*VISUAL REVIEW* | 2023 | ISSN 2695-9631
*International Visual Culture Review / Revista Internacional de Cultura Visual*
https://doi.org/10.37467/revvisual.v10.4568


# LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR

## Una revisión histórica-normativa de este derecho fundamental en el país suramericano

The protection of personal data in Ecuador
A historical-normative review of this fundamental right in the South American country

GABRIELA ROSAS-LANAS [1], GEOCONDA PILA-CÁRDENAS [2]

[1] Universidad Internacional del Ecuador, Ecuador
[2] Universidad Complutense de Madrid, España

**KEYWORDS**

*Personal data*
*Ecuador*
*Data Protection*
*Digital rights*
*Data Protection Law*

**ABSTRACT**

*ICTs are essential tools for satisfying the basic needs of human beings. However, the digital age not only brings vast benefits; it also implies multiple challenges and risks for citizens.*
*The objective of this work is to carry out a historical review of the process of recognition of the fundamental right to the protection of personal data in Ecuador until the enactment of the Organic Law on the Protection of Personal Data in 2021. The review that we present is descriptive, using the technique exploratory and allowed us to conclude that, in Ecuador, the constitutional recognition of this right is recent.*

**PALABRAS CLAVE**

*Datos personales*
*Ecuador*
*Protección de datos*
*Derechos digitales*
*Ley de Protección de Datos*

**RESUMEN**

*Las TIC constituyen herramientas indispensables para la satisfacción de las necesidades básicas del ser humano. Sin embargo, la era digital no solo supone amplios beneficios; sino que también implica múltiples desafíos y riesgos para los ciudadanos.*
*El presente trabajo tiene como objetivo realizar una revisión histórica del proceso de reconocimiento del derecho fundamental a la protección de datos personales en Ecuador hasta la promulgación de la Ley Orgánica de Protección de Datos Personales en 2021. La revisión que presentamos es descriptiva, empleando la técnica exploratoria y nos permitió concluir que, en Ecuador el reconocimiento constitucional de este derecho es reciente.*

Recibido: 20/ 09 / 2022
Aceptado: 26/ 11 / 2022

## 1. Introducción

Las tecnologías de la información y comunicación (TIC) constituyen herramientas indispensables para la satisfacción de las necesidades básicas del ser humano. En otras palabras, son parte fundamental de la sociedad del siglo XXI, cuyas interrelaciones se construyen sobre la base de los nuevos desarrollos tecnológicos, que incluyen la inteligencia artificial y la internet. Sin embargo, la era digital no solo supone amplios beneficios; sino que también implica múltiples desafíos y riesgos para los ciudadanos, quienes son mucho más propensos a sufrir vulneraciones a sus derechos fundamentales.

De igual manera, la forma y la velocidad con las que se mueve la información provoca desconcierto social, que se atenúa por la carencia de mecanismos de protección que regulen su tratamiento. Esto último en virtud de que gran parte de esta se construye sobre la base de los datos personales que, utilizados o tratados inadecuadamente, pueden llegar a afectar el ejercicio de los derechos fundamentales del ser humano. Es decir, la recopilación, el procesamiento o la comunicación mal intencionada se traducen en la exclusión del titular de sus derechos más básicos, tales como el acceso a servicios públicos, la salud, la vida, la integridad física y mental, entre otros.

En Ecuador, los riesgos propios de la era digital se evidencian en robos, ataques o exposiciones ilegítimas de bases de datos de carácter público y privado, lo que ha generado múltiples perjuicios sociales y económicos. Ante esta realidad, varios sectores demandaron la construcción de un sistema de protección de datos personales, concordante con los estándares internacionales; a fin de, tutelar los derechos fundamentales de los ciudadanos y, a su vez, construir un país confiable para la transferencia de datos de este carácter, que hoy en día son la base de las relaciones comerciales y la cooperación internacional. Como consecuencia, el 26 de mayo de 2021 se publicó la Ley Orgánica de Protección de Datos Personales; sin embargo, el análisis de sus aportes principales no es posible si no se revisan previamente los antecedentes internacionales y nacionales; así como, los fundamentos propios de la sociedad del siglo XXI.

En ese sentido, el objetivo principal de este trabajo es realizar una revisión histórica del proceso de reconocimiento del derecho fundamental a la protección de datos personales, que busca responder a las siguientes interrogantes: ¿cuáles son los principales desarrollos a nivel global y regional -América- en esta materia?, ¿cuáles son los fundamentos jurídicos internos sobre los que Ecuador construyó la Ley Orgánica de Protección de Datos Personales?, ¿qué delitos cibernéticos afectan la integridad de los datos personales? Y ¿cuáles son los mecanismos para el ejercicio de derechos y los nuevos enfoques teóricos?

Para responder a estos cuestionamientos, este trabajo de revisión se adentra en la discusión, aprobación y posterior reforma de la Ley Orgánica de Protección de Datos Personales de Ecuador, pero también analiza los instrumentos jurídicos internacionales que sirvieron de base para la discusión de esta temática en América Latina, así como los fundamentos teóricos que sustentan estos desarrollos normativos.

## 2. Método

Este artículo de revisión es un estudio detallado, selectivo y crítico que integra la información esencial en una perspectiva unitaria y de conjunto como describen lo que Icart y Canela (1994). La revisión, para Guirao-Goris et al. (1989) se puede considerar "como un estudio en sí mismo, en el cual el revisor tiene un interrogante, recoge datos (en la forma de artículos previos), los analiza y extrae una conclusión".

Si bien investigadores como Cué Brugueras et al. (2008) proponen una completa lista de etapas de elaboración de este tipo de trabajos, las autoras nos hemos decantado por las fases propuestas por Icart y Canela (1994) que se sintetizan en: definición de objetivos, búsqueda bibliográfica, organización de la información y redacción del artículo. El tipo de revisión que hemos desarrollado es descriptiva (Pulido, 1989) empleando la técnica exploratoria.

Debido a que nuestro objetivo principal es realizar una revisión histórica del proceso de reconocimiento del derecho fundamental a la protección de datos personales hasta la promulgación, en el ordenamiento jurídico ecuatoriano, de la Ley Orgánica de Protección de Datos Personales el 21 de mayo de 2021, hemos recurrido a una búsqueda exhaustiva en bases de datos especializadas, tanto científicas como jurídicas que, gracias a diversas estrategias de búsqueda y la guía de algunos expertos en el tema, nos permitieron localizar y analizar fuentes primarias, sin limitar la búsqueda a los últimos años, puesto que en el aspecto legal nos interesaba analizar la evolución del derecho a la protección de datos personales, tanto en la legislación ecuatoriana como en legislación comparada de otros países e instrumentos internacionales.

En cuanto al rastreo teórico, también hemos recurrido a la revisión de fuentes primarias centrándonos en las cuatro principales tendencias contemporáneas en esta materia que son: *compliance*, privacidad por diseño PbD, sistemas de corresponsabilidad y resiliencia cibernética. Finalmente, antes de la redacción del artículo, para la fase de la organización de la información (Guirao-Goris et al., 1989; Pulido, 1989) nos servimos de recursos como tablas de análisis y síntesis que nos permitieron elaborar el guion que sirvió de base para la redacción del informe final (Day, 2005).

## 3. Resultados

### *3.1. Antecedentes*

Actualmente, los datos personales representan un bien altamente valorado no solo por las instituciones públicas o privadas que operan legalmente, sino también por los ciberdelincuentes, quienes los usan como insumos para materializar fraudes, estafas o cualquier otro tipo de delitos cibernéticos (Pérez, 2015). De ahí que, 115 Estados hayan diseñado sistemas de protección especializados (DLA Piper, 2021), que tutelan la integridad de los ciudadanos, cada vez más vulnerables ante las amenazas y riesgos propios de la era digital. Sin embargo, la regulación de este fenómeno no es reciente ni estática, más bien se ha venido desarrollando desde las primeras décadas del siglo XX, especialmente en el continente europeo.

En ese sentido, desde una visión histórico - normativa, el origen del reconocimiento constitucional del derecho a controlar la información depositada en los sistemas de información está en la Constitución alemana de Weimar de 1919, que estableció que los funcionarios públicos tenían derecho a revisar sus expedientes personales y a impugnarlos (Ojeda Bello, 2015). Empero, desde un enfoque histórico – doctrinal, se tiene que el antecedente remoto del derecho a la protección de datos personales -concebido como dependiente del derecho a la intimidad- se encuentra en la obra The Right of Privacy de Samuel D. Warren y Louis B. Brandies, publicada en 1890, en los Estados Unidos (Ojeda Bello, 2015). De igual manera, en 1960, en Europa, los aportes doctrinarios de Vittorio Frosini ya hablaban de una nueva libertad fundamental -autodeterminación informativa-, que permitía a los ciudadanos ejercer el dominio sobre sus datos personales, en un contexto electrónico.

Posteriormente, en los Estados Unidos de Norteamérica, en 1967, Alan F. Westin redefinió el derecho a la vida privada en términos de protección de la información personal, al afirmar que la privacidad es la capacidad de las personas naturales para determinar autónomamente qué datos personales podrían transmitirse mediante las nuevas tecnologías de la información y comunicación -en adelante TIC-.

En 1970, el derecho a la protección de datos personales surgió en Alemania, que fue el primer país en reconocer -en su Ley de Hesse- las amenazas existentes en los procesos de recolección y tratamiento automatizado de los datos personales (Garriga Domínguez, 2016). En 1980, la Organización para la Cooperación y el Desarrollo Económico OCDE adoptó las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, con el objetivo de proveer una guía general para los procesos de recolección y tratamiento (Remolina Angarita, 2012). En 1981, el Convenio 108 desarrolló una definición amplia de datos personales; pues, se afirmó que estos incluyen todo rasgo que puede atribuirse a una persona y, por ende, la pueden hacer identificable (Araujo Carranza, 2009; Oró Badia, 2016).

Posteriormente, el 14 de diciembre de 1990, la Organización de Naciones Unidas adoptó la Resolución 45/95 de la Asamblea General, mediante la cual se establecieron los principios mínimos que las legislaciones nacionales debían reconocer. En octubre de 1995, el Parlamento y el Consejo Europeo emitieron la Directiva 95/46/CE, con la finalidad de tutelar el derecho a la intimidad, en lo relativo al tratamiento de los datos personales.

En el año 2000, la Carta de Derechos Fundamentales de la Unión Europea (2000) reconoció, en su artículo 8, el derecho fundamental a la protección de datos personales; a fin de, otorgar a los ciudadanos europeos el control sobre el uso y destino de sus datos. De manera que, el último hito mencionado implicó el reconocimiento de un nuevo derecho fundamental, autónomo e independiente. Posteriormente, en el 2003, en la Declaración de Santa Cruz de la Sierra se llevó a cabo la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, celebrada en Bolivia, en donde manifestaron su preocupación frente a la protección de datos personales como un derecho fundamental de las personas y destacaron la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos y esto dio lugar a la creación de la Red Iberoamericana de Protección de Datos.

Asimismo, en el Foro de Cooperación Económica Asia Pacífico (2004) se publicó el Marco de Privacidad APEC, que estableció las condiciones mínimas para la protección de la información personal de los ciudadanos de sus Estados miembros. Finalmente, desde el 25 de mayo de 2018, el Reglamento General de Protección de Datos de la Unión Europea (Reglamento general de protección de datos, 2016) regula el tratamiento de los datos personales y, a su vez, norma la regulación transfronteriza de tales datos.

En el contexto latinoamericano, los procesos de reconocimiento constitucional y legal del derecho a la protección de datos personales, entendido como dependiente de la vida privada, han sido recientes. Pues, Guatemala, en 1985 y, Nicaragua, en 1987, instituyeron constitucionalmente que sus ciudadanos tienen derecho a la protección de su vida privada frente a los sistemas de información del Estado (Ojeda Bello, 2015; Remolina Angarita, 2012). Posteriormente, Brasil reconoció en su Constitución de 1988 (Constitución de Brasil, 1988) el derecho a la protección de la intimidad y, además, estableció la garantía jurisdiccional de *habeas data*, con el fin de tutelar este nuevo derecho. En 1991, la Constitución de Colombia (Constitución Política de Colombia, 1991) redefinió el derecho a la intimidad en un sentido amplio, que debía ser observado por los sistemas públicos y privados. En la misma década, Paraguay, Perú y Venezuela normaron la protección de datos personales, tanto para el ámbito público como para el privado. Mientras que, en el presente siglo, países como México (Constitución

Política de los Estados Unidos Mexicanos, 2007), Ecuador (Constitución de la República del Ecuador, 2008) y Bolivia (Constitución Política del Estado, 2009)se desplazaron ríos, se formaron lagos. Nuestra amazonia, nuestro chaco, nuestro altiplano y nuestros llanos y valles se cubrieron de verdores y flores. Poblamos esta sagrada Madre Tierra con rostros diferentes, y comprendimos desde entonces la pluralidad vigente de todas las cosas y nuestra diversidad como seres y culturas. Así conformamos nuestros pueblos, y jamás comprendimos el racismo hasta que lo sufrimos desde los funestos tiempos de la colonia. El pueblo boliviano, de composición plural, desde la profundidad de la historia, inspirado en las luchas del pasado, en la sublevación indígena anticolonial, en la independencia, en las luchas populares de liberación, en las marchas indígenas, sociales y sindicales, en las guerras del agua y de octubre, en las luchas por la tierra y territorio, y con la memoria de nuestros mártires, construimos un nuevo Estado. Un Estado basado en el respeto e igualdad entre todos, con principios de soberanía, dignidad, complementariedad, solidaridad, armonía y equidad en la distribución y redistribución del producto social, donde predomine la búsqueda del vivir bien; con respeto a la pluralidad económica, social, jurídica, política y cultural de los habitantes de esta tierra; en convivencia colectiva con acceso al agua, trabajo, educación, salud y vivienda para todos. Dejamos en el pasado el Estado colonial, republicano y neoliberal. Asumimos el reto histórico de construir colectivamente el Estado Unitario Social de Derecho Plurinacional Comunitario, que integra y articula los propósitos de avanzar hacia una Bolivia democrática, productiva, portadora e inspiradora de la paz, comprometida con el desarrollo integral y con la libre determinación de los pueblos. Nosotros, mujeres y hombres, a través de la Asamblea Constituyente y con el poder originario del pueblo, manifestamos nuestro compromiso con la unidad e integridad del país. Cumpliendo el mandato de nuestros pueblos, con la fortaleza de nuestra Pachamama y gracias a Dios, refundamos Bolivia. Honor y gloria a los mártires de la gesta constituyente y liberadora, que han hecho posible esta nueva historia. EVO MORALES AYMA PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA Por cuanto, el Pueblo Boliviano a través del Referéndum de fecha 25 de enero de 2009, ha aprobado el proyecto de Constitución Política del Estado, presentado al H. Congreso Nacional por la Asamblea Constituyente el 15 de diciembre de 2007 con lo…“,“container-title“:“Constitución Política del Estado (CPE han plasmado en sus constituciones el derecho en cuestión y, además, a nivel político, la Declaración de Santa Cruz de la Sierra (2003) determinó que la protección de datos personales es un nuevo derecho fundamental (Remolina Angarita, 2012).

En ese orden de ideas, García (2007) sostiene que el derecho a la protección de datos personales fue recogido inicialmente en los ordenamientos jurídicos internos, pero en calidad de derecho derivado de la vida privada. Puesto que, hasta finales del siglo XX, los juristas y los académicos sostenían que el bien jurídico -afectado por la injerencia de la tecnología- era la intimidad y, por ello, fue indispensable redefinir los límites tradicionales de este derecho humano. Empero, con el nacimiento de la tercera generación de derechos humanos, la protección de datos personales adquirió carácter autónomo -a nivel constitucional, especialmente- y, además, se resaltó su importancia trascendental para prevenir posibles injerencias en la vida íntima del ser humano.

En la misma línea argumental, Naranjo (2017) sostiene que el desarrollo de las TIC, el establecimiento de una nueva generación de derechos humanos y los aportes jurisprudenciales de Europa propiciaron el surgimiento de este nuevo derecho fundamental.

Sobre los derechos fundamentales, cabe hacer algunas precisiones, a fin de entender por qué la protección de datos personales ha alcanzado este estatus, especialmente en los países europeos. En ese sentido, Araujo (2009) manifiesta que los derechos fundamentales son el conjunto de derechos humanos positivados en un ordenamiento jurídico interno, más específicamente en la Constitución y, además, cuentan con un conjunto de garantías y mecanismos para su tutela. De manera que, esta categoría de derechos posee un valor jurídico superior, que los hace inalienables, indispensables e irrenunciables. Además, para su ejercicio efectivo, la normativa prevé un conjunto de principios, prerrogativas, procedimientos, órganos y autoridades. Bajo esas ideas, el derecho en cuestión ha alcanzado la condición de fundamental, al ser reconocido en las constituciones -europeas y americanas, principalmente- y, al ser dotado de normas, procedimientos y mecanismos de tutela.

Desde el enfoque revisado anteriormente, la protección de datos personales es irrenunciable y, a su vez, prevalece sobre otros derechos que no están reconocidos constitucionalmente (Gil, 2015). Además, se establece que el Estado tiene la obligación de proteger a todos sus ciudadanos de posibles tratamientos no autorizados, que podrían devenir en la vulneración de otros derechos fundamentales, como la salud, la vida, el acceso a servicios públicos, entre otros (Martínez-Martínez, 2018). De igual manera, el reconocimiento de la autonomía e independencia permitió concebir este derecho en dos sentidos amplios, que responden a las dinámicas propias de un mundo globalizado y digital (García González, 2007). En cuanto al primero, este derecho adquiere un estatus negativo o garantista, por cuanto se procura tutelar los datos de una persona determinada. Mientras que, en un segundo plano, también se atribuye un estatus positivo, según el cual el titular ejerce control sobre la información que provee en los escenarios digitales.Ahora bien, es importante ahondar sobre las principales dinámicas que hacen imprescindible adecuar permanentemente las normas nacionales e internacionales. En ese sentido, en la época actual -economía digital-, los datos personales representan un factor clave de producción que, entre otras cosas, demuestra que el mercado tradicional ha migrado hacia la esfera digital (Cohen, 2017,

como se citó en (Martínez-Martínez, 2018). Es decir, en la sociedad de la información, el poder ya no se define en términos coercitivos, sino que se concibe como la capacidad que tienen los actores públicos y privados para usar la información y conseguir fines específicos (García González, 2007). En medio de esta realidad, las TIC han modificado totalmente la disponibilidad del "nuevo petróleo" del siglo XXI; pues, los datos ya no se generan únicamente en espacios físicos y en tiempos definidos, sino que han traspasado los límites territoriales y temporales.

Igualmente, las redes de comunicación han generalizado los procesos de recolección y tratamiento de la información personal, que puede ser obtenida con o sin el consentimiento de su titular (Garriga Domínguez, 2016). En este último punto, los motores de búsqueda y las redes sociales se han convertido en rastreadores especializados de cada uno de sus usuarios, con el objetivo de obtener datos personales que pueden ser empleados con fines legales o no. Estas nuevas tecnologías implican riesgos sustanciales para los titulares, quienes principalmente experimentan fenómenos como la suplantación de identidad, la disminución de oportunidades laborales y económicas o la lesión de su integridad física y psicológica (Garriga Domínguez, 2016).

Por otra parte, el internet de las cosas ha propiciado la recolección exhaustiva de datos personales en los hogares, lo que supone el seguimiento minucioso de las actividades que los miembros de una familia hacen en la intimidad de sus casas (Garriga Domínguez, 2016). Como resultado, los actores públicos y privados que acceden a esta materia prima podrían procesarla -sin el consentimiento del titular- para elaborar perfiles detallados de los individuos, con diversos fines. Así también, las tecnologías de geolocalización no solo han facilitado la vida del ser humano, sino que también han propiciado la extracción de información íntima de los usuarios.

Así también, la inteligencia artificial supone el procesamiento de datos masivos, entre los que constan los de carácter personal; por tanto, resulta imprescindible contar con una legislación apropiada y acorde a la era digital. Sobre esta tecnología, es importante resaltar la existencia de dos elementos primordiales. El primero se denomina *computing power*, que es el conjunto de sistemas computacionales que facilitan el procesamiento de datos, en tiempos mínimos y con una ingente capacidad de almacenamiento (Martínez-Martínez, 2018). El segundo elemento es el *big data*, que se refiere al gran volumen de datos generados por diversas fuentes -humanas, digitales y biométricas, principalmente- y que son la materia prima para la construcción de perfiles, empleados con fines legítimos o no.

Bajo esas ideas, la sociedad digitalizada experimenta una lógica de control permanente, que implica la obtención, el procesamiento y el archivo de la información personal, por parte del mercado y del Estado, con o sin el consentimiento de los titulares. Sin embargo, el problema real no recae únicamente en la falta de voluntad y conocimiento del ciudadano o en la recolección indiscriminada de datos, sino en los usos favorables o desfavorables que puedan darles los múltiples actores de la sociedad global, ya sean públicos o privados. Así, el tratamiento mal intencionado de datos personales podría traducirse en la exclusión de los servicios de un seguro de vida privado, de un crédito, del acceso a una vivienda o un empleo, entre otros (Garriga Domínguez, 2016).

De manera concordante, García (2007) argumenta que los peligros que genera la era digital al individuo no están relacionados directamente con la acumulación de los datos personales, más bien tienen que ver con la pérdida de control que el titular tiene sobre la disposición, destino y objeto del tratamiento de su información. Dicha amenaza se puede traducir en el sufrimiento de todo tipo de delitos, que resultan del procesamiento doloso del rastro digital. Por ello, uno de los desafíos más importantes del Estado es la protección y seguridad jurídica de los consumidores-usuarios, que proveen sus datos personales en las diferentes plataformas digitales.

Frente a estos retos crecientes y tareas pendientes, en mayo de 2021, Ecuador adoptó la Ley Orgánica de Protección de Datos Personales para garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre los datos de este carácter. De modo que, la norma prevé la protección de los ciudadanos ante cualquier utilización no autorizada de la información que lo hace identificable y, por tanto, puede incidir en el ejercicio de otros derechos fundamentales, tales como la salud o el trabajo. Con el propósito de ampliar esta información, se revisarán los principales instrumentos internacionales y nacionales, que sustentan el actual sistema de protección ecuatoriano.

### *3.2. Marco jurídico normativo internacional*

En el contexto internacional, los Estados han adoptado múltiples instrumentos jurídicos, que reconocen el derecho fundamental a la protección de datos personales y, a su vez, proponen un sistema de tutela sólido, que garantice el ejercicio real de este derecho, aun cuando las amenazas digitales son crecientes. Entre estos instrumentos internacionales están: las Directrices de la Organización para la Cooperación y el Desarrollo Económico (1980), la Resolución 45/95 de la ONU (1990), la Propuesta de Protección de Datos Personales en las Américas (2012), la Resolución A/HRC/RES/28/16 del Consejo de Derechos Humanos (2015), la Guía Legislativa sobre la Privacidad y la Protección de Datos Personales en las Américas (2015), la Estrategia de la Red Iberoamericana de Datos Personales 2020 (2016), el Protocolo de Adhesión de Ecuador al Acuerdo Comercial Multipartes con la Unión Europea (2016), los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (2017) y la Estrategia de la Red Iberoamericana de Datos Personales 2021 – 2025 (2020).

En ese orden, las Directrices de la OCDE que regulan la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales, de 23 de septiembre de 1980, establecen las directrices y principios que los Estados miembros deberán adoptar en sus legislaciones nacionales y, a su vez, observar en el desarrollo de las relaciones comerciales, que requieren el flujo transfronterizo de datos personales. Entre los principios reconocidos constan: a) minimización de datos, b) calidad, c) especificación de fines, d) limitación de uso, e) transparencia, f) acceso -titular- y, g) libre flujo y restricciones legítimas. De esa manera, el Organismo Internacional reconoció la necesidad de armonizar los ordenamientos jurídicos y tutelar los datos de este carácter, mismos que son esenciales para el establecimiento de relaciones comerciales y de cooperación.

Por su parte, la Resolución 45/95 de la ONU, de 14 de diciembre de 1990, instituyó los principios rectores para la reglamentación de los ficheros computarizados de datos personales, con el propósito de orientar los procesos legislativos internos. Entre los principios a observar constan: a) licitud, b) exactitud, c) respeto a la finalidad inicial, d) acceso de la persona interesada - titular, e) seguridad, f) flujo transfronterizo de datos y, g) control y sanción. De ese modo, la Organización Internacional propuso un marco común y mínimo de protección, que precautela los datos personales de las personas naturales -como derecho derivado de la intimidad personal- y, a su vez, reconoce su importancia en el establecimiento de relaciones interestatales.

Asimismo, la Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas, de 9 de marzo de 2012, determina 12 principios básicos que los Estados miembros de la Organización de Estados Americanos -en adelante OEA- deben observar para diseñar sus leyes, que protegen a los ciudadanos de todo riesgo de obtención, procesamiento o uso indebido de sus datos personales. Paralelamente, el instrumento reconoce que el dato personal constituye un elemento esencial en la economía de la información. Bajo esa lógica, se instituyen los principios de: 1. propósitos legítimos y justos; 2. Consentimiento previo; 3. Pertinencia y necesidad; 4. Uso limitado y retención -límite temporal-; 5. Confidencialidad; 6. Protección y seguridad; 7. Fidelidad de la información; 8. Acceso y corrección; 9. Información sensible -tratamiento especializado-; 10. Responsabilidad; 11. Flujo transfronterizo de datos; y, 12. Publicidad por excepciones -asuntos relacionados con la seguridad y defensa nacional-.

Por otro lado, la Resolución A/HRC/RES/28/16 del Consejo de Derechos Humanos, de 01 de abril de 2015, observa con preocupación los efectos negativos que pueden tener el desarrollo de Internet y las TIC en el ejercicio de los derechos de las personas, especialmente el de privacidad, según el cual nadie podrá ser objeto de injerencias ilícitas o arbitrarias en su vida privada. Además, el instrumento reconoce que las dinámicas de vigilancia e interceptación de comunicaciones a gran escala amenazan la integridad física, psicológica y moral del ser humano, que en muchas ocasiones ha sido víctima de los delitos informáticos. En dicho marco, este Órgano de la ONU nombró al Relator Especial sobre el derecho a la privacidad, quien tiene como tarea fundamental el monitoreo de las legislaciones nacionales; así como de los crecientes riesgos cibernéticos.

De igual manera, la Guía Legislativa sobre la Privacidad y la Protección de Datos Personales en las Américas, publicada en agosto de 2015, resalta la importancia de proteger los datos personales ante los efectos propios de la era digital y, a su vez, provee una guía especializada -que amplía el contenido de cada uno de los principios inscritos en la Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas, de 2012-; a fin de, apoyar a los Estados miembros de la OEA en el proceso de armonización de sus ordenamientos jurídicos internos, en el fomento de la cooperación regional y en el establecimiento de antecedentes jurídicos clave para la futura adopción de un instrumento regional vinculante.

Igualmente, la Estrategia de la Red Iberoamericana de Datos Personales 2020, de noviembre de 2016, tuvo por objetivo fundamental impulsar procesos regulatorios armónicos, que permitan consolidar un sistema de protección de datos común para todos los países miembros. Sobre este objetivo, en 2017, el Organismo Internacional logró consolidar los Estándares de Protección de Datos Personales para los Estados Iberoamericanos -instrumento que será revisado más adelante-. Así también, el Plan buscó fortalecer la institucionalidad de los Estados miembros y promover mayores niveles de cooperación entre autoridades nacionales; en este punto, en 2019, la Red constituyó el Grupo Permanente de Autoridades Nacionales para la Protección de Datos, que se encarga de monitorear y evaluar las políticas de protección de datos personales y, a su vez, analizar nuevas amenazas a la privacidad.

En la misma línea, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, de 20 de junio de 2017, constituyen las directrices orientadoras para los países de la región iberoamericana que aún no cuentan con una regulación específica, que proteja los datos personales. Sin embargo, el instrumento también promueve la modernización y armonización de las legislaciones existentes, por cuanto reconoce que los riesgos cibernéticos crecen exponencialmente, conforme se desarrollan las TIC. De igual forma, los estándares proponen un marco regulatorio común, que facilita el flujo transnacional de información personal indispensable para el desarrollo económico y la cooperación interestatal.

Asimismo, la Estrategia de la Red Iberoamericana de Datos Personales 2021 – 2025, publicada el 04 de diciembre de 2020, reconoce los crecientes retos para la protección de datos personales en el contexto de la nueva normalidad -generada por la COVID-19-. Dicho instrumento plantea 12 líneas de trabajo, que pueden ser resumidas en 3 premisas: 1. Impulso de procesos normativos armónicos en la región, buscando crear o modernizar

los ordenamientos jurídicos internos conforme a los estándares internacionales promovidos por la comunidad europea y por los organismos internacionales propios del continente americano; 2. Fomento de la cooperación entre autoridades iberoamericanas de protección de datos personales y de la cooperación interinstitucional -especialmente con la academia-; con el objetivo de establecer directrices comunes para el tratamiento de datos personales y, a su vez, desarrollar investigaciones académicas de impacto; y, 3. Promoción de políticas públicas encaminadas a reducir las amenazas propias de la era digital, con especial énfasis en el fenómeno de la violencia digital. De ese modo, el Organismo regional contribuye al establecimiento de un sistema de protección común, que garantice el ejercicio del derecho a la protección de datos personales.

Por otro lado, el Protocolo de Adhesión del Acuerdo Comercial entre la Unión Europea y sus Estados Miembros, por una parte, y Colombia y el Perú, por otra, para tener en cuenta la Adhesión de Ecuador, de 11 de noviembre de 2016, tiene por propósito principal reforzar las dinámicas de comercio e inversión entre la Unión Europea y los países andinos. Sin embargo, la carencia de una Ley de Protección de Datos Personales -hasta antes de mayo de 2021- no permitió que Ecuador acceda a los beneficios propios del Acuerdo. Debido a que, las lógicas de intercambio comercial -en la mayoría de los casos- demandan el flujo transfronterizo de datos, situación que no es viable en los países que carecen de una legislación específica para esta materia.

### *3.3. Marco jurídico normativo interno*

En Ecuador, la primera aproximación al reconocimiento constitucional del derecho a la protección de datos personales fue la reforma constitucional de 1996, que modificó la Constitución de 1976, incluyendo así la garantía jurisdiccional del *habeas data* (Naranjo Godoy, 2017). Sin embargo, no fue hasta el año 2008 en que el país reconoció constitucionalmente el derecho autónomo a la protección de datos personales desde la visión europea, que promueve altos estándares de tutela. En ese sentido, la Constitución de la República establece que:

> El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (Constitución de la República del Ecuador, 2008, Artículo 66, Numeral 19)

Sobre la disposición citada, Naranjo (2017) comenta que el reconocimiento del nuevo derecho fundamental se construyó sobre la base de la libertad a la autodeterminación informativa, que es el derecho individual a controlar la obtención, tratamiento, tenencia y transmisión de datos personales. Adicionalmente, se estableció que los datos personales son el bien jurídico tutelado, que debe ser tratado de acuerdo con el principio de legalidad y, respondiendo únicamente a los fines para los cuales fueron obtenidos. En otras palabras, el texto constitucional tutela a los datos en sí; puesto que, tienen el potencial de ser procesados para generar un perfil individualizado y concreto del titular, quien es susceptible de sufrir múltiples vulneraciones a sus derechos fundamentales.

A modo de crítica, Enríquez Álvarez (2017) resalta que la disposición constitucional deja muchas aristas abiertas a la interpretación, por cuanto no se establece una definición de datos personales. De igual manera, el texto constitucional no define regulaciones preventivas, ni tampoco determina reglas para el tratamiento de los datos personales, ya sea para instituciones públicas o privadas, nacionales o internacionales. En la misma línea, Naranjo (2017) manifiesta que la Constitución emplea erróneamente el término información como un sinónimo de dato, cuando en realidad existe una marcada diferencia entre ambos. Puesto que, el dato es la unidad mínima, que representa hechos, instrucciones o conceptos; mientras que, la información es el resultado del procesamiento del dato -etapa en la que se le atribuye valor y funcionalidad-.

Por otra parte, la doctrina sostiene que la garantía jurisdiccional de *habeas data* tutela el derecho a la protección de datos personales; puesto que, con ella se protege todo dato personal que se encuentra en tenencia o administración del Estado o una entidad privada. De ahí que, Naranjo (2017) sostenga que esta garantía permite el ejercicio de los derechos ARCO, es decir, de acceso, rectificación, cancelación y oposición. Sin embargo, sobre la disposición constitucional es pertinente hacer algunas precisiones, a fin de clarificar cuál es el objeto tutelado. Debido a que, la Constitución de la República (2008), en su artículo 92, emplea los términos documentos, bancos o archivos de datos personales, datos genéticos e informes como sinónimos.

En cuanto a los documentos, la doctrina reconoce tanto los formatos físicos como los electrónicos; puesto que, tienen las mismas funciones y efectos jurídicos según las disposiciones legales internas. Por ende, la garantía resguardará -por igual- los datos personales digitales y físicos, entendiendo que los últimos son susceptibles de ser digitalizados. Con relación al dato genético, la norma salvaguarda los resultados del procesamiento de los datos médicos, que viene a ser información de carácter sensible, que puede afectar el ejercicio de otros derechos fundamentales. Referente a los bancos o archivos de datos personales, Naranjo (2017) sostiene que el legislador protegió expresamente al conjunto de datos personales, olvidándose que existen datos sueltos que pueden hacer identificable a una persona. Por último, los informes se refieren al instrumento que contiene, de forma detallada, los datos personales de un ciudadano. Tras esas precisiones, se entiende que la acción de *habeas data* efectivamente tutela el derecho a la protección de datos personales.

En el ámbito interno, el Estado también ha desarrollado planes y estrategias encaminadas a proteger los datos personales. En ese sentido, el Libro Blanco de la Sociedad de la Información y del Conocimiento (2018) estableció que la seguridad de la información y la protección de los datos personales es un eje estratégico para el establecimiento de la sociedad de la información y del conocimiento y, a su vez, para incrementar la confianza ciudadana en el uso de las TIC. Asimismo, el Plan de la Sociedad de la Información y del Conocimiento 2018 – 2021 (Avendaño et al., 2018), en su eje de trabajo 6, relativo a la protección de datos personales, estableció 3 proyectos encaminados a promover el tratamiento adecuado de los datos personales, por parte de entidades públicas y privadas y, paralelamente, fomentar la corresponsabilidad ciudadana.

De igual forma, el Plan Nacional de Gobierno Electrónico 2018 – 2021 (2018), dentro del programa "Gobierno abierto", estableció como estrategia número 3 la protección de la información y de los datos personales. Para lo cual, la principal tarea fue construir una norma jurídica, sobre la cual se construya el sistema de protección de este derecho fundamental. En la misma línea, el Plan Ecuador Digital 2021 (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021), dentro de su eje de trabajo "Ecuador eficiente y ciberseguro", reconoció que trabajar en asuntos de ciberseguridad y protección de datos personales es indispensable para proteger al ciudadano frente a los riesgos cibernéticos y, paralelamente, fomentar el desarrollo de la economía digital. En el marco de este último instrumento, el Gobierno ecuatoriano se comprometió con la construcción del Proyecto de Ley Orgánica de Protección de Datos Personales, que fue debatido y aprobado por la Asamblea Nacional.

### *3.4. Ley Orgánica de Protección de Datos Personales*

El 26 de mayo de 2021, en el Registro Oficial Suplemento 459, se publicó la Ley Orgánica de Protección de Datos Personales -en adelante la Ley-, con el objetivo de garantizar el ejercicio del derecho fundamental a la protección de datos personales, "que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección" (Ley Organica De Proteccion De Datos Personales, 2021, Artículo 1). Para ello, el legislador instituyó principios, derechos, obligaciones y mecanismos de tutela, que serán observados y aplicados tanto por las instituciones públicas como por las privadas. Además, la Ley prevé efectos territoriales, que aseguran la tutela de los datos personales de los ciudadanos ecuatorianos, aun cuando sean procesados en otros Estados.

De igual manera, la Ley reconoce que el consentimiento válido del titular, para el tratamiento de sus datos personales, debe ser libre, específico, informado e inequívoco. En otras palabras, al ciudadano se le atribuye la capacidad de decidir sobre la base del análisis de quién, cómo, cuándo y para qué va a procesarse su información personal. Así también, la norma prevé que todo procesamiento de datos personales deberá tener fines legítimos, que podrán ser revisados por la Autoridad de Protección de Datos Personales. Bajo esas ideas generales, es pertinente revisar la definición jurídica que se atribuye a dato personal.

En ese sentido, el artículo 4, de la ley en mención (Ley Organica e Protección de Datos Personales, 2021), establece que el dato personal es el "dato que identifica o hace identificable a una persona natural, directa o indirectamente". De manera que, la unidad mínima -objeto de tutela- puede ser de diverso contenido y naturaleza y, puede estar disponible en cualquier formato; ya que, la condición esencial es que permita identificar a su titular, con o sin la ejecución de procedimientos informáticos. De ahí que, autores como Gil (2015) defiendan la existencia de una lista amplia y dinámica de datos personales, que no solo incluye los relativos a la identidad, las finanzas, las relaciones laborales o los cultos religiosos, sino también lo referente al comportamiento digital -huella digital-. Por tanto, la normativa analizada regula el tratamiento de una diversidad de datos personales, cuyo procesamiento mal direccionado puede afectar -en mayor o menor medida- el ejercicio de otros derechos fundamentales.

Tras esa precisión, se procede con la revisión de los aportes más relevantes. En ese orden, la ley establece 16 principios rectores del sistema de protección de datos personales, que han sido recogidos ampliamente en los instrumentos internacionales y en la doctrina. Así, los principios de lealtad, transparencia, finalidad, minimización de datos, proporcionalidad, confidencialidad, exactitud y conservación fueron reconocidos inicialmente en las Directrices de la OCDE que regulan la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales (1980), la Resolución 45/95 de la ONU (1990) y, la Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas (2012). Mientras que, la responsabilidad proactiva ha sido analizada desde los nuevos enfoques de protección, tales como *Privacy by Design* y Resiliencia Cibernética, que reclaman mayores niveles de responsabilidad a los encargados del tratamiento de datos personales.

Por otra parte, la normativa reconoce una serie de derechos, que garantizan la protección efectiva de los datos personales. Entre ellos, el derecho a la información resulta trascendental, por cuanto reconoce que el titular debe ser informado -de manera leal y transparente- sobre los fines del tratamiento, la base legal correspondiente, el tiempo de conservación, los datos del responsable del tratamiento y, las consecuencias, principalmente. En la misma línea, la ley reconoce los derechos de acceso, rectificación y actualización, eliminación -olvido- y oposición, según los cuales el titular deberá ser atendido -en el plazo de 15 días- cuando requiera conocer sobre su información personal, modificar datos personales inexactos o incompletos, eliminar datos u oponerse a los tratamientos que no observan las disposiciones vigentes.

Igualmente, la ley instituye el derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas, con el propósito de proteger al titular de posibles vulneraciones a sus derechos y libertades fundamentales, que pudieren resultar de la elaboración de perfiles. Para el caso de los niños, niñas y adolescentes, la normativa reconoce este derecho desde una visión altamente garantista, reafirmándose así que este grupo vulnerable demanda mecanismos de protección especializados. Por otro lado, la normativa introduce un nuevo derecho, que promueve la educación digital de los ciudadanos, con el propósito de fomentar el uso y manejo adecuado de las TIC y, a su vez, reducir las disparidades socioeconómicas del país.

Entre otros aportes importantes, la normativa reconoce cuatro categorías especiales de datos personales, cuyo tratamiento está prohibido o limitado. Dicha clasificación incluye los datos sensibles, datos de niñas, niños y adolescentes, datos de salud y, datos de personas con discapacidad y de sus sustitutos -relativos a la discapacidad-. Sobre la primera categoría, la ley establece dos subcategorías: 1. Datos personales de personas fallecidas, que podrán ser solicitados, rectificados, actualizados o eliminados por cualquier sucesor, siempre que el titular de dichos datos, durante su vida, no haya indicado su destino; y, 2. Datos crediticios, que podrán ser tratados únicamente para evaluar negocios, la conducta comercial o la capacidad de pago de su titular.

Sobre lo anterior, la sensibilidad de los datos personales se ha determinado en función de los perjuicios o daños que puede generar a un individuo la exposición pública de dicha información. En otras palabras, los datos especialmente protegidos o las categorías especiales de datos personales incluyen a aquellos que, de ser tratados de modo indebido, afectan directamente a la intimidad del ser humano e inciden en el ejercicio de otros derechos fundamentales (Pérez, 2015). Así, las finanzas, la salud o el origen étnico son ejemplos de esta categoría, que requiere un tratamiento jurídico especial (Gil, 2015).Por otro lado, la ley prevé que los datos personales pueden transferirse o comunicarse a terceros, siempre que los propósitos sean legítimos, estén relacionados con las funciones propias del responsable del tratamiento o del destinatario y, adicionalmente, se cuente con el consentimiento del titular. De modo que, la normativa restringe las posibilidades de transferencia de información personal, buscando proteger al ciudadano de cualquier procedimiento mal intencionado, que pueda afectar su integridad o el ejercicio de sus derechos. Sin embargo, la norma también establece que no se considerará transferencia o comunicación a terceros cuando exista un instrumento contractual, que establezca claramente las finalidades y límites del procesamiento de los datos personales.

En cuanto a la seguridad de los datos personales, la normativa prevé diversas medidas que los responsables o encargados del tratamiento deben observar, con el fin de evitar posibles vulneraciones de derechos. Entre estas medidas resaltan las de anonimización, seudonimización y protección desde el diseño y por defecto, que han sido ampliamente recogidas en instrumentos internacionales sobre la materia, siendo el mayor ejemplo el Reglamento Europeo de Protección de Datos (2016). Sobre estos mecanismos, Martínez-Martínez (2018) resalta la importancia de que los actores que procesan la información personal asuman la responsabilidad desde su propia realidad, procurando respetar siempre la libertad de decisión del titular y su derecho a ser informado previamente. Pues, la tutela efectiva requiere de acciones conjuntas, en las que participen el Estado, los titulares y los responsables o encargados del tratamiento.

Así también, la ley establece 15 obligaciones que el responsable y el encargado del tratamiento de datos personales tiene que cumplir. Dichos deberes incluyen emplear procesos y herramientas legítimas y legales, implementar sistemas de evaluación y verificación sobre los sistemas de tratamiento y seguridad, desarrollar políticas de prevención de riesgos y amenazas, ofrecer mecanismos de protección suficientes, entre otras. De ese modo, la normativa procura determinar claramente las responsabilidades de este actor fundamental, quien tiene el acceso y control de los datos personales. En la misma lógica, se prevé la designación de un delegado de protección de datos personales, cuando: 1. el tratamiento sea efectuado por un actor público, 2. el procesamiento sea a gran escala y verse sobre las categorías especiales de datos y, 3. los datos estén relacionados con la seguridad y defensa nacional. Por su parte, el delegado ejercerá funciones de asesoría, supervisión y cooperación, procurando ser un aliado importante de la Autoridad de Protección de Datos Personales.

En concordancia con los instrumentos internacionales, la normativa establece la transferencia o comunicación internacional de datos personales a países, organizaciones o personas jurídicas que proporcionen niveles adecuados de protección y, a su vez, se sujeten a los estándares internacionales. Para ello, se instituye un régimen específico de mecanismos de control, que incluye -entre las principales medidas- el reconocimiento por parte de la Autoridad de Protección de Datos de que el receptor cuenta con un sistema de protección adecuado y la provisión de las garantías suficientes por parte del encargado del tratamiento. En ese sentido, se entiende que la ley reconoce la importancia de los flujos internacionales de información personal, que en la era digital representan uno de los elementos fundamentales para establecer relaciones de comercio y cooperación.

En referencia al régimen disciplinario, la Ley establece medidas correctivas, que se aplicarán cuando las disposiciones legales -en materia de protección de datos personales- no hayan sido observadas, por parte de los encargados o responsables del tratamiento. Entre dichas medidas constan el cese del procedimiento, la eliminación de datos y la imposición de medidas técnicas, jurídicas o administrativas. Así también, la normativa prevé sanciones pecuniarias, que serán aplicadas por la Autoridad de Protección de Datos Personales, con estricto

apego al principio de proporcionalidad. En ese sentido, las sanciones leves implican el pago de uno a diez salarios básicos unificados o multa de 0.1% a 0.7% del volumen del negocio de la organización privada. Mientras que, para las sanciones graves, se determina el pago de diez a veinte salarios básicos unificados o multa de 0.7% a 1% del volumen del negocio de la organización privada.

En el ámbito de la institucionalidad, la normativa dispone la creación de la Autoridad de Protección de Datos Personales, que será la encargada de garantizar el derecho a la protección de datos personales; así como, de controlar y vigilar el cumplimiento de la ley en cuestión, su reglamento y las regulaciones que ella dicte. Para la consecución de sus objetivos, la ley dotó a este órgano de funciones de regulación, control, legislación y ejecución, todas ellas encaminadas a tutelar los derechos y libertades fundamentales de las personas naturales, en lo relativo al tratamiento de sus datos personales.

3.5. Crimen cibernético y protección de datos personales

A pesar de la existencia de normas que tutelan los derechos a la protección de datos personales y a la privacidad, el desarrollo permanente de las TIC y su uso generalizado han propiciado la comisión tanto de infracciones en materia de protección de datos personales como de conductas delictivas, sancionadas en las legislaciones internas. Entre las conductas ilícitas más comunes constan el acoso, las amenazas, la revelación de secretos, los delitos sexuales, las coacciones, la violencia de género y las estafas (Agencia Española de Protección de Datos, 2018). En concordancia, Martínez Devia (2019)(2018) menciona que entre los riesgos que enfrentan los ciudadanos titulares están el robo de identidad, las extorciones, las estafas digitales, el acoso cibernético y la persecución política.

Sobre las conductas delictivas mencionadas, cabe resaltar que los delincuentes cibernéticos emplean los datos personales como un medio para afectar la integridad física, psicológica o moral de su titular o, a su vez, incidir en el ejercicio de otros derechos fundamentales. Por ello, es importante realizar algunas precisiones sobre los actos ilícitos más comunes: *sexting*, *grooming*, ciberacoso, violencia de género, *phishing*, *carding*, *trashing* y *pharming*. En primer lugar, el *sexting* implica enviar fotografías, videos o audios de carácter sexual de manera voluntaria a un destinatario, quien puede reenviar este tipo de datos personales sin el consentimiento del titular. Consecuentemente, la víctima puede ver afectado su derecho a la vida privada. Sobre este delito, la legislación penal ecuatoriana no prevé un tipo penal específico; sin embargo, la autoridad competente ha sancionado esta práctica mediante el artículo 178, referente a la violación a la intimidad; el artículo 174, relativo a la intimidación; y, el artículo 103, que versa sobre pornografía con utilización de niñas, niños y adolescentes (Vásquez, 2020).

En segundo lugar, el *grooming* implica que un adulto contacte a un menor de edad con propósitos sexuales; para lo cual, en un primer momento, obtiene datos personales relativos a gustos y preferencias y, posteriormente, accede a fotos o videos de carácter sexual, que más tarde le sirven para coaccionar a la víctima. En el caso ecuatoriano, el Código Orgánico Integral Penal (COIP) sanciona esta conducta delictiva mediante el artículo 173, relativo al contacto con finalidad sexual con menores de dieciocho años por medios electrónicos (2021). En tercer lugar, el ciberacoso consiste en amenazar, hostigar o controlar a una persona, mediante las TIC y con la utilización de información personal de la víctima; sin embargo, en Ecuador, esta conducta no se sanciona a través de un tipo penal autónomo, por cuanto se la incluye dentro del delito de acoso sexual -artículo 166 del COIP-.

En cuarto lugar, la violencia digital de género consiste en acosar, amenazar o extorsionar a una mujer, a través del uso de imágenes, videos o audios de carácter sexual, generalmente. En este caso, la legislación ecuatoriana tampoco prevé un tipo penal específico, sino que sanciona estas conductas mediante el artículo 155 del COIP, referente a los delitos de violencia contra la mujer y los miembros del núcleo familiar. Por otro lado, el *phishing* implica obtener información personal sensible -datos financieros, principalmente- mediante el uso de las TIC, con el propósito de causarle pérdidas económicas al titular. En cuanto a la sanción de la estafa digital, la autoridad competente aplica las descritas en el artículo 186 del COIP, que versa sobre el delito de estafa.

En sexto lugar, el *carding* consiste en emplear de manera ilegítima las tarjetas de crédito de otras personas, con la finalidad de obtener ventajas económicas. Para ello, el delincuente roba los números de la tarjeta -datos personales sensibles- y, posteriormente, los emplea en una diversidad de transacciones, materializando así una forma de estafa. De ahí que, en el país, esta conducta se sancione bajo el tipo penal de estafa, recogido en los artículos 186 o 190 del COIP, referentes a la apropiación fraudulenta por medios electrónicos. En cuanto al *trashing*, el delincuente obtiene información de su víctima a través de la recuperación de documentos, directorios o archivos, que reposan en la papelera del dispositivo; en este caso, la sanción aplicable sería la del artículo 190 citado.

Por último, el *pharming* es una modalidad de *phishing*, en la que se obtienen datos personales crediticios, a través de la suplantación de identidad de una institución financiera legal. De igual manera, al no existir un tipo penal específico, las autoridades competentes sancionan esta conducta mediante los artículos 186 y 190 del COIP. Tras estas disquisiciones, se puede afirmar que la legislación penal ecuatoriana -en muchos casos- no prevé tipos penales específicos para los denominados delitos informáticos, más bien los sanciona como modalidades de otros delitos. Sin embargo, cabe resaltar que, en el período 2019 – 2021, la Asamblea Nacional debatió esta problemática en el marco del Proyecto de Ley Orgánica Reformatoria del Código Orgánico Integral Penal para

Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha contra los Delitos Informáticos, cuya objeción parcial fue publicada el 10 de junio de 2021.

### *3.6. Medios para el ejercicio de los derechos*

Frente a la diversidad de riesgos y amenazas cibernéticas, Ecuador -antes de la aprobación de la Ley Orgánica de Protección de Datos Personales- estableció el proceso para ejercer los derechos de Acceso y Rectificación, que debían implementar todas las organizaciones públicas encargadas del tratamiento de datos personales (Acuerdo Minsiterial 012-2019, 2019). Dicho procedimiento formó parte integral de la Política Institucional de Protección de Datos Personales y, procuró garantizar el pleno ejercicio de estos derechos. Actualmente, con la entrada en vigor de la normativa en cuestión, el titular ya no accede únicamente a los mencionados derechos, sino que también puede ejercer los relativos a la eliminación, oposición y portabilidad, ante los responsables del tratamiento, ya sean públicos o privados, nacionales o extranjeros.

En ese sentido, los encargados o responsables del tratamiento deben establecer los mecanismos que permitan ejercer plenamente estos derechos, observando las siguientes prerrogativas legales: a) acceso: el titular podrá solicitar información detallada de sus datos personales y debe ser atendido en el término de 15 días; b) rectificación y actualización: el titular puede requerir la rectificación y actualización de datos personales erróneos e incompletos y será atendido en el plazo de 15 días; c) eliminación u olvido: el titular podrá pedir la supresión de sus datos personales cuando el tratamiento no haya respetado las disposiciones legales propias de la materia; dicha solicitud será atendida en el término de 15 días; d) oposición: el titular puede oponerse al tratamiento de sus datos personales, que tengan fines de mercadotecnia o afecten sus derechos fundamentales; dicho requerimiento se atenderá en el plazo de 15 días; y, e) portabilidad, sobre el cual la Autoridad de Protección de Datos Personales dictará el procedimiento específico.

En una lógica comparada, México establece el Procedimiento para el ejercicio de los derechos ARCO, que debe efectuarse ante la persona natural o jurídica que posee los datos personales (Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales, 2016). Por su parte, el titular presentará una solicitud ante el responsable del tratamiento, en la que consten claramente sus datos de contacto y aquellos sobre los cuales pretende ejercer sus derechos. Dicho requerimiento deberá aprobarse en el término de 20 días y, en el caso de que proceda, el responsable efectuará las gestiones necesarias, en un plazo no mayor a 15 días. En caso de inconformidad fundada, dentro de los 15 días hábiles posteriores a la resolución del responsable, el titular podrá presentar una solicitud de protección de derechos ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), que solventará la petición en un término de 50 días. Este último proceso constituye la instancia final y, por tanto, de este podrán resultar medidas de protección, reparación y las sanciones correspondientes.

Por otra parte, la Constitución de la República prevé la garantía jurisdiccional de *habeas data* -revisada anteriormente-, con el propósito de tutelar los derechos fundamentales de acceso a la información y protección de datos personales. Sobre lo anterior, Quiroz (2016) menciona que esta garantía constitucional efectiviza dos derechos fundamentales: a. acceso a la información, que esté contenida en archivos y registros públicos o privados, siempre y cuando esta cumpla una función pública; y, b. autodeterminación informativa o protección de datos personales, que incluye los derechos de acceso, rectificación, actualización, supresión y reserva; a fin de evitar tratamientos mal intencionados, que pueden devenir en vulneraciones a otros derechos fundamentales. De esta manera, la carta constitucional garantiza el pleno ejercicio de derechos o su reparación al titular de los datos personales.

## 4. Discusión

Las TIC suponen retos permanentes; ya que, su constante desarrollo provoca que las herramientas y mecanismos legales diseñados para proteger los datos personales no sean altamente eficaces. Ante ello, la sociedad demanda medios transparentes, lícitos, claros y modernos para el ejercicio de sus derechos fundamentales; así como, nuevos enfoques que permitan comprender la magnitud de las amenazas cibernéticas y, a su vez, diseñar respuestas oportunas, que no se centren únicamente en una visión reactiva. Bajo dichas consideraciones, el presente apartado revisa cuatro tendencias contemporáneas: a. *compliance*, b. *privacidad por diseño PbD*, c. sistemas de corresponsabilidad y, d. resiliencia cibernética.

En primer lugar, compliance constituye un sistema de origen anglosajón, introducido en los ordenamientos jurídicos de Europa y América Latina; con el propósito de instituir la responsabilidad penal de las personas jurídicas. Sin embargo, su definición primigenia refiere al conjunto de regulaciones, políticas y estrategias previstas por el Estado para: a) garantizar el cumplimiento de la normativa vigente, b) sancionar el incumplimiento de la ley y, c) determinar la identidad del delincuente, que puede ser una persona natural o jurídica, tanto nacional como extranjera (Muriel Bedoya, 2017). En un primer momento, la práctica de compliance se centró en los asuntos de corrupción; por cuanto se originó en los Estados Unidos para sancionar los hechos corruptos cometidos por personas -naturales o jurídicas-, con las cuales el país mantenía una relación contractual. Pero, actualmente, a

nivel internacional, este sistema abarca otros tipos de delitos, tales como el lavado de activos, el terrorismo, los delitos de cuello blanco, entre otros (Muriel Bedoya, 2017).

Ecuador reconoció formalmente el sistema de *compliance* en su legislación penal, mediante una ley reformatoria publicada en el Registro Oficial Suplemento No. 392, de 17 de febrero de 2021. En esta reforma, la responsabilidad penal de las personas jurídicas opera únicamente para los tipos penales, que explícitamente les determinan una sanción. Así, la trata de personas (art. 91 y art. 94), la estafa (art. 186), la falsificación de marcas y piratería lesiva contra los derechos de autor, entre otros. Sin embargo, para el caso de los delitos informáticos, el legislador no ha previsto sanciones para estas personas; por lo que, debería explorarse esta posibilidad. Asimismo, de conformidad con el artículo mencionado, el *compliance normativo penal* está conformado por los sistemas de integridad, las normas, los programas y las políticas de cumplimiento, prevención y dirección, que deben cumplir con una serie de requisitos mínimos legales. Bajo esas ideas, el *compliance* aplicado a la protección de datos personales permitiría supervisar y garantizar que los encargados del tratamiento cumplen con las disposiciones legales vigentes.

Por su parte, la privacidad por diseño o Privacy By Design -en adelante PbD- es un enfoque relativamente moderno, que propone introducir los fundamentos de la protección de datos en las TIC, en los modelos de negocios y en la infraestructura de red -estructura física- (Brian Nougrères, 2012); con el objeto de, implementar los mecanismos y medidas necesarias para garantizar la privacidad de los usuarios. Para ello, esta visión propone un modelo específico, cuyos cimientos son: a) las buenas prácticas -justas- en el tratamiento de los datos personales y, b) la seguridad de datos, referida a las prácticas de manejo y control de la información. Sobre estas bases, PbD define cinco ejes fundamentales: 1. Leyes, normas y supervisión independiente, que son medios reactivos de intervención; 2. Educación y concientización, entendidas como las claves para el empoderamiento de las organizaciones y de los ciudadanos; 3. Transparencia y rendición de cuentas -*Accountability*-; 4. Auditorías y control, que permiten evaluar y reformular procesos; y, 5. Fuerzas de mercado, entendiendo que el desarrollo de las TIC potencializa el comercio electrónico y las amenazas cibernéticas.

En ese sentido, PbD es una visión que promueve la integración de la privacidad desde el diseño mismo de la tecnología y desde la construcción de los sistemas informáticos y de negocios (Brian Nougrères, 2012). En otras palabras, la privacidad se concibe como un modelo proactivo de gestión empresarial, por cuanto las iniciativas organizacionales autónomas van más allá del mero cumplimiento de la legislación. Consecuentemente, el respeto por la vida privada de los usuarios/consumidores es una realidad, que se materializa permanentemente en cada etapa del desarrollo y provisión de productos y servicios.

Así también, Martínez-Martínez (2018) sostiene que los titulares juegan un papel fundamental dentro de la protección de sus datos personales; puesto que, ellos son quienes los proveen, en muchas ocasiones de manera inconsciente, desmedida o sin tener conocimiento total de las implicaciones. Es decir, los usuarios de las TIC -generalmente- no efectúan un ejercicio de lectura consciente y juicioso, cuando se trata de suscribir los términos y condiciones del uso de estas herramientas. Además, gran parte de los ciudadanos desconocen sus derechos y las políticas públicas diseñadas para precautelarlos y, por ende, tienden a entregar todo tipo de información personal, incluso la sensible. Frente a este último factor, Ecuador reconoció en la Ley Orgánica de Protección de Datos Personales el derecho a la educación digital, con el objetivo de promover el uso adecuado, responsable y seguro de las nuevas tecnologías.

Por su parte, Martínez-Martínez (2018) sugiere algunas medidas de seguridad que los usuarios deberían adoptar, entre estas constan: a) limitar los datos personales que exponen en la red, evitando compartir información sobre su localización o finanzas; b) reducir el número de datos compartidos por mensajería privada, especialmente cuando estos tratan de contraseñas; c) emplear la navegación incógnita y borrar el historial de búsquedas; d) leer conscientemente los términos y condiciones de las tecnologías de la información y de la comunicación; y, e) emplear redes privadas de conexión. Sin embargo, estas medidas no son suficientes, si no se trabaja en programas de empoderamiento ciudadano, que propicien la construcción de sociedades más conscientes de los derechos que portan y, también, de los riesgos de la era digital. En este ámbito, cabe resaltar las buenas prácticas de la Agencia Española de Protección de Datos que, desde el año 2018, ha trabajado en la elaboración de guías y herramientas didácticas que transmiten de manera clara y concisa información sobre delitos cibernéticos y datos personales y, seguridad cibernética en el sector público y privado.

Bajo esas ideas, el enfoque de la corresponsabilidad plantea la construcción de un sistema de protección de datos personales sobre la base de un trabajo cooperativo. Es decir, propone que cada actor asuma -de manera proactiva- sus responsabilidades. De modo que, desde esta visión, el trabajo debería efectuarse al menos en tres ejes: a) armonización y actualización de los ordenamientos jurídicos internos, con el propósito de construir marcos estandarizados de tutela efectiva; b) fomento de la responsabilidad proactiva de los encargados del tratamiento; y, c) reconocimiento de derechos y obligaciones para los titulares; así como los procedimientos que permitan materializar la norma (Maqueo Ramírez et al., 2017).Por otro lado, la visión de resiliencia informática o cibernética, propuesta por el Foro Económico Mundial en 2012, propone abandonar la visión de seguridad cibernética, que únicamente busca mitigar las amenazas de las TIC. En esta nueva corriente, la prevención

de riesgos y la corresponsabilidad de todos los actores de la sociedad son componentes fundamentales para consolidar un verdadero sistema de protección de derechos (Orellana Robalino, 2017). En dicho contexto, el Foro propone cuatro principios: a) Interdependencia, que implica que todos los actores sociales contribuyan en el proceso de construcción de un espacio digital resiliente; b) Autorregulación, según el cual los líderes institucionales deben promover la gestión del riesgo cibernético; c) Gestión integrada del riesgo, mediante programas que son evaluados y redefinidos permanentemente; y, d) Promoción de la corresponsabilidad, que consiste en fomentar altos niveles de conciencia y responsabilidad en todas las partes interesadas (Foro Económico Mundial, 2012).

En ese sentido, la resiliencia cibernética insta a fortalecer las prácticas de ciberseguridad, con el objetivo de prevenir ataques o vulneraciones a los sistemas de procesamiento de información. A su vez, promueve el diseño e implementación de estrategias de recuperación inmediata, que permitan minimizar los efectos propios de las amenazas digitales. En otras palabras, el diseño de programas resilientes implica fusionar dos visiones distintas, una preventiva y otra reactiva. Sin embargo, este enfoque no fue diseñado para proteger los datos personales, sino los datos en general, que constituyen un factor fundamental para el desarrollo socio-económico. A pesar de ello, autores como De Salvador Carrasco (2015) y Orellana (2017) proponen la adopción de programas de resiliencia informática en instituciones públicas y privadas, que manejan datos personales; a fin de que, los responsables del tratamiento adopten medidas preventivas que proporcionan mayores niveles de seguridad; ya que, cuentan con especificaciones técnicas, procedimentales y organizativas.

Tras la revisión de estos nuevos enfoques, se infiere que los retos y riesgos de la era digital son cada vez mayores y, por ende, es imprescindible desarrollar mecanismos de protección acordes a los fenómenos cibernéticos. En ese sentido, entre los desafíos más importantes están: a) Desactualización normativa, generada por el rápido desarrollo tecnológico que está modificando todas las formas de interrelación humana. Entre las nuevas tecnologías destacan la inteligencia artificial, el cloud computing y Big Data, cuya potencialidad real aún es desconocida; b) Falta de observancia del principio de minimización de datos, por parte de los encargados de procesarlos; ya que, en la práctica, el levantamiento de información es excesivo; c) Resistencia a adoptar mecanismos de autorregulación, por parte de los responsables de tratamiento; d) Exceso de confianza en la figura del consentimiento informado del titular, quien autoriza la recolección desmedida de sus datos; debido a que, la lectura -a consciencia- de las políticas de privacidad no es una práctica común y, e) Sistemas de sanción débiles por cuanto establecen únicamente sanciones administrativas, que no constituyen un sistema disuasorio efectivo (Martínez-Martínez, 2018).

## 5. Conclusiones

En definitiva, el reconocimiento del derecho a la protección de datos personales supone un proceso complejo, que inició a finales del siglo XIX, en los Estados Unidos; con el objetivo de repensar el derecho a la privacidad, en un contexto de creciente desarrollo tecnológico. De ahí que, durante el siglo XX, varios países europeos y latinoamericanos hayan concebido, a nivel constitucional y legal, el derecho a la autodeterminación informativa como dependiente de la vida privada. Sin embargo, a inicios del siglo XXI, la Unión Europea reconoció el carácter fundamental, autónomo e independiente de este nuevo derecho; consecuentemente, los Estados de Europa y América repensaron este derecho y, paralelamente, construyeron sistemas de protección dotados de mecanismos e instrumentos de tutela efectiva. A pesar de ello, las dinámicas propias de la era digital han provocado que las reglas legales se reformulen constantemente; con el objetivo de, prevenir y mitigar los peligros cibernéticos.

A nivel internacional, los Estados han plasmado su preocupación por las amenazas digitales en múltiples instrumentos internacionales, que tienden a promover altos estándares de protección de datos personales. Así, en el seno de la ONU, la Unión Europea y la OEA se han promulgado una serie de principios básicos que los Estados miembros deberían observar para diseñar, reformar o actualizar sus leyes; puesto que, estos organismos reconocen la necesidad de contar con ordenamientos jurídicos armónicos, que no solo tutelen los derechos fundamentales del ciudadano, sino que también faciliten el flujo transnacional de información, indispensable para fomentar el desarrollo socio-económico.

En Ecuador, el reconocimiento constitucional del derecho a la protección de datos personales es reciente; por cuanto, la Constitución de 2008 le otorgó el estatus de derecho fundamental y autónomo. Sin embargo, el texto constitucional no determinó los alcances ni los mecanismos para su ejercicio y, por ende, se requería de una ley orgánica que defina claramente los componentes del sistema de protección de este derecho. Consecuentemente, en el marco del Plan Ecuador Digital 2021, la Ley Orgánica de Protección de Datos Personales fue promulgada el 26 de mayo de 2021 y, con ello, se establecieron los principios rectores del sistema, los derechos y obligaciones de los actores involucrados, la institucionalidad, los mecanismos y medios para ejercer derechos y, el régimen de sanciones.

A pesar de la legislación existente, la experiencia internacional demuestra que los riesgos y las amenazas cibernéticas crecen exponencialmente, conforme evolucionan las TIC. Muestra de ello es la tipificación de los delitos informáticos, que no solo afectan los derechos de protección de datos personales y de intimidad, sino que también suponen la vulneración de otros derechos fundamentales, como la vida, la salud o el trabajo. Por ello, la

Academia y los organismos internacionales proponen adoptar nuevos enfoques de protección, que promueven: a) la prevención antes que la reacción o corrección, b) la responsabilidad proactiva de los encargados del tratamiento, c) la corresponsabilidad ciudadana y, d) la armonización normativa.

## Referencias


Agencia Española de Protección de Datos. (2018). *Protección de datos y prevención de delitos*. https://www.aepd.es/es/documento/guia-proteccion-datos-y-prevencion-de-delitos.pdf

Araujo Carranza, E. (2009). El derecho a la información y la protección de datos personales en el contexto general y su construcción teórica y jurídica. *IUS. Revista del Instituto de Ciencias Jurídicas de Puebla A.C.*, *23*, 174-213. https://www.redalyc.org/articulo.oa?id=293222963009

Principios rectores para la reglamentación de los ficheros computarizados de datos personales, Resolución 45/95 (1990). http://www.ordenjuridico.gob.mx/TratInt/Derechos Humanos/OTROS 15.pdf

Código Orgánico Integral Penal, (2021). https://tinyurl.com/2p8nuhs6

Ley Organica e Protección de Datos Personales, (2021).

Avendaño, X., Ayo, M., Chiluiza, J., Veintimilla, N., Donoso, E., Espinosa, A., Fernández, C., Guzmán, D., Jácome, K., Lalangui, D., Malla, R., Ortega, J., Rivera, O., Simbaña, F., Tituaña, N., Torres, J., Valverde, A., & Vera, J. (2018). *Plan de la Sociedad de la Informacion y del Conocimiento 2018-2021*. Ministerio de Telecomunicaciones y de la Sociedad de la Información. https://tinyurl.com/3bxppy6n

Brian Nougrères, A. (2012). La protección inteligente de los datos personales: *Revista Internacional de Protección de Datos Personales*, *1*, 1-15. https://tinyurl.com/57xv9ztt

Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas, CJI/RES. 186 (LXXX-O/12) (2012). http://www.oas.org/es/sla/cji/docs/CJI-RES_186_LXXX-O-12.pdf

Guía Legislativa sobre la privacidad y la protección de datos personales en las Américas, (2015). http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_Guia_Legilsativa_CJI.pdf

El derecho a la privacidad en la era digital, Resolución aprobada por el Consejo de Derechos Humanos 28/16 (2015). https://doi.org/10.18268/bsgm1908v4n1x1

Constitución de Brasil, (1988). https://www.constituteproject.org/constitution/Brazil_2017.pdf?lang=es

Constitución de la República del Ecuador, Pub. L. No. Registro Oficial No. 449 del 20 de octubre de 2008 (2008). http://bit.ly/2LVz1Tf

Constitución Política de Colombia, (1991). https://pdba.georgetown.edu/Constitutions/Colombia/colombia91.pdf

Constitución Política de los Estados Unidos Mexicanos, Diario Oficial de la Federación el 5 de febrero de 1917 (2007). http://www.upsin.edu.mx/assets/archivos/const_pol_mex.pdf

Constitución Política del Estado, Constitución Política del Estado (CPE) (7-Febrero-2009) 1 (2009). https://www.oas.org/dil/esp/constitucion_bolivia.pdf

Cué Brugueras, M., Díaz Alonso, G., Díaz Martínez, A. G., & de la C. Valdés Abreu, M. (2008). El artículo de revisión. *Revista Cubana Salud Pública*, *34*(4). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-34662008000400011

Day, R. (2005). Cómo escribir y publicar trabajos científicos. En *Publicación Científica y Técnica* (Número 598). https://www.paho.org/hq/dmdocuments/como-escribir-escritos-cientificos-2010.pdf

De Salvador Carrasco, L. (2015). Ciber-Resiliencia. *Instituto Español de Estudios Estratégicos*, *35*, 1-15. https://tinyurl.com/2p9yh7kr

DLA Piper. (2021). *Data protection laws of the world*. https://www.dlapiperdataprotection.com/

Enríquez Álvarez, L. (2017). Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. *FORO. Revista de Derecho*, *27*, 42-61. https://revistas.uasb.edu.ec/index.php/foro/article/view/500/487

Foro de Cooperación Económica Asia Pacífico. (2004). *Marco de privacidad del foro de cooperación Asia Pacífico (APEC)*. https://archivos.juridicas.unam.mx/www/bjv/libros/12/5669/19.pdf

Foro Económico Mundial. (2012). *Asociación por la resiliencia cibernética*. http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012_SP.pdf

García González, A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. *Boletín Mexicano de Derecho Comparado*, *120*, 743-778. https://www.redalyc.org/articulo.oa?id=42712003

Garriga Domínguez, A. (2016). *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua* (1.ª ed.). Dykinson, S.L. https://www.jstor.org/stable/j.ctt1k85c6p

Gil, E. (2015). *Big data, privacidad y protección de datos*. Agencia Española de Protección de Datos.

Guirao-Goris, J. A., Olmedo Salas, Á., & Ferrer Ferrandis, E. (1989). El artículo de revisión. *Medicina clinica*, *93*(19), 43-44. https://www.uv.es/joguigo/valencia/Recerca_files/el_articulo_de_revision.pdf

Icart, M. T., & Canela, J. (1994). El artículo de revisión. *Enfermería clínica*, *4*(4), 180-184.

Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales. (2016). *Guía práctica para ejercer el derecho a la protección de datos personales*. https://sistemas.cgever.gob.mx/2016/pdf/GuiaPracticaEjercerelDerecho.pdf

Maqueo Ramírez, M. S., Moreno González, J., & Recio Gayo, M. (2017). Protección de datos personales, privacidad y vida privada: La inquietante búsqueda de un equilibrio global necesario. *Revista de Derecho*, *30*(1), 77-96. https://doi.org/10.4067/S0718-09502017000100004

Martínez-Martínez, D. F. (2018). Unification of personal data protection in the European Union: Challenges and implications. *Profesional de la Informacion*, *27*(1), 185-194. https://doi.org/10.3145/epi.2018.ene.17

Martínez Devia, A. (2019). La inteligencia artificial, el Big Data y la era digital: ¿una amenaza para los datos personales? *Revista La Propiedad Inmaterial*, *27*, 5-23. https://revistas.uexternado.edu.co/index.php/propin/article/view/6071/7789

Acuerdo Minsiterial 012-2019, (2019). https://tinyurl.com/2p8h844n

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2021). *Agenda digital del Ecuador*. https://tinyurl.com/y56tzbb2

Ministerio de Telecomunicaciones y Sociedad de la Infomración (MINTEL). (2018). *Libro Blanco de la Sociedad de la Información y del Conocimiento*. Ministerio de Telecomunicaciones y Sociedad de la Infomración (MINTEL). https://tinyurl.com/387wtcn7

Ministerio de Telecomunicaión y de la Sociedad de la Informcación. (2018). *Plan Nacional de Gobierno Electrónico 2018-2021*. Ministerio de Telecomunicaciones y de laSociedad de la Información. https://tinyurl.com/4ur5mwcp

Muriel Bedoya, B. S. (2017). Compliance: su evolución y desafíos en Ecuador: ¿Hacia dónde ir? *USFQ Law Review*, *IV*, 159-183. https://doi.org/10.18272/lr.v4i1.993

Naranjo Godoy, L. (2017). El dato personal como presupuesto del derecho a la protección de datos personales y hábeas data en Ecuador. *Foro. Revista de Derecho*, *27*, 63-82. https://revistas.uasb.edu.ec/index.php/foro/article/view/501/488

Ojeda Bello, Z. (2015). El derecho a la protección de datos personales desde un análisis histórico-doctrinal. *Tla-Melaua. Revista de Ciencias Sociales*, *9*(38), 58-70. https://doi.org/10.32399/rtla.9.38.82

Orellana Robalino, C. (2017). De la seguridad cibernética a la resiliencia cibernética aplicada a la protección de datos personales. *Foro, Revista de Derecho*, *27*, 5-21. https://revistas.uasb.edu.ec/index.php/foro/article/view/498

Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales, Pub. L. No. 326- 04- 034-7 (1980). http://www.oas.org/es/sla/ddi/docs/directrices_ocde_privacidad.pdf

Oró Badia, R. (2016). *La protección de datos*. Universitat Oberta de Catalunya. https://www.digitaliapublishing.com/a/43996/la-proteccion-de-datos

Carta de Derechos Fundamentales de la Unión Europea, Pub. L. No. 2000/C 364/01, Diario Oficial de las Comunidades Europeas 145 (2000). https://www.europarl.europa.eu/charter/pdf/text_es.pdf

Reglamento general de protección de datos, 78 (2016). https://tinyurl.com/26p22k49

Protocolo de Adhesión del Acuerdo Comercial entre la Unión Europea y sus Estados Miembros, por una parte, y Colombia y el Perú, por otra, para tener en cuenta la adhesión de Ecuador, (2016). https://tinyurl.com/u977adn8

Pulido, M. (1989). El artículo de revisión. *Medicina clínica*, *93*(19), 43-44. http://158.227.10.240/Fundamentos/Doctorado/cursos/Metodo/MedClin89a.pdf

Quiroz Papa de García, R. (2016). El Hábeas Data, protección al derecho a la información y a la autodeterminación informativa. *Letras (Lima)*, *87*(126), 23-49. https://doi.org/10.30920/letras.87.126.2

Estrategia de la Red Iberoamericana de Datos Personales 2020, (2016). https://www.redipd.org/sites/default/files/inline-files/Texto_definitivo_RIPD_2020.pdf

Estándares De Protección De Datos Personales Para Los Estados Iberoamericanos, (2017). https://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf

Red Iberoamericana de Protección de Datos. (2020). *Plan estratégico2021-2025 Red Iberoamericana de Protección de Datos (RIPD)*. https://www.redipd.org/sites/default/files/2020-12/Plan-Estrategico-RIPD-2021-2025.pdf

Remolina Angarita, N. (2012). Aproximación constitucional de la protección de datos personales en Latinoamérica. *Revista Internacional de Protección de Datos Personales*, *1*, 1-13. https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf

Vásquez, L. A. (2020). *Sexting y el riesgo de victimización*. Biblioteca Derecho Ecuador. https://derechoecuador.com/sexting-y-el-riesgo-de-victimizacion/

Declaración de Santa Cruz de la Sierra, (2003). https://www.segib.org/wp-content/uploads/DeclaraciondeSantaCruz.pdf