%. Véase la Gráfica 2.

[109] OBS, Business School, ¿Qué es ciberseguridad y de qué fases consta?. Disponible en: https://obsbusiness.school/es/blog-investigacion/sistemas/que-es-ciberseguridad-y-de-que-fases-consta, consultado el: 05/03/2021.
[110] Guía de Ciberseguridad para uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo, Secretaría de Comunicaciones y Transportes, 2000.
[111] Idem.

Gráfica 2. Seguridad en TIC´s y riesgos percibidos en el ciberespacio (2020)

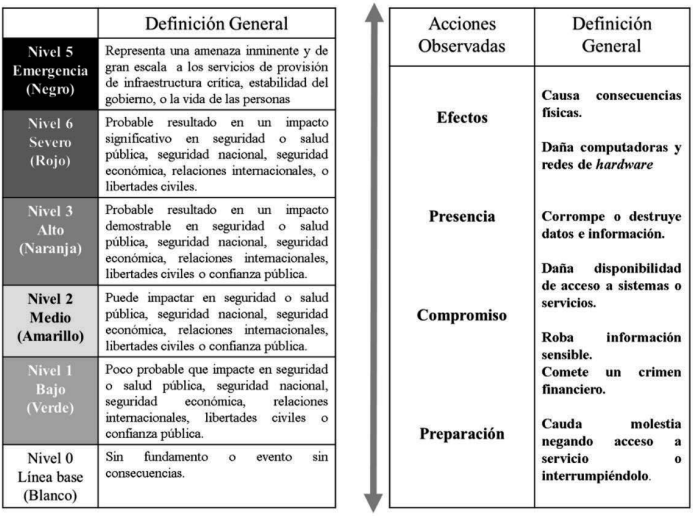
Fuente: http://www.seguridadinternacional.es/resi/index.php/revista/article/view/303/349

Derivado de lo anterior, la ciberseguridad se ha vuelto un estándar necesario tanto para países, empresas, organismos internacionales y hasta para el ciudadano. Por ello, la ciberseguridad se ha convertido en una herramienta habitual que engloba un gran número de técnicas y métodos para el cuidado de los sistemas de información a fin de evitar que estén expuestos a grandes riesgos.

Es importante señalar que cada nivel de ciberataque corresponde a diversos tipos de amenazas y grados de afectación, desde los que desactivan páginas de Internet hasta los que llegan a ser una amenaza real para la seguridad nacional.[112] Sobre estos niveles, la Directiva de política presidencial sobre la coordinación de incidentes cibernéticos de los Estados Unidos puede proporcionar un estándar de las escalas de riesgo cibernético vinculados a las ciberamenazas. Véase Figura 1.

[112] Aguilar Antonio, Juan Manuel, La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas, Revista de Estudios en Seguridad Internacional, col. 6, no. 2, Universidad Nacional Autónoma de México, México, 2020, p. 22.

Figura 1. Niveles de riesgo de la Directiva de política presidencial sobre la coordinación de incidentes cibernéticos de los Estados Unidos



	Definición General
Nivel 5 Emergencia (Negro)	Representa una amenaza inminente y de gran escala a los servicios de provisión de infraestructura crítica, estabilidad del gobierno, o la vida de las personas
Nivel 6 Severo (Rojo)	Probable resultado en un impacto significativo en seguridad o salud pública, seguridad nacional, seguridad económica, relaciones internacionales, o libertades civiles.
Nivel 3 Alto (Naranja)	Probable resultado en un impacto demostrable en seguridad o salud pública, seguridad nacional, seguridad económica, relaciones internacionales, libertades civiles o confianza pública.
Nivel 2 Medio (Amarillo)	Puede impactar en seguridad o salud pública, seguridad nacional, seguridad económica, relaciones internacionales, libertades civiles o confianza pública.
Nivel 1 Bajo (Verde)	Poco probable que impacte en seguridad o salud pública, seguridad nacional, seguridad económica, relaciones internacionales, libertades civiles o confianza pública.
Nivel 0 Línea base (Blanco)	Sin fundamento o evento sin consecuencias.

Acciones Observadas	Definición General
Efectos	**Causa consecuencias físicas.** **Daña computadoras y redes de *hardware***
Presencia	**Corrompe o destruye datos e información.**
Compromiso	**Daña disponibilidad de acceso a sistemas o servicios.** **Roba información sensible.** **Comete un crimen financiero.**
Preparación	**Cauda molestia negando acceso a servicio o interrumpiéndolo.**

Fuente: http://www.seguridadinternacional.es/resi/index.php/revista/article/view/303/349

En este sentido, las diferentes herramientas tecnológicas pueden impactar del nivel 0 al 5, desde afectar el sistema informático de una sola persona hasta bloquear una red gubernamental, como fue el caso del ciberataque de Estonia en 2007 o generar una brecha de información que puede afectar la reputación de un individuo, hasta generar tensiones entre Estados, como fue el caso de Wikileak que afectó las relaciones entre México y EUA.[113]

Pero entonces qué es la ciberseguridad. A ésta se le ha denominado, de acuerdo con la Resolución 181 (UIT-TX1205), de la Conferencia de Plenipotenciarios de la UIT, adoptada en Guadalajara, México, en el año 2010, como:

> El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, planes de seguridad nacional, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno. Los activos de la organización y los usuarios son los dispositivos informáticos

[113] Ibidem. p. 23.

> conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciber entorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciber entorno.[114]

Entonces, en líneas generales se le considera como la seguridad de bases de información digital almacenada en redes electrónicas, aunque no existe un consenso.[115] Cabe diferenciar la noción de seguridad de la información de la ciberseguridad, ya que a pesar de ser utilizados como sinónimo, en muchos casos la primera se refiere a la actividad de empresas[116] o profesionales de las tecnologías de la información, mientras que la segunda se vincula con la política, específicamente a la seguridad nacional.[117]

La ciberseguridad es importante porque nos ayuda a preservar datos, proteger información de manipulaciones, blindar el acceso a información, asegurar la operatividad de sistemas y su integridad, evitar

[114] OBS, Business School, op. cit.

[115] Ibarra, Virginia, La seguridad internacional determinada por un mundo on-line: el estado ante el desafío del terrorismo y la ciberseguridad, VII Congreso de Relaciones Internacionales, 23, 24 y 25 de noviembre de 2016. Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/58156/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y, consultado el: 05/03/2021.

[116] Las empresas privadas comercializan para otras empresas y particulares estrategias que van desde la prevención hasta la reacción: • Prevención: La prevención reducirá el riesgo de ciberataques, por ello es fundamental actuar de manera temprana y determinar las posibles amenazas, lo cual permite estar preparados. • Localización: después de sufrido el ataque, es necesario ubicar el problema o debilidad del sistema, en algunos casos de pueden pasar varios días desde el momento que se inicia el ataque y el momento en el que se detecta el problema. • Reacción: Una vez localizada la amenaza, se da una respuesta técnica, desconectando los equipos de la red, haciendo un análisis del sistema, cambios de contraseñas, limpieza a fondo del sistema, entre otros, dependiendo del nivel de afectación y del tipo de ataque que se haya recibido (Véase OBS, Business School, ¿Qué es ciberseguridad y de que fases consta?. Disponible en: https://obsbusiness.school/es/blog-investigacion/sistemas/que-es-ciberseguridad-y-de-que-fases-consta, consultado el: 05/03/2021.

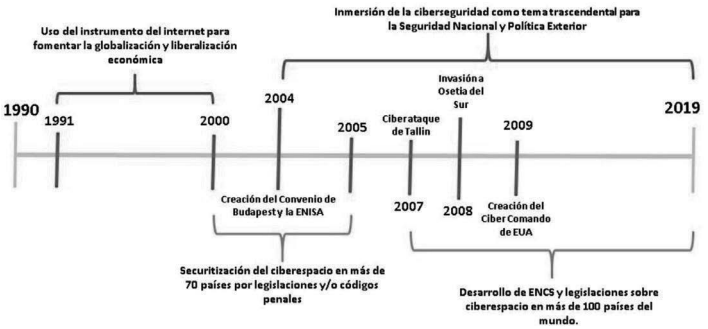
[117] Ibarra, Virginia, op.cit.

instalación de espías y robos, eludir caballos de troya y defender los dispositivos.[118]

Dada su importancia, los Estados han buscado desde el año 2000, generar una regulación y administración del uso del Internet, y en algunos casos se ha llegado al bloqueo y la censura. Pero fue a partir de esa fecha que al menos 70 países y 289 proveedoras de servicios de Internet crearon legislaciones para el control de las actividades en la web. Consolidándose un periodo de securitización, con énfasis en la delimitación de los delitos, actividades ilícitas, sanciones y cooperación entre los Estados.

Por ello más de 100 países incluyeron en sus códigos de justicia y sistemas jurídicos los tipos penales en materia de ciberdelitos, adicionalmente organismos internacionales como la Organización para la Cooperación Económica (OCDE), la Unión Europea (UE), la Unión Internacional de Telecomunicaciones (ITU), crearon diversos acuerdos hasta culminar con la adopción del Convenio de Budapest, en 2004.[119] En este sentido, la ciberseguridad se transformó en un aspecto clave de la estrategia de seguridad nacional. Véase Figura 2.

Figura 2. Fases de regulación del Internet e inclusión de la ciberseguridad en la seguridad nacional



Fuente: http://www.seguridadinternacional.es/resi/index.php/revista/article/view/303/349

Muchos Estados se encuentran realizando inversiones masivas para ampliar o fortalecer sus capacidades digitales contra ciberataques.

[118] INSOC CiberSecurity, ¿Por qué es importante la ciberseguridad?. Disponible en: https://www.insoc.com.mx/post/por-qu%C3%A9-es-importante-la-ciberseguridad, consultado el: 05/03/2021.

[119] Aguilar Antonio, Juan Manuel, op. cit. pp. 21.

Queda claro que una buena ciberdefensa y ciberseguridad puede hacer que los ataques sean mucho más manejables.

De conformidad con la encuesta 2020 realizada por Comparitech, en la cual se analizó y calificó los comportamientos y vulnerabilidades cibernéticas de 60 países, los datos que obtuvo revelaron que el país con mejor ciberseguridad es Dinamarca, le siguen Suecia, en segundo lugar, Alemania en tercero, Irlanda en cuarto, Japón en quinto, Canadá en sexto, Francia en noveno, y EUA en 17º. Cabe mencionar que México ocupó el puesto número 34, quedando como uno de los países con muchas áreas de oportunidad en materia de ciberseguridad.[120]

Además de los recursos económicos, queda claro que los países mejor blindados han puesto a la seguridad cibernética en un lugar central de sus políticas públicas a través de sus propias legislaciones. Estas normas se encuentran vinculadas a la protección de datos, estandarización de la seguridad informática, protección de firmas digitales, transacciones electrónicas, responsabilidad y compromiso de servicios de Internet y la obligación de las empresas privadas a resguardar la protección de su información, con el fin de proteger a clientes.[121]

3.2 Ciberseguridad en América Latina

América Latina ha sido víctima de diversos ataques, hasta 2017, el costo de éstos ascendió a un promedio de 90,000 millones de dólares al año, debido a la falta de respuesta oportuna orientada a contrarrestar los ciberdelitos.[122] Asimismo, de acuerdo con una estadística de 2016, realizada por la empresa PwC, estableció que del total de delitos ciber-

[120] FORBES, Selección Forbes 2020, Éstos son los países más ciberseguros del mundo. Disponible en: https://www.forbes.com.mx/radiografia-cuales-son-los-paises-mas-ciberseguros-del-mundo/, consultado el: 05/03/2021.
[121] MasContainer, Los países de Latinoamérica con más bajos estándares en ciberseguridad. Disponible en: https://www.mascontainer.com/los-paises-de-latinoamerica-con-mas-bajos-estandares-en-ciberseguridad/, consultado el: 05/03/2021.
[122] León Gavilánez, Fernando e Izaguirre Olmedo, Jorge, Análisis de los ciberataques realizados en América Latina, INNOVA Research Journal, vol. 3, no. 9, Universidad Internacional del Ecuador, Ecuador, septiembre de 2018, p. 175.

néticos a nivel global, el 32% se habían llevado a cabo en AL, lo que ponía a la región en el segundo lugar de la lista.[123]

Por ejemplo, en México, en el año 2016, el Servicio de Administración Tributaria (SAT) sufrió un ataque que afectó el funcionamiento de su página de Internet, por un periodo aproximado de 3 horas. Este ataque se sumó a los que, en esa misma semana, se cometieron contra la Comisión Nacional para la Protección y Defensa de los usuarios de servicios financieros (CONDUSEF) y al Banco de México (BANXICO). Todos ellos adjudicados al Grupo Anonymous México.[124]

En el caso de Colombia, en el año 2018, recibió 28,000 ataques de *bots* dirigidos a la página web de la Registraduría Nacional del Estado Civil (RNEC) encargada del proceso electoral, tan sólo tres días antes de sus elecciones parlamentarias.[125] Caso paradigmático fue el de Jorge Maximiliano Pachón Viola, que en el año 2012 fue capturado por los delitos de acceso abusivo a sistemas informáticos en concurso con hurto por medios informáticos y semejantes, ya que existían indicios de que esta persona había retirado más de 600 millones de pesos con tarjetas clonadas en diferentes cajeros automáticos en territorio colombiano.[126]

No obstante, considerando las problemáticas expuestas, de conformidad con diversos *ranking* sobre ciberseguridad, los países latinoamericanos se encuentran entre los de menor fortaleza en la materia.

En la encuesta de *MasContainer*, considerando 7 criterios de análisis, como: porcentaje de ataques de *malware* financiero, a móviles y computadoras, criptomonedas, legislación de los países, entre otros. Los países de la región Latinoamericana figuran casi a la mitad del

[123] Ibidem. p. 177.

[124] El Economista, SAT sufrió ataque en sus sistemas informáticos. Disponible en: https://www.eleconomista.com.mx/sectorfinanciero/SAT-sufre-ataque-cibernetico-informacion-de-los-contribuyentes-esta-segura-dice-Buenrostro-20200709-0039.html, consultado el: 05/03/2021.

[125] Deutsche Welle: Actualidad, Detectan ataques cibernéticos a entidad electoral de Colombia. Disponible en: https://www.dw.com/es/detectan-ataques-cibern%C3%A9ticos-a-entidad-electoral-de-colombia/a-42898310, consultado el: 05/03/2021.

[126] Fiscalía General de la Nación, Asegurado por hurto de 600 millones con tarjetas clonadas. Disponible en: https://www.fiscalia.gov.co/colombia/noticias/asegurado-por-hurto-de-600-millones-con-tarjetas-clonadas/, consultado el: 05/03/2021.

rankig: México en el no. 42, Colombia en el 39 y Argentina en el 37.[127]

En la encuesta realizada por la empresa de ciberseguridad Symantec, que valoró las amenazas a la ciberseguridad en 157 países basado en 8 criterios: *malware, spam*, *phishing hosts*, *bots,* ataques a la red, ataques web, *ransomware* y *cryptojacking*. En América Latina, los países que resultaron ser más inseguros fueron: Brasil, México y Venezuela.[128]

Con resultados similares, el informe del *Global Cybersecurity index*, que mide el compromiso de los Estados para contrarrestar las amenazas de seguridad en la red, países como Chile, Brasil, Panamá y Ecuador se encuentran en el segmento medio.[129]

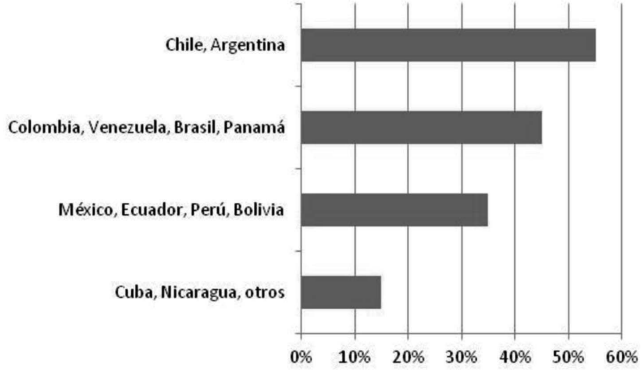
Adicionalmente, de acuerdo con *Symantec* de 2013, destaca que el 4.2% de los ciberataques en la región ocurrieron en Venezuela, país que tuvo una infección por *malware* del 23% del total de computadoras analizadas y el 5% del total de *spear phishing* suscitado en el continente.[130]

Del mismo modo, en el *National Cyber security Index* elaborado por la *e-Governance Academy Foundation* de Estonia, los países de América Latina, tienen dos áreas a las que han prestado nula o escasa atención: la protección de servicios esenciales, incluyendo infraestructura, y las ciber-operaciones militares.[131]

Asimismo, acorde con datos de la ITU, del mismo año, la región se dividía en 4 grupos de países de acuerdo a su nivel de conectividad: el primer grupo arriba del 55% Chile y Argentina, segundo grupo con 45-55% Colombia y Venezuela; tercer grupo 35-45% México, Ecuador, Perú y Bolivia; en el cuarto grupo se encontraban Cuba, Nicaragua y otros países de Centroamérica.[132] Véase Gráfica 3.

[127] MasContainer, op. cit.
[128] Idem.
[129] Idem.
[130] León Gavilánez, Fernando e Izaguirre Olmedo, Jorge, op. cit., p. 175.
[131] Álvarez Valenzuela, Daniel, Ciberseguridad en América Latina y ciberdefensa en Chile, Revista chilena de derecho y tecnología, vol. 7, no. 1, junio 2018, Chile, Disponible en: https://scielo.conicyt.cl/scielo.php?pid=S0719-25842018000100001&script=sci_arttext, consultado el: 05/03/2021.
[132] León Gavilánez, Fernando e Izaguirre Olmedo, Jorge, p. 176.

Gráfica 3. Niveles de penetración de Internet por países (2015)



Fuente: http://201.159.222.115/index.php/innova/article/view/837/779

En este panorama, un esfuerzo temprano fue el realizado por la Unión de Naciones Suramericanas (UNASUR) que incluyó la ciberseguridad en sus planes de acción de 2012, 2013 y 2014, en donde se definen planes de acción y políticas regionales para detener o disminuir los ciberataques.[133]

Asimismo, en 2015, la Organización de Estados Americanos (OEA), de conformidad con los objetivos de su Carta (1948) y buscando impulsar la colaboración de los países miembros para defender su soberanía y seguridad nacional,[134] presentó un Programa de Seguridad Cibernética para los países de América Latina y el Caribe, con el fin de desarrollar una política integral regional de seguridad.[135]

En congruencia, algunos países comenzaron a modificar sus legislaciones nacionales para contemplar los crímenes cometidos en el ciberespacio, como: Argentina, Costa Rica, México, Bolivia, Guatemala, Paraguay y Perú, otros generaron leyes específicas sobre la materia, como: Colombia, Chile, Brasil y Venezuela.[136]

[133] Ibídem. p. 177.
[134] López Velarde Campa, Jesús Armando, Derecho Internacional Contemporáneo, Miguel Ángel Porrúa, México, 2015, pp. 106-107.
[135] León Gavilánez, Fernando e Izaguirre Olmedo, Jorge, p. 177.
[136] Ibidem. pp. 177-178.

Asimismo, la mayoría de los países de la región se encuentran trabajando en la protección de datos y la privacidad, para atender ataques antes de que se produzcan es decir con mecanismos de prevención.[137]

Sin embargo, a pesar de los esfuerzos mencionados, en la primera edición del Informe Ciberseguridad 2016 ¿Estamos preparados en América Latina y el Caribe?, una colaboración del Banco Interamericano de Desarrollo, la OEA, y el Centro Global del Capacitación de Seguridad Cibernética (GCSCC por sus siglas en inglés) de la Universidad de Oxford, señalan que la región presenta vulnerabilidades potencialmente devastadoras.[138] El mensaje fue claro en el sentido de que los países latinoamericanos están muy poco preparados para contrarrestar las amenazas de los ciberdelitos.[139]

A pesar de los resultados poco optimistas, en la región se continuó avanzando. En el caso de Chile, desde el 2015 adoptó medidas sectoriales contenidas en su Política Nacional de Ciberseguridad, que consistían en generar una política en materia de ciberdefensa que fijará objetivos de cumplimiento gradual hasta el año 2022.[140]

Este documento fue elaborado con la colaboración de diversos sectores como las fuerzas armadas, entidades académicas, sociedad civil, gobierno y especialistas sobre estas temáticas. Siendo este documento la respuesta del Estado chileno a los nuevos riesgos y amenazas que el ciberespacio genera para las capacidades de defensa nacional que incluyen información, infraestructura y operaciones de defensa.[141]

Para 2018, 8 países contaban con políticas o estrategias nacionales de ciberseguridad, como son: Colombia, Trinidad y Tobago, Jamaica, Panamá, Chile, Costa Rica, México y Paraguay. A éstos se le sumaron República Dominicana y Guatemala. Cabe mencionar que estas iniciativas estuvieron apoyadas muy de cerca por la OEA a través de su Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo (CICTE),[142] que ha impulsado a los Estados a unir esfuerzos con el sector privado y la sociedad civil en pos de la identificación

[137] Idem.
[138] Ibarra Virginia, op. cit.
[139] Idem.
[140] Álvarez Valenzuela, Daniel, op. cit.
[141] Idem.
[142] Idem.

de las necesidades nacionales de seguridad cibernética y la formulación de políticas específicas.[143]

En la segunda edición del Reporte Ciberseguridad 2020 denominado Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe, una edición del BID y la OEA, se hace referencia a la importancia del contexto de la pandemia por COVID 19 y el resultante incremento de la actividad digital que se ha generado en la región. Asimismo, tanto la OEA como el BID se complacen al observar la importancia que ha cobrado la agenda de ciberseguridad en la región en los últimos años (2016-2020), donde gobiernos, ciudadanos y empresas han mostrado un creciente interés por este tópico.[144]

Sin embargo, de acuerdo con el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones(CMM por sus siglas en inglés), en donde el nivel 1 es Etapa Inicial y el 5 se refiere a la etapa Dinámica o Avanzada, la región todavía se encuentra entre el nivel 1 y 2,[145] variando por subregiones y países:

- Subregión del Cono Sur: es la subregión más alta en el CMM, con un promedio de entre 2 y 3, con el criterio de "Marco legal y regulatorio" más desarrollado. Aunque en todos los criterios tuvieron un avance similar, lo que significa que en esta subregión se está trabajando el tema de manera integral.[146]
- Grupo Andino: el nivel promedio del CMM es 2. Estos países han concentrado sus esfuerzos de seguridad cibernética para fortalecer el despliegue de estándares y controles técnicos y alentar la divulgación responsable. Cabe mencionar que Colombia fue el país con más desarrollo, particularmente en las dimensiones "Política y estrategia" y Cultura y sociedad".[147]
- Centroamérica y México: su promedio es de 2 en las dimensiones "Cultura y sociedad" y "Educación, capacidades y habilidades" mientras que en "Política y estrategia" y "Estándares, organizaciones y tecnología", el puntaje ha sido inferior a 2. Cuentan con áreas de oportunidad en la mejora de estándares

[143] Ibarra Virginia, op. cit.
[144] OEA y BID. Reporte de Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe, 2020, p. 16.
[145] Ibidem. p. 17.
[146] Idem.
[147] Idem.

de seguridad cibernética y controles técnicos, así como en fomentar el desarrollo de un mercado de ciberseguridad. Se debe destacar que México presenta la mejor posición de la región, con un nivel de madurez entre 2 y 3 en casi todas las dimensiones.[148]

- El Caribe: cuenta con un promedio entre 1 y 2 en todas las dimensiones. Igual que en el reporte 2016, la dimensión más avanzada era "Marcos legales y regulatorios", la "Política y estrategia" es la menos fortalecida. Los países con más desarrollo en esta región son Trinidad y Tobago y Jamaica.[149]

Es decir, que en América Latina se ha comenzado a formular iniciativas de seguridad cibernética, incluidas medidas para la creación de leyes y capacidades, algunas de ellas ya están siendo implementadas, pero aún de manera *ad hoc*, o sin coordinación política entre los actores clave.[150]

En el plano regional, la política de ciberdefensa y ciberseguridad constituyen un esfuerzo por promover la implementación de diversas medidas, siendo estas imprescindibles para mantener la paz y seguridad internacionales de la región.[151]

No obstante, aún falta mucho trabajo por realizar, ya que muchos de los países latinoamericanos no cuentan con una codificación general y sistemática sobre ciberdefensa o ciberseguridad, que señale objetivos y establezca responsabilidades para las distintas entidades gubernamentales, que defina la seguridad cibernética nacional, o que contribuya al diseño de tecnologías que sirvan para defenderse de los ciberataques.[152]

---

[148] Idem.
[149] Idem.
[150] Idem.
[151] Álvarez Valenzuela, Daniel, op. cit.
[152] León Gavilánez, Fernando e Izaguirre Olmedo, Jorge, op. cit., p. 178.

Capítulo 4. Brecha digital en los países en desarrollo y la búsqueda de la independencia digital

Introducción

Las TIC han traído consigo muchas ventajas, como mayor acceso a la información, conectividad, el poder laborar desde nuestros hogares, estár conectados a Internet desde nuestros autos, saber en tiempo real de acontecimientos del otro lado del mundo, por mencionar algunas. No obstante, existe un desequilibrio en el acceso a ellas y en la forma en que éstas pueden ser aprovechadas por las personas. A dicha desigualdad se le ha denominado brecha digital.

Estas diferencias han impactado de diversas maneras y niveles a los ciudadanos del mundo desde que se desarrollaron las TIC, más aún a partir del año 2020 con la pandemia del COVID 19, por la cual las personas se han visto obligadas a realizar muchas veces sus funciones laborales, educativas y de esparcimiento mediante plataformas virtuales.

Este fenómeno es importante si consideramos que para 2019, casi el 87% de las personas en países desarrollados utilizaba Internet, dato que contrasta con el 47% de los países en desarrollo. Estas brechas evidencian el abismo tecnológico existente entre los países desarrollados y los que se encuentran en vías de desarrollo, lo que impacta, por un lado a nivel internacional en el crecimiento económico de los países; por el otro a nivel nacional a su población, ya que no se está generando de manera importante el acceso a las redes, así como el proceso de aprendizaje que permita a las personas adquirir competencias que les permitan aprovechar el potencial educativo, económico y social que representan las TIC.

Por lo anterior, en el presente capítulo se profundiza en un primer apartado sobre el fenómeno de la brecha digital en los países en desarrollo, qué significa este concepto y qué implicaciones tiene al exterior y al interior de los países. En un segundo apartado, se abordan los esfuerzos realizados por los países de América Latina a fin de paliar la brecha digital y proporcionar a sus poblaciones, no solo el acceso sino

las herramientas necesarias para el aprovechamiento de las TIC en su vida cotidiana.

4.1. Brecha digital de los países en desarrollo

Las TIC han generado cambios significativos en la vida de las personas y en general de la sociedad, se han convertido en fuente de oportunidades, mecanismo de cambio social, de crecimiento económico, de fortalecimiento de los sistemas democráticos e incentivo a la participación de los ciudadanos, así como parte de mejoras en las condiciones de vida, especialmente en países en desarrollo.[153] En este sentido, las TIC se han convertido en un elemento clave para los países en desarrollo.

No obstante, no todas las personas tienen acceso a las TIC ni todos los países cuentan con el mismo nivel en acceso de su población. Este fenómeno es lo que se ha llamado en la literatura "brecha digital". No existe una definición unánime que podamos adaptar a todas las realidades socio-económicas de los Estados, ya que existen factores que debemos considerar:

- Si se toma en cuenta únicamente el acceso o no a las TIC, dejamos fuera otros elementos como el uso y la apropiación de las mismas por parte de las personas.
- Si determinamos un grupo de TIC corremos el riesgo de dejar otras tecnologías fuera, ya que existe una gama numerosa de éstas que para algunas sociedades son relevantes y para otras no.
- Adicionalmente, tendríamos que señalar el tipo de usuario de Internet, dónde se utiliza, en casa o en la escuela, quiénes son los usuarios, a partir de qué edad consideramos que los individuos tienen acceso, etc.[154]

[153] Betancourt, Valeria, El problema de la brecha digital: más allá de las fronteras de la conectividad, Revista de Opinión para el Desarrollo de las Bibliotecas Públicas, 2004, vo. 1, n. 3.

[154] Rodríguez Gallardo, Adolfo, La brecha digital y determinantes, Tecnologías de la Información, Centro Universitario de Investigaciones Bibliotecológicas, UNAM, México, 2006.

Estas circunstancias hacen complejo el conceptualizar la brecha digital de manera generalizada, aplicable a todos los individuos y a todos los países, ya que cada sociedad posee características diferentes en cuanto a factores demográficos, socioeconómicos y geográficos.

Por ello, es importante analizar las asimetrías de los países o regiones, países en vías de desarrollo y desarrollados, es lo que se llama brecha externa o internacional que implica diferencias tecnológicas entre países pobres y ricos; y las diferencias de acceso dentro de los propios países, llamada brecha nacional, doméstica o interna, que hace referencia a las desigualdades tecnológicas existente entre la población de un país.[155]

Respecto al primer caso, de acuerdo con datos del Banco Mundial, el 48% de la población mundial tiene acceso a Internet. Esta medida varía dependiendo del país, por ejemplo en Canadá el 93% de la población cuenta con Internet, en EUA el 88%. No obstante, en América Latina, países como Guatemala tan solo el 41%, Honduras 32% y Nicaragua 28%.[156]

Es decir, se observa un mundo dividido en 2: por un lado los países del "norte global" como los escandinavos, América del Norte y Europa Occidental son las áreas más desarrolladas; y por el otro el "sur global" zonas de Europa Central u Oriental, algunos países de Asia y el Pacífico, Medio Oriente, América del Sur y África se encuentran en el lado negativo de la brecha.

En la siguiente tabla se concentra información sobre diversos instrumentos tecnológicos como radio, computadoras personales, televisores, diarios, teléfonos fijos y móviles y se obtiene un índice del promedio de todos los nuevos elementos tecnológicos.[157] Véase Tabla 2.

[155] Márquez A., Acevedo J., et al., La brecha digital y la integración de tecnologías de información y comunicación en los Colegios de Estudios Científicos y Tecnológicos de la región Valles Centrales de Oaxaca, México, Congreso Iberoamericano de Ciencia, Tecnología, Innovación y Educación, México, S/A, p. 40.

[156] Banco Mundial, Personas que usan Internet (% de la población). Disponible en: https://datos.bancomundial.org/indicador/IT.NET.USER.ZS?locations=CA, consultado el: 05/03/2021.

[157] Rodríguez Gallardo, Adolfo, op. cit., p. 48.

Tabla 2. Proporción de la población que utiliza nuevos y viejos medios

Región	Población en línea 2000	Servidores 2000	PCs 1998	Radios 1997	Televisores 1998	Diarios 1996	Teléfonos fijos 1998	Teléfonos móviles 1998	Índice Soc-Info
Escandinavia	35	11	36	112	58	45	64	47	80
América del Norte	27	10	28	118	61	16	47	15	63
Europa Occidental	12	3	27	79	53	21	53	24	52
Europa Central y Oriental	3	0.3	6	45	32	13	21	4	30
Asia-Pacífico	5	1	8	35	19	11	13	8	27
Medio Oriente	3	0.2	6	39	25	11	19	8	22
América del Sur	1	0.1	5	38	22	8	15	3	18
África	0.3	0.1	1	17	5	1	3	0.5	6
Desarrollo									
Alto	14	4	23	83	49	26	46	23	53
Medio	1	0.1	3	32	21	6	11	2	15
Bajo	0.02	0.03	0.3	14	3	1	1	0.1	4
Total	**4**	**1**	**9**	**40**	**24**	**10**	**18**	**7**	**38**
Número de naciones	169	179	125	140	139	133	179	139	101

Nota: Todas la figuras se expresan como porcentaje de la población. Para mayores detalles véase la tabla 3.1. Porcentaje de radios (1997), televisiones (1998), teléfonos moviles (1998) y PCs (1998) del World Development Indicators 2000, Banco Mundial. El nivel de desarrollo está clasificado de acuerdo al UNDP (1999). Los 100 puntos del índice de la Soc-Info están calculados mediante la combinación de todos los indicadores en una escala estandarizada.
Fuente: Rodríguez Gallardo, Adolfo, La brecha digital y determinantes, Tecnologías de la Información, Centro Universitario de Investigaciones Bibliotecológicas, UNAM, México, 2006.

Respecto a la región de Asia-Pacífico, en medio de la tabla, presenta una revolución digital en las últimas décadas, que genera grandes esperanzas en cuanto a la brecha digital, esta revolución se basa en 3 pilares: telefonía móvil, banda ancha y medios de comunicación sociales.[158]

En materia de TIC, en dicha región, la India ha experimentado un cambio espectacular desde los años 90 a la fecha, convirtiéndose en el primer exportador mundial de *software* y servicios informáticos, también es el país con mayor número de ingenieros calificados y el tercero en mayor reserva de mano de obra tecnológica. Esto lo ha conseguido a través de: la innovación e investigación del sector académico, la de-

[158] ONU, Crónica, La tecnología digital en Asia y el Pacífico en el siglo XXI. Disponible en: https://www.un.org/es/chronicle/article/la-teconologia-digital-en-asia-y-el-pacifico-en-el-siglo-xxi, consultado el: 05/03/2021.

terminación empresarial, el apoyo institucional, mano de obra calificada, altos estándares de calidad y acceso a mercados poco explorados.[159]

A la mitad de la tabla, se encuentra Medio Oriente, sin embargo, a pesar de que no se encuentra entre las regiones con mayor penetración de las TIC, no se puede negar que en la región se están realizando importantes esfuerzos en dicha área.

Caso paradigmático es Arabia Saudita, que a través de su programa de reformas Visión 2030, tiene por objetivo impulsar la innovación y el crecimiento económico mediante la utilización de tecnologías digitales, cuyos pilares son la digitalización y la inteligencia artificial. Para ello cuentan con diversas metas, entre las que se encuentra la utilización de la nube, para facilitar las actividades del e-gobierno, con el objetivo de mejorar la eficiencia y productividad del sector público.[160] También, se implementó el Centro Nacional de Información (NIC por sus siglas en inglés), como el centro nacional que unifica la gestión de datos; asimismo se estableció la Autoridad Nacional de Ciberseguridad y la Federación Saudita para la Ciberseguridad y la Programación.[161]

En el último lugar de la tabla se encuentra el continente Africano, en cuanto al acceso de su población tanto en nuevos medios como en viejos. En 2013, la tasa de penetración digital fue: en el norte de África del 27%, en el sur del 13%; en África Oriental del 12%, África Occidental del 9,5% y en Africa Central del 4.5%. No obstante, a nivel continente, en África hay menos de 5 suscriptores de Internet por cada 100 habitantes.[162]

Un país con avances importantes en la región es Kenia, que en 2013, tuvo la iniciativa de abrir una ventanilla digital para el registro de actividades económicas de las empresas, facilitando el proceso de búsqueda de compañías y de recaudación; también creó un portal de

[159] El País, El impulso tecnológico sitúa a India como uno de los cinco países más atractivos para invertir. Disponible en: https://elpais.com/tecnologia/2005/11/29/actualidad/1133256483_850215.html, consultado el: 05/03/2021.

[160] Alannsary, Mohammed y Hausawi, Yasser, Adopting and implementing a government Cloud in Saudi Arabia, an integral part of Vision 2030, EPIC series in computing, Vol. 58, 2019, p. 387.

[161] Ibidem, p. 388.

[162] García Jiménez, Antonio y González Pascual, Alberto, Internet y África: de la brecha a la esperanza digital. Redes, libertades y comunicación, Revista Index. Comunicación, no 3(2), 2013, Universidad Rey Juan Carlos, p. 114.

datos de la administración pública con indicaciones de más de 400 categorías de gestión[163]; implementó la aplicación de una app que da a los granjeros información actualizada sobre los mercados, para obtener mejores precios. A estos servicios pueden tener acceso desde sus teléfonos, ello es importante si consideramos que el 99% de los suscriptores de Kenia a Internet, unas 16 millones de personas, tienen acceso a la red desde sus dispositivos móviles.[164]

En consecuencia, la tabla nos muestra que la brecha digital se encuentra vinculada con el desarrollo económico de los países, ya que:

- Las regiones no conectadas a Internet pierden competitividad y son incapaces de sumarse al nuevo modelo de desarrollo de la economía del conocimiento;
- Las empresas que no incorporan las TIC en sus procesos productivos, administrativos y comerciales, no pueden elevar su competitividad, y
- Las personas que no cuenten con habilidades tecnológicas, pierden la oportunidad de integrarse a puestos de trabajo, más modernos y mejor pagados.[165]

En este sentido, la brecha digital se convierte en una nueva expresión de la desigualdad social, es decir es una forma de segregación basada en la utilización de las TIC y vinculada al desarrollo social y económico de los Estados. Por ello, se han desarrollado múltiples iniciativas por parte de diferentes sectores estatales e internacionales, a fin de impulsar la disminución de la brecha digital dentro de los países (interna) y fuera de ellos (externa).

Los gobiernos, sectores privados, sociedad civil, organizaciones internacionales, regionales y transnacionales han tenido diversidad de experiencias, unas de mayor éxito que otras, han demostrado la necesidad de generar estrategias concretas para eliminar la brecha digital.[166]

No obstante, si se quiere que las TIC tengan un impacto real en los países en desarrollo se recomienda:

---

[163] Ibidem, p. 123.

[164] ShareAmerica, Kenia: el centro de la innovación en África. Disponible en: https://share.america.gov/es/kenia-el-centro-de-innovacion-de-africa/, consultado el: 05/03/2021.

[165] Márquez A., op. cit., p. 40.

[166] Betancour, Valeria, op. cit.

- Tener acceso real a las TIC: El acceso se entiende como la posibilidad de utilizar ciertos recursos, pero en materia de brecha digital implica no sólo poder utilizar una computadora, sino que esté conectada a Internet, es decir, que pueda acceder a la red y pueda el usuario comunicarse con otras personas. Ello implica adicionalmente tener determinados servicios como: electricidad, teléfonos y equipos de comunicaciones, fibra óptica o banda ancha.[167]

  El acceso a las TIC se determina por 3 factores a saber:

  I. La infraestructura vinculada con la disponibilidad de recursos físicos que incluye aspectos como la penetración de Internet, avances tecnológicos, grado de conectividad en la región o país.

  II. Recursos humanos, se refiere a la capacidad de las personas para el manejo de tecnología. Por ello, es fundamental la capacitación, educación y empleos en el sector de las telecomunicaciones.

  III. La competitividad de los proveedores de TIC, tiene un papel importante en la provisión de nuevas tecnologías.[168] La cuestión del acceso no se refiere únicamente al incremento en el número de personas que puedan tener un dispositivo, sino todas las herramientas necesarias para utilizarlas y poder comunicarse.[169]
- El uso de las tecnologías: es un aspecto fundamental ya que varía dependiendo de cuestiones sociales, económicas y culturales. La brecha digital se relaciona tanto con el aspecto tecnológico como económico-social. El uso de los dispositivos ha creado nuevas prácticas sociales de comunicación con amigos y familiares a través del correo electrónico, *facebook* o *messenger*. Las personas se encuentran comunicadas en cualquier momento y lugar.[170]
- Apropiación social de las TIC: La posibilidad de que las personas usen una computadora y tengan acceso a Internet, no es el objetivo final, ésto sólo es importante en el sentido de que sea útil a las personas, para su vida cotidiana, de ahí el interés en la formación de recursos humanos, ya que no será igual la

[167] Márquez A., op. cit.
[168] Rodríguez Gallardo, Adolfo, op. cit., p. 40.
[169] Idem.
[170] Ibidem, p. 50.

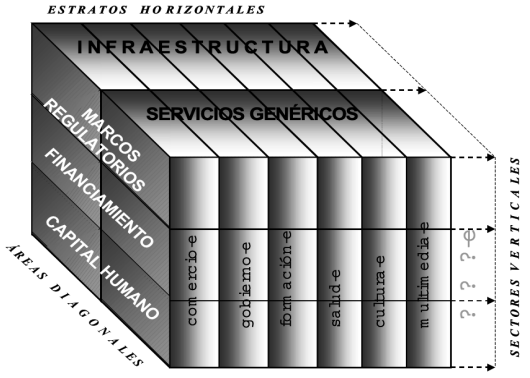
experiencia y la potencialidad del uso de un dispositivo de una persona experta, que de una que sólo realiza búsquedas básicas o no sabe buscar en la red.[171]

Basada en la categorización de acceso, uso y apropiación, la Unión Internacional de Telecomunicaciones (UIT), ha generado un plan para disminuir la brecha digital de los Estados, a partir de tres etapas:

- Elevar el nivel de infraestructura de red y acceso a las TIC;
- Incrementar el nivel de uso de las TIC por la sociedad, y
- Acrecentar el impacto de las TIC, como la capacidad de obtener beneficios por el uso de tecnologías.

Por su parte, la Comisión Económica para América Latina y el Caribe (CEPAL), impulsa un modelo integrado por dos etapas: 1.- brecha digital que incluye las diferencias de acceso a las TIC; y 2.- se refiere a las diferencias de uso y apropiación.[172] Asimismo, impulsa una visión tridimensional de los retos para enfrentar la brecha digital, que implican: como estratos horizontales la infraestructura y servicios genéricos; como áreas diagonales los marcos regulatorios financiamiento y capital humano, y los sectores verticales el e-comercio-e, gobierno-e, información-e, salud-e, cultura-e y multimedia-e. Véase Figura 3.

Figura 3. Estratos horizontales, sectores verticales y áreas diagonales de la sociedad de la información



Fuentes: Los caminos hacia una sociedad de la información en América Latina y le Caribe, Santiago de Chile, CEPAL, 2003, p. 15.

[171] Ibidem, p. 40.
[172] Márquez A., op. cit., 42.

La infraestructura implica computadoras y comunicaciones, en cambio los servicios genéricos se refieren a *software* y programación. La áreas diagonales incluyen el contexto que los países deben dar a través de políticas públicas, en un primer plano están los marcos regulatorios que deben impulsar y favorecer el acceso, uso y apropiación de las TIC; en segundo lugar el financiamiento que se debe otorgar como resultado de las políticas públicas y que debe asegurar que los objetivos de éstas se cumplan; y en tercer lugar el capital humano que garantice la adecuada ejecución de los programas en materia de las TIC.

Respecto a los sectores, enuncia diversos aspectos en los que las TIC han impactado en la vida cotidiana de las personas, como por ejemplo el comercio-e, que con la emergencia sanitaria causada por el COVID 19, se ha reafirmado como un mecanismo de comercio confiable, mediante el cual se pueden realizar transacciones de manera interactiva, con una o más personas, en tiempo real y a precios asequibles.[173]

La UNESCO presentó un informe denominado "Sociedad digital: brechas y retos para la inclusión digital en América Latina y el Caribe" de 2017, donde centra su análisis en el reto de conectar a más de 200,000 personas en América Latina que no cuentan con acceso a las TIC. Para ello, presenta 3 recomendaciones:

- Conectar a las escuelas: dotar a las instituciones de equipos, conectividad y capacitación a los docentes.
- Promover servicios en línea relevantes para los no conectados: impulsar el contenido de servicios en línea como parte de las políticas de inclusión digital en la región.
- Subsidio de acceso residencial condicionado: a través de programas de transferencia condicionada que buscan romper con la pobreza intergeneracional pueden los gobiernos apoyar a las familias para poder contratar banda ancha residencial, ya que actualmente los precios son inasequibles para muchas familias.

En otro ámbito, encontramos a las ONG's que trabajan para disminuir la brecha digital, por ejemplo, la Asociación para el Progreso de las Comunicaciones (APC) enfoca sus esfuerzos al "acceso real". Es una iniciativa desarrollada por Bridges.com, con sede en Sudáfrica, que

[173] López Velarde Campa, Jesús Armando, Derecho Comercial y globalización. Temas selectos, Miguel Ángel Porrúa, México, 2016, p. 17.

promueve el uso efectivo de las TIC en los países en desarrollo. Con una visión integral del acceso, que va más allá de la infraestructura física y la conectividad, sino que se instituyan las bases y condiciones para que las TIC impacten en la calidad de vida de las personas.[174]

Por otra parte, los Estados hacen mayor énfasis en las políticas de acceso y servicio universal, si bien este es el primer paso resulta insuficiente si los Estados no avanzan hacia las siguientes etapas de uso y apropiación. De hecho, la dificultad para tener acceso a tecnologías no es algo nuevo, las sociedades en desarrollo y desarrolladas "han necesitado largos periodos para llegar a tener una cobertura total de los servicios telefónicos, de la misma forma en que lo hicieron para disfrutar de la electricidad",[175] donde los grupos sociales con mayores recursos económicos obtuvieron de manera más sencilla y rápida el acceso a estos servicios y en las zonas urbanas, que las personas de menores recursos y en zonas rurales.

No obstante, de acuerdo a Manuel Castelles, el combatir la brecha digital es mucho más complejo que sólo el acceso, tiene que ver con lo que él ha llamado disociación entre el crecimiento económico y el desarrollo social en la era de la información, "que solamente será solventada mediante estrategias de largo plazo orientadas a implementar actualizaciones tecnológicas masivas en el planeta, basadas en el más alto interés humano y social".[176]

Valeria Betancourt, Coordinadora de la Revista Monitor de Políticas de TIC en América Latina, considera 12 elementos fundamentales para que los países en desarrollo disminuyan las brechas digitales internas e internacionales:

Tabla 3. Brecha Digital. Elementos y explicación

Elemento	Explicación
1.- Acceso físico a la tecnología	El acceso se refiere a la infraestructura de telecomunicaciones. computadoras, conectividad a Internet.
2.- Aplicación de la tecnología apropiada	Existe una gran variedad de tecnologías, pero no todas son la mejor opción para atender las necesidades de las personas en determinadas regiones, comunidades o países, en este sentido "las empresas desarrolladoras de tecnologías deberían tratar a los países en desarrollo como mercados en definición y ofrecer alternativas y productos para atender sus necesidades" locales.

[174] Betancourt, Valeria, op. cit.
[175] Rodríguez Gallardo, Adolfo, op. cit., p. 44.
[176] Idem.

Elemento	Explicación
3.- Bajo costo para el uso de la tecnología	El costo de la infraestructura de acceso a las TIC debe ser asequible, ya que los altos costos tienen como efecto la exclusión de comunidades del uso de las TIC. Se pueden buscar soluciones comunitarias y sostenibles.
4.- Generación de capacidades	No basta con tener acceso a la infraestructura (equipos, líneas telefónicas, electricidad, conexión a Internet) si no se cuenta con las capacidades para el manejo de las mismas, que entiendan las potencialidades que las TIC pueden dar a su vida.
5.- Contenido local relevante	El contenido debe causar el interés de la gente por lo cual debe ser acorde a su contexto cultural, sus condiciones e idioma.
6.- Integración en las rutinas diarias	Si el uso de las tecnologías se vuelve una carga al añadirse a las rutinas de las personas, se corre el riesgo que no sea mayoritario. Debe ser parte de la vida de las personas de una forma natural.
7.- Factores socio-culturales	Frecuentemente los factores socio-culturales, como el género o la raza, ponen a las personas en situaciones de desigualdad frente a las TIC.
8.- Confianza en la tecnología	Es importante que además del acceso a las TIC, se lleve a cabo un entendimiento de las mismas, más cuando se ha implementado, por ejemplo, el e-commerce.
9.- Marco legal y regulatorio	El marco legal de un país puede fortalecer u obstaculizar el acceso, uso y apropiación de las tecnologías. Por lo cual, si los Estados quieren disminuir la brecha digital están conscientes de las implicaciones de sus legislaciones.
10.- Contexto económico local	La situación económica de la localidad, región o país determinan en gran medida el uso de las TIC, por ello es importante la promoción para el desarrollo de pequeñas y medianas empresas o industrias sociales y comunitarias.
11. Contexto y situación económica macro	La política económica nacional crea un entorno favorable para la integración de las TIC. Fomenta la transparencia, la desregulación, la inversión y el empleo impactan de manera positiva en la disminución de la brecha digital.
12.- Voluntad política	Los gobiernos nacionales y locales juegan un papel fundamental en la creación de un entorno favorable a las TIC para el desarrollo de infraestructura, generación de capacidades y de fuerza laboral preparada.

Fuente: Elaboración propia con datos de: Betancourt, Valeria, El problema de la brecha digital: más allá de las fronteras de la conectividad, Revista de Opinión para el Desarrollo de las Bibliotecas Públicas, 2004, vo. 1, n. 3.

La misma autora sostiene que los gobiernos que demuestran compromiso en implementar estos cambios para integrar la tecnología han llevado a sus países hacia la sociedad del conocimiento.[177] En este sentido, la diferencia entre los países se da en función de la velocidad de adopción de las TIC.

Para Teresa Peter, las TIC tiene la capacidad de transformar la calidad de vida de las personas, son un mecanismo de transformación social y una importante arma contra la pobreza; tienen un gran potencial para que los habitantes de países en desarrollo[178] puedan: 1. Hacer frente a problemas sociales, 2. Fortalecer las instituciones democráticas y la prensa libre, y 3. Impulsar las economías locales.

[177] Betancourt, Valeria, op. cit.
[178] Rodríguez Gallardo, Adolfo, op. cit., p. 50.

No obstante, en regiones como Latinoamérica, los progresos son poco significativos, ya que en la mayoría de los casos los Estados tratan de lograr metas a corto plazo, por lo que fallan en la la planeación de políticas de largo alcance que apunten al beneficio social colectivo o limitan sus esfuerzos a reducir únicamente las disparidades en cuanto a acceso a TIC.[179] Se requieren estrategias desde diferentes sectores (público, privado y social) en el ámbito local, nacional e internacional.

4.2 Los esfuerzos en América Latina por eliminar la brecha digital

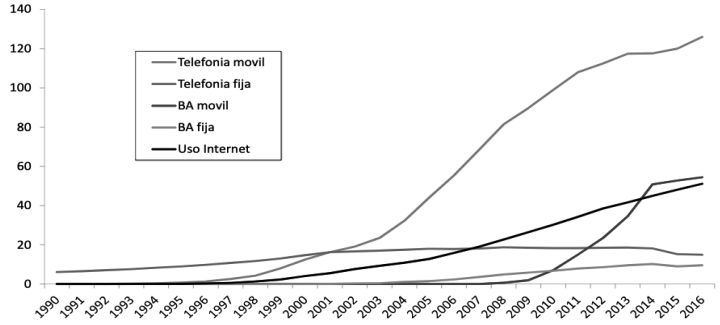
En el informe CEPAL denominado "Estrategias, programas y experiencias de superación de la brecha digital y universalización del acceso a las nuevas tecnologías de la información y comunicación (TIC). Un panorama regional de 2005", en el que construyó un índice que mide la preparación de las naciones para aprovechas las oportunidades de las TIC, encontraron que las naciones andinas y la mayoría de los paíse de América Central, se encontraban en el grupo de menor preparación para usar las TIC.[180]

Adicionalmente, a pesar de que la conectividad vía móvil se ha incrementado en la región, como lo señala el informe "Sociedad digital: Brecha y retos para la inclusión digital en América Latina y el caribe" 2017, de la UNESCO, durante el periodo de 1980 a 2016. Véase Gráfica 4.

[179] Betancourt, Valeria, op. cit.

[180] Villatoro, Pablo y Silva Alisson, Estrategias, programas y experiencias de superación de la brecha digital y universalización del acceso a las nuevas tecnologías de la información y comunicación (TIC). Un panorama regional, CEPAL, 2005. p. 12.

Gráfica 4. Suscripción TIC por c/100 habitantes y usuarios de Internet. América Latina, (1980-2016)

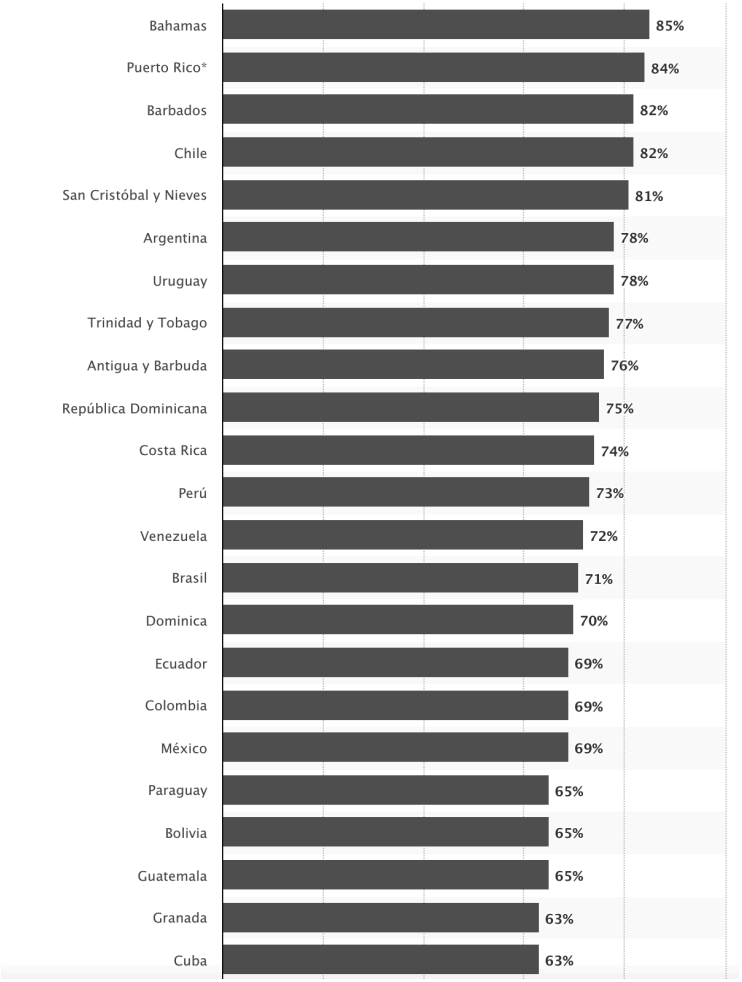


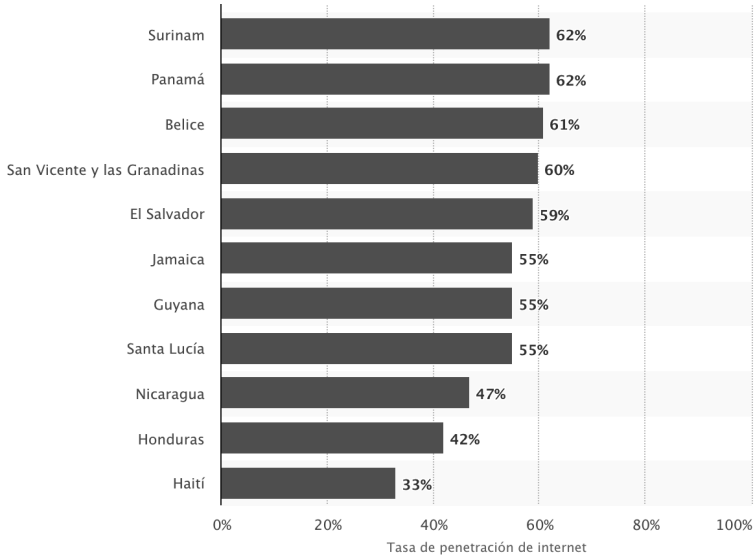
Fuente: UNESCO. Sociedad digital: brechas y retos para la inclusión digital en América Latina y el Caribe, 2016.

En la gráfica se observa una impresionante tendencia de penetración de la telefonía móvil, a partir de 1996, en contraste con la telefonía fija que tiene su pico en 2008 pero después viene a la baja. Respecto a la banda ancha móvil siguen la tendencia a la alta de la telefonía móvil, no obstante está lejos de ella, y la banda ancha fija ha ido en decremento.

No obstante lo anterior, encontramos que, al año 2020, en muchos países latinoamericanos el acceso de su población está en el 65% o menos, es el caso de Paraguay, Bolivia, Guatemala, Granada, Cuba, Surinam, Panamá, Belice, San Vicente y las Granadinas, El Salvador, Jamaica, Guyana, Santa Lucía, Nicaragua, Honduras y Haití. Véase Gráfica 5.

Gráfica 5. Porcentaje de la población con acceso a Internet en América Latina y Caribe por país (2020)





FUENTE: Statista. Porcentaje de la población con acceso a Internet en América Latina y Caribe por país en 2020. https://es.statista.com/estadisticas/1136646/tasa-penetracion-mas-altas-Internet-america-latina-caribe/

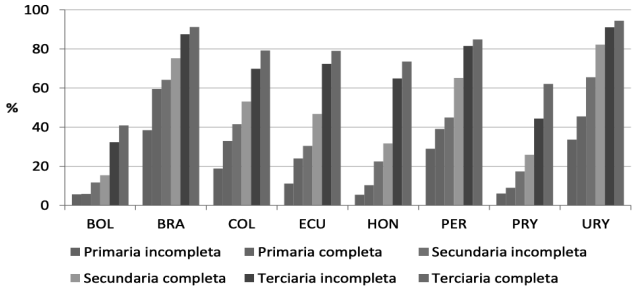
Países como Nicaragua, Honduras y Haití, son los que menor porcentaje de su población tiene acceso a Internet, pero más allá de las generalidades podemos señalar la existencia en el continente de grupos de mayor vulnerabilidad que por sus propias condiciones no cuentan con acceso a las TIC.

El informe de la UNESCO denominado "Sociedad Digital: brechas y retos para la inclusión digital en América Latina y el Caribe" de 2017, en América Latina no solo la falta de ingresos familiares repercute en el acceso a las TIC, sino que factores socio-demográficos también tienen implicaciones, particularmente relevantes resultan el nivel educativo del padre de familia, edad, género, zona, lengua, presencia de menores en edad escolar y personas con discapacidad. En este sentido, es importante analizar las siguientes gráficas y datos, a fin de observar los retos más significativos para los países de la región.

En términos de educación, dicho informe sostiene que, el nivel educativo del jefe de hogar se vincula directamente con el acceso residencial a Internet, por ejemplo, si comparamos una persona que no ha completado la primaria con una que cuenta con nivel de secundaria

completa, esta última tiene una probabilidad de 9% contra 24% de mayor acceso a Internet en el hogar.[181] Véase Gráfica 6.

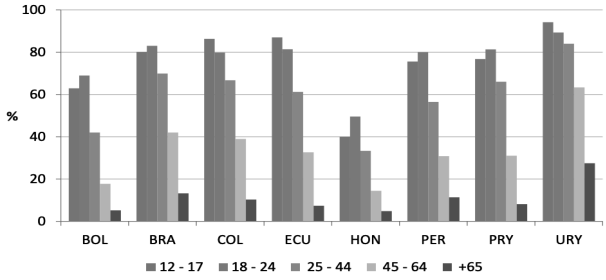
Gráfica 6. Internet residencial según nivel educativo. América Latina (2017)



Fuente: Sociedad Digital: Brechas y retos para la inclusión digital en América latina y el Caribe 2017.

En cuanto a la edad, sostiene que la utilización de Internet también está vinculada con ésta, en América Latina es muy alta la población menor a 24 años que tiene acceso a Internet, va reduciendo su utilización conforme se incrementa la edad de las personas hasta llegar a los 65 años. Particularmente esta población (65 años) es la que más rezago tiene en cuanto acceso, utilización y apropiación de las TIC.[182] Véase Gráfica 7.

Gráfica 7. Uso de Internet según franja etaria. América Latina (2017)

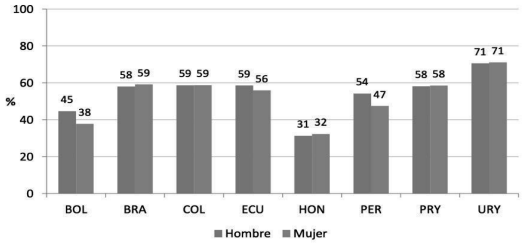


Fuente: Sociedad Digital: Brechas y retos para la inclusión digital en América latina y el Caribe 2017.

[181] UNESCO, Sociedad Digital: brechas y retos para la inclusión digital en América Latina y el Caribe, 2017.
[182] Idem.

Respecto al género, a pesar de los esfuerzos nacionales e internacionales, como los de la ONU que ha reconocido el papel del sexo femenino y que en 1982, lo decretó como el Año Internacional de la Mujer,[183] aún existe una preponderancia por parte del género masculino en el acceso a Internet, en algunos casos como: Bolivia (7 puntos porcentuales), Ecuador (3 puntos porcentuales) y Perú (7 puntos porcentuales).[184] Véase Gráfica 8.

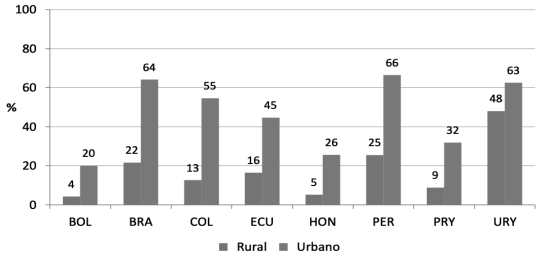
Gráfica 8. Uso de Internet según género. América Latina (2017)



Fuente: Sociedad Digital: Brechas y retos para la inclusión digital en América latina y el Caribe 2017.

En cuanto a la zona geográfica de la residencia, se encontró que las zonas rurales siguen siendo un reto para los Estados, ya que existe una diferencia sustancial en el acceso a las TIC. En el ámbito rural y el urbano esta diferencia es, en los casos más extremos, de 42 puntos porcentuales como en Brasil y Colombia y 40 en Perú.[185] Véase Gráfica 9.

Gráfica 9. Acceso residencial en áreas urbanas vs rurales. América Latina (2017)

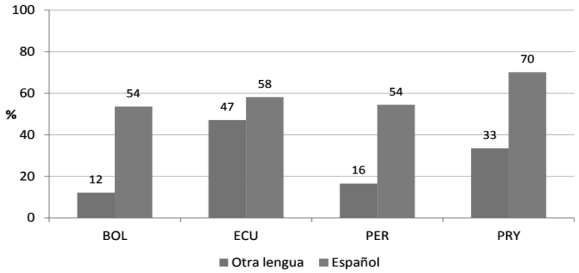


Fuente: Sociedad Digital: Brechas y retos para la inclusión digital en América latina y el Caribe 2017.

[183] López Velarde Campa, Jesús Armando, Vientos de cambio, LIII Legislatura, México, 1989, p. 35.
[184] UNESCO, op.cit.
[185] Idem.

Con lo que respecta a la lengua de las personas, en América Latina donde existen cientos de lenguas indígenas que aún se hablan en la actualidad, esta diversidad multilingüe no se ve reflejada en Internet. Esto constituye un obstáculo, ya que solo un puñado de lenguas, como el español y el inglés, dominan los contenidos de la red. Esto se confirma en la gráfica 5 en la que observamos que se incrementan las posibilidades de utilizar Internet si tu idioma familiar o primario es el español.[186] Véase Gráfica 10.

Gráfica 10. Uso de Internet según la lengua principal del hogar. América Latina (2017)

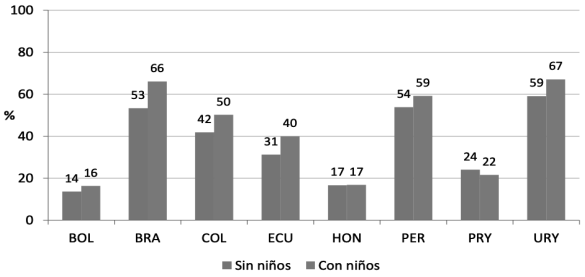


Fuente: Sociedad Digital: Brechas y retos para la inclusión digital en América latina y el Caribe 2017.

En el mismo documento, se sostiene que la presencia de niños en edad escolar, es un factor preponderante en la decisión de contar con Internet residencial o no. En la mayoría de los países observados en la gráfica 10 podemos ver que en los hogares con niños en edad escolar tienen una mayor probabilidad de estar conectados. Las familias aún con escasos recursos contratan en su residencia Internet a fin a apoyar a los menores en su desempeño escolar.[187] Véase Gráfica 11.

[186] Idem.
[187] Idem.

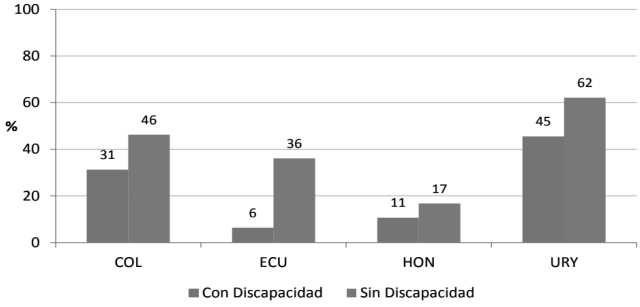
Gráfica 11. Acceso residencial según presencia de niños en edad escolar. América Latina (2017)



Fuente: Sociedad Digital: Brechas y retos para la inclusión digital en América latina y el Caribe 2017.

De la mayor importancia, es hacer una reflexión sobre el acceso a las TIC de personas con discapacidad. En el documento, se afirma la existencia de una brecha significativa entre las personas que cuentan con una discapacidad y las que no, esta diferencia en casos extremos va hasta los 30 puntos porcentuales, es decir las personas con discapacidad tienen menos oportunidades de tener acceso a Internet.[188] Véase Gráfica 12.

Gráfica 12. Acceso residencial según situación de discapacidad del jefe del hogar. América Latina (2017)



Fuente: Sociedad Digital: Brechas y retos para la inclusión digital en América latina y el Caribe 2017.

Estos datos nos brindan un panorama de los focos rojos de acceso a las TIC en América Latina, que impactan en la "distribución de la información y el conocimiento, la participación ciudadana y la repre-

[188] Idem.

sentación política, en el acceso a los servicios sociales y en la inclusión en la vida cultural comunitaria (local, nacional, regional o mundial)"[189] de los latinoamericanos. Cabe señalar entonces que la falta de acciones redistributivas por parte de los Estados podría implicar la consolidación de esta nueva forma de discriminación y exclusión social de los grupos analizados.[190]

En este sentido, el continente se encuentra en transición hacia una sociedad de la información, un contexto que coloca a los países de la región en una situación de desventaja para incorporarse a la economía y desarrollo de las TIC, por lo cual los desafíos para superar el déficit de conectividad y fomentar el desarrollo económico, social y cultural son muy altos.

Reconociendo ésto, en América Latina se están realizando diversas iniciativas para eliminar la brecha digital, tanto internacional como nacional. En el Informe CEPAL denominado "Estrategias, programas y experiencias de superación de la brecha digital y universalización del acceso a las nuevas tecnologías de la información y de la comunicación (TIC). Panorama regional de 2005, se realiza una revisión de las estrategias nacionales de 13 países latinoamericanos para abolir la brecha digital, entre las que se encuentran:

- Generación de iniciativas de universalización del acceso a las TIC, el fomento de la e-democracia;
- La prestación de servicios de gobierno electrónico, el fortalecimiento y digitalización de las pequeñas y medianas empresas;
- La promoción del e-comercio;
- La capacitación y formación de recursos humanos;
- El mejoramiento de la calidad de la educación;
- La aplicación de las nuevas TIC al desarrollo local, y
- El incremento de la cooperación e integración regional a través de redes.[191]

Donde los ámbitos temáticos prioritarios son: la modernización de la infraestructura y la universalización del acceso a las TIC, la implementación de e-gobierno en los procesos gubernamentales, el fomento del

[189] Villatoro, Pablo y Silva Alisson, op. cit., p. 13.
[190] Ibidem, p. 12.
[191] Ibidem, p. 13.

e-comercio, y la formación de recursos humanos capacitados en las TIC. Véase el Tabla 4.

Tabla 4. Prioridades temáticas y etapas en las estrategias hacia la sociedad de la información en 12 países de América Latina y el Caribe

PAIS - ESTRATEGIA	PRIORIDAD TEMÁTICA	ETAPA
ARGENTINA 2000- Programa nacional para la sociedad de la información (PSI) (http://www.psi.qov.ar/)	- Infraestructura y acceso universal a las TIC - Formación RR.HH. en las nuevas TIC - Gobierno electrónico	- Reconstrucción de visión estratégica
BOLIVIA 2002-Agenda Bolivia digital. (http://www.enlared.org.bo/etic/cgdefault.aso)	- Gobierno electrónico	- La estrategia se encuentra en proceso de elaboración y formulación de políticas
BRASIL 1999-Programa sociedad de la información en Brasil (http://www.socinfo.com.br/)	- Gobierno electrónico - Infraestructura y servicios genéricos	- Reformulación de políticas
CHILE 2003-Programa sociedad de la información en Chile (desde 1998)	- Gobierno electrónico	- Implementación y seguimiento
COLOMBIA 2000-Agenda de conectividad (http://www.aoenda.qov.co/)	- Gobierno electrónico - Infraestructura TIC - Comercio electrónico	- Implementación y seguimiento
ECUADOR 2000-Agenda nacional de conectividad (http://www. conectividad.gov.ec/	- Infraestructura y acceso universal a las TIC	- Implementación y seguimiento
REPUBLICA DOMINICANA 2003-2004- Estrategia nacional de TIC para el desarrollo (http://www.edominicana.gov.do/)	- Infraestructura TIC - Formación RR.HH. en las nuevas TIC - Gobierno electrónico	- Estrategia recientemente formulada
TRINIDAD Y TABAGO 2003-Plan nacional de las TIC VENEZUELA 2000-Decreto presidencial mandatario	- Infraestructura TIC - Formación RR.HH. en las nuevas TIC - Gobierno electrónico - Infraestructura TIC - Formación RR.HH. en las nuevas TIC	- Estrategia formulada - La falta de entidad coordinadora ha impedido la ejecución consistente de las iniciativas
JAMAICA 2002-Plan estratégico de las tecnologías de la información (http://www.janc.org/programs/ja itolan.odf)	- Gobierno electrónico	- Se cuenta con una visión y plan estratégico
MXICO 2000-Sistema nacional e-México (http://www.e-mexico.qob.mx/wb2/eMex/Home	- Infraestructura TIC - Gobierno electrónico	- Implementación y seguimiento
PERU 2003-2004-Programa nacional para el desarrollo de la sociedad de la información	- Infraestructura TIC - Formación RR.HH. en las nuevas TIC - Gobierno electrónico	- Formulación de políticas. Se está desarrollando el programa

Fuente: Elaborado por los autores, sobre la base de los datos contenidos en el estudio CEPAL (2003).

Adicionalmente, en el mismo documento de la CEPAL, se enlistan las acciones que están instrumentando los Estados latinoamericanos para disminuir la brecha digital. Véase Tabla 5.

Tabla 5. Principales áreas de acción definidas en las estrategias hacia la sociedad de la información en 13 países de América Latina y el Caribe

PAIS - ESTRATEGIA	AREAS DE ACCION
ARGENTINA 2000- Programa nacional para la sociedad dela información (PSI)	- Universalización de Internet y otras redes digitales de datos - Desarrollo delcomercio electrónico - Formación de recursos humanos especializados en las TIC - Fomento de lasinversiones en las nuevas TIC 11 + DI
BOLIVIA 2002-Agenda Bolivia digital.	- Desarrollo delgobierno electrónico - Fomento de la conectividad - Prestación de políticas sociales conel apoyo delas nuevas TIC: e-capacitación, e-salud y e-empleo - Desarrollo delcomercio electrónico
BRASIL 1999-Programa sociedad de la información en Brasil	- Universalización del acceso a las nuevas TIC - Fomento delempleo y deldesarrollo productivo - E-gobierno:digitalización de la gestión y servicios públicos - Educación para la SocInfo,contenidos eidentidad cultural - Fomento de la investioación v desarrollo en las nuevas TIC
CHILE 2003-Programa sociedad de la información enchile (desde 1998)	- Universalización del acceso a las nuevas TIC - Educación y capacitación enlas nuevas TIC - Gobierno electrónico - Comercio electrónico: industria digital y uso empresarial de TIC: desarrollo de marcos iurfdicos
COLOMBIA 2000-Agenda de conectividad	- Acceso a la infraestructura de las nuevas TIC - Educación y capacitación - Desarrollo empresarial - Fomento a la inversión enlas nuevas TIC - E-gobierno: digitalización de los servicios de gobierno
ECUADOR 2000-Agenda nacional de conectividad	- Gobierno electrónico: prestación de servicios públicos con ayuda de las TIC: tele-educación y tele-salud - Comercio electrónico - Modernización de la infraestructura de telecomunicaciones
REPUBLICA DOMINICANA 2003-2004- Estrategia nacional de TIC para eldesarrollo	- Universalización del acceso a las TIC - Uso de las TIC como un instrumento de lucha contra la pobreza - Gobierno electrónico: uso de las TIC para mejorar los procesos y servicios públicos y privados ala ciudadanía - Comercio electrónico
TRINIDAD Y TABAGO 2003-Plan nacionalde las TIC	- Universalización del acceso a las TIC - Modernización de la infraestructura de telecomunicaciones e informática - E-gobierno - E-comercio, conénfasis en la creación de marcos jurídicos apropiados - Capacitación de recursos humanos
VENEZUELA 2000-Decreto presidencial mandatario	- Universalización del acceso a las TIC - E-gobierno:digitalización de los procesos y servicios públicos - Prestación de servicios comunitarios

PAIS - ESTRATEGIA	AREAS DE ACCION
JAMAICA 2002-Plan estratégico de las tecnologlas de la información	- E-gobierno: entrega de servicios públicos eficientes a través de las TIC - E-comercio - Universalización del acceso a las TIC, con énfasis en las instituciones educacionales
MÉXICO 2000-Sistema nacional e-México	- Universalización del acceso,con énfasis en comunidades pobres - Capacitación en las nuevas TIC a comunidades pobres o en situación de vulnerabilidad - E-gobierno: prestación de servicios públicos por medio de las TIC (tele salud, tele educación, etc.)
PERU 2003-2004-Programa nacional para el desarrollo de la sociedad de la información	- Modernización de la infraestructura TIC - Formación de RR.HH. - Fomentar la aplicación de las TIC en programas de carácter social - Gobierno electrónico - Comercio electrónico v desarrollo oroductivo
PANAMA e-Panamá (http://www.e-panama.aob.oa/programa.html)	- Gobierno electrónico y transparencia dela gestión pública - Fomento deldesarrollo productivo y de la competitividad empresarial - Mejorar la calidad de la educación - Promover que la salud pública alcance a todos las areas de población

Fuente: Elaborado por los autores, sobre la base de los datos contenidos en el estudio CEPAL (2003).

Dentro de los proyectos de universalización de las TIC, destacan en el cuadro que 7 países (Bolivia, Brasil, Ecuador, Venezuela, México, Perú y Jamaica), establecen la prestación de servicios sociales como e-educación, e-salud, e capacitación, e-empleo, a través de las TIC. En el caso de Brasil, la estrategia sobre e-educación incluye "fomentar el desarrollo de contenidos pertinentes a las realidades locales y procurando la preservación de las identidades culturales".[192]

En este sentido, fomentar el acceso a las TIC a bajo costo y proporcionar conectividad han sido tareas fundamentales de los Estados. Datos de la CEPAL de 2005, señalan que en América Latina el 42% de los usuarios tuvieron acceso a Internet a través de la red de su hogar, en tanto que el 58% lo utilizó mediante redes en el trabajo, escuela o lugares de acceso público. En Perú el uso de Internet está vinculado a lugares como cabinas públicas o cafés donde se cuenta con el acceso; en Brasil, Costa Rica y México, se atribuye el incremento del uso de Internet a redes escolares, lo mismo que en Chile, que se llevó a cabo una dotación masiva de terminales para el sistema educativo[193] El modelo más utilizado de acceso compartido se ha desarrollado a través la instalación de computadoras en escuelas públicas.

[192] Idem.
[193] Ibidem, p. 33.

La colocación de computadoras en escuelas públicas vinculado a la idea de mitigar el analfabetismo, poniendo en práctica métodos y proyectos de alfabetización basados en las TIC en la región.[194] Se han basado en la implementación de reformas en los sistemas educacionales para mejora de las calidad y equidad en la educación, así como en la formación de recursos humanos altamente capacitados y especializados en el uso de las TIC.[195]

Desde hace tres décadas, en América Latina se han llevado a cabo programas nacionales para la inclusión de las TIC en el ámbito educativo, con semejanzas, diferencias y sus propias particularidades en cuanto al diseño, planificación, institucionalización, participantes de otros sectores y con diferentes grados de éxito. Podemos visualizar este crisol atendiendo a las experiencias de 8 Estados de la región que han implementado dicha estrategia.

En Brasil, en abril de 1997, fue creado el Programa Nacional de Informática en Educación PROINFO, cuyo objetivo era promover la inserción de las TIC en la educación básica y media, a través de apoyo para mejorar la calidad de los procesos de enseñanza- aprendizaje. Dicho programa depende del Ministerio de Educación de Brasil y del Consejo Nacional de Secretarios Estatales de Educación, pero su implementación se dejó a las Comisiones Estatales de Informática en la Salud, que eran las encargadas de la instalación de las TIC en las escuelas básicas y medias. Asimismo, el PROINFO se coordinó con el Programa Nacional de TV Escolar, para tener a su disposición un canal de televisión, que apoyara en la labor pedagógica.[196]

A partir de diciembre de 2007, a través del Decreto No. 6.300, se reestructuró con el objetivo de promover el uso de las TIC únicamente en las escuelas a nivel básico, apoyando a profesores y estudiantes de escuelas públicas. Trabajó en colaboración con los Estados y Municipios quienes realizaron la compra de equipos de cómputo al Plan de Acción Articulado (PAR), luego de la aprobación por parte del PAR, se transfieren los recursos a las entidades educativas para la adquisición de los equipos.

Adicionalmente, uno de los ejes de acción es el "Proyecto una computadora por alumno (UCA)" que se implementó con el obje-

[194] Ibidem, p. 12.
[195] Ibidem, p. 34.
[196] Ibidem, p. 35.

tivo de intensificar las tecnologías de la información y comunicación en las escuelas mediante la distribución de computadores portátiles a estudiantes. Otra de las líneas de acción, es la distribución de tabletas a los profesores de educación secundaria, tomando en consideración lo siguiente: ser profesor de un bachillerato urbano, tener Internet de banda ancha, pertenecer al laboratorio del Programa Nacional de Tecnología Educativa (ProInfo) y red inalámbrica (wi-fi).[197]

Las tabletas tenían características de hardware y software específicos, para ser adquiridas se requería un proceso igual que para la obtención de equipos en las escuelas, es decir: se incluía la orden de compra en la adhesión al Plan de Acción Conjunta (PAR). Luego de unirse y con la aprobación del PAR, el Fondo Nacional de Desarrollo Educativo (FNDE) se les transfería fondos a los Estados. Eran los Estados los que compraban los equipos directamente a las empresas ganadoras de la subasta.[198] En 2009 alcanzó la cifra de 53,000 laboratorios instalados y 52 millones de estudiantes beneficiados.

Otro ejemplo de implementación de políticas públicas para abolir la brecha digital es Costa Rica. En este país se instrumentó el Programa de Informática Educativa PIE MED-FOD, creado en 1988 por el Ministerio de Educación Pública y la Fundación Omar Dengo y que sigue vigente al 2021. Es una iniciativa de asociación del Estado y la sociedad civil, que tienen como propósito mejorar la calidad educativa de estudiantes del I y II ciclo de enseñanza básica pública, mediante el uso de las computadoras.

Desde una visión constructivista, el modelo que están implementando busca que educadores y estudiantes se relacionen entre sí y con los elementos computacionales para incrementar sus oportunidades de aprendizaje, por lo cual el programa incluye capacitaciones anuales de los docentes, también se pone a disposición de la comunidad educativa herramientas de programación, red temática educativa y una biblioteca digital.

Es importante destacar que las poblaciones de escasos recursos, tanto rurales como urbanos, son prioridad del programa. Consideran que los laboratorios de informática son un espacio generador de

[197] PROINFO, Programa Nacional de Informática na Educaçao. Disponible en: https://www.fnde.gov.br/index.php/programas/proinfo?view=default, consultado el: 05/03/2021.
[198] Idem.

cambio al interior de las escuelas, buscan que los estudiantes puedan aprender que la tecnología es un recurso útil para explorar el mundo.

La escuelas beneficiarias se eligen sobre los criterios de: interés manifiesto en el Programa, tamaño de la escuela, condición socio-económica de la población, disponibilidad de la comunidad para hacer aportaciones, es decir, las comunidades son responsables de generar la infraestructura necesaria para el funcionamiento de Programa en las escuelas, por lo que deben aportar el aula, es decir construirla, la instalación eléctrica, aire acondicionado, mobiliario y sistema de seguridad.[199]

El programa implica poner a disposición de los estudiantes el uso de recursos tecnológicos como: herramienta de programación, con procesador de textos de palabras, hoja electrónica, editor de documentos, una red telemática educativa que permite promover el intercambio de ideas utilizando tecnologías digitales y la biblioteca digital.[200]

En México, en 1997 se creó el Programa Red Escolar, operada por el Instituto Latinoamericano de Comunicaciones Educativas (ILCE), ONG internacional con sede en México, que trabaja en colaboración con la red Edusat, que presta de servicios de televisión educativos, así como con la Secretaría de Educación Pública.

El objetivo de la Red es impulsar la incorporación de TIC en las escuelas de educación básica, es decir de primaria y secundaria, basada en un enfoque constructivista. Para ello, la Red entrega a las escuelas computadoras con conexión a Internet, desarrolla proyectos colaborativos en línea, pone a disposición cursos virtuales para la actualización docente a través de cursos y talleres, implementación de salas de cómputo en escuelas, videotecas y televisión satelital. A 2020, también cuenta con una app móvil gratuita llamada Inspira para escuelas, para comunicación con los padres de familia, que cuenta con espacios para publicar noticias, agendar eventos y mensajería instantánea.

El proyecto busca identificar y difundir las prácticas educativas de las escuelas que en contextos vulnerables logran la inclusión. Al 2020, la Red está constituida por más de 14 mil escuelas, su portal en pro-

[199] Programa de Informática Educativa MEP FOD. Disponible en: https://issuu.com/andreshernandezcordoba/docs/programa_de_inform__tica_educativa_, consultado el: 05/03/2021.
[200] Idem.

medio se recibe un total de 2.5 millones de visitas diarias, atiende semestralmente a más de 200 mil estudiantes y 4 mil docentes.[201]

Entre los proyectos colaborativos nacionales de otoño 2020, están diversas temáticas como: las fábulas, la moraleja y el refrán, para estudiantes de 3 y 4 de primaria; sexualidad: conoce, cuida y decide sobre tu cuerpo para estudiantes de 5 y 6 de primaria así como de 1, 2 y 3 de secundaria; *Bullying*, acoso escolar para estudiantes de 5 y 6 de primaria así como de 1, 2 y 3 de secundaria; los derechos de los niños con responsabilidad social y Expresa lo que sientes, para estudiantes de 4, 5 y 6 de primaria, y Nuestra tierra: los desastres naturales, para 5, 6 de primaria y 1, 2 y 3 de secundaria.[202]

En Colombia, entre 1997 y 1999, se implementó el Programa de Informática y Bilingüismo, en ese entonces se implementó en 757 aulas de informática y la capacitación de 1500 profesores en la utilización del *software*. Asimismo, se creó el Programa de Nuevas Tecnologías, por el cual el Ministerio de Educación puso a disposición de los estudiantes de escuelas públicas un mayor número y con mayor calidad de recursos computacionales.[203]

Este programa tuvo como finalidad la integración de las TIC en los ambientes escolares de enseñanza básica y media, asimismo consideró su implementación como una herramienta pedagógica, en un esquema de acompañamiento. El plan contempló llegar a 650 escuelas con aulas de nuevas tecnologías dotadas de computadoras con Internet, así como capacitar a 2000 docentes en el manejo de las computadoras, *software* básico e Internet.[204]

Parte fundamental de este proyecto fue la creación de una Comunidad Educativa Virtual, que permitiera: "a) el intercambio de experiencias entre estudiantes, profesores e instituciones, b) la creación de contenidos educativos pertinentes a la realidad colombiana y, c) el fortalecimiento de una

[201] Red de escuelas. Disponible en: https://aprenderdelasescuelas.cippec.org/que-nos-inspira/red-escolar/, consultado el: 05/03/2021.
[202] Proyectos colaborativos nacionales, Otoño 2020. Disponible en: https://redescolar.ilce.edu.mx/images/inicio/2020/calendario_oto20.pdf, consultado el: 05/03/2021.
[203] Villatoro, Pablo y Silva Alisson, op. cit., p. 37.
[204] Idem.

nueva cultura de la información entre los diferentes actores del sistema educativo".[205]

En Perú, se implementó el Programa Nacional Huascarán en 2002, como un mecanismo para instalar computadoras con conexión a Internet en espacios escolares a nivel primaria y secundaria. Este programa es dirigido por el Ministerio de Educación, para su instrumentación contó con la colaboración de la Fundación Omar Dengo de Costa Rica, no obstante es un programa intersectorial en el que también participan el Ministerio de Transporte, Comunicaciones, albergue y construcción.[206]

El Proyecto contempla el incremento de la cobertura y calidad de las escuelas con la incorporación de aulas con computadoras y la implementación de programas de educación a distancia, busca alcanza especialmente a grupos urbanos marginados en área de alta densidad demográfica como a poblaciones de áreas rurales, selva y frontera, facilitando el acceso a información intercultural sustentada en valores.[207] Es decir este proyecto no solo busco el acceso universal sino el uso y apropiación de las TIC, por lo que:

> Este modelo implicaba hacer al Programa más inclusivo en tanto se trabajaba con los propios beneficiarios para conocer las condiciones en las que se brindaría el acceso, las características del uso de estas herramientas, la forma en que los estudiantes se benefician y las formas en que el aprendizaje y uso de TIC podría hacerse sostenible.[208]

No obstante, este programa tuvo dificultades vinculadas a los cuestionamientos de padres de familia y a la situación de los maestros de esta modalidad. Por lo que, en 2004 y 2005, este programa perdió apoyo y pasó a formar parte del Viceministerio de Gestión Pedagógica. De ahí se observan los principales problemas que enfrentó el gobierno peruano con la instrumentación de las TIC de manera universal en el sistema educativo del país: 1.- La poca claridad con respecto a los objetivos educativos y 2. la inadecuada planificación e implementación de los programas.[209] Más tarde en 2007, el Proyecto Huascarán, fue

[205] Idem.
[206] Idem.
[207] Idem.
[208] Balarin, María, Las políticas TIC en los sistemas educativos de América Latina: Caso Perú, UNICEF, 2013, p. 17.
[209] Ibidem, p. 16.

absorbido por la Dirección General de Tecnologías Educativas (DIGETE).[210]

Ese mismo año, se implementó una política de tecnologías que consistió en la compra y distribución de computadora a través del Programa una Laptop por Niño, ejecutado por la Dirección General de Tecnologías Educativas del Ministerio de Educación, en colaboración con el Programa Internacional *One Laptop per Child* (OLPC), que puso a Perú como beneficiario de este programa internacional. La muestra de las computadoras se presentaron al ejecutivo y posteriormente ante el Legislativo a fin de que aprobara la compra de 250 mil laptops para niños.[211]

El Programa OLPC, tiene como objetivo mejorar el aprendizaje de los niños en las regiones más pobres del mundo, con la entrega de laptop resistentes, baratas, de bajo consumo de electricidad y con contenido y *software* diseñados para aprendizajes colaborativos. En este contexto, en gobierno de Perú, busca llegar a las zonas de mayor pobreza, con altas tasas de analfabetismo, exclusión social, dispersión de población y bajas tasas de concentración de población escolar para contribuir con la equidad educativa de áreas rurales.[212]

La primera experiencia de Argentina por introducir el acceso universal en sus escuelas, fue el Plan de Educación Social de 1994 a 1999, cuyo objetivo fue promover la integración tecnológica para mejorar la calidad y equidad educativa, para ello implementó cursos de capacitación docente y la donación masiva de computadoras en las escuelas públicas. Este programa tuvo un alcance limitado, solo el 5.2% de las escuelas del país tenían acceso a Internet, y la densidad informática nacional era de 1 computadora por cada 240 estudiantes.

En el año 2000, se creó el programa educ.ar, dependiente del Ministerio de Educación, Ciencia y Tecnología, en el que participa el sector privado, representantes gremiales de las empresas vinculadas a las TIC, universidades privadas y la Cámara del Libro. El objetivo del programa es que el 100% de las escuelas argentinas cuentan con Internet, un portal de contenidos educativos, capacitación docente y un plan de conectividad.

[210] Ibidem, p. 19.
[211] Ibidem, p. 21.
[212] Ibidem, p. 23.

Adicionalmente, el programa funciona con aportes de empresas, instituciones y equipos profesionales para integrar el patrimonio de educ.ar y con la colaboración de diversos actores de las comunidades educativas, profesores, padres de familia, directivos, entre otros.[213]

En Uruguay se creó el Programa de Conectividad Educativa "Todos en red", esfuerzo que impulsa la Presidencia de la República, junto con la Administración Nacional de Telecomunicaciones (ANTEL), financiado por el Fondo Japonés de Consultoría (FJC) a través del Banco Interamericano de Desarrollo (BID), cuya finalidad es la incorporación de las TIC en todos las escuelas de educación pública.

En Chile se instrumentó el proyecto Red Enlaces, dependiente del Ministerio de Educación en colaboración con universidades públicas y privadas del país, cuyo objetivo es crear una red educacional nacional entre todas las escuelas y liceos del país, en este sentido no se trata simplemente de la instalación de las computadoras sino que se busca integrar la red nacional que permita el intercambio de ideas y experiencias.[214]

Este programa inició en 1992, con 12 escuelas, el periodo de prueba se extendió hasta 1995, y durante 1998, se adoptó la materia de informática como parte transversal de la currícula de educación secundaria. Para 2002, el "programa Red Enlaces pone a disposición de la comunidad escolar un portal web que cuenta con una Red Escolar, estudios en el ámbito de la aplicación de las nuevas TIC a los procesos de aprendizaje, herramientas de gestión educacional y una Red de Asistencia Técnica".[215]

[213] Pablo Villoro y Silva Alisson, op. cit., p. 38.
[214] Ibidem, p. 39.
[215] Idem.

Capítulo 5. Grandes compañías tecnológicas estadounidenses

Introducción

En la actual cuarta revolución industrial, que como las anteriores está llamada a transformar todo el proceso productivo, desde el cómo producimos, cómo consumimos, cómo nos relacionamos, hasta cómo nos comunicamos, es decir, transformará nuestra sociedad. Las TIC, como tercer revolución, han permitido la llegada de la llamada economía del conocimiento,[216] de los datos o digital.

Pero hay que entender que el dato por sí mismo no genera riqueza, sino es el proceso de refinamiento, procesamiento y análisis, lo que le da su valor. Los datos de los ciudadanos, empresas y administraciones han aumentado exponencialmente en los últimos 30 años y con la llegada de la 5G se espera que el crecimiento de los datos, del *big data,* sea exponencial.[217] De acuerdo con información de *Software and Information Industry Association*, en 2013 la información almacenada en el mundo alcanzó los 161 exabytes (EB= 10 a la potencia 18 bytes) por año, mientras que en el 2020 se prevé que el tráfico de datos supere los 15 zettabytes (ZB= 10 a la potencia de 21 bytes).[218]

Las TIC, en el marco de la época digital, han permitido la posibilidad de dar un valor a los datos, monetizarlos, al generar las herramientas necesarias para capturarlos, procesarlos, almacenarlos y analizarlos a bajo costo. El *big data* es importante para desarrollar un mayor conocimiento sobre el cliente, reducción de costes mediante la detección de ineficiencias, creación de nuevos productos dependiendo de las necesidades de los consumidores, entre otros.

En los siguientes años, se espera que el volumen de datos se multiplique por 11, la velocidad de transferencia será cien veces más que

[216] Ontiveros, Emilio (Dir.) y López Sabater, Verónica (Coord), Economía de los datos. Riqueza 4.0, Editorial Ariel, España, 2017, p. 11.
[217] Ibidem, p. 26.
[218] Idem.

la que se dispone actualmente, en el futuro los recursos más valiosos serán los datos.[219]

En consecuencia, en el primer apartado, nos acercamos al fenómeno de la monetización de los datos, desde el ámbito económico, desde la definición del dato, el proceso de transformación del mismo y las estrategias desarrolladas por las empresas para poder insertarse en la era de la economía digital; en un segundo apartado nos referimos a las consecuencias económicas y políticas de la existencia de grandes empresas monetizadoras de los datos, fundamentalmente en los Estados Unidos y la reacción del gobierno ante éstas.

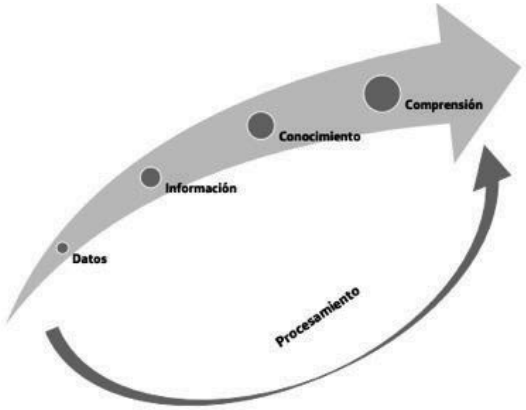
5.1 Monetización. La acumulación de datos

Los datos son representaciones simbólicas que pueden ser numeradas, gráficas, alfabéticas, algorítmicas, etc. de un atributo o variable cuantitativa o cualitativa, que pueden estar contenidos en fotografías, mensajes, redes sociales, conversaciones de voz. Estos datos se acumulan, en la era digital, de diversas maneras, por ejemplo: a través de las búsquedas en Internet, las páginas que visitas, mediante las compras online, los anuncios que revisas o la información de tu perfil que dejas en tus redes sociales, como la música que te gusta, tu localización geográfica, etc. Todos estos datos son recogidos a través de *cookies* que previamente tienes que aceptar para visualizar la información que estás buscando.

No obstante, todos estos datos por sí mismos no proporcionan un valor, una imagen sin un contexto o tratamiento, no significa nada para una empresa, para que éstos tengan un valor, es decir sean monetizados se requiere un procesamiento, se requiere transformarlos para ser insumos de valor y utilidad.[220] Este procesamiento implica: tener el dato, tener información, conocimientos y comprensión del mismo, es el ciclo del dato. Véase Figura 4.

[219] Idem.
[220] Ibidem, p. 24.

Figura 4. El ciclo del dato



Fuente: https://www.fundacioncarolina.es/wp-content/uploads/2018/11/Libro-Economia-de-los-Datos-Ontiveros.pdf p.24

En este sentido, de manera amplia, la monetarización de datos significa el aprovechar los datos obtenidos por una empresa para adquirir oportunidades, beneficios e ingresos, que incluye la generación de una estrategia y modelo de negocio para la venta de datos a otras empresas.[221] Esto potenciado por las TIC, no solo significa el promover interacciones entre clientes y consumidores, sino generar todo tipo de estrategias debido al volumen, variedad y velocidad de los datos.

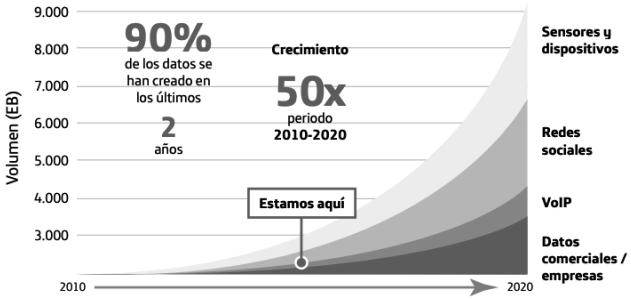
El fenómeno de la monetización y comercialización de datos esta de la mano con elementos clave:

- Disponibilidad y posibilidad de acceder a datos, estructurados y no estructurados, de manera masiva.
- Costes de almacenamiento más bajos de la historia.[222]
- Creación de nuevas herramientas de tratamiento del Big data.
- Proliferación de dispositivos conectados a Internet.
- Interconectividad social.

[221] Monetización de datos: estrategia más rentable de analytics. Logicalis Architects of Change. Disponible en: https://blog.es.logicalis.com/analytics/monetizacion-de-datos-la-estrategia-mas -rentable-de-analytics, consultado el: 05/03/2021.
[222] Idem.

Respecto al primer punto, la disponibilidad masiva de datos y el incremento en el volumen de la información, así como la gran variedad de éstos y la capacidad para analizarlos, son factores crucial en el proceso de monetización de los mismos. En la Gráfica 13 se muestra el crecimiento de los datos en la última década, de 2010 a 2020.

Gráfica 13. Volumen de *big data* (2010-2020)



Fuente: https://www.fundacioncarolina.es/wp-content/uploads/2018/11/Libro-Economia-de-los-Datos-Ontiveros.pdf p.27

Destaca que de 2018 a 2020, los datos han presentado un incremento del 90%, ello como consecuencia del abaratamiento de la computación en los últimos años, el crecimiento de las redes sociales, *cloud computing* o computación en nube y la utilización de herramientas analíticas; lo cual ha fortalecido la economía de los datos.

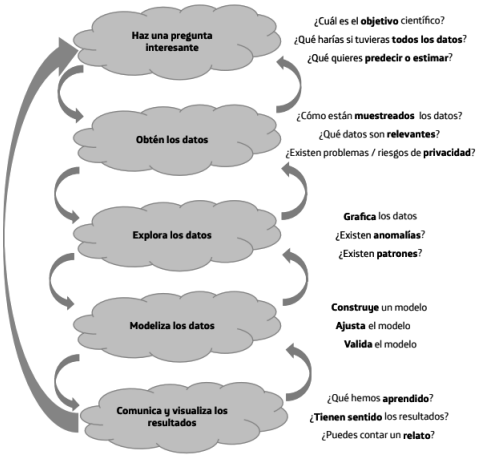
Con referencia al segundo punto, costes de almacenamiento bajos y la computación en nube han permitido utilizar la capacidad de almacenamiento de manera remota, masiva y muy asequible. Se basa en la "conversión de la capacidad de procesamiento computacional de un producto a un servicio contratable por una tarifa que posibilita hacer uso de unos recursos".[223] En este sentido, evita el costo para el cliente de una gran inversión en infraestructura, plataformas y *software*.

Respecto al tercer punto, las TIC, brindan la posibilidad de observar un solo dato, analizarlo, comprenderlo y utilizarlo, no obstante, también nos permiten poder hacer el mismo ejercicio con miles o millones de datos, a través de nuevas herramientas:

[223] Ontiveros, Emilio (Dir.) y López Sabater, Verónica (Coord), op. cit., p. 28.

- *Business intelligence* o inteligencia de negocio: permiten crear cuadros de mando con visualizaciones de la información o informes de errores.
- *Data science* o ciencia de los datos: permite realizar análisis descriptivos a fin de anticipar o predecir sucesos futuros y prescriptivos. Estos análisis se utilizan para generar mejoras de eficiencia, ahorro en costes, realizar estudios pormenorizados de los clientes, prevención de fraude, redes sociales y tratamiento de Internet.[224] Véase Figura 5.

Figura 5. El proceso de la ciencia de los dato



Fuente: https://www.fundacioncarolina.es/wp-content/uploads/2018/11/Libro-Economia-de-los-Datos-Ontiveros.pdf p. 42

La *data science* es el conjunto de técnicas que nos permiten pasar de un conjunto de datos a un procesamiento de los mismos y por tanto a su monetización. El utilizar estas herramientas puede implicar el trabajo de una sola empresa o la colaboración de distintas empresas, ya que su utilización dista de ser homogénea en los distintos sectores y en distintos territorios, por lo cual sus efectos en algunos casos se han potencializado, y en otros aún falta por explotar todas sus capacidades.

Respecto al cuarto punto, el incremento de dispositivos conectados a Internet, como teléfonos y tabletas, principalmente, a los que

[224] Ibidem, p. 25.

se suman sensores inteligentes en relojes, coches o incluso casas que permiten conectividad a la red. Estos permiten a las personas estar conectados ininterrumpidamente, tener acceso a Internet en cualquier momento y en cualquier lugar, la ubicuidad de la red.

En cuanto al quinto punto, las redes sociales como fenómeno que ha crecido exponencialmente en los últimos años, conjuga elementos que van desde compartir historias, imágenes, videos, hasta interactuar en el mundo laboral y formativo escolar-académico. Estás comprenden a los individuos y la mejora de la oferta de servicios, de forma casi personalizada.

En este sentido, la era digital genera condiciones favorables a los procesos de monetización de los datos y a la economía digital, que son aprovechadas por las empresas a fin de obtener un beneficio económico. Ello a través de dos vertientes: por un lado mediante una estrategia interna, que implica mejorar la experiencia de clientes y el aumento del rendimiento corporativo; por el otro, a través de una estrategia externa, que implica la venta de los datos, comercializando los insumos que se obtienen a partir de su análisis.[225]

Para llevar a cabo dichas estrategias, las empresas toman en consideración aspectos importantes de la monetización:

- Información de alta frecuencia: son los más valiosos en términos de monetización y se refieren a movimientos de tarjetas de débito y crédito, búsqueda en web móvil o cualquier tipo de transacción que se lleve a cabo varias veces al día.
- Conocimiento de los hábitos de los consumidores: se refiere a la información sobre el comportamiento de los clientes o usuarios, que sirven para identificar sus preferencias. ello a través del análisis de sus hábitos en el uso de dispositivos, geolocalización, transacciones financieras, entre otras.
- Identificación de los consumidores: estos datos tienen valor en el sentido de que permiten realizar perfiles de los consumidores, ya que esta incluye nombre, dirección, números telefónicos, trabajo, familia.[226] Por lo que hay que tener presente la legislación local e internacional de protección de datos personales y el derecho al olvido.

[225] Monetización de datos: estrategia más rentable de analytics, op. cit.
[226] Idem.

- Usabilidad de los datos: se debe estar seguro de que los datos son accesibles y utilizables.
- Valor de los datos: la intención de las empresas es maximizar el valor de los datos.
- Modelo de datos: es la estrategia que se busca crear para potenciar el valor de los datos.[227]

En muchos casos una empresa por sí sola no cuenta con las capacidades para llevar cabo todo el proceso de monetización de los datos, por ello, la cadena de monetización se encuentra integrada por diferentes agentes que intervienen y que han tenido que modificar sus formas de producción, consumo, planificación, gestión, distribución y movilidad, por ejemplo:

- Empresas generadoras de datos.
- Empresas tecnológicas.
- Compañías de servicios analíticos.
- Reguladores y entidades académicas.

En esta cadena las empresas utilizan diversas tecnologías que suponen un reto a sus propias capacidades, por lo que las grandes empresas usualmente son las que se ven beneficiadas con el valor de los datos. Son éstas las que cuentan con las capacidades para insertarse en la economía del conocimiento o de la información, son éstas las que tienen los grandes capitales de inversión y capital físico capacitado. Aunque con la creación de la nube (*cloud*) más empresas pequeñas o medianas se han podido incorporar.

El poder dar valor a los datos ha favorecido el surgimiento de nuevos negocios *startups* nacidos de forma nativa en la economía digital y de las empresas tradicionales que tuvieron que transformarse en *data-driven companies* para poder monetizar los datos, pero también reconfigurando la estructura de los mercados y sectores productivos; y reorganizando los negocios tradicionales, en donde éstos funcionan a partir de la transmisión de datos, basados en la transparencia, como: empresas de contenidos educativos, informativos, culturales, de transporte, alojamiento y compraventa.[228]

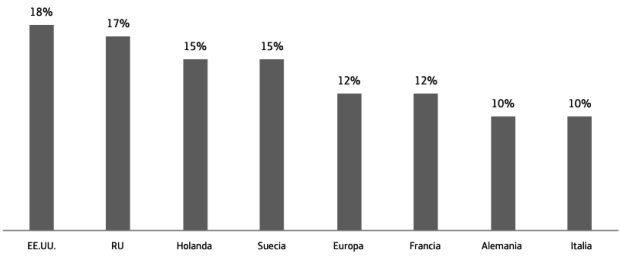
[227] Data Monetization: aprovecha el potencial de tus datos. Data Centric. Disponible en: https://www.datacentric.es/blog/marketing/data-monetization-datos/, consultado el: 05/03/2021.
[228] Ontiveros, Emilio (Dir.) y López Sabater, Verónica (Coord), op. cit., p. 21.

En este sentido, los datos se convierten en insumos esenciales, en el centro de la nueva economía digital, "en la medida en que habilitan la innovación, la eficiencia de procesos y la sofisticación de los medios y servicios que se producen".[229]

A pesar de lo complicado que es realizar la cuantificación de la economía de los datos, dada su diversificación, de acuerdo con información de la Comisión Europea, se estima que en la Unión Europea los datos tuvieron un valor de 272 millones de euros en 2015. En el caso de los Estados Unidos, se estima que la monetización de los datos podría alcanzar en 2025, 2,2 billones de dólares.[230]

No obstante, a pesar de que el 90% de los datos se ha generado en los últimos 2 años, solamente se ha procesado el 1% en todo el mundo. Se estima que Europa ha procesado el 12% y EUA el 18%, como lo muestra la Gráfica 14.

Gráfica 14. Grado de aprovechamiento del potencial de la digitalización en varios países (2020)



Fuente: https://www.fundacioncarolina.es/wp-content/uploads/2018/11/Libro-Economia-de-los-Datos-Ontiveros.pdf, p.29.

Este potencial y procesamiento de datos no se ha maximizado en diversos países derivado de distintos factores, por ejemplo:

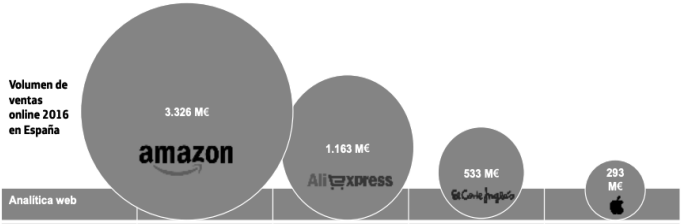
- La dificultad de instrumentar proyectos con datos, ya que cuentan con un componente científico y exploratorio que no es sencillo implementar para muchas empresas, por lo cual los proyectos basados en datos pueden no ser viables, así como sus costes y por tanto se alarguen en el tiempo.
- La existencia de poco personal capacitado para manejar proyectos de datos, específicamente de *data science*. Normalmente,

[229] Idem.
[230] Ibidem, p. 29.

muchas empresas son incapaces de generar estos recursos humanos.
- La incertidumbre en las estimaciones de las ganancias de retorno de las inversiones en proyectos de datos.
- Los aspectos regulatorios nacionales e internacionales sobre la protección de datos personales y el derecho al olvido.
- El análisis de datos es un trabajo cotidiano que muchas empresas consideran complicado de operativizar.

En conclusión, se observa que las grandes empresas tecnológicas usualmente son las que se encuentran en posibilidad de monetizar los datos, pensemos por ejemplo en el comercio *on line*, donde los grandes portales están facturando miles de millones de transacciones y obteniendo datos como: ¿qué compró?, ¿Cuánto pagó?, ¿cómo pago? ¿dónde estaba cuando realizó la compra?.[231] Véase Gráfica 15.

Gráfica 15. Los gigantes del comercio en la web. España (2016)



Analítica web				
Promedio de visitantes únicos /mes	14.100.000	7.900.000	6.800.000	2.900.000
Número de pedidos únicos /año	33.264.000	12.924.000	2.862.000	1.332.000
Ticket medio (EUR)	100	90	186,5	220
Tráfico generado en España	85,1%	91,0%	92,3%	95,4%
Tiempo medio por visita	5:43	3:57	4:17	3:53
Páginas vistas por visita	6,6	6,1	4,8	4,4
Compradores vía motor de búsqueda 2015	36,2%	65,4%	63,2%	72,0%
Tasa de rebote	33,0 %	42,9%	37,6%	48,1%
Tasa de conversión	3%	3%	1,5%	1,5%

Fuente: https://www.fundacioncarolina.es/wp-content/uploads/2018/11/Libro-Economia-de-los-Datos-Ontiveros.pdf, p.36.

[231] Ibidem, p. 36.

5.2 Grandes empresas monetizadoras de los Estados Unidos y la guerra comercial contra China

De acuerdo con datos de la Conferencias de las Naciones Unidas sobre Comercio y Desarrollo, los principales ganadores en materia económica a nivel mundial en los últimos 30 años, en la llamada era digital, han sido las grandes empresas tecnológicas de los EUA.[232] ¿Cómo lo han hecho?, pues como señalamos en el apartado anterior sólo un par de empresas en el mundo cuentan con la capacidad de monetizar los datos de manera masiva, generando grandes monopolios de la utilización de datos en la economía digital.

Por ejemplo Facebook, cuando compró WhatsApp en 2014, no se preveía que para 2016, cambiaría su política de privacidad, con el objetivo de compartir los números de teléfono de sus usuarios de Whatsapp con Facebook. Lo cual significó, además de mayores avisos publicitarios, menos privacidad[233] para sus usuarios de redes sociales.

En ese momento, las reacciones no se hicieron esperar, la Comisión Europea anunció la imposición de una multa de 120 millones de dólares a la empresa Facebook, por información engañosa para sus usuarios al utilizar WhatsApp,[234] ya que en reiteradas ocasiones Mark Zukenber, señaló que no vincularía las cuentas de ambos servicios, por lo que no solo engañó a las instituciones europeas sino a los propios usuarios.[235]

Al vincularlas, Facebook ha utilizado estos datos para:

- Realizar sugerencias de amistad, es decir a través de tu número de telefono, Facebook accede a tus contactos con los cuales has intercambiado mensajes de texto, pero que no tenías agregados en la red social;

[232] La concentración de poder de las grandes tecnológicas es perjudicial para los Estados Unidos. TyN Magazine. Disponible en: https://www.tynmagazine.com/ft-la-concentracion-de-poder-de-las-grandes-companias-tecnologicas-es-perjudicial-para-eeuu/, consultado el: 05/03/2021.
[233] BBC Mundo, 3 maneras en las que facebook usa tu información de WhatsApp, Tecnología. Disponible en: https://www.bbc.com/mundo/noticias-39961792, consultado el: 05/03/2021.
[234] Idem.
[235] Idem.

- Enviar publicidad personalizada, basta con hacer una búsqueda en Google sobre un tema concreto para que aparezca anuncios publicitarios en la red social sobre lo que preguntaste en el buscador, los anuncios también son enviados a las redes sociales por categorías de edad, intereses, zona geográfica, etc. A futuro, la idea es que las empresas paguen a WhatsApp a cambio de poder mandar mensajes a los usuarios de la aplicación a través de anuncios segmentados por categorías, y
- Saber en qué momento te conectaste por última vez a WhatsApp, a fin de generar estrategias y estadísticas de tus hábitos en la red social.

Otro ejemplo de empresas monetizadoras, es Amazon, en la sección de Amazon Afiliados, que apoya a creadores de contenido, editores y blogueros a monetizar su tráfico de usuarios, ofreciendo millones de productos y programas disponibles en Amazon, y que pueden ser utilizados a través "de herramientas de creación de enlaces para dirigir a su audiencia a sus recomendaciones y así ganar dinero de las compras"[236] de sus usuarios.

Asimismo, esta empresa del e-comercio en su división de Amazon Web Services (AWS), está ampliando sus lazos de colaboración con Toyota, a fin de que la fabricante de autos pueda recopilar datos de vehículos conectados a la nube y aplicarlos en el diseño y desarrollo de nuevos coches. Es Amazon la que está construyendo la plataforma que ayude a Toyota a desarrollar, implementar, administrar y monetizar los datos recopilados por sus autos inteligentes en todo el mundo, ampliando su Plataforma de Servicios de Movilidad que ya incluye, compartir viajes, el *leasing,* notificaciones proactivas de mantenimiento o de seguros de auto basados en el comportamiento y hábitos del conductor.[237]

Asimismo, AWS cuenta con acuerdos con Volkswagen para desarrollar a la automotriz un portal de datos y *software* basados en la computación de nube con el objetivo de permitir a sus clientes comer-

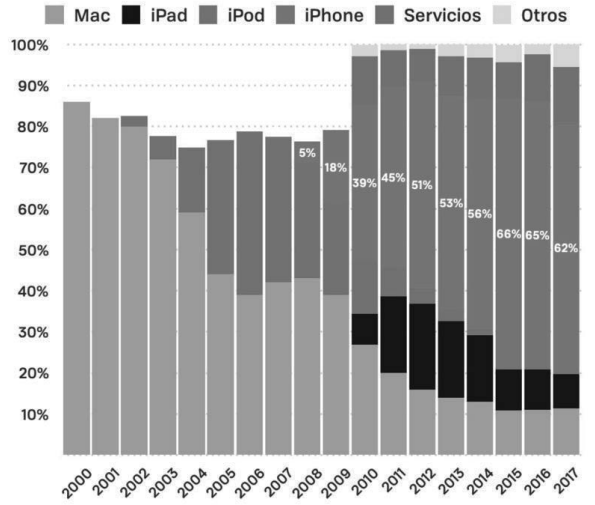
[236] Amazon Afiliados. Disponible en: https://afiliados.amazon.com.mx/, consultado el: 05/03/2021.

[237] Amazon ayudará a Toyota a monetizar los datos recopilados por sus coches. Motorpasión. Disponible en: https://www.motorpasion.com/toyota/amazon-esta-ayudando-a-toyota-a-monetizar-datos-recopilados-sus-coches, consultado el: 05/03/2021.

ciales, comprar y vender sus aplicaciones industriales. También, cuenta con asociaciones con Uber y Avis, Nvidia, Aptiv y Panasonic.[238]

Debemos mencionar a Apple, la denominada empresa más valiosa del mundo, la primera en superar el billón de dólares de valoración. Esta empresa tiene en el centro de su negocio el Iphone, en 2017, el 62% de sus ventas se debía a este producto, como lo podemos ver en la Gráfica 16.

Gráfica 16. ¿De qué ha ido dependiendo Apple? (2000-2017)



Fuente: https://www.xataka.com/empresas-y-economia/asi-como-gana-dinero-apple-iphone-llegando-a-su-techo-hora-sacar-dinero-sus-propietarios

No obstante, se observa que a partir de 2010, cobra fuerza el apartado de "servicios" y "otros", que incluyen accesorios, Apple TV, cables, iPods y Apple Watch, los productos complementarios del Iphone, pero también productos de *software* que implican la venta de almacenamiento en iCloud Drive, Apple Music, Apple Pay, entre otros. En este sentido, el principal negocio de Apple es el Iphone, pero no solo de su venta física sino también de sus *software*s y accesorios.[239]

[238] Idem.

[239] Así es como gana dinero Apple: con el Iphone llegando a su techo es hora de sacar más dinero a sus propietarios. Xalaka. Empresas y Economía. Disponible en: https://www.xataka.com/empresas-y-economia/asi-como-gana-dine-

Complementa sus ingresos con la venta, alquiler y transmisión de información, no personal como indica su política de privacidad: almacenan, utilizan, transfieren y revelan datos no personales. En su página de Internet indica que "la información que almacena puede estar relacionada con las actividades de los usuarios en la iTunes Store, App Store, Apple TV y iBooks Store, así como en otros productos y servicios, indicando que la información es agregada y utilizada para ofrecer a sus usuarios información y entender qué partes de su sitio web, productos y servicios son más importantes para ellos".[240]

Aunado a lo anterior, estas empresas ejercen prácticas monopólicas que dañan la economía de los Estados Unidos, por lo que su gobierno está preparando diversas estrategias para poder controlar el poder a las grandes compañías tecnológicas, particularmente contra Amazon, Apple, Google y Facebook, cuyo valor conjunto estimado total es de más de 5 billones de dólares. El gobierno estadounidense las acusa del debilitamiento de su economía, al menguar el porcentaje del PIB que representa la mano de obra nacional, que se ha visto disminuida sustancialmente.

En el informe elaborado por la Cámara de Representantes sobre las grandes empresas tecnológicas como Amazon, Facebook, Google y Apple, se menciona la palabra monopolio 120 veces.[241] En dicho informe, presentado en octubre de 2020, son duramente cuestionadas las empresas estadounidenses, por mucho las principales monetizadoras de datos en el mundo, sobre el abuso de su posición dominante en los mercados para establecer reglas, precios, búsquedas, redes sociales y publicidad en línea, entre otros. Sostienen que las empresas tienen demasiado poder y éste debe ser controlado.[242]

En este sentido, los legisladores recomendaron desmembrar a las grandes empresas y restaurar la competencia, aplicando marcos jurídicos estrictos antimonopolios y evitar que estos gigantes compren nue-

---

ro-apple-iphone-llegando-a-su-techo-hora-sacar-dinero-sus-propietarios, consultado el: 05/03/2021.

[240] Apple es demandada por vender datos de sus usuarios a terceros. Tecnología. Disponible en: https://industriamusical.es/apple-es-demandada-por-vender-datos-de-sus-usuarios-a-terceros/, consultado el: 05/03/2021.

[241] La ofensiva en EE.UU. para desmembrar las grandes empresas tecnológicas acusadas de monopolio. BBC New. Tecnología. Disponible en: https://www.bbc.com/mundo/noticias-54458049, consultado el: 05/03/2021.

[242] Idem.

vas empresas emergentes.[243] Por ejemplo, Amazon, que es proveedora de infraestructura, plataformas digitales para e-comercio, pero al mismo tiempo compite con esas empresas como vendedor de productos, lo que le da una ventaja sobre sus competidores.[244]

Adicionalmente, el gobierno ha emprendido una lucha, pero también alianzas, con estas empresas a fin de que disminuya su poder, es el caso del Departamento de Justicia que presentará una demanda contra el gigante Google por su dominio en el campo de las búsquedas en Internet, por monopolizar las búsquedas y publicidad *online*, aplicando estrategias anticompetitivas que incluyen privilegiar su propio contenido por encima de las otras webs; este sería el caso antimonopolio más grande desde los últimos 20 años.

Pero, aunque no se han confirmado los alegatos, se sabe que incluirán temas sobre los precios a los consumidores, así como el daño que suponen para la economía estadounidense las transacciones digitales que se valoran en datos y no en dólares. Esto dificultará los alegatos, ya que las grandes empresas como Google, controlan también el acceso a los algoritmos y pueden cobrar diferentes precios a distintos clientes por el mismo producto, los datos.[245]

En tanto, Amazon, Apple y Facebook, están siendo investigadas por parte del Departamento de Justicia, por la Comisión Federal de Comercio y por los fiscales generales de casi todos los Estados del país,[246] por: Facebook, monopolio en el mercado de redes sociales, ejerciendo una táctica de adquirir, copiar o matar a cualquier empresa intervenga en sus dominios; Amazon por prácticas monopólicas en el ámbito de las ventas en *online* cerrando las puertas a otras empresas a las que denomina competidores internos; Apple por ejercer un monopolio de venta a través de la *App Store,* que utiliza para crear y aplicar a la competencia medidas excluyentes dando preferencia a sus propias ofertas.[247]

---

[243] Idem.

[244] Idem.

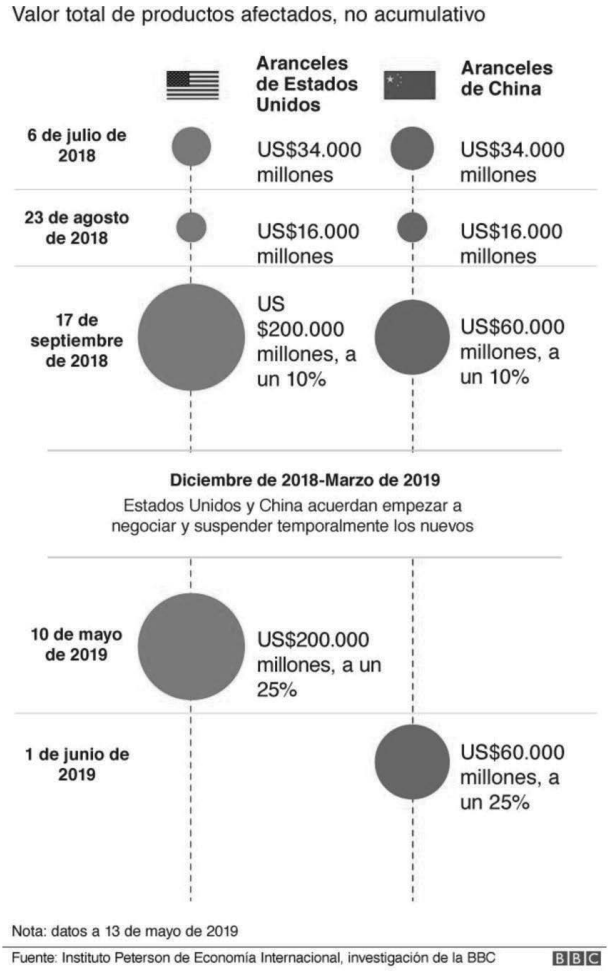
[245] La concentración de poder de las grandes tecnológicas es perjudicial para los Estados Unidos. TyN Magazine. Disponible en: https://www.tynmagazine.com/ft-la-concentracion-de-poder-de-las-grandes-companias-tecnologicas-es-perjudicial-para-eeuu/, consultado el: 05/03/2021.

[246] La ofensiva en EE.UU. para desmembrar las grandes empresas tecnológicas acusadas de monopolio. op. cit.

[247] Idem.

Sumado a lo anterior, se han visto afectadas por la guerra emprendida por los Estados Unidos contra China, en la cual ambos países han incrementado sus aranceles a la importaciones, ello con la finalidad de que los productos del país contrario sean menos atractivos para sus ciudadanos y se reduzcan las ventas en el país afectado. Véase Gráfica 17.

Gráfica 17. Cómo se ha intensificado la guerra comercial entre China y Estados Unidos (2018-2019)



Nota: datos al 13 de mayo de 2019.
Fuente: Instituto Peterson de Economía Internacional, investigación de la BBC.

A pesar de que no se ha producido el *boom* de empleo y producción nacional en los EUA, en esta lucha contra las importaciones, los aranceles y limitaciones impuestas al comercio con compañías chinas, especialmente en el ámbito tecnológico, están obligando a las empresas estadounidenses a buscar proveedores alternativos para sus suministros, así como mover sus capacidades fuera de China, como México y Vietnam, al incrementar sus importaciones a los EUA.[248]

Con esta guerra, empresas como Facebook que tiene muy pocas operaciones en China, no se ve afectada, no obstante Microsoft y Google, tienen un grave problema ya que sus productos son distribuidos por empresas Chinas en todo el mundo.[249] En este último caso, el veto de Trump, en mayo de 2019, al incluir a Huawei en la *Entity List*, por cuestiones de seguridad nacional, señalando que la empresa está controlada por el Ejército Popular, le impide hacer negocios con empresas americanas.[250] Asimismo, ha señalado su intención de prohibir la red social TikTok.

Ésto también daña a las empresas estadounidenses, en particular a Google que no prestará sus servicios Android a la empresa china, lo cual significa que no puede ofrecer Google Play y otras aplicaciones de Google en su telefonía.[251]

Otra empresa afectada es Apple que, por un lado, sus ventas en China no se ven afectadas, ya que fabrica en ese país, por el otro, cómo produce en China sus ventas en EUA si se verán impactadas con el incremento de aranceles. Por su parte, Amazon no cuenta con grandes ventas en China, por lo cual la afectación será mínima.

Adicionalmente, al igual que Huawei, en octubre de 2019, EUA decidió incluir en su lista negra a 28 empresas chinas, incluidos Hikvisión, fabricante de equipos de videovigilancia y *Sense Time Group Ltd*, desarrolladores de inteligencia artificial o Danua Technology des-

[248] EE.UU. vs China: escenarios de la nueva guerra fría. El País. Disponible en: https://elpais.com/internacional/2020-07-25/ee-uu-vs-china-escenarios-de-la-nueva-guerra-fria.html, consultado el: 05/03/2021.

[249] Así nos afecta la Guerra comercial entre EE.UU. y China al resto del mundo. Xataka. Empresas y Economía. Disponible en: https://www.xataka.com/empresas-y-economia/asi-nos-afecta-guerra-comercial-eeuu-china-al-resto-mundo, consultado el: 05/03/2021.

[250] EE.UU. vs China: escenarios de la nueva guerra fría. op. cit.

[251] Así nos afecta la Guerra comercial entre EE.UU. y China al resto del mundo. op. cit.

tacada en la tecnología de reconocimiento facial, por participar en abusos contra la etnia uigur en la región de Xinjiang, al occidente de China, por lo cual estas empresas están impedidas de comprar productos tecnológicos de firmas estadounidenses sin la aprobación de Washington.[252]

En un informe realizado por Deutsche Bank, el impacto negativo en occidente será de 3.2 billones de euros, que dejarán de ingresar a los EUA debido a la pérdida de la demanda china para las empresas estadounidense, que incluye también los costos de movilización de la cadena de suministros y mayores gastos operativos.[253]

En el mismo sentido, además de las empresas, los que han salidos afectados por esta guerra arancelaria son los consumidores, ya que las empresas probablemente aumentarán sus precios sobre los productos que venden o con "anuncios más intrusivos para monetizar mejor sus servicios gratuitos".[254]

Según datos de dos estudios académicos de 2019, uno de ellos del Banco de la Reserva Federal de Nueva York, la Universidad de Princeton y la Universidad de Columbia y el otro escrito por Pinelopi Goldberg, economista jefa del Banco Mundial, y otras instituciones, señalan que las empresas y consumidores estadounidenses pagaron casi el costo total de los aranceles impuestos por los EUA a las importaciones Chinas.[255] Ello a pesar de lo que sostienen los analistas del Deutsche Bank, que un 41% de los estadounidenses rechaza los productos chinos y el 35% de los chinos no quiere adquirir productos estadounidenses.[256]

---

[252] Guerra comercial entre EE.UU. y China: qué hay detrás del veto de Washington a empresas tecnológicas chinas clave. BBC News. Tecnología. Disponible en: https://www.bbc.com/mundo/noticias-49962766, consultado el: 05/03/2021.

[253] La guerra comercial tecnológica entre China y EE.UU. costará 3.2 billones. Crónica Business. Disponible en: https://cronicaglobal.elespanol.com/business/guerra-tecnologica-china- eeuu-32-billones_369327_102.html, consultado el: 05/03/2021.

[254] Así nos afecta la Guerra comercial entre EE.UU. y China al resto del mundo. op. cit.

[255] ¿Quién pierde en la Guerra comercial entre China y Estados Unidos? BBC News Tecnología. Disponible en: https://www.bbc.com/mundo/noticias-internacional-48265320, consultado el: 05/03/2021.

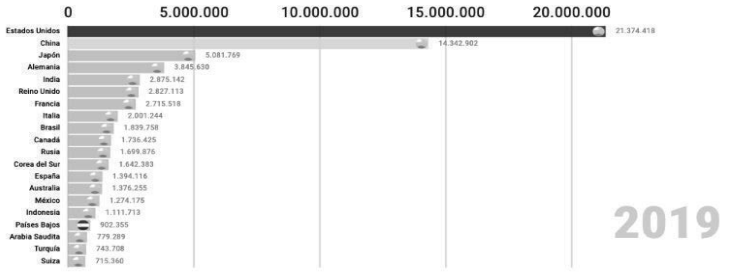
[256] La guerra comercial tecnológica entre China y EE.UU. costará 3.2 billones. op. cit.

No obstante, la guerra arancelaria ha tenido efectos colaterales que lejos de dañar a la economía China, están impulsando a las empresas chinas a acelerar su autosuficiencia. Por ejemplo, después de que Huawei fue incluida en la lista negra de los EUA, limitando su acceso al sistema Android de Google, comenzó a desarrollar su propio *software* operativo y en agosto de 2019, durante la *Huawei Developer Conference*, presentó Harmony OS 1.0, un sistema operativo para todos los dispositivos: tablet, ordenador, coche, reloj o teléfono inteligente.[257]

En este sentido, la guerra arancelaria puede devenir en una guerra fría tecnológica, ya que con el gobierno de Baiden, no se espera que termine la guerra arancelaria contra China y sus empresas tecnológicas, de hecho ha presentado un programa económico que retoma parte del nacionalismo de Trump, con el lema "compra productos americanos".

La guerra no terminará, si consideramos que China arrebató a Japón la segunda posición en la lista de economías más potentes del mundo. Como se observa en la Gráfica 18.

Gráfica 18. Los 20 países con mayor PIB (1980-2019)



Fuente: Banco Mundial.

A pesar de estar lejos aún, una economía de 14, 342, 902 millones de dólares en PIB chinos a los 21,374,418 millones de dólares de PIB estadounidenses, el crecimiento del PIB chino en los últimos años ha sido mayor que el de los EUA.

En consecuencia, las grandes empresas al monetizar los datos de sus usuarios o apoyando a otras empresas a realizar los mismos proce-

[257] Todo lo que sabemos de Harmony OS, el nuevo sistema operativo de Huawei, tras un año del bloqueo de EE.UU. Xataka. Servicios. Disponible en: https://www.xataka.com/servicios/todo-que-sabemos-harmonyos-nuevo-sistema-operativo-huawei-ano-bloqueo-eeuu, consultado el: 05/03/2021.

dimientos, acumulan cantidades exorbitantes de recursos económicos y generan imperios monopólicos gigantescos, a pesar de los estrategias contra ellas y las afectaciones por la guerra arancelaria de EUA contra China.

Otro actor importante en el contexto de la guerra comercial de EUA contra China, es Rusia. A más de 50 años de las tenciones entre Mao Zedong y el revisionismo comunista, Vladimir Putin y Xi Jinping, aseguran que los vínculos entre China y Rusia están en "sus mejores momentos",[258] firmando, en 2019, una treintena de acuerdos que prometen reforzar la cooperación entre ambos países. Lo anterior, se ha señalado como respuesta al enemigo común, EUA, que desde 2014 ha tenido al Kremlin aislado de occidente.[259]

Asimismo, es importante señalar que Rusia está apoyando a empresas emergentes en el área de las TIC, como: BioSmart, quien ha presentado el lector biométrico de la palma de la mano; Native Robotics, diseña modelos de robots hiperrealistas; F2 Innovations, tecnologías de impresión 3D a base de fibra de carbono; Head Kraken, plataforma de *software* y *hardware* que recopila información para detectar el estado psicoemocional; MedVR, es un simulador médico basado en realidad virtual, entre otras.[260]

[258] BBC News Mundo, Guerra comercial: como Rusia y China están reforzando sus lazos a "un nivel sin precedentes" como respuesta a Estados Unidos. Disponible en: https://www.bbc.com/mundo/noticias-internacional-48562474, consultado el: 05/03/2021.

[259] Idem.

[260] Desde Rusia con tecnologías: 19 empresas emergentes que merecen la atención. Disponible en: https://wwwhatsnew.com/2020/06/08/desde-rusia-con-tecnologias-19-empresas-emergentes-que-merecen-la-atencion/, consultado el: 05/03/2021.

Capítulo 6. China y el control digital

Introducción

Con el nacimiento de las TIC, surgieron dos posturas respecto a las tecnologías, la optimista y la pesimista. Los primeros consideran que las tecnologías darán paso a procesos de mayor democratización en el mundo, y los segundos, piensan que éstas cuentan con un gran potencial para ser utilizadas como mecanismos de control social.

No obstante, las prácticas nacionales nos han enseñado que estas posturas no son excluyentes entre sí, sino que en un mundo tan diverso como en el que vivimos, las TIC se han utilizado en ambos sentidos.

Las redes sociales, los buscadores, las localizadores, entre otros medios que utilizamos en la Internet, pueden ser grandes herramientas para el intercambio de información, localizar personas extraviadas o autos, generar relaciones sociales, incluir a los ciudadanos en las decisiones de gobierno, etc.

No obstante, los mismos mecanismos, pueden ser utilizados para rastrear los comentarios positivos y negativos de los ciudadanos en cuanto a su gobierno, establece sistemas de premios y castigos para las personas que se consideran de confianza o no, entre otros.

En este sentido, el Internet se ha convertido en un factor importante en los procesos gubernamentales, por ello en este capítulo nos permitimos abordar uno de los casos más paradigmáticos del control social en el mundo, el caso de China. En el primer apartado abordamos las corrientes ciber pesimistas y ciber optimistas, para continuar con el análisis del sistema de control social chino.

6.1 El Internet como mecanismo democratizador o medio de control social

Algunas tecnologías tienen la capacidad de cambiar los contextos en los que se desenvuelven, a éstas se les ha nombrado tecnologías disruptivas, capaces de provocar un cambio en los actores, sus estrategias

y sus acciones.[261] Un ejemplo de ello, fue en su momento la televisión cuya fascinación originó una revolución por su influencia y papel de los procesos sociales, por la vinculación entre las innovaciones tecnológicas y el cambio político y social que generó.[262]

En la actualidad con el surgimiento de las TIC a finales del siglo XX y particularmente con el ascenso del Internet en el mundo, se observaron 2 corrientes respecto a los impactos de la red sobre los procesos políticos nacionales, denominados: los ciber optimistas y los ciber pesimistas.

Por un lado, los ciber optimistas consideraron a las tecnologías como promotoras de la democracia a nivel global, ello derivado de sus propias características de descentralización, inmediatez global e individual de la comunicación digital, se pensó en ellas como un mecanismo democratizador, un espacio de participación e intercambio entre los ciudadanos y los gobiernos.

Este argumento se fortaleció con el abaratamiento y acceso más generalizado del Internet, robustecido por los episodios de liberalización política que se llevaron a cabo en distintos países, como la Revolución naranja en Ucrania (2004), la Revolución de los Cedros en Líbano (2005), el movimiento Un millón de voces contra las FARC en Colombia (2008), la Revolución de los Jazmines en Túnez (2010) y la Primavera Árabe en Egipto (2011), solo por mencionar algunos ejemplos.

En esta óptica, las TIC rompen el paradigma de la comunicación unidireccional mediada por el Estado como se ha desarrollado a través de los medios tradicionales, como periódicos, radio o TV, cambiando los mecanismos de comunicación, de estadios cerrados a proceso abiertos en los que los ciudadanos llevan a cabo una participación activa. En este sentido, el Internet, se volvió un mecanismo liberador, no mediado por el poder, sino omnidireccional.[263]

---

[261] Torres Soriano, Manuel R., Internet como motor del cambio Político: Ciber optimistas y ciber pesimistas, Revista del Instituto Español de Estudios Estratégicos, No. 1, 2013, España, pp-127-148.

[262] Idem.

[263] Aribau Sorolla, Óscar, Las TIC y la ciber soberanía en China: la base del presidente Xi Jinping para perfeccionar el control social maoísta, Tesis de Maestría, España, 2018, pp. 3-50.

Como promotores de esta visión podemos observar a las diferentes administraciones norteamericanas, que han asumido a Internet como un aliado natural de su política exterior y de sus procesos de democratización. Condolezza Rice afirmó: "el Internet es posiblemente una de las más grandes herramientas para la democratización y la libertad individual que nunca antes habíamos visto".[264] Dentro de las grandes empresas tecnológicas, que se han pronunciado como ciber optimistas, es el ejecutivo de Google, Wael Ghonim, quien señaló: "Si tú quieres liberar una sociedad, sólo dale Internet".[265]

Los principales argumentos de los ciber optimistas son: el Internet dota de poder a los individuos; facilita la circulación de la información; fomenta la participación de los ciudadanos en la toma de decisiones políticas, promueve la transparencia y la responsabilidad de los gobernantes; incentiva la libertad de expresión; impulsa las relaciones intergrupales, generando conexiones entre los grupos y los individuos, nacionales e internacionales; abre espacios de acciones colectivas; hace que los sucesos locales se transformen en internacionales, limitando el poder de los gobiernos para que la información traspase las fronteras; los ciudadanos pueden moverse con mayor anonimato que los periodistas; potencia el desarrollo económico y modernización social; incrementa el volumen y velocidad de la información, lo que repercute también en los procesos de innovación científica y en la productividad empresarial.[266]

Por el otro lado, los ciber pesimistas observan al Internet como un instrumento de consolidación del autoritarismo y la represión política. Aprovechándose de que el ejercicio práctico de la vida digital deja huella en la web hasta de los más mínimos detalles de nuestro día a día, incluyendo: gustos musicales, geolocalización, compras, búsquedas, redes sociales, etc. Este volumen de datos, el *big data*, permite crear sistemas de vigilancia constante construidos a costa de la privacidad de las personas.[267]

[264] Dobriansky, P., New Media vs. New Censorship: The Assault, remarks to Broadcasting Board of Governors, Washington D.C. 2008.
[265] Oreskovic, A., Egyptian Activist Creates Image Issue for Google, Reuters, 2011.
[266] Torres Soriano, Manuel R., op. cit.
[267] Aribau Sorolla, Óscar, op. cit.

Esta corriente pone en duda los postulados optimistas, considerando que el Internet, cuenta con una serie de características que provocan la involución política, debilitan la capacidad de movilización de las sociedades y potencian los aparatos represivos y de control de los regímenes autoritarios.[268]

Esta visión sostiene los siguientes argumentos para reafirmarse: Internet genera burbujas democráticas o espejismos de que se desarrollan procesos democráticos; la debilidad de los grupos formados a través de Internet, es decir, los vínculos de estos grupos son débiles, así como aparecen desaparecen por lo que sus acciones pueden ser escasamente efectivas; sólo una minoría de ciudadanos utiliza el Internet como medio político; el ciberactivismo lejos de obtener los resultados deseados, pone a las personas en situación de mayor vulnerabilidad, ya que los regímenes autoritarios reaccionan con mayor dureza contra las personas que identifican como potenciales amenazas; y la posición de que los dictadores pueden generar sistemas que les permitan controlar Internet.

Más allá de estas posturas teóricas, desde el ámbito jurídico, la vigilancia masiva es ilegal, de conformidad con instrumentos jurídicos internacionales en materia de Derechos Humanos, por ejemplo la Declaración Universal de los Derechos Humanos, Art. 12 establece que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni en su honra o reputación.[269] Estos derechos también se encuentran consagrados en las legislaciones nacionales que los garantizan y sólo un juez puede autorizar la intervención de las comunicaciones de los ciudadanos.[270]

No obstante, estos marcos normativos se han visto modificados y limitados a través de las legislaciones nacionales. Ejemplo de ello son los sistemas occidentales denominados democráticos que, a través de discursos sobre la seguridad y la luchas contra el terrorismo, han justificado su intervención en la vida privada de los ciudadanos.[271]

---

[268] Torres Soriano, Manuel R., op. cit.

[269] Declaración Universal de los Derechos Humanos de 1948.

[270] Amnistía Internacional, Vigilancia Masiva. Disponible en: https://www.es.amnesty.org/en-que-estamos/temas/vigilancia-masiva/, consultado el: 05/03/2021.

[271] El Diario.es, La vigilancia en Internet avanza con la complicidad de los gobiernos. Disponible en: https://www.es.amnesty.org/en-que-estamos/temas/vigilancia-masiva/, consultado el: 05/03/2021.

En este escenario, cada vez más países que se habían mostrado ciber optimistas, ahora están modificando sus leyes para permitir el monitoreo de Internet y acceso a los datos sin autorización judicial para llevar a cabo vigilancia indiscriminada sobre sus ciudadanos.[272] Por ejemplo, Francia permite interceptar masivamente comunicaciones y retener información sin previa autorización judicial; el Reino Unido ha incluido en su normatividad mayores poderes de espionaje; Polonia ha dado facultades a la policía y a otras agencias para poder ejecutar mecanismos de vigilancia.[273] En México, en 2021, el senador Ricardo Monreal anunció que presentará una iniciativa para regular Internet las redes sociales, a fin de quitar a las empresas privadas el control sobre las mismas y que sea el Estado quien las regule.[274]

Mención aparte merece un ejemplo paradigmático de las posturas ciber pesimistas y de cómo pueden llevarse a cabo acciones deliberadas para regular Internet, a fin de convertirlo en un mecanismos de control y vigilancia a sus ciudadanos, tal es el caso de China. Sobre el cual se realizarán algunas disertaciones en el siguiente apartado.

6.2 China y su concepción de ciberseguridad. La utilización de las TIC a favor del Estado

A partir de la llegada del Partido Comunista Chino (PCCh) en 1949, la intimidad y lo privado se consideraron el enemigo del sistema. En este sentido, durante los últimos 70 años, los líderes de dicho partido, han basado su legitimidad y hegemonía en la eliminación de la crítica y transformación al ámbito público todo lo que pudiera ser de la esfera privada de los ciudadanos.[275]

Con las reformas realizadas en materia económica, para implementar el modelo liberal en China, parecía que ello traería como consecuencia también la apertura política, hacia un régimen democrático, pero no fue así. La situación de China, sería resumida en una sola

[272] Idem.
[273] Amnistía Internacional, op. cit.
[274] Aristegui Noticias, Anuncia Monreal iniciativa para regular las redes sociales en México. Disponible en: https://aristeguinoticias.com/0102/mexico/anuncia-monreal-iniciativa-para-regular- las-redes-sociales-en-mexico/, consultado el: 05/03/2021.
[275] Aribau Sorolla, Óscar, op. cit.

frase de Deng Xiaoping: "Un país, dos sistemas". Bajo dicho sistema socialista se desarrolló un sistema económico de mercado pero manteniendo el control social autoritario sobre la información y las comunicaciones.[276]

En este proceso de adaptación de los dos sistemas en China, las TIC y con ellas la desaparición de las fronteras y la circulación de información proveniente de todo el mundo, supuso un gran reto. No obstante, con la llegada de Xi Jinping, en 2012, éstas se observaron como una gran oportunidad para utilizarlas en beneficio de las propias estructuras estatales y como mecanismo de control ciudadano.[277]

Así pues, durante los primeros 6 años de gobierno de Xi, éste adoptó medidas encaminadas a fortalecer la jerarquía y obediencia al líder y a eliminar a sus adversarios, ideologizando a la población y a su partido. Las tecnologías formaron parte esencial para alcanzar éstos objetivos.

Su concepto de ciber soberanía le sirvió para diseñar un modelo de gobernanza de redes, transformando las amenazas de las TIC en oportunidades. Para él no es posible tener una red global autorregulada, donde los gobiernos son meros espectadores de la evolución del ciberespacio, sino que apuesta a la utilización del mismo al servicio de los intereses gubernamentales controlado y monitoreado por el Estado para evitar focos rojos que puedan llegar a afectar al Estado.

Es decir, Xi aplica al mundo digital las regulaciones sociales de la vida real, en este sentido ha seguido las directrices de la época maoísta y ha utilizado a los medios de comunicación como voceros del gobierno y el partido para dominar a las masas.[278]

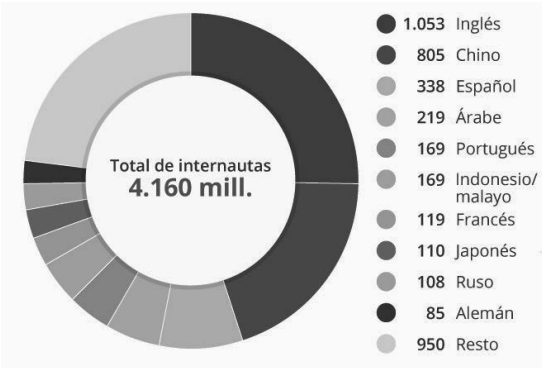
Desde 2012, Xi ha puesto énfasis en el microcontrol de los comentarios que junto con la ley de ciberseguridad de 2017, han profundizado la vigilancia del comportamiento de los ciudadanos. Limitando también el uso de la Virtual Private Networks (VPN), red privada por la cual muchas personas se conectaban a la red internacional.[279]

China cuenta con una penetración de Internet de 64.5 % en 2020 y con un crecimientos de 4.9% porcentual en comparación con 2018, además cuenta con 897 millones de personas con acceso a la red a

[276] Idem.
[277] Idem.
[278] Idem.
[279] Hannig Sascha, Distopía Digital: Cuatro herramientas que China usa para controlar a su población, Fundación para el Progreso, Chile, pp. 1-16.

través de sus telefonías móviles, muy por encima de los datos de 2018, que eran aproximadamente de 79.92 millones, lo que representó un incremento del 99.3% para el 2020.[280] Ello explica que el Chino sea el segundo idioma más utilizado en la red. Véase Gráfica 19.

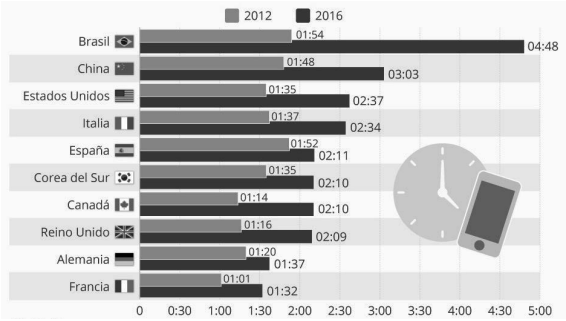
Gráfica 19. Las lenguas de Internet (2017)



Fuente: https://es.statista.com/grafico/13576/china-un-mercado-con-mas-de-800-millones-de-usuarios-de-Internet/

A ello, se le suma que en el periodo de 2012 a 2016, China fue el segundo lugar de uso diario de *smartphones* en el mundo. Véase la Gráfica 20.

Gráfica 20. El uso diario de smartphones en el mundo (2012-2016)

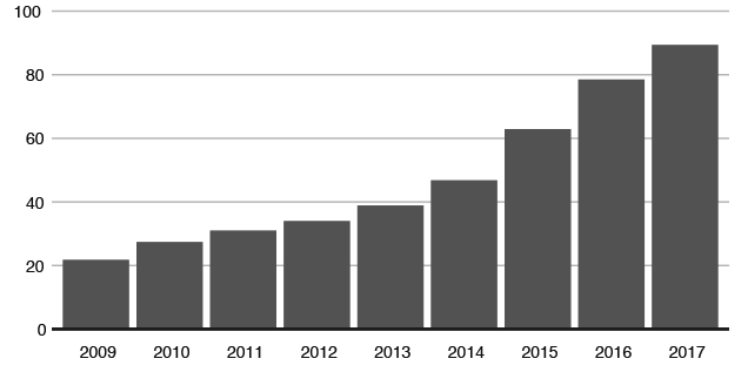


Fuente: https://es.statista.com/grafico/9576/la-adiccion-al-movil-crece-en-todo-el-mundo/

[280] Xinhua Español, Población de internautas de China crece hasta 904 millones, según informe. Disponible en: http://spanish.xinhuanet.com/2020-04/28/c_139014693.htm#:~:text=La%20penetraci%C3%B3n%20de%20Internet%20en,Red%20de%20Internet%20de%20China, consultado el: 05/03/2021.

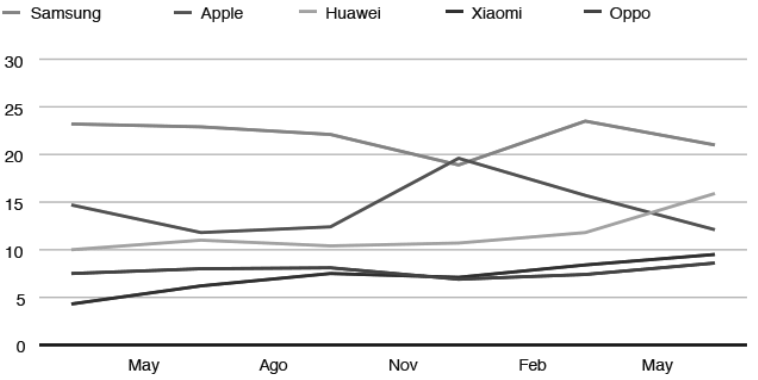
Adicionalmente, la empresa china Huawei ha crecido muy rápidamente en los últimos 10 años, tanto que ha desplazado en preferencias mundiales a la empresa norteamericana Apple, a la cual superó en 2018. Como se observa en las Gráficas 21, 22 y 23.

Gráfica 21. Huawei creció rápidamente la última década (2009-2017)



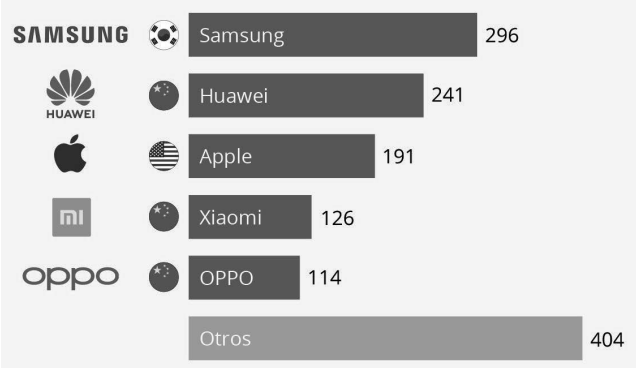
Fuente: https://www.bbc.com/mundo/noticias-46507846

Gráfica 22. Huawei ya vende más que Apple (2018)



Fuente: https://www.bbc.com/mundo/noticias-46507846

Gráfica 23. Las marcas de smartphones preferidas (2019)



Fuente: https://es.statista.com/grafico/20783/envios-de-smartphones-en-el-mundo-en-2019/

Empresa sobre la cual se ha ceñido el escándalo, derivado de sus conexiones con el gobierno chino y la posible instalación de *backdoors* (puertas traseras), que consisten en secuencias especiales dentro del código de programación capaces de burlar la seguridad del algoritmo por el cual se puede acceder al sistema, capaces de servir para espiar a través de la red, acceder a llamadas telefónicas y comunicaciones en Internet de los usuarios.[281]

Ello derivado de la detención en Polonia, de un directivo de la empresa Huawei, de nacionalidad china, acusado de espionaje contra los intereses polacos, junto con un funcionario polaco de servicios de seguridad estatales, que había trabajado en una empresa de telefonía.[282]

No obstante, la mayor preocupación se enfoca en Ren Zhengfei, el multimillonario fundador de la compañía y gran defensor del Partido Comunista Chino, quien era parte también del ejército. Con esta coalición, el gobierno utilizaría a dicha empresa para obtener una gran

[281] BBC News, Mundo, Escándalo por espionaje sobre Huawei: qué son las puertas traseras de Internet y qué tienen que ver con el gigante de la telefonía chino. Disponible en: https://www.bbc.com/mundo/noticias-47554996, consultado el: 05/03/2021.

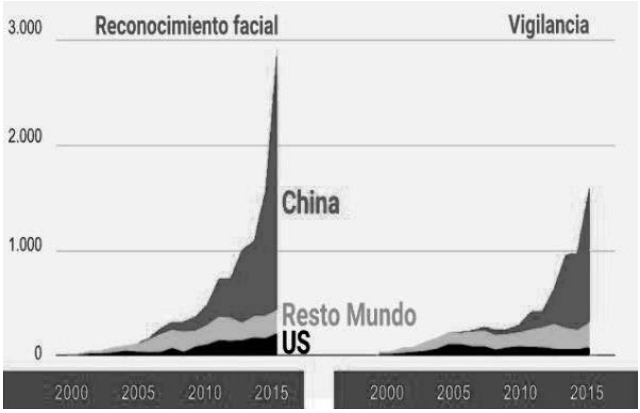
[282] BBC News, Mundo, Huawei: el nuevo escándalo por espionaje que sacude al gigante tecnológico chino tras la detención de unp de sus directivos en Polonia. Disponible en: https://www.bbc.com/mundo/noticias-internacional-46853250, consultado el: 05/03/2021.

cantidad de datos de sus ciudadanos, utilizando el *big data* como un recurso esencial de control social.[283]

Adicionalmente, el gobierno utiliza los datos que obtiene de su población, desde cámaras de vigilancia en las calles con lo último en inteligencias artificiales, la obligación de llevar un chip RFID en todos los coches, hasta policías con gafas de reconocimiento facial. Por ejemplo, si cruzas la calle de forma inadecuada, recibes un MSM a tu celular con la infracción, el lugar, fecha y hora de la misma.[284]

Desde 2017, casi la mitad (48%) de sus fondos para desarrollo de tecnología se destinó a la investigación en reconocimiento facial. La compañía Megvii, con la que colabora el gobierno, recibió una nueva inversión de 750 millones de dólares, por lo que para el año 2019 valía aproximadamente 4.000 millones. Se acerca rápidamente a las empresa Sense Time, la compañía china líder en inteligencia artificial.[285] En este sentido, China se pone a la cabeza de la tecnología de vigilancia. Véase Gráfica 24.

Gráfica 24. China lidera la tecnología en vigilancia (2015)



Fuente:https://www.niusdiario.es/economia/empresas/reconocimiento-facial-limites-retos-datos-biometricos-cara_18_2817945044.html

[283] Aribau Sorolla, Óscar, op. cit.

[284] Esquire, El crédito social chino: cuando el gobierno te pone nota. Disponible en: https://www.esquire.com/es/actualidad/a30361853/credito-social-chino-que-es/, consultado el: 05/03/2021.

[285] Nius, Todo por la cara: límites y retos del reconocimeinto facial, 2019. Disponible en: https://www.niusdiario.es/economia/empresas/reconocimiento-facial-limites-retos-datos-biometricos-cara_18_2817945044.html, consultado el: 05/03/2021.

Con este impulso económico y con aproximadamente 626 millones de cámaras en 2020 (lo cual significa una relación de 1 cámara por cada 7 habitantes), todas ellas con tecnología de reconocimiento facial, éstas son utilizadas para realizar un sinfín de tareas, como: medir la atención de los estudiantes en clases, controlar dispensadores de papel higiénico en los baños públicos, dar el visto bueno de un pago, vigilar aeropuertos, identificar individuos peligrosos, entre otras.[286] Por ejemplo, para 2018 existían 62 aeropuertos que habían puesto en marcha el reconocimiento facial para acelerar los controles de seguridad.[287]

En 2019, el Instituto de Secundaria Número 11 de la ciudad china de Hangzhou instaló cámaras de reconocimiento facial en los pupitres de sus estudiantes, en donde cada 30 segundos se escanea el rostro de los alumnos y se les clasifica de acuerdo con 7 emociones: feliz, triste, decepcionado, molesto, asustado, sorprendido o neutro, para medir su nivel de concentración en clases.[288]

En 2020 y en un contexto de post pandemia en China, el aeropuerto de Beijing, en la capital del país y el segundo más transitado del mundo en 2019, inició su proyecto de vuelos sin contacto, que brinda a los viajeros la oportunidad de realizar el *check-in*, la entrega del equipaje, los controles de migración, etc. a través de sistemas automatizados con base en el reconocimiento facial, lo cual hace que se evite cualquier contacto con el personal del aeropuerto, mayor eficiencia, menor tiempo y más distanciamiento social para los pasajeros.[289]

En el mismo año 2020, se implementó el Sistema de Crédito Social, puesto a prueba desde 2014, que funcionaba como una base de datos unificada de los registros financieros, industriales y comerciales, pagos de impuestos, seguridad social e infracciones de tránsito. No obstante, se le han sumado datos como: las búsquedas de Internet,

[286] Idem.

[287] Aribau Sorolla, Óscar, op. cit.

[288] La vanguardia, La inquietante apuesta china por el reconocimiento facial, 2019. Disponible en: https://www.lavanguardia.com/tecnologia/20190518/462270404745/reconocimiento-facial-china-derechos-humanos.html, consultado el: 05/03/2021.

[289] Osteltur, El aeropuerto de Beijing estrena una nueva normalidad: vuelos sin contacto, 2020. Disponible en: https://www.hosteltur.com/138912_el-aeropuerto-de-beijing-estrena-una-nueva-normalidad-vuelos-sin-contacto.html, consultado el: 05/03/2021.

medios sociales, cámaras de vigilancia, geolocalización, transacciones comerciales, entre otros.[290]

Todo ello se traduce en una calificación que marca el grado de confianza social de cada persona en China. Este sistema vincula la vida digital con la real, en la cual un número sintetiza las acciones que podrás o no realizar, es decir se base en incentivos y desprestigio.[291] Con este sistema se conecta la infraestructura de supervigilancia cibernética con un sistema de puntuación similar al que se usa para la evaluación financiera.

Este sistema tiene como finalidad, de acuerdo con el Documento Oficial del Consejo de Estado de 2014, establecer las leyes fundamentales, regulaciones y estándares de crédito social, en un sistema de investigación que incorpore a toda la sociedad y su información con mecanismos que promuevan la confianza y castiguen la mala fe o la desconfianza.[292] Así como tener elementos preventivos y disuasivos, eliminando las posibilidades de que las personas realicen acciones contrarias a la armonía del país.[293]

Se basa en la reputación del ciudadano, por la cual el Estado le brinda un puntaje, de entre 350 a 950, según su grado de confiabilidad, si no pagas una multa o cometes un delito menor como tener música muy alta en tu casa o fumar en un lugar prohibido, pierdes puntos, a ello se le suma que también puedes disminuir tu puntaje por tus creencias religiosas o por tus opiniones políticas o las de tus amigos cuando no estén en línea con las posiciones gubernamentales.[294] Adicionalmente, este puntaje es público y compartido a todos tus contactos, por lo que tener amigos con bajo puntaje baja el puntaje de las personas.

Los castigos por tener bajo puntaje pueden tener como consecuencias multas, la imposibilidad de viajar al extranjero o la prisión. En 2018, 23 millones de viajes fueron cancelados por el gobierno por no contar con crédito social suficiente.[295]

[290] Aribau Sorolla, Óscar, op. cit.
[291] Idem.
[292] Hannig Sascha, op. cit.
[293] Idem.
[294] Esquire, op cit.
[295] Hannig Sascha, op. cit.

La vigilancia y el método de premios y castigos, no sólo se fundamenta en el cumplimiento de la ley, sino de una evaluación moral, basada en las ideas que tengan los ciudadanos a favor o en contra del partido. Un caso emblemático es la aplicación WeChat, con más de 1000 millones de usuarios; Alibaba, la tercera tecnológica más grande del mundo; ZTE, el gigante de las telecomunicaciones; Tencent duela de Blizzard, entre otras empresas que brinda información al gobierno.[296]

Estas políticas son impuestas a todas las empresas a través de la normatividad nacional, aún a las que están en contra de ello, lo cual han generado debates y acciones en cuanto a la responsabilidad ética de entrar al enorme mercado chino. Por ejemplo, Apple traspasó las operaciones de iCloud China a ese país para cumplir con su reglamentación e incluso se ha sumado a la censura, Siri el agente virtual de Apple, guarda silencio cuando un ciudadano chino pregunta sobre los acontecimientos en la Plaza de Tiananmén en 1989.[297]

En cambio, Google abandonó ese país en 2010 debido a la censura, pero tiene planes de reingresar, pese a que tendría que cumplir con la regulación que violenta la privacidad de sus usuarios.[298] Yahoo también es una de las empresas que ha tenido que implementar la autocensura o incorporar en mayor o menor medida los requerimientos de China.[299]

Asimismo, China está tomando muestras de material genético, como registros de ADN de su población, que acompañan el sistema de vigilancia, enfocados a evitar cualquier insurrección.[300] En este sentido, al espionaje general, se le suma el focalizado, por ejemplo, la vigilancia realizada a grupos que se consideran conflictivos.

A la región de Xinjiang, la mayoría de la población correspondiente a la etnia musulmana, se le ha estado vigilando y se obtuvo información en tiempo real de 2.5 millones de ciudadanos, en los que se incluían datos personales, laborales y hasta de los lugares que frecuentaban.[301] El país considera que para mantener la estabilidad debe

[296] Idem.
[297] Delgado Antonio, Nuevas (y viejas) formas de censura de la información en Internet, Cuadernos de Periodistas, número 29, España, 2014, pp. 110-118.
[298] Hannig Sascha, op. cit.
[299] Delgado Antonio, op. cit.
[300] Hannig Sascha, op. cit.
[301] Nius, op. cit.

recurrir a un fuerte control de la población utilizando las tecnologías que tenga disponibles.

En este sentido, si tiene un alto nivel de confianza significa que el Estado confía en ti, ello implica que podrás viajar al extranjero, ser funcionario o llevar a tus hijos a la escuela que desees, al contrario si tu nivel de confianza es bajo, podrán negarte la venta de vuelos al extranjero, la tramitación de un pasaporte o la utilización de plataformas de Internet dedicadas al comercio. Puedes incrementar tu crédito de confianza, si realizas trabajos de voluntariado cómo cuidar ancianos, limpiar espacios comunes o realizar donaciones al gobierno.[302] Además de premiar, a través del propio sistema, a las personas cuando están a favor del gobierno. También, cuenta con unidades dedicadas a diseminar en Internet contenidos favorables a la administración, esta técnica se llama *astroturfing*.[303]

Adicionalmente, en China el Internet no solo funge como un poderoso aparato propagandístico y de control de masas, sobre todo como un proyecto de censura efectivo y adaptativo, donde se actualizan innumerables algoritmos de *software* para bloquear sitios web indeseables, ya sean nacionales o extranjeros.[304]

En China se tiene un sistema de censura de Internet y se están empleando mecanismos para rastrear la ruta de numerosos sitios web en el extranjero. El gobierno escanea el ciberespacio en busca de palabras o expresiones que se consideran sediciosas o incendiarias, siendo el ciberespacio estrictamente vigilado y controlado a través de 6 operadores de Internet propiedad estatal, entre los que se encuentran las empresas de telecomunicación: China Telecom, China Unicom y China Mobile; los demás operadores son más pequeños y cuentan con sus propias redes.[305]

Aunque todos los países del mundo realizan en cierta medida la censura, su contenido puede variar. En occidente, se preocupan principalmente por cuestiones sobre difamación, obscenidad, racismo, instigación a la violencia, el extremismo y delitos cibernéticos.

---

[302] Esquire, op. cit.
[303] Delgado Antonio, op. cit.
[304] Guangchao Charles Feng y Zhongshi Guo Steve, Tracing the route of China´s Internet censorship: An empirical study, Science Direct, Vol. 30, número 4, Noviembre 2013, pp. 335-345.
[305] Idem.

En cambio, en Oriente existe una lista de noticias y comentarios que deben ser prohibidos por los censores, entre los que se encuentran todo lo que manche la imagen del Partido Popular de China, que ataque el sistema o aluda a los sistemas democráticos occidentales, por ejemplo, la mención de los sindicatos.[306] Asimismo, en algunos casos son los propios ciudadanos los que realizan la censura social, a través del *shaming* (avergonzamiento público) contra las personas que hablen en contra del gobierno.[307]

En China la conexión de Internet se canaliza a través de pasarelas controladas por el gobierno, en donde los sitios bloqueados cambian constantemente, por lo cual es difícil distinguir entre el bloqueo intencional y una falla en la red.

Autores como Guangchao Charles Feng y Steve Zhongshi Guo, señalan, con respecto a los bloqueos específicos, que existen 5 métodos de censura que podrían estarse realizando en China: Control ACL, Bloqueo de URL y DNS, secuestro de BGP y Bloqueo de palabras clave.

A estos mecanismos se les pueden sumar: corrupción de la respuesta DNS, ataque de predicción del número de secuencia, respuesta de sincronización falsificada y colusión del motor de búsqueda. Se pueden bloquear los enrutadores a algunos destinos al hacer coincidir las direcciones IP de los destinos con los paquetes de listas de acceso, aunque lo sitios web pueden cambiar sus direcciones IP para eludir el control.[308]

Ejemplo de lo anterior es el caso de uno de los aliados del gobierno Chino, la empresa *Byte Dance*, creadores de Tik Tok, aplicación disponible en 150 países y 75 idiomas, que permite al usuario subir videos a la red. Esta ha bloqueado videos que denuncian la vulneración de derechos humanos en China, particularmente lo referente a la situación étnica uigur en la provincia de Xinjiang, donde más de un millón de personas fueron víctimas de encarcelamiento masivo. Uno de los casos más conocidos fue el de la adolescente estadounidense

[306] Hannig Sascha, op. cit.
[307] Idem.
[308] Guangchao Charles Feng y Zhongshi Guo Steve, op. cit.

Feroza Aziz, quien tuvo bloqueada su cuenta de Tik Tok en noviembre de 2017, después de subir un video sobre el tema.[309]

En cuanto a servidores de nombres de dominio, hay tres clases: raíz, dominio de nivel superior y autorizados, los nombres de dominio inician con el sufijo "cn" y son sitios web que usualmente tiene sede física en China. Estos dominios deben primero ser aprobados por la Agencia Estatal responsable de todo el registro de nombres. En este sentido, si existen sitios con materiales subversivos y los dueños se niegan a eliminarlos, el gobierno podría obligarlos a cumplir so pena de descontinuar su dominio.[310]

Adicionalmente, el gobierno y sus aliados, empresas nacionales de tecnología, manipulan las búsquedas de páginas web para poner en los primeros lugares las informaciones aprobadas por el oficialismo antes que las páginas no oficiales o extranjeras[311] o a través de la censura de éstas. En 2013, las webs de medios como New York Times, Bloomberg, El País y el Consorcio Internacional de periodistas fueron bloqueadas por publicar una investigación sobre la acumulación de riqueza de las principales familias chinas y el uso de paraísos fiscales.[312]

En agosto de 2013, se publicó un artículo titulado *The velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions*, sobre la censura China y el servicio de Internet Weibo, una red de mensajería similar a Twitter. En un estudio del comportamiento de esta red en 2012, señala que el 30% de los mensajes se borraban entre 5 y 30 minutos después de su publicación y que en las primeras 24 horas se borra el 90% de los mensajes censurados. Éstos pueden ser suprimidos de forma temporal o permanente, o pueden dejar el post de un usuario visible solo para él.[313]

Además de las tecnologías utilizadas por la empresas se suman los censores humanos, que se encargan de realizar las tareas que las máquinas aún no pueden detectar como la ironía o mensajes cifrados en blogs, redes sociales, foros o cualquier forma de desarrollar infor-

[309] El País, El lado oscuro de Tik Tok, el rey chino de los videos relámpago, 2020. Disponible en: https://elpais.com/economia/2020/01/16/actualidad/1579191053_051932.html, consultado el: 05/03/2021.
[310] Guangchao Charles Feng y Zhongshi Guo Steve, op. cit.
[311] Delgado Antonio, op. cit.
[312] Idem.
[313] Idem.

mación en Internet. Estos recursos humanos también tienen acceso a correos electrónicos, mensajes instantáneos y llamadas telefónicas.[314]

Como se observa, China ha puesto todos los recursos a su disposición, monetarios, tecnológicos y humanos, para llevar a cabo procesos de control y vigilancia hacia sus ciudadanos a favor del gobierno, a través de los medios digitales en dos sentidos importantes: por un lado, para realizar propaganda a favor del Estado; y por el otro, para censurar todas las opiniones en su contra.

[314] Idem.

Capítulo 7. Europa ante los retos del uso de las criptomonedas y el euro digital

Introducción

La era digital ha trastocado todos los ámbitos de la vida humana incluyendo el ámbito financiero y monetario, dando respuesta a fenómenos que hoy en día no podían ser resueltos a través de los medios tradicionales de gestión de pagos, ni con los marcos jurídicos actuales, problemáticas como el utilizar valores infinitamente pequeños o muy elevados, el realizar transferencias internacionales en tiempo real o usar dinero que se adapte a la operatividad de las computadoras que trabajan con otras computadoras en línea,[315] son solo algunos ejemplos en los que el dinero físico se ha visto superado por las tecnologías.

En este sentido, la creación y emisión de criptomonedas fueron la respuesta de la sociedad, dada la deficiencia de las monedas físicas para integrarse a las tecnologías, así como de las fallas del mercado financiero global. Como afirma Polanyi, el dinero es un convencionalismo social, por tanto podemos cambiar su naturaleza y la forma en que lo concebimos.[316]

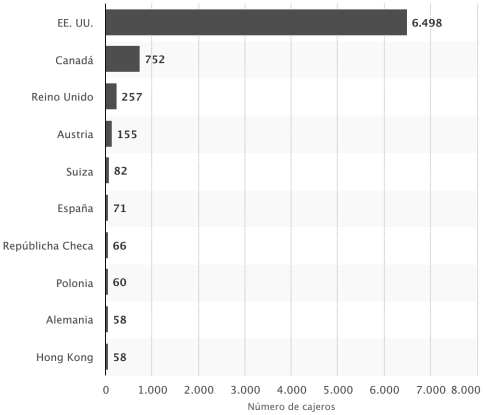
Así, en la búsqueda de oportunidades de desarrollo con base en las TIC, y más aún si se pueden obtener ganancias y beneficios económicos, se generaron las primeras monedas virtuales en 2009, siendo la pionera la llamada Bitcoin, aunque actualmente existen otras como: Litecoin, Deshcoin, Peercoin y Dogecoin.[317] No obstante, Bitcoin sigue siendo una de las criptomonedas más fuertes a nivel mundial. Véase Gráfica 25.

[315] Así será el euro digital: Europa pone en fase de pruebas su alternativa a las criptomonedas y a las divisas electrónicas de China y Rusia. Reuters. Disponible en: https://www.businessinsider.es/euro-digital-fase-pruebas-te-afectara-como-consumidor-709401, consultado el: 05/03/2021.

[316] Wesley c. Marshall, Deflación y criptomonedas, Análisis, UAM Iztapalapa, Vol. ii, No. 30, mayo-agosto, 2018, pp. 29-30.

[317] Las criptomonedas en Europa, Europa Press. Disponible en: https://www.europapress.es/asturias/noticia-criptomonedas-europa-20190325145016.html, consultado el: 05/03/2021.

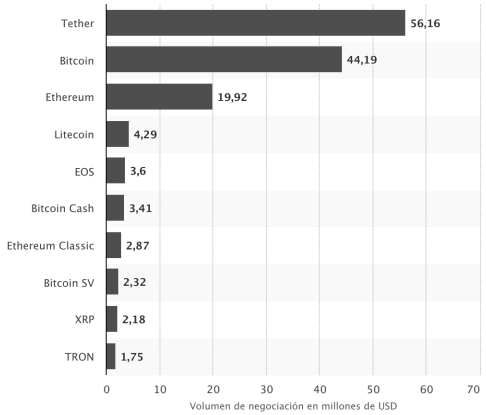
Gráfica 25. Ranking de los países con más cajeros Bitcoin instalados (2020)



Fuente:https://es.statista.com/estadisticas/658296/paises-con-mas-cajeros-bitcoin-instalados-a-nivel-mundial/

Con las TIC, las criptomonedas se han multiplicado en los últimos años, en marzo de 2019, existían más de 1,500 monedas y para el año 2020, la principal criptomoneda, Tether, manejaba ya alrededor de 56 millones de dólares. Véase: Gráfica 26.

Gráfica 26. Ranking de las principales criptomonedas en el mundo (2020) según el volumen de negociación (millones de dólares)



Fuente: https://es.statista.com/estadisticas/657259/principales-criptomonedas-por-volumen-de-negociacion-a-nivel-mundial/

7.1 Las criptomonedas y la propuesta europea

Las criptomonedas se han definido como "un tipo de dinero no regulado, digital, que se emite y por lo general se controla por sus desarrolladores y que es utilizado y aceptado entre los miembros de una comunidad virtual aceptada".[318] Éstas se caracterizan por:

- No tener un emisor concreto y no estar bajo la regulación de un banco central, con un ámbito de aplicación global, no tiene una zona geográfica determinada, sino que vive en el Internet.[319]
- No se sabe si es un medio de pago o de intercambio.
- No posee el mismo estatuto jurídico de la moneda o dinero, pero es aceptada por algunas personas como un medio de cambio en medios electrónicos.
- Son cuasi anónimas, ya que los usuarios son solo conocidos por sus direcciones públicas, sin saber su identidad real. No existe algún Estado donde sean de curso legal, o sean la moneda oficial.[320]
- Los intercambios se hacen de persona a persona, sin intermediarios, a través de la web.
- Carecen de supervisión y son emitidos por entes privados.
- Su valor depende de que existan otros usuarios que tengan la intención de adquirirlas.
- Solo pueden ser utilizadas en las tiendas *online* y en algunos establecimientos físicos.
- Las criptomonedas son diferentes al dinero emitido por los bancos centrales porque sus precios son volátiles al carecer de un valor intrínseco, sin una institución que los respalde.[321] Se emiten al margen de gobiernos e instituciones.

[318] Idem.
[319] Idem.
[320] Idem.
[321] Así se plantea el euro digital, la moneda virtual complementaria del efectivo por la que apuesta el Banco Central Europeo, Genbeta. Disponible en: https://www.genbeta.com/a-fondo/asi-se-plantea-euro-digital-moneda-virtual-complementaria-efectivo-que-apuesta-banco-central-europeo, consultado el: 05/03/2021.

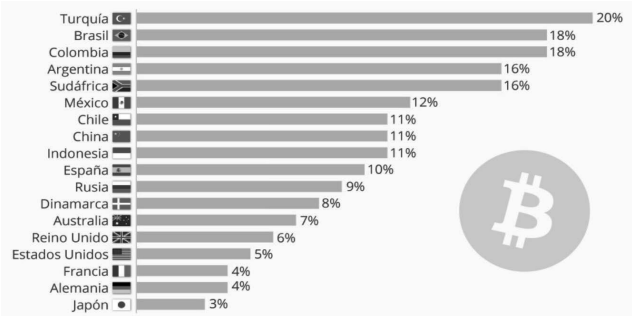
En este sentido, distan mucho de lo que de manera ordinaria llamamos moneda. Las criptomonedas, de hecho contradicen las narrativas previas sobre qué es el dinero y de dónde viene, por ello se ha buscado cambiar su denominación a activos virtuales o cripto activos.[322]

Asimismo, no se saben tampoco cuáles serán sus implicaciones a futuro, pero sí que suponen una revolución a la estructura actual del sistema financiero y de la política monetaria tradicional[323] vinculadas al desarrollo de las TIC.

Las criptomonedas son altamente riesgosas y volátiles, no pueden garantizar los derechos de los consumidores, ni están reguladas.[324] Asimismo, han sido criticadas por los bancos centrales, como activos especulativos.

No obstante, a pesar de ser riesgosas, los usuarios consideran que es positivo tenerlas y usarlas. Ésto lo demuestra una encuesta realizada por *Statista Global Consumer Survey* (2019), que dedica una pregunta al mercado global de criptomonedas, sobre la tasa de adopción de criptomonedas. Destaca Turquía, país en el que el 20% de los encuestados dijo usar o poseer alguna moneda digital, en México tan sólo el 12%, China el 11% y EUA el 5%. Véase la Gráfica 27.

Gráfica 27. ¿Qué tan comunes son las criptomonedas en el mundo? Porcentaje de encuestados que afirman usar o poseer criptomonedas (2019)



Fuente: https://es.statista.com/grafico/18425/adopcion-de-las-criptomonedas-en-el-mundo/

[322] Las criptomonedas en Europa, op. cit.
[323] Así será el euro digital: Europa pone en fase de pruebas su alternativa a las criptomonedas y a las divisas electronicas de China y Rusia, op. cit.
[324] Las criptomonedas en Europa, op. cit.

Adicionalmente, también debemos reconocer que han sido un experimento de cómo se están desarrollando las tecnologías de pago a nivel mundial, por lo que diversos académicos han dado su respaldo a éstas, las grandes empresas tecnológicas han iniciado esfuerzos importantes para su creación y instrumentación, así como varios países y organismos internacionales y regionales, entre ellos la Unión Europea (UE), se están preparando estructural y legalmente para adoptarlas, ello con características particulares y diversas en cada caso.

Por ejemplo, en 2015, JP Morgan crea Digital Asset Holdings, empresa dedicada a la tecnología *Blockchain*. A finales de 2016, William Muogayar informó que había 25 consorcios o alianzas de *Blockchain*. Adicionalmente, JPMorgan se unió a Santander y otras 30 empresas, incluido Microsoft, para crear la red Ethereum,[325] similar a Blockchain, y cuya criptomoneda Ether (ETH) es la segunda más grande del mercado. Ethereum existe como un sistema financiero autónomo de pares, libre de intervenciones gubernamentales.[326]

El *Blockchain*, o cadena de bloques, es una tecnología DLT (*Distributed Ledger Technology*) que nos brinda la posibilidad de acceder a un repositorio compartido por los miembros de una red, que a través de mecanismos de acceso seguros pueden ver la información que ahí se produce de forma directa, en el que se intercambian activos de manera segura, que una vez hecha la transacción o movimiento, no puede ser alterada ni por medios automáticos ni humanos, lo cual aporta un alto nivel de transparencia y confiabilidad.[327]

Adicionalmente en 2019, 28 empresas de renombre, como Visa o Vodafone, lideradas por Facebook, publicaron un Libro Blanco, proponiendo la creación de una nueva criptomoneda llamada Libra, cuyo objetivo es constituirse en una moneda estable con base en *Blockchain*, respaldada por una reserva de activos y gobernada por una asociación independiente. Este proyecto pretende ser el más ambicioso desde que se lanzó el bitcoin, asimismo, se determinó que ésta no sería tan volátil

[325] Wesley C. Marshall, op. cit., p. 52.

[326] ¿Qué es Ethereum y cómo funciona?, IG.com. Disponible en: https://www.ig.com/es/ethereum-trading/que-es-ether-y-como-funciona, consultado el: 05/03/2021.

[327] Loiacono, Stella, Blockchain, sus aplicaciones más allá de las criptomonedas, Revista abierta de Informática Aplicada, Vol. 2., n 1., 2018, pp. 47-48.

como otras criptomonedas, ya que su valor estará determinado por el valor de los activos.

Estos activos son monedas fiduciarias creadas por bancos centrales y comerciales, con ello se busca que el valor de la criptomoneda coincida siempre con el valor de los activos subyacentes. Ésta es una estrategia de Facebook también para evitar que estas empresas asociadas a Libra, colaboren con sus competidores potenciales de criptomonedas, como son Apple, Amazon o Google.[328] Libra se caracteriza por estar respaldada por activos, entre los cuales están los depósitos de dinero convencionales, el oro, bonos estatales a corto plazo.[329]

El riesgo que se corre con Libra es, por un lado, que las transferencias de dinero son libres y permiten a los usuarios realizar transferencias con seudónimos, que no necesariamente están vinculados a sus identidad en el mundo real, y por el otro, es importante generar nuevas reglas y marcos jurídicos sobre el secreto bancario en el Blockchain.[330]

Asimismo, se espera que el proyecto crezca y se conviertan en 100 empresas y como hay pocas empresas europeas capaces de integrarse a la asociación, lo más probable es que haya un predominio de empresas estadounidenses, en este sentido, Libra pudiera convertirse en la moneda mundial bajo los auspicios de los EUA, incrementando su poder financiero[331] y que los millones de personas que cuentan con Facebook, utilicen a Libra como su mecanismo de pago cotidiano.

Otro importante esfuerzo, es el realizado por China, que ha invertido en los últimos 10 años, de 2010 al 2020, en un sistema de moneda digital, que se ha convertido en una amenaza al sistema europeo, basado en el modelo económico industrial, por lo cual es importante que europa transite de éste a uno basado en el Internet, a fin de poder competir con China.[332]

---

[328] Mayer, Thomas, A digital euro to compete with libra, Ecomomists´Voice, 2019. p. 1.

[329] La Unión Europea se compromete a regular las monedas digitales, MCPRO. Disponible en: https://www.muycomputerpro.com/2019/10/09/union-europea-regular-monedas-digitales, consultado el: 05/03/2021.

[330] Mayer, Thomas, op.cit., p. 2.

[331] Ibidem, p. 3.

[332] Así será el euro digital: Europa pone en fase de pruebas su alternativa a las criptomonedas y a las divisas electrónicas de China y Rusia, op. cit.

Paralelo al confinamiento por el COVID 19, en China sus principales bancos ya están ensayando con el yuan digital, que desde el 2017, Alipay y WeChat Pay ya permiten pagos digitales.[333] En el modelo chino, se conjuntan la colaboración pública y privada, entre bancos centrales y empresas tecnológicas.[334] En este sentido, es muy probable que el Banco Popular Chino sea la primera institución en emitir una versión digital de su moneda, ya que sus pruebas se encuentran muy avanzadas.[335]

Otros bancos centrales que están discutiendo posibilidades en torno a las monedas digitales, son la reserva federal de los EUA y el banco de Inglaterra, pero hasta ahora tienen pocos planes para actuar. La idea de las monedas digitales ha surgido de la conciencia nacional e internacional sobre el incremento de las criptomonedas a partir del Bitcoin, de sus posibilidades, así como de la propuesta de Facebook, Libra.[336]

En Europa, por ejemplo, la plataforma 2gether de origen español que opera con 13 criptomonedas (BTC, ETH, DASH, XLM, ADA, BCH, LTC, QTUM, DAI, XRP, BAT y WAVES), presentó en enero de 2020, un estudio sobre el mercado europeo que analiza el comportamiento del pago con criptomonedas, con una muestra de 10,000 usuarios, dieron como resultado:

- "55% de usuarios que gastan criptomonedas tienen entre 26 y 45 años, de estos el 25% son *millennials* y el 31% generación X.
- 15% tienen nivel educativo alto (estudios de licenciatura) y el 11% son estudiantes.
- 77% de los usuarios son hombres y el 23% mujeres.
- 37% de los pagos a través de la plataforma se realizan con criptomonedas y el 63% con euros.
- La criptomoneda más utilizada es el Bitcoin con 51%, la segunda con Ethereum 39%, Ripple 2%, Bitcoin Cash 1%.

[333] Idem.
[334] Idem.
[335] Look, Carolynn, ECB Takes Major Step Toward Introducing a Digital Euro, Bloomberg.
[336] Wallace, Tim, ECB plots digital euro as online revolution takes off, Daily Telegraph.

- La media, los usuarios de la plataforma española gastan 112,56 euros al mes en criptomonedas.
- La mayoría de las criptomonedas las gastan en el sector de restaurantes y hotelería (32%) y alimentación (19%)".[337]

En respuesta a todas estas iniciativas y a la utilización de los ciudadanos europeos de las criptomonedas, el Banco Central Europeo (BCE), órgano comunitario que se encarga de la política monetaria de la Unión,[338] dirigido por Christine Lagarde, inició el proceso de adopción de una moneda digital, proyecto *Central Bank Digital Currency* (CBDC), diferente en su naturaleza de las criptomonedas, el euro digital, que funcionará como el euro físico, preservando su valor y regulada por el BCE. Es decir, sería una forma electrónica de dinero del BCE,[339] que responderá a la necesidad de realizar transacciones de manera rápida y sin necesidad de contacto físico.[340]

El BCE está llevando a cabo las acciones necesarias para la creación del euro digital, la moneda virtual que complementaria al euro físico, que "garantiza a los ciudadanos de la zona euro el libre acceso a un medio de pago sencillo, universalmente aceptado, seguro y fiable",[341] según señala el BCE.

Este proyecto lo están trabajando el BCE en colaboración con 19 bancos centrales, que han detectado el incremento de la demanda de pagos electrónicos en la zona euro y un descenso significativo en el uso del efectivo o moneda física.[342]

---

[337] Así son los usuarios de criptomonedas en Europa, El Mundo. Disponible en: https://www.elmundo.es/tecnologia/innovacion/2020/01/21/5e26db5cfdddffc-c088b4602.html, consultado el: 05/03/2021.

[338] López Velarde Campa, Jesús Armando, La Unión Europea. Paradigma para la integración en América del Norte, Universidad Autónoma de Aguascalientes, México, 2006, p. 132.

[339] Así será el euro digital: Europa pone en fase de pruebas su alternativa a las criptomonedas y a las divisas electrónicas de China y Rusia, op.cit.

[340] Alberto Giordano, The Euro, digital versión, Global Finance. Disponible en: https://www.gfmag.com/magazine/november-2020/euro-digital-version, consultado el: 05/03/2021.

[341] Así se plantea el euro digital, la moneda virtual complementaria del efectivo por la que apuesta el Banco Central Europeo, op.cit.

[342] Primera regulación para las criptodivisas en europa, Sabadell, Competencia y mercados. Disponible en: https://estardondeestes.com/movi/es/articulos/primera-regulacion-para-las-criptodivisas-en-europa, consultado el: 05/03/2021.

Este fue puesto a consideración de los ciudadanos europeos a través de una consulta pública de fecha 12 de octubre de 2020, que busca recabar información desde los bancos nacionales y BCE, decidirá a mediados de 2021 si es viable o no la creación de esta moneda.[343] Adicionalmente, el BCE solicitó, el 22 de septiembre de 2020, el registro del término "Euro digital" ante la Oficina de la Propiedad Intelectual de la Unión Europea.[344]

Asimismo, se está trabajando en el concepto del euro digital, experimentando con su diseño y discutiendo con los miembros de la UE y otros socios internacionales, con el objetivo de asegurar que esta moneda digital cuente con las siguientes cualidades: facilidad de acceso, solidez, seguridad, eficiencia, privacidad y se adecue a la normatividad.

Por lo que, se encuentran analizando los beneficios y riesgos de este proyecto. Para el BCE, defensor de esta moneda, los argumentos a su favor son que:

- Se realizan transacciones tanto emitiendo billetes como transfiriendo depósitos electrónicos a bancos y a otras instituciones,[345] por lo que el uso de monedas o recursos en el ámbito electrónico no es algo nuevo.
- Haría que los pagos que usualmente ya realizan los habitantes de la zona euro fueran más fáciles, rápidos y seguros.
- En un momento dado en que el efectivo físico desaparezca o peligre su existencia como en eventos de desastres naturales o pandemias, la moneda virtual estará preparada para afrontar este reto y amortiguar su impacto.[346]
- En las pandemias, el distanciamiento social modifica los hábitos de pago de los consumidores, que incluso pueden ver en el dinero físico un factor de infección y contagio, por lo que estarán menos dispuestos a utilizarlo.

[343] Así se plantea el euro digital, la moneda virtual complementaria del efectivo por la que apuesta el Banco Central Europeo, op. cit.
[344] Look, Carolyn, op. cit.
[345] Así se plantea el euro digital, la moneda virtual complementaria del efectivo por la que apuesta el Banco Central Europeo, op. cit.
[346] Idem.

- Es más fácil llevar las tasas de interés a negativo, porque las personas no sacarían su efectivo , ni lo guardaban debajo de sus colchones.[347]

Para Luis Gavira, profesor de finanza de ICADE *Business School*, destaca que el euro digital supondrá más control a nivel de políticas públicas y eso significa menos oportunidad de fraude y menos robo, también señala que si en este momento desapareciera el efectivo, Italia pudiera ganar unos 30.000 millones de euros solo por concepto de IVA.[348]

Así también, el BCE inició con el proceso de pruebas. En abril de 2020, el Banco Central Francés comenzó a probar la moneda digital con la finalidad de verificar si es un medio eficiente de pagos,[349] y en junio de 2020, la Asociación Bancaria Italiana (ABI), con más de 700 bancos afiliados, aprobó las directrices para el lanzamiento del euro digital, señalando que el euro digital deberá cumplir con las directrices monetarias del órgano regulador europeo.[350]

Actualmente y después de ser probado por Francia e Italia, en septiembre de 2020 inició el turno de 5 bancos españoles para probar el euro digital, basado en *Blockchain*. Los bancos elegidos son; Santander, BBVA, Caixabank, Bankia y Banco Sabadell, así como la compañía de pagos Iberpay.[351]

Luis Gavira, señaló que la adopción del euro digital será un proceso difícil y largo, incluso aún cuando se dé el visto bueno en 2021, llevará tiempo su creación, ya que no sería una criptomoneda.

No obstante, el Gobernador del Banco Central de Francia, Francois Villeroy de Galhau, sostuvo, en la conferencia Virtual "Banca y pagos en el mundo digital" de septiembre de 2020, que a Europa le queda poco tiempo para decidir sobre la adopción del euro digital, Europa se enfrenta a decisiones urgentes y estratégicas en materia de pagos,

[347] Wallace, Tim, op. cit.
[348] Así será el euro digital: Europa pone en fase de pruebas su alternativa a las criptomonedas y a las divisas electrónicas de China y Rusia, op. cit.
[349] France starts testing digital euro, Global Banking News.
[350] Italy becomes latest nation to propose digital euro, Global Banking News.
[351] Así será el euro digital: Europa pone en fase de pruebas su alternativa a las criptomonedas y a las divisas electrónicas de China y Rusia, op. cit.

decisiones que tendrán implicaciones importantes en la soberanía financiera europea de los próximos decenios.[352]

En el mismo sentido, la directora del BCE, Christine Lagarde, de manera optimista señaló que podría lanzarse el euro digital en 2 o 4 años, después de su aprobación en 2021, sostuvo también que éste va a contribuir a "una mayor soberanía monetaria, una mejor autonomía para la zona del euro".[353]

Paralelamente, la carrera por la regulación del euro digital y las criptomonedas se encuentra a marchas forzadas dentro de la UE, que considera prioritario, por un lado, la creación del marco jurídico que brinde el contexto necesario para la adopción del euro digital en la euro zona, y por el otro, la regulación de las criptomonedas que observan como un riesgo latente para los mecanismos financieros tradicionales y para los medios de pagos en la región, dadas sus características de anonimato y volatilidad puede ser vulnerable al lavado de dinero y terrorismo y a desestabilizar los mercados financieros europeos.

7.2 Regulación jurídica europea ante el uso de las criptomonedas

La regulación de las criptomonedas y monedas virtuales como el euro digital, se encuentra en una etapa temprana en la UE, por lo que ha sido lento el incremento en el número de países que cuentan con algún tipo de normatividad, y ha sido casi inexistente la creación de un marco jurídico regional. Es decir, las instituciones comunitarias no han profundizado, a través de su actividad normativa, en la creación de un régimen regulatorio sobre la materia.[354]

En el verano de 2019, Monerium, emisor de dinero electrónico respaldado por Consensys, se convirtió "en la primera empresa del mundo en obtener una licencia de los reguladores islandeses, como

[352] Francia advierte que es urgente que Europa decida sobre emisión de moneda digital, Observatorio Blockchain. Disponible en: https://observatorioblockchain.com/cbdc/francia-advierte-que-es-urgente-que-europa-decida-sobre-emision-de-moneda-digital/, consultado el: 05/03/2021.

[353] Lagarde says digital euro could materialise in two to four years, Global Banking News.

[354] López Velarde Campa, Jesús Armando, Unión Europea e integración latinoamericana, Miguel Ángel Porrúa, México, 2014, pp. 140-141.

parte de un nuevo marco regulatorio europeo para los servicios de dinero electrónico, utilizando cadenas de bloques de Ethereum y Algorand.[355]

Desde el año 2000, la Comisión Europea había descrito, en una directiva, que el dinero electrónico era una alternativa digital al efectivo.[356]

No obstante, muy recientemente, en 2019, es que el Comisario de Finanzas de la Unión Europea, Valdis Dombrovskis, se comprometió a realizar una propuesta de normativas que ayuden a regular los activos digitales o criptomonedas.[357]

El interés del Comisario surgió apenas a mediados del año 2019, cuando apareció en el escenario mundial la divisa digital Libra de Facebook, que señaló: "supone una serie de riesgos dentro de la Unión Europea, ya que millones de usuarios de Facebook en Europa podían pagar con la nueva moneda digital",[358] dejando a las empresas a cargo de una enorme cantidad de pagos, desplazando a los sistemas monetarios gubernamentales nacionales, regionales y supranacionales.

Asimismo, afirmó que dicha normatividad tendría que centrarse en defender la estabilidad financiera, proteger a los consumidores y afrontar los riesgos del lavado de dinero.[359]

Por otro lado, el tribunal de justicia de la Unión Europea (TJUE) adoptó una postura frente a los bitcoins, a propósito de la resolución de un procedimiento prejudicial de carácter fiscal relacionado con la directiva del IVA, mediante la sentencia del 22 de octubre de 2015, asunto C-264/14, en la que señaló que esta criptomoneda es una "divisa virtual de flujo bidireccional"[360] que "no puede calificarse como

[355] La empresa blockchain monerium cree que Europa "ya tiene" un euro digital, Cointelegraph. Disponible en: https://es.cointelegraph.com/news/blockchain-firm-monerium-thinks-europe-already-has-a-digital-euro, consultado el: 05/03/2021.

[356] Idem.

[357] Unión Europea se compromete a regular las monedas digitales, Bitcoin México. Disponible en: https://www.bitcoin.com.mx/union-europea-se-compromete-a-regular-las-monedas-digitales/, consultado el: 05/03/2021.

[358] Idem.

[359] Idem.

[360] Regulación legal del bitcoin y otras criptomonedas en España, Algoritmo Legal. Disponible en: https://www.algoritmolegal.com/tecnologias-disruptivas/

bien corporal",[361] cuya finalidad es ser un medio de pago exento de impuestos como el IVA, pero no es considerada una divisa tradicional.

Asimismo, la Directiva 2018/843/UE relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, adoptada por el Parlamento Europeo y el Consejo Europeo el 30 de mayo de 2018, que modifica la Directiva 2015 del 20 de mayo de 2015, y en vigor hasta el 10 de enero de 2019, establece un marco jurídico general para hacer frente a los fondos y bienes correspondientes al terrorismo y lavado de dinero.

Como parte del esfuerzo para regular las criptomonedas la Directiva incluye su definición:

> Representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatus jurídico de moneda o dinero, pero que es aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos.[362]

En ésta se admite que las criptomonedas pueden ser un medio de pago y de cambio, que se pueden transferir, almacenar y negociar, pero no son monedas de curso legal, no deben confundirse con dinero electrónico (uso de la moneda de curso legal en transacciones electrónicas), con el valor monetario almacenado en instrumentos exentos o con monedas de juegos.

Asimismo, considera que las criptomonedas pueden ser susceptibles de uso indebido o delictivo, dada su propia naturaleza de anonimato, por lo que debe ser crucial mantener el control de los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias, así como otorgar a las Unidades de Inteligencia Financieras (UIF) nacionales las facultades para obtener información que les permita asociar al usuario o propietario con las criptomonedas.[363]

---

regulacion-legal-del-bitcoin-y-de-otras-criptomonedas-en-espana/, consultado el: 05/03/2021.

[361] Idem.

[362] Idem.

[363] Entra en vigor la nueva directiva de la Unión Europea para poner cerco a las criptomonedas, Legal Today. Disponible en: https://www.legaltoday.com/practica-juridica/derecho-mercantil/mercantil/entra-en-vigor-la-nueva-directi-

Ello es fundamental ya que hasta el 2020 los proveedores de criptomonedas han podido operar en la UE, sin que existan marcos normativos para poder llevar a cabo un control de los capitales que se manejan en criptomonedas. Con la entrada en vigor de la Directiva 2018/843/UE en 2019, la plataforma Eribit, dedicada al intercambio de derivados establecida en Amsterdam, decidió cambiar sus oficinas centrales a Panamá, al igual que ésta, empresas como Binance y OkEx, pudieran abandonar la UE.[364]

Es importante, que se apliquen medidas atenuantes o contramedidas adecuadas que aseguren que no se lleve a cabo el lavado de dinero y el terrorismo, así como el que las UIF puedan recoger y analizar información con miras a establecer vínculos entre transacciones sospechosas de actividades delictuosas, notificando a las autoridades competentes cuando hay sospecha de blanqueamiento de capitales.[365]

Adicionalmente, el 19 de febrero de 2020, la Comisión envió una comunicación (COM 2020/66) al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones, en el que señalaba como acciones clave:

"Creación de un marco que permita una financiación digital apropiada, competitiva y segura, en particular propuestas legislativas sobre los cripto activos y la ciber resiliencia y la resiliencia operativa digital en el sector financiero, así como una estrategia hacia un mercado de pagos integrado de la UE compatible con soluciones y servicios de pagos digitales paneuropeos (tercer trimestre de 2020)".[366]

En concordancia, en octubre de 2020, la Comisión Europea aprobó un paquete de medidas sobre finanzas digitales, que incluyen propuestas legislativas para continuar la regulación de las criptomonedas:

- Se creará, siguiendo la propuesta realizada en septiembre de 2020 por diversos miembros de la UE, un organismo específico para la regulación y vigilancias de las criptomonedas, un colegio de supervisores de criptomonedas, integrado por las

va-de-la-union-europea-para-poner-cerco-a-las-criptomonedas-2020-02-03/, consultado el: 05/03/2021.

[364] Idem.

[365] Idem.

[366] COM 2020/67 final, del 9 de febrero de 2020. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Configurar el futuro digital de Europa.

autoridades nacionales y comunitarias como la Autoridad Europea de valores y Mercados, presidido por la Autoridad Bancaria Europea (ABE), este ente tomaría el control del sector de criptomonedas en la región.[367]

Se encargará de revisar el funcionamiento y uso de las criptomonedas como Libra, Bitcoin, entre otras,[368] con aplicación en escala de las disposiciones, imponiendo reglas más estrictas a las criptomonedas que se consideren más riesgosas y menos a las que sean más confiables, también tendrá la facultad de solicitar a los emisores de criptomonedas que mantengan fondos propios; podrá revocar autorizaciones si hay incumplimiento grave de la normatividad; realizar investigaciones e inspecciones; imponer multas de hasta el 5% de la facturación anual de los emisores, o del doble de las ganancias obtenidas o pérdidas evitadas con la infracción; se revisará que los emisores presenten a los usuarios un documento técnico con información sobre el emisor, el token o la plataforma de negociación, este documento previa aprobación del nuevo organismo; y se verificará que los emisores se hayan convertido en una institución de crédito o de dinero electrónico con requisitos estrictos.

- Adopción de medidas de salvaguardas necesarias contra cualquier riesgo de su inclusión a las economías comunitarias, como son: requisitos de capital, custodia de activos, procedimiento obligatorio de reclamación para inversores y respeto a los derechos del inversor frente al emisor, entre otros; y presencia física en alguno de los territorios de los Estados miembros.[369]
- Las legislaciones nacionales sobre criptomonedas se deberán armonizar con la legislación comunitaria.

Con estas medidas la Comisión Europea se propone brindar seguridad jurídica, apoyar la innovación, proteger tanto a consumidores como inversionistas, garantizar la estabilidad financiera y la integridad del mercado de la UE. Este plan regulatorio presentado por el Comisión,

[367] Comisión Europea propone crear organismo supervisor para las criptomonedas, Criptonoticias. Disponible en: https://www.criptonoticias.com/regulacion/comision-europea-propone-crear- organismo-supervisor-criptomonedas/, consultado el: 05/03/2021.

[368] Idem.

[369] Primera regulación para las criptomonedas en Europa, op. cit.

fue respaldado por Alemania, Francia, Italia, España y los Países Bajos, pero añaden que las *stable coins* (monedas estables) tengan una paridad 1:1 con activos de reserva denominados en euros o monedas de los Estados miembros y que se depositen en una institución aprobada por la UE.[370]

Es decir, se ven pasos claros hacia una normatividad comunitaria europea para regular las criptomonedas y poder implementar el euro digital, no obstante aún hay cuestiones por definir y propuestas por adoptar. No se puede negar el esfuerzo de la UE en la materia pero tampoco el atraso que lleva en comparación con otras grandes potencias, como son Rusia y China, o con otras empresas tecnológicas, como Facebook con su propuesta, Libra. Sin duda un gran reto para la UE.

[370] Comisión Europea propone crear organismo supervisor para las criptomonedas, op. cit.

Referencias

CAPÍTULO 1

Ávila Pinto, Renata, ¿Soberanía digital o colonialismo digital?, Sur 27, V. 15, No. 27, 2018.

BBC News Mundo, Alexei Navalny: líder opositor ruso es detenido tras aterrizar en Moscú, 5 meses después de su envenenamiento, https://www.bbc.com/mundo/noticias-internacional-55698266

BBC News Mundo, Rusia intervino en las eleciones para promover la victoria de Donald Trump, https://www.bbc.com/mundo/noticias-internacional-38274334

BBC News Mundo, Trump rectifica: ahora acepta que Rusia sí interfirió en las elecciones presidenciales de los Estados Unidos en 2016, https://www.bbc.com/mundo/noticias-internacional-44867589

ED Economía Digital, Rusia aprueba su ley de "desconexión" de Internet. https://www.economiadigital.es/tecnologia-y-tendencias/rusia-aprueba-su-ley-de-desconexion-de-Internet_622796_102.html

¿Estamos perdiendo la soberanía digital?, www.andinalinkvirtual.

Expansión, Revista digital, Biden llama "asesino" a Putin y sube la tensión entre EU y Rusia, https://expansion.mx/mundo/2021/03/17/biden-llama-asesino-a-putin-y-sube-la-tension-entre-eu-y-rusia

López Velarde Campa, Jesús Armando (Coord.), La Gobernanza en la Ciudad de México. Visiones multidisciplinaria, Instituto de Investigaciones Jurídicas, UNAM, Asamblea Legislativa del Distrito Federal, VII Legislativa, México, 2018.

Martínez Cabezudo, Fernando, Soberanía tecnológica y gobierno abierto. Profundizando en las necesidades democráticas de la participación desde la tecnopolítica, Revista Internacional de Pensamiento Político, I Época, vol. 10, 2015.

Ministerio de Perú, Embajada de Francia en Lima, Discurso de Emmanuel Macron, Por un renacimiento Europeo. https://pe.ambafrance.org/Discurso-de-Emmanuel-Macron-Por-un-Renacimiento-Europeo

Rivera España, Calos Alberto, Elaboración de un concepto de soberanía digital en base al estudio de los casos de Julian Assange y Ed-

ward Snowden, Instituto de Altos Estudios Nacionales, Ecuador, 2017.
Sabiguero, Ariel, et al, Relaciones entre soberanía y tecnología en los tiempos de Internet, Revista de la Facultad de Derecho, No. 41, Jul-Dic, Uruguay, 2016.
Sachverständigenrat Für Verbraucherfragen, Soberanía Digital. Estudios Científicos del Consejo de Expertos en materia de Asuntos del Consumidor, Alemania, 2017.
Unión Internacional de Telecomunicaciones (UIT), Estadísticas, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

CAPÍTULO 2

Biblioteca del Congreso Nacional de Chile, Convenio sobre Ciberdelincuencias: Convenio de Budapest, https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26882/1/Convenio_de_Budapest_y_Ciberdelincuencia_en_Chile.pdf
Centeno Danya, México y el Convenio de Budapest: Posibles incompatibilidades, 2018.
Código Frontera, Snowden y Assange: héroes y villanos. 2017. http://www.codigoyfrontera.space/2017/05/24/snowden-y-assange-heroes-y-villanos/
E&N, Centroamérica y Mundo, Los ciberataques (en el mundo) cuestan US$575.000 millones anuales, https://www.estrategiaynegocios.net/centroamericaymundo/1111615-330/los-ciberataques-en-el-mundo-cuestan-us575000-m-anuales
El Comercio, Política, Conozca quién es Julian Assange y la cronología del caso, 2012. https://www.elcomercio.com/actualidad/politica/conozca-julian-assange-y-cronologia.html
El Diario, Assange contra Snowden: parecidos y diferencias. 2014. https://www.eldiario.es/turing/vigilancia_y_privacidad/assange-snowden-parecidos-diferencias_1_5089118.html
El Mundo, Wikileaks: cronología de un escándalo, 2011. https://www.elmundo.es/elmundo/2011/11/02/internacional/1320232744.html
El País, Economía, Nube de cifras. Ciberseguridad: las cifras de los ataques informáticos, Revista Retina, https://retina.elpais.com/retina/2020/07/17/tendencias/1594958904_685745.html

El Tiempo, El cibercrimen no descansa, éstas son las proyecciones para el 2020, https://www.eltiempo.com/tecnosfera/dispositivos/cifras-de-ciberataques-de-2019-y-tendencias-para-el-2020-435508

Expansión, México está entre el top 10 de países con más *phishing* por el COVID-19 https://expansion.mx/tecnologia/2020/04/16/mexico-esta-entre-el-top-10-de-paises-mas-*phishing*-covid-19

France 24, La historia por la que Julian Asange lleva una década en la mira de EE.UU. 2020. https://www.france24.com/es/historia/20200227-historia-julian-assange-wikileaks-extradicion-juicio

Fundación Karisma, Convenio de Budapest: Aplicación en Colombia frente a derechos humanos, 2018.

INFOBAE, El caso de Snowden: historia del genio cyber que traicionó a su patria y huyó a Rusia protegido por Putin, 2019. https://www.infobae.com/america/mundo/2019/04/20/el-caso-snowden-historia-del-genio-cyber-que-traiciono-a-su-patria-y-huyo-a-rusia-protegido-por-putin/

INTERPOL. Estrategia mundial contra la ciberdelincuencia. Secretaría General de INTERPOL. 2017.

ITU, Ciberseguridad. Comprensión del Ciberdelito: Fenómenos, Dificultades y Respuesta Jurídica, Informe. 2014.

Karin Wahl, Jorgensen, et al, The Normalization of Surveillance and the Invisibility of Digital Citizenship: Media Debates After the Snowden Revelations, International Journal of Communication 11(2017), 740–762.

Notimérica, Papeles de Panamá, Snowden y Wikileaks: similitudes y diferencias de las 3 filtraciones. 2016. https://www.notimerica.com/sociedad/noticia-papeles-panama-snowden-wikileaks-similitudes-diferencias-tres-mayores-20160412160516.html

Página 12, Diario del juicio a Julian Assange, 2020. https://www.pagina12.com.ar/293866-diario-del-juicio-a-julian-assange

Proceso, Assange presenta depresión severa y comportamientos suicidas, 2020. https://www.proceso.com.mx/649615/assange-presenta-depresion-severa-y-comportamientos-suicidas

Rayón Ballesteros, María Concepción y Gómez Hernández, José Antonio, Cibercrimen: particularidades en su investigación y enjuiciamiento, Anuario Jurídico y Económico, XLVII (2014).

Rees, Stuart, Julian Assange and Wikileaks: a case study in the criminalization of dissent, University of Sydney, Australia, 2019.

Wright, David, European responses to the Snowden Revelations, Increasing Resilience in Surveillance Societies, December 2013.

CAPÍTULO 3

Álvarez Valenzuela, Daniel, Ciberseguridad en América Latina y ciberdefensa en Chile, Revista chilena de derecho y tecnología, vol. 7, no. 1, junio 2018, Chile, https://scielo.conicyt.cl/scielo.php?pid=S0719-25842018000100001&script=sci_arttext

Aguilar Antonio, Juan Manuel, La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas, Revista de Estudios en Seguridad Internacional, Vol. 6, no. 2, Universidad Nacional Autónoma de México, México, 2020.

BBC NEWS, Mundo, Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país, https://www.bbc.com/mundo/noticias-39800133

BBC NEWS, Mundo, El virus que tomó control de mil máquinas y les ordenó autodestruirse, https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

Deutsche Welle: Actualidad, Detectan ataques cibernéticos a entidad electoral de Colombia, https://www.dw.com/es/detectan-ataques-cibern%C3%A9ticos-a-entidad-electoral-de-colombia/a-42898310

El Economista, SAT sufriço ataque en sus sistemas informáticos, https://www.eleconomista.com.mx/sectorfinanciero/SAT-sufre-ataque-cibernetico-informacion-de-los-contribuyentes-esta-segura-dice-Buenrostro-20200709-0039.html

Espinosa, Edgar Iván, Hacia una estrategia nacional de ciberseguridad en México, Revista de Administración Pública, vol. L, no. 136.

Fiscalía General de la Nación, Asegurado por hurto de 600 millones con tarjetas clonadas, https://www.fiscalia.gov.co/colombia/noticias/asegurado-por-hurto-de-600-millones-con-tarjetas-clonadas/

FORBES, Selección Forbes 2020, Éstos son los países más ciberseguros del mundo, https://www.forbes.com.mx/radiografia-cuales-son-los-paises- mas-ciberseguros-del-mundo/

Guía de Ciberseguridad para uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo, Secretaría de Comunicaciones y Transportes, 2000.

Ibarra, Virginia, La seguridad internacional determinada por un mundo on-line: el estado ante el desafío del terrorismo y la ciberseguridad, VII Congreso de relaciones Internacionales, 23, 24 y 25 de noviembre de 2016, http://sedici.unlp.edu.ar/bitstream/handle/10915/58156/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

INSOC CiberSecurity, ¿Por qué es importante la ciberseguridad?, https://www.insoc.com.mx/post/por-qu%C3%A9-es-importante-la-ciberseguridad

León Gavilánez, Fernando e Izaguirre Olmedo, Jorge, Análisis de los ciberataques realizados en América Latina, INNOVA Research Journal, vol. 3, no. 9, Universidad Internacional del Ecuador, Ecuador, septiembre de 2018.

López Velarde Campa, Jesús Armando, Derecho Internacional Contemporáneo, Miguel Ángel Porrúa, México, 2015.

MasContainer, Los países de Latinoamérica con más bajos estándares en ciberseguridad, https://www.mascontainer.com/los-paises-de-latinoamerica-con-mas-bajos-estandares-en-ciberseguridad/

OBS, Business School, ¿Qué es ciberseguridad y de qué fases consta?, https://obsbusiness.school/es/blog-investigacion/sistemas/que-es-ciberseguridad-y-de-que-fases-consta

OEA y BID. Reporte de Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe, 2020.

OTAN, Nuevas amenazas: el ciberespacio, Revista de la OTAN, https://www.nato.int/docu/review/2011/11-september/cyber-threads/es/index.htm

CAPÍTULO 4

Alannsary, Mohammed y Hausawi, Yasser, Adopting and implementing a government Cloud in Saudi Arabia, an integral part of Vision 2030, EPIC series in computing, Vol. 58, 2019.

Banco Mundial, Personas que usan Internet (% de la población) https://datos.bancomundial.org/indicador/IT.NET.USER.ZS?locations=CA

Betancourt, Valeria, El problema de la brecha digital: más allá de las fronteras de la conectividad, Revista de Opinión para el Desarrollo de las Bibliotecas Públicas, 2004, vo. 1, n. 3.

Balarin, María, Las políticas TIC en los sistemas educativos de América Latina: Caso Perú, UNICEF, 2013.

CEPAL, Los caminos hacia una sociedad de la información en América Latina y le Caribe, Santiago de Chile, 2003.

El País, El impulso tecnológico sitúa a India como uno de los cinco países más atractivos para invertir, https://elpais.com/tecnologia/2005/11/29/actualidad/1133256483_850215.html

García Jiménez, Antonio y González Pascual, Alberto, Internet y África: de la brecha a la esperanza digital. Redes, libertades y comunicación, Revista Index.Comunicación, no 3(2), 2013, Universidad Rey Juan Carlos.

López Velarde Campa, Jesús Armando, Vientos de cambio, LIII Legislatura, México, 1989.

López Velarde Campa, Jesús Armando, Derecho Comercial y globalización. Temas selecto, Miguel Ángel Porrúa, México, 2016.

Márquez A., Acevedo J., et al., La brecha digital y la integración de tecnologías de información y comunicación en los Colegios de Estudios Científicos y Tecnológicos de la región Valles Centrales de Oaxaca, México, Congreso Iberoamericano de Ciencia, Tecnología, Innovación y Educación, México, S/A.

ONU, Crónica, La tecnología digital en Asia y el Pacífico en el siglo XXI, https://www.un.org/es/chronicle/article/la-teconologia-digital-en-asia-y-el-pacifico-en-el-siglo-xxi

Programa de Informática educativa MEP FOD. https://issuu.com/andreshernandezcordoba/docs/programa_de_inform__tica_educativa_

PROINFO, Programa Nacional de Informática na Educaçao. https://www.fnde.gov.br/index.php/programas/proinfo?view=default

Proyectos colaborativos nacionales, Otoño 2020, https://redescolar.ilce.edu.mx/images/inicio/2020/calendario_oto20.pdf

Red de escuelas, https://aprenderdelasescuelas.cippec.org/que-nos-inspira/red-escolar/

Rodríguez Gallardo, Adolfo, La brecha digital y determinantes, Tecnologías de la Información, Centro Universitario de Investigaciones Bibliotecológicas, UNAM, México, 2006.
UNESCO, Sociedad Digital: brechas y retos para la inclusión digital en América Latina y el Caribe, 2017.
Unión Internacional de Telecominicaciones (UIT) https://www.itu.int/es/mediacentre/backgrounders/Pages/digital-inclusion-of-all.aspx
ShareAmerica, Kenia: el centro de la innovación en África, https://share.america.gov/es/kenia-el-centro-de-innovacion-de-africa/
Statista. Porcentaje de la población con acceso a Internet en América Latina y Caribe por país en 2020. https://es.statista.com/estadisticas/1136646/tasa-penetracion-mas-altas-Internet-america-latina-caribe/
Villatoro, Pablo y Silva Alisson, Estrategias, programas y experiencias de superación de la brecha digital y universalización del acceso a las nuevas tecnologías de la información y comunicación (TIC). Un panorama regional, CEPAL, 2005.

CAPÍTULO 5

3 maneras en las que facebook usa tu información de WhatsApp, BBC Mundo Tecnología. https://www.bbc.com/mundo/noticias-39961792
Amazon Afiliados. https://afiliados.amazon.com.mx/
Amazon ayudará a Toyota a monetizar los datos recopilados por sus coches. Motorpasión. https://www.motorpasion.com/toyota/amazon-esta-ayudando-a-toyota-a-monetizar-datos-recopilados-sus-coches
Apple es demandada por vender datos de sus usuarios a terceros. Tecnología. https://industriamusical.es/apple-es-demandada-por-vender-datos-de-sus-usuarios-a-terceros/
Así es como gana dinero Apple: con el iphone llegando a su techo es hora de sacar más dinero a sus propietarios. Xalaka. Empresas y Economía. https://www.xataka.com/empresas-y-economia/asi-como-gana-dinero-apple-iphone-llegando-a-su-techo-hora-sacar-dinero-sus-propietarios

Así nos afecta la Guerra comercial entre EE.UU. y China al resto del mundo. Xataka. Empresas y Economía. https://www.xataka.com/empresas-y-economia/asi-nos-afecta-guerra-comercial-eeuu-china-al-resto-mundo

BBC News Mundo, Guerra comercial: como Rusia y China están reforzando sus lazos a "un nivel sin precedentes" como respuesta a Estados Unidos.

Data Monetization: aprovecha el potencial de tus datos. Data Centric. https://www.datacentric.es/blog/marketing/data-monetization-datos/

Desde Rusia con tecnologías: 19 empresas emergentes que merecen la atención, https://wwwhatsnew.com/2020/06/08/desde-rusia-con-tecnologias-19-empresas-emergentes-que-merecen-la-atencion/

EE.UU. vs China: escenarios de la nueva guerra fría. El País. https://elpais.com/internacional/2020-07-25/ee-uu-vs-china-escenarios-de-la-nueva-guerra-fria.html

Guerra comercial entre EE.UU. y China: qué hay detrás del veto de Washington a empresas tecnológicas chinas clave. BBC News. Tecnología. https://www.bbc.com/mundo/noticias-49962766

La concentración de poder de las grandes tecnológicas es perjudicial para los Estados Unidos. TyN Magazine. https://www.tynmagazine.com/ft-la-concentracion-de-poder-de-las-grandes-companias-tecnologicas-es-perjudicial-para-eeuu/

La guerra comercial tecnológica entre China y EE.UU. costará 3.2 billones. Crónica Business. https://cronicaglobal.elespanol.com/business/guerra-tecnologica-china-eeuu-32-billones_369327_102.html

La ofensiva en EE.UU. para desmembrar las grandes empresas tecnológicas acusadas de monopolio. BBC New. Tecnología. https://www.bbc.com/mundo/noticias-54458049

Monetización de datos: estrategia más rentable de analytics. Logicalis Architects of Change, https://blog.es.logicalis.com/analytics/monetizacion-de-datos-la-estrategia-mas-rentable-de-analytics

Ontiveros, Emilio (Dir.) y López Sabater, Verónica (Coord), Economía de los datos. Riqueza 4.0, Editorial Ariel, España, 2017.

¿Quién pierde en la Guerra comercial entre China y Estados Unidos? BBC News Tecnología. https://www.bbc.com/mundo/noticias-internacional-48265320

Todo lo que sabemos de Harmony OS, el nuevo sistema operativo de Huawei, tras un año del bloqueo de EE.UU. Xataka. Servicios. https://www.xataka.com/servicios/todo-que-sabemos-harmonyos-nuevo-sistema-operativo-huawei-ano-bloqueo-eeuu

CAPÍTULO 6

Amnistía Internacional, Vigilancia Masiva, https://www.es.amnesty.org/en-que-estamos/temas/vigilancia-masiva/

Aribau Sorolla, Óscar, Las TIC y la ciber soberanía en China: la base del presidente Xi Jinping para perfeccionar el control social maoísta, Tesis de Maestría, España, 2018, pp. 3-50.

Aristegui Noticias, Anuncia Monreal iniciativa para regular las redes sociales en México https://aristeguinoticias.com/0102/mexico/anuncia-monreal-iniciativa-para-regular-las-redes-sociales-en-mexico/

BBC News, Mundo, Escándalo por espionaje sobre Huawei: qué son las puertas traseras de Internet y qué tienen que ver con el gigante de la telefonía chino https://www.bbc.com/mundo/noticias-47554996

BBC News, Mundo, Huawei: el nuevo escándalo por espionaje que sacude al gigante tecnológico chino tras la detención de uno de sus directivos en Polonia https://www.bbc.com/mundo/noticias-internacional-46853250

Declaración Universal de los Derechos Humanos de 1948.

Delgado Antonio, Nuevas (y viejas) formas de censura de la información en Internet, Cuadernos de Periodistas, número 29, España, 2014, pp- 110-118.

Dobriansky, P., New Media vs. New Censorship: The Assault, remarks to Broadcasting Board of Governors, Washington D.C. 2008

El Diario.es, La vigilancia en Internet avanza con la complicidad de los gobiernos https://www.es.amnesty.org/en-que-estamos/temas/vigilancia-masiva/

El País, El lado oscuro de Tik Tok, el rey chino de los videos relámpago, 2020 https://elpais.com/economia/2020/01/16/actualidad/1579191053_051932.html

Esquire, El crédito social chino: cuando el gobierno te pone nota https://www.esquire.com/es/actualidad/a30361853/credito-social-chino-que-es/

Guangchao Charles Feng y Zhongshi Guo Steve, Tracing the route of China´s Internet censorship: An empirical study, Science Direct, Vol. 30, número 4, Noviembre 2013, pp- 335-345.

Hannig Sascha, Distopía Digital: Cuatro herramientas que China usa para controlar a su población, Fundación para el Progreso, Chile, pp. 1-16.

La vanguardia, La inquietante apuesta china por el reconocimiento facial, 2019 https://www.lavanguardia.com/tecnologia/20190518/462270404745/reconocimiento-facial-china-derechos-humanos.html

Nius, Todo por la cara: límites y retos del reconocimeinto facial, 2019 https://www.niusdiario.es/economia/empresas/reconocimiento-facial-limites-retos-datos-biometricos-cara_18_2817945044.html

Oreskovic, A., Egyptian Activist Creates Image Issue for Google, Reuters, 2011.

Osteltur, El aeropuerto de Beijing estrena una nueva normalidad: vuelos sin contacto, 2020 https://www.hosteltur.com/138912_el-aeropuerto-de-beijing-estrena-una-nueva-normalidad-vuelos-sin-contacto.html

Torres Soriano, Manuel R., Internet como motor del cambio político: Ciber optimistas y ciber pesimistas, Revista del Instituto Español de Estudios Estratégicos, No. 1, 2013, España, pp-127-148.

Xinhua Español, Población de internautas de China crece hasta 904 millones, según informe, http://spanish.xinhuanet.com/2020-04/28/c_139014693.htm#:~:text=La%20penetraci%C3%B3n%20de%20Internet%20en,Red%20de%20Internet%20de%20China.

CAPÍTULO 7

Alberto Giordano, The Euro, digital versión, Global Finance. https://www.gfmag.com/magazine/november-2020/euro-digital-version

Así será el euro digital: Europa pone en fase de pruebas su alternativa a las criptomonedas y a las divisas electrónicas de China y Rusia. Reuters. https://www.businessinsider.es/euro-digital-fase-pruebas-te-afectara-como-consumidor-709401

Así se plantea el euro digital, la moneda virtual complementaria del efectivo por la que apuesta el Banco Central Europeo, Genbeta. https://www.genbeta.com/a-fondo/asi-se-plantea-euro-digital-moneda-virtual-complementaria-efectivo-que-apuesta-banco-central-europeo

Así son los usuarios de criptomonedas en Europa, El Mundo. https://www.elmundo.es/tecnologia/innovacion/2020/01/21/5e26db5cfddffcc088b4602.html

COM 2020/67 final, del 9 de febrero de 2020. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Configurar el futuro digital de Europa.

Comisión Europea propone crear organismo supervisor para las criptomonedas, Criptonoticias. https://www.criptonoticias.com/regulacion/comision-europea-propone-crear-organismo-supervisor-criptomonedas/

Entra en vigor la nueva directiva de la Unión Europea para poner cerco a las criptomonedas, Legal Today. https://www.legaltoday.com/practica-juridica/derecho- mercantil/mercantil/entra-en-vigor-la-nueva-directiva-de-la-union-europea-para-poner-cerco-a-las-criptomonedas-2020-02-03/

France starts testing digital euro, Global Banking News.

Francia advierte que es urgente que Europa decida sobre emisión de moneda digital, Observatorio Blockchain. https://observatorioblockchain.com/cbdc/francia-advierte-que-es-urgente-que-europa-decida-sobre-emision-de-moneda-digital/

Italy becomes latest nation to propose digital euro, Global Banking News.

Del autor

Nació en la Ciudad de Aguascalientes en 1955. Licenciado y doctor en Derecho por la Universidad Nacional Autónoma de México (UNAM); maestro por la Universidad Autónoma de Aguascalientes (UAA). Investigador visitante en el Instituto de Investigaciones Jurídicas de la UNAM (IIJ). Su especialidad es el Derecho Internacional Público. Ha ejercido la docencia en diversas instituciones públicas y privadas de educación superior en su estado natal.

Fungió como Secretario del H. Ayuntamiento y posteriormente Regidor de la Capital. Fue, Presidente del Tribunal de Arbitraje de los Trabajadores al Servicio del Estado y Diputado local en cuatro ocasiones, tres en Aguascalientes y una en la Asamblea Legislativa de la Ciudad de México.

Fue Secretario en la primera Embajada de México ante la Santa Sede, Coordinador General para la Modernización Administrativa de la Educación en la Secretaría de Educación Pública (SEP), Director General de Asuntos Religiosos y Coordinador de Asesores de la Subsecretaría de Población y Asuntos Migratorios de la Secretaría de Gobernación (SEGOB).

Ha escrito 10 libros: "La mexicanidad del Mar Bermejo" (1980), "Vientos de Cambio" (1990), "La Unión Europea, paradigma para la integración en América del Norte" (2006), "Unión Europea e Integración Latinoamericana" (2014), "Derecho Internacional Contemporáneo" (2015), "Derecho Comercial y globalización. Temas Selectos" (2018), "Los invisibles. Niñas, niños y adolescentes en situación de calle en la Ciudad de México" (2017 con otros), "La gobernanza en la Ciudad de México. Visiones multidisciplinarias" (2018 con otros) y "Ley Modelo Interamericana de acceso a la información pública. Avances y retos de su implementación en México" (2019). Asimismo, cuenta con un libro de carácter biográfico "Andanzas de Armando López Campa. A 25 años de la reforma constitucional en materia Eclesiástica" (2018), en el que se recopilan sus conversaciones con la historiadora Mónica Uribe.

Unión Europea se compromete a regular las monedas digitales, MCPRO. https://www.muycomputerpro.com/2019/10/09/union-europea-regular-monedas-digitales

La empresa blockchain monerium cree que Europa "ya tiene" un euro digital, Cointelegraph. https://es.cointelegraph.com/news/blockchain-firm-monerium-thinks-europe-already-has-a-digital-euro

Las criptomonedas en Europa, Europa Press. https://www.europapress.es/asturias/noticia-criptomonedas-europa-20190325145016.html

Lagarde says digital euro could materialise in two to four years, Global Banking News.

Loiacono, Stella, Blockchain, sus aplicaciones más allá de las criptomonedas, Revista abierta de Informática Aplicada, Vol. 2, n. 1, 2018, pp. 47-48.

Look, Carolynn, ECB Takes Major Step Toward Introducing a Digital Euro, Bloomberg.

López Velarde Campa, Jesús Armando, La Unión Europea, Paradigma para la integración en América del Norte, Universidad Autónoma de Aguascalientes, México, 2006.

_____, Unión Europea e integración latinoamericana, Miguel Ángel Porrúa, México, 2014.

Mayer, Thomas, A digital euro to compete with libra, Ecomomists´-Voice, 2019.

Primera regulación para las criptodivisas en europa, Sabadell Comparenca y mercados. https://estardondeestes.com/mpvi/es/articulos/primera-regulacion-para-las-criptodivisas-en-europa

¿Qué es Ethereum y cómo funciona?, IG.com. https://www.ig.com/es/ethereum-trading/que-es-ether-y-como-funciona

Regulación legal del bitcoin y otras criptomonedas en España, Algoritmo Legal. https://www.algoritmolegal.com/tecnologias-disruptivas/regulacion-legal-del-bitcoin-y-de-otras-criptomonedas-en-espana/

Unión Europea se compromete a regular las monedas digitales, Bitcoin México. https://www.bitcoin.com.mx/union-europea-se-compromete-a-regular-las-monedas-digitales/

Wallace, Tim, ECB plots digital euro as online revolution takes off, Daily Telegraph.

Wesley c. Marshall, Deflación y criptomonedas, Análisis, UAM Iztapalapa, Vol. II, No. 30, mayo-agosto, 2018, pp. 29-30.

Derechos de la soberanía digital

Se terminó de imprimir en los talleres de Ediciones La Biblioteca, S.A. de C.V.,
ubicados en Azcapotzalco la Villa 1151, Colonia San Bartolo Atepehuacan,
Alcaldía Gustavo A. Madero, CDMX, C.P. 07730,
el 27 de agosto de 2021.

El cuidado de edición y la composición tipográfica
son del autor y la producción editorial
de Ediciones La Biblioteca.

Su edición consta de 600 ejemplares

El trabajo es novedoso, por la actualidad de los temas que aborda, y pertinente, por el desarrollo expositivo que se logra. A lo largo del libro, se va dejando evidencia de la experiencia de nuestro autor en el ámbito de la academia y el oficio del quehacer público. Así, el Dr. López Velarde Campa ofrece claves para entender de manera amplia problemas complejos, con una visión global, con perspectiva jurídica y de impacto político.

Es importante reconocer que el resultado del esfuerzo del autor, el libro que nos ofrece, es un texto valioso para fines académicos, pero también, es relevante como obra de consulta para los operadores jurídicos, políticos o cualquier persona interesada en entender de mejor manera los retos que las nuevas tecnologías suponen a la sociedad.

José Manuel López Libreros
Doctor en Derecho Internacional por la Universidad Complutense
Profesor Investigador del Departamento de Derecho
Universidad Autónoma de Aguascalientes

9 786078 733392 >

UNIVERSIDAD AUTÓNOMA DE AGUASCALIENTES

LA BIBLIOTECA