SITUACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR

SITUATION OF PERSONAL DATA PROTECTION IN ECUADOR

SITUAÇÃO DA PROTEÇÃO DOS DADOS PESSOAIS NO EQUADOR

*Lorena Naranjo**

Recibido: 01/05/2020
Aprobado: 10/06/2020

Resumen

Durante los últimos años, se han suscitado en el Ecuador hechos que evidencian trasgresiones al derecho a la protección de datos personales. Si bien, desde el año 2008, la Constitución de la República consagra en el numeral 19 del artículo 66 tal derecho, no se ha dictado ninguna normativa específica que desarrolle su contenido, regule los principios que lo gobiernan y establezca sanciones a los responsables de un mal tratamiento de datos. La normativa vigente es dispersa, sectorial y contradictoria, de forma que es necesaria la promulgación inmediata de una ley que permita garantizar una protección integral de los individuos en su manifestación digital.

Palabras clave: Derecho a la protección de datos personales; Privacidad; Datos personales; Responsable de tratamiento; Titular del dato personal

Summary

During the last few years, facts have arisen in Ecuador that evidence transgressions of the right to personal data protection. Although, since 2008, the Constitution of the Republic has enshrined the aforementioned right in paragraph 19 of article 66; however, no specific regulations have been issued to develop its content, regulate the principles governing it and establish the responsibilities of those responsible for processing it. The regulations in force are dispersed, sectoral and contradictory, and it is therefore necessary to enact a law immediately to guarantee comprehensive protection of individuals in their digital manifestations.

Key words: Right to protection of personal data; Privacy; Personal data; Responsibility; Subject of right to protection of personal data

Resumo

Durante os últimos anos, no Equador ocorreram fatos que evidenciam transgressões ao direito a proteção de dados pessoais. Mesmo que no ano de 2008, a Constituição da Republica prevê no numeral 19 dos artigos 66 tal direito, não se publicou nenhuma normativa específica que desenvolve seu conteúdo, regule os princípios que o direcionem e estabeleça sanções aos responsáveis de um mal tratamento de dados. A normativa vigente é dispersa, direcional e contraditória, de forma que é necessário a promulgação imediata de uma lei que permita garantir uma proteção integral dos indivíduos em sua manifestação digital.

Palavras chave: Direito a proteção de dados pessoais; Privacidade; Dados pessoais; Responsável no tratamento; Titular do dado pessoal

* La autora es Magíster en Derecho de Nuevas Tecnologías y candidata a PhD en Ciencias Jurídicas y Políticas por la Universidad Pablo de Olavide de Sevilla. Se desempeña actualmente como docente de la Universidad de las Américas y como Directora Nacional de Registro de Datos Públicos del Ecuador. Correo electrónico: lorena.naranjo@udla.edu.ec

LA PROTECCIÓN DE DATOS PERSONALES EN EL MARCO JURÍDICO ECUATORIANO

1. Realidad ecuatoriana

En Ecuador existe, como práctica arraigada, la realización de sorteos, para los cuales se solicita, de forma presencial, telefónica o por medio de promociones en cadenas de comercio, datos personales que, después, serán usados para finalidades completamente distintas a las propuestas inicialmente. También es común la oferta de premios, regalos o cenas que captan a futuros clientes, a los que se les exige portar su tarjeta de crédito para adquirir productos; de negarse a pagar, en muchos casos, se cobra las supuestas recompensas, y, en varios otros, pueden incluso propiciarse situaciones de maltrato. Varias personas han denunciado estas acciones abusivas, evidenciándolas incluso como fraude, porque aseguran que firmaron documentos para retirar un supuesto agasajo y resultó que firmaban un *voucher* de consumo. Todas estas situaciones se producen porque existen bases de datos personales que se usan para vender o promocionar la adquisición de bienes o servicios, ya sea por medios físicos o telemáticos. Ni en los documentos escritos, ni en los contactos telefónicos o electrónicos existe un espacio disponible para registrar la voluntad del titular de entregar los datos, y menos aún se transparenta el motivo de la recolección, ni los propósitos para los cuales se utilizará la información. De igual modo es común recibir publicidad escrita, virtual y telefónica no solicitada. Además, es abrumador el crecimiento del *telemarketing*, que interrumpe jornadas laborales para ofrecer diversidad de productos. Este comportamiento abusivo motiva a no contestar números desconocidos, ante la posibilidad de que sean promociones u ofertas de productos[1].

Es evidente que en Ecuador existe un mercado negro de base de datos personales; se comercializan incluso mediante páginas de comercio electrónico. En este sentido, se han presentado varias denuncias penales que actualmente se hallan en proceso de indagación previa para investigar estos hechos fácticos y sus responsables[2].

Asimismo, se producen transgresiones que no han sido reconocidas como un atentado al derecho a la protección de datos personales. Por ejemplo, en 2014, un ciudadano denunció a la Defensoría del Pueblo del Ecuador que un Banco le negó la creación de una cuenta de ahorros, debido a que constaba dentro de la base de datos de personas indiciadas, procesadas y sentenciadas por ilícitos sancionados en la Ley de Sustancias Estupefacientes y Psicotrópicas. Y es que esta base de datos se encuentra a disposición de todas las entidades bancarias, sin que medie autorización del titular, mandato de ley u orden judicial que habilite su tratamiento[3].

Cesiones de datos personales no aprobadas por sus titulares, entre bancos y aseguradoras, que han propiciado cobros indebidos por servicios no autorizados, han producido un reclamo generalizado de la sociedad ante la falta de controles en distintos niveles que revelan atentados contra los derechos de los consumidores, cuenta ahorristas o usuarios de la banca, así como contra titulares de datos personales[4].

Por otro lado, la sociedad ecuatoriana y el Estado también han sufrido la ausencia de esta normativa con varios sucesos que han causado conmoción social. Uno

1 "Ecuador no tiene ley para proteger datos personales", *El Universo*, 29-IV-2018, https://www.eluniverso.com/noticias/2018/04/29/nota/6736146/ecuador-no-tiene-ley-proteger-datos-personales.

2 Interceptación ilegal de base de datos. Proceso N°. 170101818064001. Fiscalía N°. 3 – Unidad para Descubrir Autores, Cómplices y Encubridores. Denunciante DINARDAP, denunciado desconocido. Quito-Ecuador. Revelación ilegal de bases de datos. Proceso N°. 170101818060469. Fiscalía de Soluciones Rápidas N°. 2. Denunciante DINARDAP, denunciado desconocido. Quito-Ecuador. Revelación ilegal de bases de datos. Proceso N°. 170101819072102. Fiscalía de Soluciones Rápidas N.° 7. Denunciante DINARDAP, denunciado DataBook. Quito-Ecuador. Revelación ilegal de bases de datos. Proceso N°. 170101819100071. Fiscalía de Soluciones Rápidas N.° 3. Denunciante DINARDAP, denunciado Novaestrat. Quito-Ecuador. Acceso no consentido a un sistema informático (base de datos). Proceso N°. 170101819110653. Fiscalía de Soluciones Rápidas N°. 3. Denunciante DINARDAP, denunciado Equivida. Quito-Ecuador.

3 Defensoría del Pueblo. Resolución N°. DPE-DGT-DNAPD-16-2014-DO, *CONSEP*, Trámite N°. DPE-DGT-DNAPD-133-2013-DO, 22-X-2014.

4 "Débitos no autorizados molestan a los clientes", *Expreso*, accedido el 24-X-2018, https://www.expreso.ec/economia/debitos-no-autorizados-molestan-a-los-cliente-NAgr_4581611.

de ellos se generó el 31 de octubre de 2017, cuando, tras un operativo realizado en Santo Domingo de los Tsáchilas, se logró determinar que personas inescrupulosas se hicieron pasar por beneficiarios del Bono de Desarrollo Humano y cobraron indebidamente 8.000.000 de dólares, en base al uso inadecuado de los datos personales que contenía una base del Ministerio de Inclusión Económica y Social[5].

Además, en el segmento semanal *El Gobierno Informa*, el propio presidente de la República, Lenín Moreno, el 29 de enero de 2018, informó a la ciudadanía del robo de la base de datos del Plan Toda una Vida, que contenía datos sensibles como nombres y contactos de varias personas y que se usa tradicionalmente para la entrega de beneficios sociales. Este delito tuvo la finalidad de usar la información extraída para enviar "un mensaje malicioso a 400.000 [...] ecuatorianos convocándoles a recibir la asignación de una casa"; información falsa que pretendía repercutir de forma negativa en la percepción popular y el apoyo al presidente, y en consecuencia directamente en la consulta popular realizada en ese año[6].

En otro hecho, en el mes de marzo de 2018, se denunció que los sistemas de la Agencia Nacional de Tránsito fueron vulnerados, al modificarse fraudulentamente la base de datos de la institución. El resultado fue que falsificadores y tramitadores entregaran 15.970 licencias de conducir de manera ilegal[7].

La alta exposición en redes sociales de problemáticas privadas y la subsecuente entrega masiva de datos personales, también supone un riesgo para la integridad de sus titulares. Y los más vulnerables son las niñas, niños, adolescentes e incluso adultos mayores, quienes no son del todo conscientes de los riesgos que asumen en el manejo de estas herramientas.

El 16 de septiembre de 2019, tras un informe de los investigadores de ZDnet y VPNmentor, expuestos en sus respectivos blogs, se reveló la exposición de datos de 20 millones de ecuatorianos, incluso de personas que ya habían fallecido.

La falta de incorporación de medidas de seguridad a los servidores, ubicados en Miami, de Novaestrat, una empresa ecuatoriana dedicada al análisis de datos; se expusieron nombres, correos electrónicos, números de teléfono, estado civil, datos bancarios, de automóviles, entre otros. En ellos se incluía información de 6.7 millones de niñas, niños y adolescentes, datos sensibles, como género o número de cuentas bancarias, así como datos detallados de familiares de titulares de la información, como dirección de residencia, números de seguros y cédulas[8], conforme señalan diversas notas periodísticas, ya que el proceso penal sigue en marcha.

Por este motivo, la Asamblea Nacional del Ecuador solicitó a la Comisión N°. 5, Especializada Permanente en Soberanía, Integración, Relaciones Internacionales y Seguridad Integral, que realizara un informe para dar cumplimiento a la Resolución del Pleno de la Asamblea Nacional de 17 de septiembre de 2019, que ordenaba investigar y determinar responsabilidades frente al caso de la filtración de datos de ciudadanos ecuatorianos. Dicho informe fue emitido el 11 de mayo de 2020 y, entre sus recomendaciones, estableció: "El manejo de datos personales en Ecuador carece de un marco jurídico que lo respalde para sus diferentes actuaciones, por ello, es necesario una reforma integral a la Ley Orgánica de Transparencia y Acceso a la Información Pública y al Código Orgánico Integral Penal con el objetivo de que todas las instituciones públicas y privadas desarrollen eficazmente sus competencias, y de no hacerlo, existan las sanciones correspondientes"[9].

5 "$ 8'000.000 del Bono de Desarrollo Humano habrían sido cobrados indebidamente; hay siete detenidos", *El Universo*, accedido 25-X-2018, https://www.eluniverso.com/noticias/2017/10/31/nota/6459943/8000000-bono-desarrollo-humano-habrian-sido-cobrados-indebidamente.

6 "Lenín Moreno denuncia el robo de la base de datos del Plan Toda Una Vida", *El Comercio*, accedido 25-X-2018, https://www.elcomercio.com/actualidad/leninmoreno-denuncia-robo-basededatos-plan.html.

7 "8.582 conductores portan licencias tipo 'B' ilegales", *El Telégrafo*, 28-III-2018, https://www.eltelegrafo.com.ec/noticias/judicial/12/conductores-licencias-ilegales.

8 "BBC revela filtración de datos sensibles de millones de ecuatorianos", *El Comercio*, accedido 25-IX-2019, https://www.elcomercio.com/tendencias/datos-ecuatorianos-filtracion-reporte-seguridad.html

9 Comisión No. 5, Especializada Permanente de Soberanía, Integración Relaciones Internacionales y Seguridad Integral, Informe para dar cumplimiento a la Resolución del Pleno de la Asamblea Nacional de 17-IX-2019.

Resulta evidente que existe una marcada falta de interés en reclamar este tipo de agresiones a la protección de datos personales, debido al desconocimiento de las personas de este derecho que les asiste, de la forma en que sus datos deben usarse de forma adecuada, de la entidad responsable de atenderles, del tipo de trámite y de las reales consecuencias que se derivan de iniciar estos procesos. Además, media el gasto desmesurado que presentan estas acciones penales y de otras que no llegan a revestir condiciones de antijuridicidad suficiente para convertirse en delito, pero que son afectaciones al consumidor y que, al considerarse de bagatela, tampoco son objeto de reclamo.

Sumado a estos problemas, si bien existen acciones constitucionales como el *habeas data,* estas no se han desarrollado y no permiten la defensa real de derechos, sino que se decantan por soluciones procesales o limitadas al acceso y rectificación de datos en sus respectivas bases. Pero estas nunca emprenden la verificación de si de facto se producen discriminaciones, barreras de acceso a derechos fundamentales, valoraciones automatizadas o brechas de seguridad, que pudieran afectar la integridad de la persona titular del dato.

En este asunto, queda en evidencia la sociedad ecuatoriana como inconsciente de sus derechos, ignorante del contenido esencial de la protección de datos personales. Es más, pese a que la ciudadanía presiente que algo es incorrecto y no funciona de manera adecuada, desconoce los riesgos que el uso indebido o incluso indiscriminado de sus datos puede acarrear no solo en el ámbito de sus derechos de personalidad como intimidad, imagen, honor u honra y protección de datos personales; sino también respecto a otros derechos.

En efecto, las valoraciones automatizadas o la existencia de datos erróneos que consten antes en dichas bases podrían impedir su acceso a la vivienda, trabajo, educación, salud, entre otros.

Ejemplos palpables de esta realidad se suscitan cuando una condición de deudor equivocada consta plasmada en una base de datos, y el ciudadano común no logra identificar el mecanismo que le permita borrar ese dato erróneo. Y, peor aún, como consecuencia de estos deslices, se han iniciado trámites coactivos que podrán repercutir en su economía hasta el punto de impedirle el acceso a créditos o afectar incluso su remuneración.

2. Insuficiencia y contradicciones de la legislación ecuatoriana sobre protección de datos personales

En el año 2008, el Ecuador consagró como derecho fundamental la protección de datos de carácter personal. Sin embargo, diez años después, no se ha promulgado una norma que desarrolle su contenido. No obstante, los derechos constitucionales son de aplicación directa al tenor de lo dispuesto en el artículo 11 numeral 3 de la Constitución que señala:

> Art. 11.- El ejercicio de los derechos se regirá por los siguientes principios: [...] 3. Los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos serán de directa e inmediata aplicación por y ante cualquier servidora o servidor público, administrativo o judicial, de oficio o a petición de parte. Para el ejercicio de los derechos y las garantías constitucionales no se exigirán condiciones o requisitos que no estén establecidos en la Constitución o la ley.
> Los derechos serán plenamente justiciables. No podrá alegarse falta de norma jurídica para justificar su violación o desconocimiento, para desechar la acción por esos hechos ni para negar su reconocimiento.

Sin embargo, el contenido, alcance, dimensión y forma de eficacia de estos derechos no se pueden materializar por la ausencia de normativas concretas. Tampoco la jurisprudencia ecuatoriana ha desarrollado los elementos necesarios para su operatividad, como son los derechos, los principios, las obligaciones, las infracciones y las sanciones.

En consecuencia, es obligación de la Asamblea Nacional dictar una norma que viabilice la vigencia efectiva del derecho; así como de la Corte Constitucional, la de dictar resoluciones que definan los matices de este derecho. La única resolución

vinculante emitida por la Corte Constitucional[10], que analiza el derecho a la protección de datos personales y las cuestiones procedimentales del *habeas data*, es la sentencia 001-2014-PJO-CC, expedida en el año 2014. En ella, se analizan, a nivel de los *obiter dicta*, varias temáticas, como el derecho a la autodeterminación informativa y la comprensión del concepto de dato personal. Pero, en la *ratio decidendi*, se limita a temas procedimentales del *habeas data* y no aborda temáticas fundamentales como la necesidad de establecer principios de tratamiento que garanticen el derecho. Por tanto, tampoco la jurisprudencia ha podido disponer de un sistema de protección jurisprudencial, como se ha intentado en países como El Salvador o Paraguay.

Como se ve, desde la vigencia de la Constitución de Montecristi, ninguna de estas dos posibilidades de regulación, por vía legislativa o jurisdiccional constitucional, se ha producido. Además, se ha avanzado muy poco en regulaciones de nivel inferior, en resoluciones de autoridad pública o jurisprudencia del ámbito ordinario que determinen un marco de aplicación mínimo para la vigencia de este derecho; de suerte que, en este terreno, hay un espacio de desprotección que debe corregirse.

Si bien existe normativa sectorial, que en algo pretende poner en práctica la disposición constitucional, ésta, lejos de aclarar el alcance del derecho a la protección de datos personales, demuestra lo dispersa, contradictoria e incompleta que es nuestra legislación en esta temática. Incluso una parte de ella se halla desactualizada, porque está asociada a la visión inicial de salvaguarda anclada en la intimidad que imperaba en la Constitución de 1998, como ocurre con el artículo 9 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; o es de aplicación exclusivamente restrictiva a ciertos ámbitos específicos, como las normas contenidas en la Ley de Telecomunicaciones o el Código Orgánico Integral Penal.

Adicionalmente, el sistema de protección de datos personales en Ecuador se limita entonces a la garantía constitucional del *habeas data*. La problemática de este sistema es que la garantía jurisdiccional, si bien evita transgresiones directas mediante los derechos de acceso, rectificación, cancelación y oposición, no permite proteger otros derechos que pueden verse conculcados. Aunque se han dictado varias resoluciones relativas a *habeas data*, esta garantía constitucional presenta una evidente limitación: solo procede ante un posible daño o un daño producido. Es decir, la tutela se restringe a una protección post, cuando existen serias presunciones o ya se ha producido una transgresión, y no establece un sistema de prevención que recoja principios, derechos y obligaciones que deben cumplirse para un adecuado manejo de los datos personales y que, en conjunto, eviten que se produzcan posibles daños.

Adicionalmente, han existido pocas iniciativas y de poco impacto para presentar y discutir proyectos de ley en esta temática. La Asamblea Nacional, en tres ocasiones fallidas, ha intentado discutir un proyecto de ley. Así, en el año 2010, el asambleísta Bethoven Chica propuso el Proyecto de Ley de Protección a la Intimidad y Datos Personales, que fue desestimado en el año 2013, tras recomendación de la Comisión Especializada Permanente de Justicia y Estructura del Estado, debido a que su contenido planteaba una visión asociada a la intimidad.

Conviene decir que esta confusión entre derecho a la intimidad y derecho a la protección de datos personales se encuentra ampliamente superada por la propia Constitución de 2008, que los consagra en distintos numerales, por su contenido autónomo e independiente, y por su ámbito de cobertura diferente. El derecho a la protección de datos personales, si bien nace de la intimidad debido a que se creía que solo era aplicable a la recopilación de datos íntimos en bases informáticas, ahora tiene contenido propio basado en la autodeterminación informativa que empodera al titular para que, bajo su decisión, se entreguen o no datos personales a responsables para su tratamiento. El avance de la tecnología y de la ciencia de datos conlleva no solo que se den abusos en el almacenamiento

10 Corte Constitucional del Ecuador, "Sentencia 001-2014-PJO-CC", Gaceta Constitucional Nº. 007, 7-III-2014.

de los datos en bases públicas o privadas, sino que se violente la información de las personas, incluso en el acopio de información.

De modo que la protección de datos personales comienza a independizarse y a encontrar autonomía respecto de otros derechos, en la medida en que encuentra un elemento de titularidad y de desarrollo de la personalidad, al descubrir que tenemos una identidad digital y que ésta se halla almacenada en bases de datos o que, debido a los actuales mecanismos de perfilamiento, puede generarse incluso de forma automatizada. Pero, se debe considerar que esta información puede estar desactualizada, ser equívoca e indebidamente tratada para finalidades ajenas a las cuales fue recabada.

En cualquiera de esas situaciones existe la posibilidad de vulnerar derechos fundamentales. Entonces, el derecho a la protección de datos personales se aparta de la intimidad, debido a que, para violentar a la persona no es preciso que exista una agresión a la esfera íntima, es decir, no se necesita que los datos sean íntimos. En efecto, el derecho a la protección de datos personales ampara al individuo, y éste determina su información en el mundo real y en el mundo virtual, incluso con datos que pudieran considerarse irrelevantes o inocuos, pero que, en conjunto, construyen un perfil completo de su personalidad.

El ex presidente de la Función de Transparencia y Control Social durante el año 2013, Fabián Jaramillo Palacios, también máxima autoridad de la Superintendencia de Telecomunicaciones, desarrolló el proyecto de Ley de Protección de Datos y Privacidad, que no se volvió público y tampoco prosperó, porque la promulgación de la Ley Orgánica de Telecomunicaciones en el Registro Oficial (en adelante, R.O.), de 18 de febrero de 2015, eliminó este órgano de control.

En 2016, la entonces presidenta de la Función Legislativa, Gabriela Rivadeneira, presentó la Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales, que el 18 de julio de 2016 fue calificado por el Consejo de Administración Legislativa, en adelante el CAL, mediante resolución CAL-2015-2017-154 y remitido a la Comisión Especializada Permanente de Justicia y Estructura del Estado para su conocimiento[11]. Sin embargo, desde su presentación no se había avanzado con su tramitación, pues no contaba ni siquiera con informe para primer debate. Por su parte, para mayo de 2018, la Dirección Nacional de Registro de Datos Públicos y varias organizaciones civiles presentaron reparos a esta propuesta y, consecuentemente solicitaron su archivo a la citada Comisión. Además, se informó que la Dirección desarrollaba una propuesta que buscaba recoger los principales avances del contenido de este derecho y, además, adaptarse a la realidad ecuatoriana[12].

En todos los casos planteados, la falta de conocimientos técnicos ha derivado en la discusión de estos textos en el plano político con temáticas completamente ajenas al derecho a la protección de datos personales, como la transparencia, la libertad de expresión o el control de redes sociales. Este fenómeno se debe a que, en estas propuestas normativas, se incluyeron normas no compatibles con el Derecho. Además, sus actores se equivocaron respecto a los argumentos de discusión, u omitieron la investigación de realidades ecuatorianas que motiven su promulgación. Por el contrario, optaron por transcripciones de legislaciones de otros países[13], con absurdas adaptaciones que trastocaron el contenido de este derecho hasta tal punto que propusieron como título del proyecto una aberración: "la protección de los derechos a la intimidad y a la privacidad sobre los datos personales", como efectivamente sucedió en el caso del texto propuesto el año 2016[14].

11 Asamblea Nacional, Sistema de Consultas de Propuestas y Proyectos de Ley. Accedido el 09-IV-2020: http://ppless.asambleanacional.gob.ec/alfresco/d/d/workspace/SpacesStore/c7a3a7ab-f233-47c0-bf9a-ba9710b65bec/Memorando%20SAN-2016-2690%20Notificaci%F3n%20Resoluci%F3n%20CAL.pdf

12 "DINARDAP cuestionó el proyecto de Ley de Protección de los Derechos a la Intimidad que analiza la Asamblea Nacional – DINARDAP". Accedido el 09-VIII-2020: https://www.dinardap.gob.ec/dinardap-cuestiono-el-proyecto-de-ley-de-proteccion-de-los-derechos-a-la-intimidad-que-analiza-la-asamblea-nacional/

13 Ibíd.

14 "Gabriela Rivadeneira: 'En ningún momento ley restringirá datos de funcionarios públicos'", *El Comercio*, 16-IX-2016. https://www.elcomercio.com/actualidad/gabrielarivadeneira-ley-datospersonales-ecuador-asamblea.html

En ese escenario, la tarea del legislador, del ejecutivo y de la función jurisdiccional se vuelve indispensable, pues todos en conjunto deben construir paulatinamente los alcances, límites y contornos de este derecho en cada ámbito en el que se aplique. Solo un sistema adecuado de prevención y control, una clara determinación de los derechos de los titulares, de los principios y de las obligaciones que deben cumplir los responsables de las bases de datos, la generación de una institucionalidad propia y de mecanismos de disuasión coercitivos pueden brindarnos un entorno normativo que viabilice el ejercicio de este derecho.

En este contexto, la Dirección Nacional de Registro de Datos Públicos, a fin de garantizar el adecuado funcionamiento del Sistema Nacional de Registro de Datos Públicos, y el respeto y ejercicio del derecho a la protección de datos personales en el intercambio de información de este carácter en la interoperabilidad de conformidad con la Ley Orgánica de Registro de Datos Públicos, con fecha 1-XII-2017, decidió crear el Anteproyecto de Ley Orgánica de Protección de Datos Personales.

Así, en un proceso de construcción participativa, donde todos los actores interesados pudieron hacer aportes a la elaboración de una norma de alto impacto a nivel nacional e internacional, se trabajó en el proyecto que se ejecutó en cuatro fases:

- Primera fase, de diagnóstico, llevada a cabo entre diciembre de 2017 y junio de 2018, en la que se realizó: 1. Identificación de problemática y actores; 2. Elaboración de borrador del anteproyecto para medir el conocimiento del sector y el Ejecutivo; 3. Definición de las estrategias de construcción.

- Segunda fase, de construcción participativa, llevada a cabo entre julio y diciembre de 2018, que incluyó: 1. Planificación de mesas de trabajo; 2. Ejecución de mesas de trabajo a nivel nacional (Quito, Ambato, Ibarra, Cuenca, Guayaquil y Manta); 3. Cooperación internacional (Perú, Colombia y Red Iberoamericana de Protección de Datos Personales); 4. Coordinación de múltiples actores interesados (sociedad civil, sector privado, sector público, academia y organizaciones internacionales).

- Tercera fase, de diálogo, llevada a cabo entre enero y mayo de 2019, en la que se realizaron las siguientes actividades: 1. Lanzamiento del borrador oficial del Anteproyecto de Ley; 2. Análisis e incorporación de observaciones; 3. Versión final Anteproyecto.

- Cuarta fase, de presentación del proyecto de ley, que se llevó a cabo de junio de 2019 a febrero de 2020. En ella se realizaron cuatro acciones: 1. Presentación de la versión final del anteproyecto al Ministerio de Telecomunicaciones; 2. Aprobación del anteproyecto de ley por parte del ministerio de telecomunicaciones y del gabinete sectorial; 3. Aprobación del anteproyecto de ley por parte de la secretaría jurídica de la presidencia; 4. Presentación del Proyecto de Ley de Protección de Datos Personales, a través del Ministerio de Telecomunicaciones y Sociedad de la Información, como ente rector en telecomunicaciones, y de la Dinardap, como entidad responsable de la redacción del texto y adscrita a este Ministerio, a la Asamblea Nacional del Ecuador, el 19 de septiembre de 2019. Seguida de la calificación del CAL el 2 de octubre de 2019 y la asignación a la Comisión de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral, como responsable de su tramitación. Así mismo, el CAL en su resolución CAL-2019-2021-099 dispuso que la Comisión Especializada de Justicia y Estructura del Estado que hasta entonces tenía bajo su conocimiento el proyecto de Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales, remita dicho texto a la Comisión de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral para que, de ser el caso, se unifique con el proyecto ahora presentado y se continúe con su tratamiento.

Adicionalmente, la Comisión N°. 5 Especializada Permanente, la de Soberanía, Integración Relaciones Internacionales y Seguridad Integral, el 11 de mayo de 2020, realizó el informe para dar cumplimiento a la resolución del Pleno de la Asamblea Nacional de 17 de septiembre de 2019, que ordenaba investigar y determinar responsabilidades frente al caso de la filtración de datos de ciudadanos ecuatorianos. En sus recomendaciones se señaló: "Dar seguimiento y celeridad al tratamiento de los proyectos de ley correspondientes

a la materia de protección de datos personales, ya que son herramientas necesarias para Ecuador"[15]. Actualmente, la Comisión se encuentra en proceso de socialización y tratamiento del texto propuesto para elaboración del informe para primer debate.

Asimismo, como parte del proceso de la elaboración normativa, la Dinardap, ente que en su momento elaboró el anteproyecto de ley, incide constantemente en la construcción de una cultura de protección de datos personales. Y, con miras a lograrla, realiza campañas de difusión para que la ciudadanía pueda exigir sus derechos, los responsables del tratamiento conozcan sus obligaciones, así como para informar sobre el avance del proceso de elaboración del proyecto de ley y sobre los beneficios de esta normativa para el Ecuador.

3. Normativa sectorial sobre protección de datos personales en Ecuador

Con la finalidad de verificar la normativa dispersa que se debe considerar en la elaboración de un sistema uniforme para la protección de los datos personales, se analizará la normativa vigente relacionada con la temática y las posibles contradicciones o incomprensiones que deben solucionarse en una nueva Ley de Protección de Datos Personales; presentando y discutiendo todos los cuerpos normativos que deben ser reformados para construir un sistema completo, armónico y coherente.

3.1 Ley de Comercio Electrónico, Firmas y Mensajes de Datos[16]

El artículo 9 de la Ley de Comercio Electrónico y Firmas Electrónicas establece que:

> Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato. El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

A través de esta norma se pretendía señalar que el Ecuador contaba con legislación que protegía los datos personales. Mas, como su contenido es desactualizado e incompleto, los responsables del tratamiento de datos no conciben con claridad la problemática actual del manejo de los datos personales ni el deficitario régimen sobre la temática que existe en el Ecuador.

Para comprender esta realidad debemos recordar que la Ley de Comercio Electrónico, Firmas y Mensajes de Datos se promulgó en el año 2002, cuando aún estaba vigente la Constitución de 1998, en la que solo se reconocía a la intimidad como derecho fundamental, de modo que, en el texto transcrito, se confunden los datos personales con los datos íntimos. Para clarificar su sentido, en esta norma se debe eliminar la frase "La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República", y sustituirla por una que diga: "La recopilación y uso de datos personales garantizará los derechos a la protección de datos personales, a la intimidad, la confidencialidad, derecho al honor, a la imagen y a la propia voz, a las libertades individuales

15 Comisión No. 5, Especializada Permanente de Soberanía, Integración Relaciones Internacionales y Seguridad Integral, "Informe para dar cumplimiento a la Resolución del Pleno de la Asamblea Nacional", 17-IX-2019. Revisado el 11-IV-2020.

16 Ecuador, *Ley 67, Ley de Comercio Electrónico, Firmas y Mensajes de Datos*, R.O. Suplemento 577, 17-IV-2002.

y otros derechos fundamentales garantizados por la Constitución de la República del Ecuador, así como permitirá e incentivará el libre flujo informacional". De esta forma se podría alcanzar una actualización y coherencia con la vigente Constitución ecuatoriana de 2008 y, además, una verdadera protección de la dignidad del titular de los datos en el ámbito del comercio electrónico.

Esa norma regula de manera simple e incompleta el tema del consentimiento, de su revocatoria y el de la recopilación de datos personales. Por este motivo hay que modificar también esta parte del articulado vigente mediante el siguiente texto: "Respecto de la recopilación de datos de fuentes accesibles al público y directamente del titular de los datos personales se estará a lo dispuesto en la ley de la materia". Así se produciría una coherencia entre la nueva Ley de protección de datos y la vigente Ley de comercio electrónico.

Por otra parte, el 5.° artículo de la mencionada Ley de Comercio Electrónico resuelve, respecto de los principios de confidencialidad y reserva, que su establecimiento se dará "para los mensajes de datos, cualquiera sea su forma, medio o intención" y, luego, añade que "Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia".

La norma indicada deberá concordar con la nueva normativa de protección de datos en la determinación de las obligaciones que los responsables y encargados de tratamiento deben cumplir, así como con la descripción y alcance del principio de confidencialidad, de manera que se incluyan estas consideraciones.

En el mismo contexto, la disposición general 9.ª de la Ley de Comercio Electrónico, que atañe al glosario de términos, indica, respecto del derecho a la intimidad, que éste "comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados." Así también se refiere como datos personales a los "datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley".

Nuevamente, el concepto de derecho a la intimidad está equivocado, pues invoca en él consideraciones propias del derecho a la protección de datos personales entendidos como datos proporcionados en cualquier relación contra terceros o su divulgación. En este sentido, esta norma debe acoplarse al tenor del artículo 66, numeral 20 de la Constitución de la República del Ecuador de 2008.

Finalmente, el concepto de datos personales debe ser eliminado para invocarse directamente los elementos que constan en la nueva Ley de Protección de Datos Personales.

3.2 Ley Orgánica de Registro de Datos Públicos[17]

La Constitución de la República del Ecuador, en su artículo 18, determina que todas las personas en forma individual o colectiva tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.
2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.

Es decir, es el derecho de las personas a acceder a información pública. Por su parte, el artículo 227 de dicha norma establece que "La administración pública constituye un servicio a la colectividad que se

17 Ley 0, R.O. Suplemento [en adelante, R.O. Suplem.] 162, 31/mar/2010. *Ley del Sistema Nacional de Registro de Datos Públicos*.

rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación". Ahora bien, el Estado no solo almacena datos públicos sino también datos personales que, por disposición de la ley, deben incluirse en registros públicos, con la finalidad de cumplir con principios como el de publicidad registral, seguridad jurídica, y que permiten materializar derechos como los de propiedad, libertad de comercio y empresa, trabajo, entre otros.

Para regular, organizar y sistematizar los registros públicos, en el Suplemento del R.O. 162, del 31 de marzo de 2010, entró en vigencia la Ley Orgánica[18] del Sistema Nacional de Registro de Datos Públicos, por la cual se creó y reguló el Sistema Nacional de Registro de Datos Públicos, en entidades públicas o privadas que administren dichas bases o registros; y su correspondiente entidad responsable: la Dirección Nacional de Registro de Datos Públicos (DINARDAP).

La Ley Orgánica del Sistema Nacional de Registro de Datos Públicos tiene como objetivo regular los registros públicos que manejan las entidades públicas o privadas, garantiza, organiza y normaliza la seguridad jurídica, de forma eficiente y eficaz. Para lograrlo, maneja adecuadamente la transparencia, publicación, accesibilidad a las nuevas tecnologías, relacionadas con el uso de datos en el ámbito registral. Esta ley es aplicable a las instituciones privadas o públicas, que manejen los registros públicos, ya sean de personas naturales o jurídicas. Esta información será entregada de forma general o específica, por escrito o a través de medios electrónicos.

Según el artículo 28 de la misma norma, el Sistema Nacional de Registro de Datos Públicos tiene por finalidad "proteger los derechos constituidos, los que se constituyan, modifiquen, extingan y publiciten por efectos de la inscripción de los hechos, actos y/o contratos determinados por la presente Ley y las Leyes y normas de registros; y con el objeto de coordinar el intercambio de información de los registros de datos públicos".

De ese modo, la Ley del Sistema Nacional de Registro de Datos Públicos establece, entre una de sus prioridades, la creación de un sistema unificado de datos públicos registrables; es decir, el registro de datos respecto de los bienes o patrimonio de las personas naturales o jurídicas por parte de las instituciones del sector público y privado que, actualmente o en el futuro, administren bases o registros de datos públicos. Esta inscripción, respecto de la titularidad de derechos reales asociados a persona o personas determinadas, tendría como finalidad la de plasmar el modo de adquirir el dominio y otros derechos reales de los bienes raíces mediante la denominada tradición; de contribuir a dar publicidad de los actos y contratos en garantía de los derechos de terceros; y de garantizar la autenticidad y seguridad de los títulos, instrumentos públicos y documentos.

El artículo 31, numeral 5, de la norma aludida, establece como atribución de la Dirección Nacional de Registro de Datos Públicos la de "Consolidar, estandarizar y administrar la base única de datos de todos los Registros Públicos, para lo cual todos los integrantes del sistema están obligados a proporcionar información digitalizada de sus archivos, actualizada y de forma simultánea conforme ésta se produzca". El artículo 13 de dicha norma prescribe que:

> La Dirección Nacional de Registro de Datos Públicos, de conformidad con la ley, expedirá las normas técnicas que contengan los estándares, mecanismos y herramientas para precautelar la seguridad, custodia y conservación de la información accesible y confidencial. La integridad y protección de los registros de datos públicos es responsabilidad de las instituciones del sector público y privado, a través de sus representantes legales, y de las personas naturales que directamente los administren.

La Ley Orgánica de Transparencia y Acceso a la Información Pública en el artículo 5 determina que: "Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las

18 Mediante Ley S/N publicada en el Segundo Suplemento del R.O. [en adelante, R.O.]. 843, 3-XII-2012, se dio el carácter de Orgánica a la Ley del Sistema Nacional de Registro de Datos Públicos.

que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado". El artículo 10 de esa ley establece que:

> Es responsabilidad de las instituciones públicas, personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción. Quienes administren, manejen, archiven o conserven información pública, serán personalmente responsables, solidariamente con la autoridad de la dependencia a la que pertenece dicha información y/o documentación, por las consecuencias civiles, administrativas o penales a que pudiera haber lugar, por sus acciones u omisiones, en la ocultación, alteración, pérdida y/o desmembración de documentación e información pública.

El artículo cuarto de dicha ley responde a la responsabilidad de la información al mencionar que:

> [...] las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este proveen toda la información. Las personas afectadas por información falsa o imprecisa, difundida o certificada por registradoras o registradores, tendrán derecho a las indemnizaciones correspondientes, previo el ejercicio de la respectiva acción legal. La Dirección Nacional de Registro de Datos Públicos establecerá los casos en los que deba rendirse caución.

La Ley del Sistema Nacional de Registro de Datos Públicos, que rige a la Dinardap, está encaminada a garantizar la seguridad jurídica, organizar, regular, sistematizar e interconectar la información entre las instituciones que integran el Sistema Nacional de Registro de Datos Públicos (Sinardap). Sin embargo, en tal ley no existe una definición de lo que es un dato público ni su clasificación, razón por la cual se debe revisar su reglamento.

En efecto, la disposición general 7ª. del Reglamento a la Ley del Sistema Nacional de Registro de Datos Públicos relativa a glosario de términos señala: "4. Datos públicos.– Exclusivamente en el ámbito de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, se entenderá como datos públicos, a todo acto y/o información relativa a las personas naturales o jurídicas, sus bienes o patrimonio, sean estos accesibles o confidenciales, generadas del sector público o privado". Esta norma, en particular, debe ser reformada para adaptarla al contenido del derecho a la protección de datos de carácter personal reconocido a nivel constitucional.

Esa misma disposición general 7ª. define, en el numeral 10, dentro de su glosario de términos, que protección de datos es "el procedimiento determinado por la Dirección Nacional de Registro de Datos Públicos para definir la accesibilidad o confidencialidad de los datos, con la finalidad de proporcionar protección jurídica". Es decir, esta norma maneja la confusión de que la protección de datos es un procedimiento, cuando más bien se trata de un doble rol: es un deber u obligación que tiene que cumplir el Estado, como responsable de tratamiento de los datos y garante de este derecho fundamental.

Como ya hemos visto, la legislación ecuatoriana no cuenta con una ley especializada sobre la protección de datos personales. De ahí que la Dinardap haya adoptado, como base jurídica, las leyes y reglamentos citados; aunque, en algunos casos, su contenido pueda llegar a ser confuso, contradictorio o incompleto. Adicionalmente, ha tenido que emitir resoluciones que pretenden establecer parámetros mínimos encaminados al tratamiento de datos registrales, entre los cuales constan datos personales, en las instituciones

que forman parte del Sistema Nacional de Registro de Datos Públicos (Sinardap), es decir en el intercambio e interconexión de datos entre los distintos registros públicos o bases de datos que forman parte de este sistema.

Por ejemplo, la Dinardap emitió la resolución 039-NG-DINARDAP-2016, publicada en el R.O. N°. 896, de 05 de diciembre de 2016, denominada "Norma que establece el procedimiento para la integración de entes registrales, fuentes externas y fuentes internas en el sistema nacional de registro de datos públicos". Su artículo 3 presenta la misma definición de la protección de datos que consta en el reglamento: un procedimiento para la accesibilidad o confidencialidad de los datos que proporciona protección jurídica. Esta misma resolución hace una clasificación de los datos públicos, desde la perspectiva de establecer los parámetros para clasificar la información que es administrada por la Dinardap y no desde un enfoque que permita garantizar la protección de datos como un derecho fundamental. Así, establece datos de carácter accesible, datos públicos y confidenciales, y este tercer ítem es el que más se acerca a una conceptualización de datos personales.

En la resolución 035-NG-DINARDAP-2016, denominada "Norma que regula la clasificación de los datos que integran el sistema nacional de registro de datos públicos", se define a los datos o información de carácter personal como "toda información no pública correspondiente a la persona, por medio de la cual se la pueda identificar, contactar o localizar, entre otras (...)"; pero, como parte de una norma de interoperabilidad, mantiene un enfoque acotado a esta temática específica y, por ende, no es posible su aplicación a bases de datos que no se encuentren integradas al Sinardap.

Por su parte, la Resolución 007-NG-DINARDAP-2019, publicada en el R.O. Edición Especial 835, de 26 de marzo de 2019, titulada "Norma para acceso al sistema nacional de registro de datos públicos", establece el procedimiento de acceso de personas naturales o jurídicas de derecho público y privado, a los datos e información que constan en bases de datos declaradas como Registros de Datos Públicos de las entidades fuentes que forman parte del Sinardap.

De las resoluciones antes citadas se evidencia que los esfuerzos de regulación sobre protección de los datos se limitan solo al tema de interoperabilidad, definida en la disposición general 7.ª, numeral 9, del Reglamento a la Ley del Sinardap, como "el intercambio y uso de información entre dos o más sistemas, aplicaciones o componentes tecnológicos" entre instituciones públicas que forman parte del Sinardap. Esta normativa está orientada la clasificación de datos, como un acto previo a la entrega de la información a otras instituciones, a fin de que éstas presten un servicio público a la ciudadanía.

Por eso, es pertinente analizar la Ley del Sistema Nacional de Registro de Datos Públicos (en adelante LSNRDP). Esta ley tiene por objeto diseñar, implementar, administrar y regular el sistema de registro de datos públicos para conformar una base de datos única de toda la información registral concerniente a personas naturales y jurídicas; también garantizar seguridad jurídica, sistematizar e interconectar la información mediante las nuevas tecnologías[19] y proveer de información válida a la sociedad ecuatoriana[20].

Son parte del sistema quienes actualmente o en el futuro administren bases o registros de datos públicos, por ejemplo: a) las dependencias públicas, desconcentradas, con autonomía registral y administrativa, como el Registro Civil, de la Propiedad, Mercantil, Societario, Vehicular, de naves y aeronaves, patentes, de propiedad intelectual, registros de datos crediticios y los que en la actualidad o en el futuro determine la

19 Ley 0, R.O. Suplem. 162, 31/mar/2010, *Ley del Sistema Nacional de Registro de Datos Públicos*. "Art. 1.- Finalidad y Objeto.- La presente ley crea y regula el sistema de registro de datos públicos y su acceso, en entidades públicas o privadas que administren dichas bases o registros./ El objeto de la ley es: garantizar la seguridad jurídica, organizar, regular, sistematizar e interconectar la información, así como: la eficacia y eficiencia de su manejo, su publicidad, transparencia, acceso e implementación de nuevas tecnologías."

20 Dirección Nacional de Registro y Datos Públicos del Ecuador, "Planificación Estratégica 2015-2017", 2015, http://www.datospublico.gob.ec/wp-content/uploads/downloads/2016/02/PLANIFICACI%C3%93N-ESTRAT%C3%89GICA-2015-2017.pdf

Dirección Nacional de Registro de Datos Públicos[21]; b) las instituciones del sector privado; y también, c) las personas usuarias de los registros públicos[22].

Determinados los actores, resta identificar qué tipos de datos forman parte del sistema de registro de datos públicos regulados por esta ley, a fin de determinar si la nomenclatura usada para agrupar este conjunto de datos es la correcta. Y también determinar si los sistemas de protección previstos en la presente norma son los pertinentes, de acuerdo a la naturaleza de cada uno de los datos que lo integran, y en especial respecto a los datos personales que son parte de esta base de datos accesible al público.

Se empezará por aquellos de mayor cuidado, los datos denominados sensibles. Pertenecen a este grupo los datos de: "ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales"[23]. Y su acceso "sólo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial"[24].

Cabe añadir que "También son confidenciales los datos cuya reserva haya sido declarada por la autoridad competente, los que estén amparados bajo sigilo bancario o bursátil, y los que pudieren afectar la seguridad interna o externa del Estado"[25]. Por otro lado, la autoridad o funcionario que custodie datos de carácter personal "deberá adoptar las medidas de seguridad necesarias para proteger y garantizar la reserva de la información que reposa en sus archivos"[26]. Y un solicitante que requiera conocer información patrimonial respecto de terceros "deberá justificar y motivar su requerimiento, declarar el uso que hará de la misma y consignar sus datos básicos de identidad, tales como: nombres y apellidos completos, número del documento de identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo reglamento se determinen. Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el/la titular de la información pueda ejercer"[27]. Finalmente, indica que "La Directora o Director Nacional de Registro de Datos Públicos, definirá los demás datos que integrarán el sistema nacional y el tipo de reserva y accesibilidad"[28].

En suma, los datos que integran el sistema de registro de datos públicos son:

a) Aquellos hechos, actos, contratos o instrumentos que deben inscribirse y/o registrarse, en virtud de la aplicación de la ley propia de cada materia[29];
b) Aquellos datos cuya reserva haya sido declarada por la autoridad competente;

21 Ley 0, R.O. Suplemento 162,31/mar/2010, *Ley del Sistema Nacional de Registro de Datos Públicos*. "Art. 13.- De los registros de datos públicos.- Son registros de datos públicos: el Registro Civil, de la Propiedad, Mercantil, Societario, Vehicular, de naves y aeronaves, patentes, de propiedad intelectual registros de datos crediticios y los que en la actualidad o en el futuro determine la Dirección Nacional de Registro de Datos Públicos, en el marco de lo dispuesto por la Constitución de la República y las leyes vigentes. / Los Registros son dependencias públicas, desconcentrados, con autonomía registral y administrativa en los términos de la presente ley, y sujetos al control, auditoría y vigilancia de la Dirección Nacional de Registro de Datos Públicos en lo relativo al cumplimiento de políticas, resoluciones y disposiciones para la interconexión e interoperabilidad de bases de datos y de información pública, conforme se determine en el Reglamento que expida la Dirección Nacional".

22 Ibíd. "Art. 2.- Ámbito de aplicación.- La presente Ley rige para las instituciones del sector público y privado que actualmente o en el futuro administren bases o registros de datos públicos, sobre las personas naturales o jurídicas, sus bienes o patrimonio y para las usuarias o usuarios de los registros públicos".

23 Ibíd., art. 6, LSNRDP.

24 Ibíd.

25 Ibíd.

26 Ibíd.

27 Ibíd.

28 Ibíd.

29 Ibíd. "Art. 3.- Obligatoriedad.–En la ley relativa a cada uno de los registros o en las disposiciones legales de cada materia, se determinará: los hechos, actos, contratos o instrumentos que deban ser inscritos y/o registrados; así como la obligación de las registradoras o registradores a la certificación y publicidad de los datos, con las limitaciones señaladas en la Constitución y la ley. / Los datos públicos registrales deben ser: completos, accesibles, en formatos libres, sin licencia alrededor de los mismos, no discriminatorios, veraces, verificables y pertinentes, en relación al ámbito y fines de su inscripción. / La información que el Estado entregue puede ser específica o general, versar sobre una parte o sobre la totalidad del registro y será suministrada por escrito o por medios electrónicos".

c) Datos de carácter personal de aquellos considerados como sensibles referidos a ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y, en especial, aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales, cuyo acceso es posible únicamente con autorización expresa del titular de la información, por mandato de la ley o por orden judicial;
d) Datos amparados bajo sigilo bancario o bursátil;
e) Datos que pudieren afectar la seguridad interna o externa del Estado.[30]

De otro lado, el artículo 4 del Instructivo de clasificación de la información de la Dirección Nacional de Registro de Datos Públicos, Registro de Datos Crediticios y Registros Mercantiles, a efectos de este sistema, prescribe que toda información que es administrada, recibida, generada, transmitida y almacenada en las instituciones que la conforman, se clasifica en información pública[31] e información confidencial[32]; y ésta, a su vez, en reservada[33] y secreta[34]. Sin embargo, los conceptos aquí delineados confunden información con documentos y no mencionan el término dato. Dicho texto, además de constituir una omisión evidente no permite comprender el alcance de la norma; es decir, si solo opera para la organización de los registros públicos o si es aplicable al cruce de información o la interoperabilidad. Adicionalmente, no guardan armonía con los conceptos que constan en otras normativas sobre esta temática, como la Ley Orgánica de Transparencia y Acceso a la Información Pública, la Ley de Seguridad Pública y del Estado y el Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público, que se analizarán en su momento.

Finalmente, el artículo 3 de la LSNRDP menciona el concepto de datos públicos registrales, al señalar que estos deben ser completos, accesibles, en formatos libres, sin licencia sobre ellos, no discriminatorios, veraces, verificables y pertinentes; además, deberán ser publicitados, con las limitaciones señaladas en la Constitución y la ley.

30 Ibíd. "Art. 6.- Accesibilidad y confidencialidad.–Son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales. / El acceso a estos datos sólo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial.
También son confidenciales los datos cuya reserva haya sido declarada por la autoridad competente, los que estén amparados bajo sigilo bancario o bursátil, y los que pudieren afectar la seguridad interna o externa del Estado.
La autoridad o funcionario que por la naturaleza de sus funciones custodie datos de carácter personal, deberá adoptar las medidas de seguridad necesarias para proteger y garantizar la reserva de la información que reposa en sus archivos.
Para acceder a la información sobre el patrimonio de las personas el solicitante deberá justificar y motivar su requerimiento, declarar el uso que hará de la misma y consignar sus datos básicos de identidad, tales como: nombres y apellidos completos, número del documento de identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo reglamento se determinen. Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el/la titular de la información pueda ejercer.
La Directora o Director Nacional de Registro de Datos Públicos, definirá los demás datos que integrarán el sistema nacional y el tipo de reserva y accesibilidad".

31 "Art. 5.- Información Pública.- Para los efectos de la presente norma, se considera Información Pública a todo documento físico y digital que emane, administre o se encuentre en poder de la DINARDAP, Registros Mercantiles y Registro de Datos Crediticios, que está sujeta al principio de publicidad". Instructivo de clasificación de la información de la Dirección Nacional de Registro de Datos Públicos, Registro de Datos Crediticios y Registros Mercantiles, Resolución 043-NG-DINARDAP-2016 (R.O. 899, 9-XII-2016).

32 "Art. 6.- Información Confidencial.- Es aquella información o conocimiento que no está sujeta al principio de publicidad, la cual es accesible únicamente a personal autorizado, de conformidad con lo establecido por el ANEXO 2 de esta norma, misma que será declarada como tal, por la máxima autoridad de la Dirección Nacional de Registro de Datos Públicos, de conformidad con lo establecido por el inciso sexto, del artículo 6 de la Ley del Sistema Nacional de Registro de Datos Públicos". Instructivo de clasificación de la información de la Dirección Nacional de Registro de Datos Públicos, Registro de Datos Crediticios y Registros Mercantiles, Resolución 043-NG-DINARDAP-2016 (R.O. 899, 9-XII-2016).

33 "Art. 6.- Información Confidencial.- [...] a) Información Reservada.- Se entiende a aquella que no es de libre acceso, pero que se pudiere otorgar el mismo, si los funcionarios de cada área, o de otras instituciones o terceros interesados, justifican legalmente el menester de tener acceso a la misma. / Por norma general, los datos de carácter personal administrados tanto por la DINARDAP, como de sus entidades adscritas, son considerados como reservados". Instructivo de clasificación de la información de la Dirección Nacional de Registro de Datos Públicos, Registro de Datos Crediticios y Registros Mercantiles, Resolución 043-NG-DINARDAP-2016 (R.O. 899, 9-XII-2016).

34 "Art. 6.- Información Confidencial.- [...] b) Información Secreta.- Es aquella información o conocimiento cuya divulgación puede poner en riesgo o comprometer la existencia de un bien jurídico de orden económico, social, de salud, de gobernabilidad, de seguridad, o amenace la prevención, investigación y sanción de las infracciones establecidas en la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos. La información clasificada como secreta, será entregada únicamente por orden judicial o cuando el uso de la misma sea imperativo para factores de auditoría, control y vigilancia de la autoridad competente". Instructivo de clasificación de la información de la Dirección Nacional de Registro de Datos Públicos, Registro de Datos Crediticios y Registros Mercantiles, Resolución 043-NG-DINARDAP-2016 (R.O. 899, 9-XII-2016).

Por tanto, es necesario identificar la naturaleza jurídica de los datos públicos registrales con la finalidad de no confundirlos, ni con el concepto de datos personales ni con el de datos públicos. De este modo, los registros públicos están conformados por datos personales y datos públicos, de forma que deben ser entendidos como datos públicos registrales y datos personales registrales, respectivamente. Pues la registrabilidad es la característica de, por voluntad de la ley, estar incorporada en un registro público o base de datos de registro público, para la generación de efectos jurídicos como la transferencia de dominio o la adquisición de derechos y obligaciones, en virtud de garantizar derechos y principios como el derecho de identidad, derecho de propiedad, derecho de libertad de comercio y empresarial, entre otros, y de los principios de publicidad, accesibilidad y el de seguridad jurídica.

Es más, por constar en un registro público, los datos personales o los datos públicos no modifican su naturaleza jurídica primigenia y, en consecuencia, el dato personal por ejemplo, no se transforma ni muta en dato público por el hecho de que conste en un registro público. Únicamente se vuelve accesible al público en virtud de la necesidad de hacer disponible este dato a fin de satisfacer intereses legítimos de terceros.

3.3 Ley Orgánica de Telecomunicaciones[35]

El Art. 78 de la Ley Orgánica de Telecomunicaciones, al referirse a la protección de datos personales, señala:

> Para la plena vigencia del derecho a la intimidad, establecido en el artículo 66, numeral 20 de la Constitución de la República, las y los prestadores de servicios de telecomunicaciones deberán garantizar, en el ejercicio de su actividad, la protección de datos de carácter personal.
> Para tal efecto, las y los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus redes con el fin de garantizar la protección de los datos de carácter personal de conformidad con la ley. Dichas medidas incluirán, como mínimo:
>
> 1. La garantía de que sólo el personal autorizado tenga acceso a los datos personales para fines autorizados por la ley.
> 2. La protección de los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos.
> 3. La garantía de la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales.
> 4. La garantía de que la información suministrada por los clientes, abonados o usuarios no será utilizada para fines comerciales ni de publicidad, ni para cualquier otro fin, salvo que se cuente con el consentimiento previo y autorización expresa de cada cliente, abonado o usuario. El consentimiento deberá constar registrado de forma clara, de tal manera que se prohíbe la utilización de cualquier estrategia que induzca al error para la emisión de dicho consentimiento.

Esta norma confunde el derecho a la intimidad, al que considera se protege al regular la protección de datos personales. Y si bien establece una serie de criterios y principios de protección, determina su ámbito de aplicación a las telecomunicaciones, se limita a señalar elementos como la seguridad, el consentimiento, la finalidad; hace alusión a un sistema de control y vigilancia que, lamentablemente, no es supervigilado por el organismo de control especializado. De acuerdo a lo citado, la norma debe reformarse o, si no, hacer remisión expresa a las disposiciones de una nueva Ley de Protección de Datos Personales, para que se pueda garantizar tanto el derecho a la intimidad como a la protección de datos personales, y para que el régimen de protección de este último sea completo y no quede restringido a los pocos principios abordados.

El artículo 85 de esta ley, al mencionar las obligaciones adicionales, dispone que:

> La Agencia de Regulación y Control de las Telecomunicación establecerá y reglamentará los mecanismos que permiten supervisar el

35 Ecuador, *Ley Orgánica de Telecomunicaciones*, R.O. Suplem. 439, 18-II-2015. https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Orgánica-de-Telecomunicaciones.pdf

cumplimiento de las obligaciones tanto de secreto de las comunicaciones como de seguridad de datos personales y, según sea el caso, dictará las instrucciones correspondientes, que serán vinculantes para las y los prestadores de servicios, con el fin de que adopten determinadas medidas relativas a la integridad y seguridad de las redes y servicios.

Estipula además que, entre las medidas constarán: "1. La obligación de facilitar la información necesaria para evaluar la seguridad y la integridad de sus servicios y redes, incluidos los documentos sobre las políticas de seguridad. 2. La obligación de someterse**,** a costo del prestador, a una auditoría de seguridad realizada por un organismo público, autoridad competente o, de ser el caso, por una empresa privada o persona natural independiente".

Finalmente, debería evitarse que la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador (Arcotel) realice las funciones de órgano de control, pues no es un organismo técnico especializado en la temática. Tal cometido debería realizarlo, como eje principal, una entidad autónoma, especializada e independiente, para que no se lo invisibilice o reste importancia frente a otras responsabilidades primigenias de este ente de control. Esta decisión facilitará que las visiones acotadas de este ámbito limitado de control, como es el de telecomunicaciones, no se superpongan al régimen general que debe primar para la tutela de los datos personales, que incluye diversos aspectos públicos, privados, comerciales, sociales, bancarios, educativos, sociales, etc.; es decir, que son transversales en toda la sociedad.

3.4 Ley Orgánica de Transparencia y Acceso a la Información Pública (Lotaip)[36]

En el sexto artículo de la Lotaip, se propone como confidencial a "aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales", y, más adelante, se añade que "el uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes". Se concluye que "no podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades, públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución Política de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno", excepto "el procedimiento establecido en las indagaciones previas".

En suma, la expresión "información pública personal" causa confusión, porque el término público no hace alusión a información estatal, sino a publicidad o accesibilidad al público. En tal sentido, información confidencial es aquella que, sea pública o personal, por motivos legítimos debe ser resguardada del conocimiento de otros. La información personal, por esencia, es confidencial, razón por la cual, la ley debe establecer los casos en los que se justifica que sea accesible al público por parte de terceros, un uso que generalmente debe ser proporcional y basado en un interés legítimo de quien busca acceder a esta información.

3.5 Código Orgánico Monetario y Financiero[37]

El artículo primero de este Código establece el objetivo principal: regular "los sistemas monetario y financiero, así como los regímenes de valores y seguros del Ecuador"[38]; ya que, por medio de normas, control, supervisiones y rendición de cuentas de las actividades realizadas, se generan sistemas de inspección. Se procura que estos procedimientos vayan acordes a la ley[39]. El artículo 152 habla de los derechos de las personas naturales o jurídica; y se reconoce como un derecho importante que se conozca su información de forma clara, precisa y no engañosa. Los datos personales que consten en entidades financieras deberán ser exactos y actualizados, conforme la ley lo disponga, porque estos sirven para generar reportes crediticios de los sujetos que consten en su base[40].

36 Ecuador, *Ley Orgánica de Transparencia y Acceso a la Información Pública*, R.O. Suplem. 337, 18-V- de mayo de 2004.
37 Ecuador, *Código Orgánico Monetario y Financiero*, R.O. Suplem. 215, 22-II-2006.
38 Ibíd.
39 Ibíd.
40 Ibíd.

Ahora bien, la Ley Orgánica para el Fomento Productivo, Atracción de Inversiones, Generación de Empleo, y Estabilidad y Equilibrio Fiscal (R.O. Suplemento 309, de 21 de agosto de 2018) estableció que será la Superintendencia de Bancos la que regule el Registro de Datos Crediticios y realice la administración de la base de datos crediticios, de manera que cree reportes de forma exacta y actualizada. Esta información es vital para la toma de decisión en créditos que se puedan otorgar a futuro[41].

Entretanto, el Código Orgánico, Monetario y Financiero menciona la protección de la información, la cual se establece en el artículo 352 y ampara los datos personales que se encuentran dentro del sistema financiero nacional. Los titulares de los datos serán los únicos habilitados para acceder a su información, a excepción de lo dispuesto en este Código. En el mismo sentido va lo dispuesto en el artículo 13 de la Codificación Superintendencia de Bancos[42], que menciona, dentro de los derechos del usuario:

> a. Exigir información y documentación de todos los actos que respalden la negociación, contratación, ejecución y terminación del contrato, y/o de la prestación de productos y servicios financieros ya sea al obligado directo o indirecto; b. Derecho a obtener los documentos que han sido debidamente cancelados o endosados por haberse subrogado en la obligación en calidad de obligado indirecto; y, c. Conocer si en las bases de datos de las entidades de los sectores financieros público y privado existe información sobre sí mismo y acceder a ella sin restricción alguna; a conocer la fuente de dicha información; y, a exigir de la misma la rectificación de los datos personales cuando dicha información sea inexacta o errónea.

Por otra parte, la codificación ya aludida propone, en el artículo 14, que "El usuario tendrá derecho a recibir protección y a demandar la adopción de medidas efectivas que garanticen la seguridad de las operaciones financieras, del defensor del cliente, de la Superintendencia de Bancos o de otras instancias administrativas o judiciales pertinentes"; principalmente en las siguientes circunstancias:

a) Recibir protección ante la existencia de cláusulas prohibidas que vayan en contra de sus derechos e intereses;
b) Recibir protección de los datos personales que las entidades financieras obtengan del usuario para la prestación de productos o servicios financieros. La información sobre dichos datos personales solo podrá ser otorgada por la entidad de los sectores financieros público y privado, en caso de consentimiento libre y expreso, especifico, inequívoco e informado, por parte del usuario, de disposición judicial o del mandato de la ley;
c) Recibir protección de los datos personales que las entidades financieras obtengan del usuario para la prestación de productos y servicios financieros prestados por vía electrónica. Las entidades financieras adoptarán específicamente las medidas de seguridad necesarias para este tipo de operaciones financieras;
d) Obtener protección de los datos personales sobre su solvencia patrimonial y crediticia, y a que las entidades financieras respeten las normas relativas al sigilo y reserva;
e) Exigir rectificación de la información de los datos personales en las bases de datos cuando ésta sea inexacta o errónea;
f) Demandar protección cuando las entidades financieras empleen métodos de cobranza extrajudicial que atenten contra su privacidad, dignidad personal y/o familiar;
g) Exigir que se mantenga la validez de las ofertas financieras. Las condiciones incluidas en los contratos tendrán fuerza vinculante si llegan a efectuarse con base en ellas;
h) Formar y participar en asociaciones para la defensa de los derechos del usuario del sistema financiero, y acudir al defensor del cliente en defensa de sus derechos; y,
i) Demandar la cobertura del fondo de garantía de depósitos, de acuerdo con la ley.

41 Ibíd.
42 Ecuador, *Codificación Superintendencia de Bancos*, publicada por Codificación Superintendencia de Bancos Nº. 810, R.O. Suplem. 123, 31-X-2017.

Estas normas, si bien establecen una serie de criterios y principios relativos a la protección de datos personales, no los engloban en su totalidad ni en su integridad. Por tal motivo, es necesario que este régimen acotado se remita a los principios, derechos y régimen general de control especializado, con la finalidad de que responsables de tratamiento tan importantes como las entidades del sistema financiero puedan garantizar un alto estándar de protección de datos personales que permita un adecuado flujo informacional al mismo tiempo que garanticen el respeto de los datos personales. Es fundamental que se mantenga la confianza en el sistema financiero, económico y crediticio a través de un adecuado manejo de los datos personales, para que se pueda realizar una adecuada estimación del riesgo sin menoscabar los derechos fundamentales de los titulares. Por ende, la norma debe adaptarse y realizar una remisión expresa a las disposiciones de una nueva Ley de Protección de Datos Personales.

3.6 Código Orgánico Integral Penal[43]

El artículo 229 del Código Orgánico Integral Penal determina el delito de revelación ilegal de base de datos por el cual:

> La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

En ese caso, el tipo penal no solo se define como garantía de la intimidad o la privacidad, sino también del derecho a la autodeterminación informativa, que es contenido esencial del derecho a la protección de datos personales, de forma que podría añadirse este término en la tipificación citada para lograr un marco normativo completo de protección de estos derechos de la personalidad en entornos digitales.

No requiere reforma, pero la existencia de una ley de protección de datos hace viable la aplicación del artículo que se cita a continuación, que consta en el título denominado "actuaciones y técnicas especiales de investigación", del segundo libro del Procedimiento del Código Orgánico Integral Penal. Este dispone, en el artículo 472, sobre la información de circulación restringida, que: "No podrá circular libremente [...] La información acerca de datos de carácter personal y la que provenga de las comunicaciones personales cuya difusión no haya sido autorizada expresamente por su titular, por la ley o por la o el juzgador".

3.7 Ley Orgánica de Salud (LOS)[44]

La Ley Orgánica de Salud, en el artículo 215, señala que "la autoridad sanitaria nacional con la participación de los integrantes del Sistema Nacional de Salud, implementará el sistema común de información con el fin de conocer la situación de salud, identificar los riesgos para las personas y el ambiente, dimensionar los recursos disponibles y la producción de los servicios, para orientar las decisiones políticas y gerenciales y articular la participación ciudadana en todos los niveles, entre otras". Por esa razón, no es necesario modificar normativa en dicho Código, sino precisar que la implementación de este sistema común de información deberá cumplir con los derechos, principios y obligaciones de una nueva Ley de Protección de Datos Personales, pues se trata de datos personales relacionados con la salud tratados por el Estado, con el Ministerio de Salud como responsable.

De otro lado, la Ley Orgánica de Salud establece la confidencialidad de varios datos de salud que deben ser resguardados desde la perspectiva de una normativa de protección de datos personales, que son:

43 Ecuador, *Código Orgánico Integral Penal*, R.O. Suplem. 180, 10-II-2014.
44 Ecuador, *Ley Orgánica de Salud*, R.O. Suplem. 353, 23-X-2018.

a) Enfermedades transmisibles, no transmisibles, crónico-degenerativas, discapacidades y problemas de salud pública declarados prioritarios, y determinar las enfermedades transmisibles de notificación obligatoria (art. 6, num. 5, LOS).
b) La historia clínica (art. 7, LOS).
c) Casos sospechosos, probables, compatibles y confirmados de enfermedades declaradas por la autoridad sanitaria nacional como de notificación obligatoria y aquellas de reporte internacional (art. 61, LOS).
d) Registro e información de pacientes que padezcan enfermedades raras o huérfanas incluidas las residentes en el extranjero que padezcan enfermedades raras o huérfanas, a fin de brindar atención oportuna en el país de residencia y de ser el caso en el territorio nacional (art. 3, LOS).

En resumen, es indispensable que no solo los datos anteriormente enumerados sean considerados confidenciales, sino que la nueva Ley de Protección de Datos Personales establezca una categoría especial de datos personales denominados datos de salud; que, además de la confidencialidad, establezca un sistema de protección reforzado como garantía frente a los riesgos de un tratamiento inadecuado de datos de naturaleza sensible de este tipo y, por ende, susceptibles a usos discriminatorios.

3.8 Código Orgánico de la Economía Social de los Conocimientos, Código Ingenios[45]

El Código Ingenios, en su artículo 67 señala que son parte de los principios para una investigación científica ética, la confidencialidad de los datos personales obtenidos en procesos de investigación. Asimismo, el artículo 116 del citado código señala que la información y el contenido de las bases de datos producto de las investigaciones financiadas con recursos públicos serán de acceso abierto. Sin embargo, si por razones de seguridad, soberanía, protección de datos personales o no personales, o de actuales o futuros derechos de propiedad intelectual, no fuere conveniente la difusión de esta información, solo deberá remitirse a la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación. Así, esta normativa propone proteger a los titulares de los datos a través de la confidencialidad o de un manejo restringido de la información. No obstante, no se establecen mecanismos de control de esta obligación, de modo que pudiera no resultar suficiente, toda vez que, al no existir normativa de protección de datos personales en el Ecuador, no existe un órgano de control encargado de la supervigilancia y promoción de este derecho.

El art. 141 de este código, ante la falta de normativa especializada, intenta establecer un régimen de uso legítimo de los datos personales, al señalar que la utilización de datos personales o no personales en contenidos protegidos o no por propiedad intelectual disponibles en bases de datos o repositorios y otras formas de almacenamiento de datos pertenecientes a personas naturales o jurídicas, sean de derecho público o privado, podrán utilizarse del siguiente modo:

> "a) Cuando se trate de información clasificada como asequible; b) Cuando cuenten con la autorización expresa del titular de la información; c) Cuando estén expresamente autorizados por la ley; d) Cuando estén autorizados por mandato judicial u otra orden de autoridad con competencia para ello; y, e) Cuando lo requieran las instituciones de derecho público para el ejercicio de sus respectivas competencias o del objeto social para el que hayan sido constituidas.
> No podrán disponerse de los datos personales o no personales so pretexto de los derechos de autor existentes sobre la forma de disposición de los elementos protegidos en las bases de datos. La información contenida en las bases de datos, repositorios y otras formas de almacenamiento de datos personales o no personales son de interés público; por consiguiente, deberán ser usados con criterios equitativos, proporcionales y en su uso y transferencia deberá primar el bien común, el efectivo ejercicio de derechos y la satisfacción de necesidades sociales".

Pese a la redacción amplia de esta norma, que intenta establecer un ámbito general de aplicación, ella no

45 Ecuador, *Código Orgánico de la Economía Social de los Conocimientos*, R.O. Suplem. 899, 9-XII-2016.

deja de ser sectorial, debido a que está contenida en una normativa de desarrollo del conocimiento y protección de la propiedad intelectual. De modo que, nuevamente, este esfuerzo resulta insuficiente en un marco de protección garantista que debe proteger al titular de los datos en todas sus interrelaciones en sociedad.

En el mismo sentido, la disposición general 26.ª de la normativa citada dispone que:

> las entidades públicas y personas naturales o jurídicas privadas que tengan bajo su poder documentos, datos genéticos, bancos o archivos de datos personales e informes sobre personas o sobre sus bienes, pondrán a disposición del público a través de un portal de información o página web la siguiente información y recursos: a) Los derechos que le asisten respecto de la protección de sus datos personales, entre ellos el derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos; y sus derechos a solicitar la rectificación, eliminación o anulación de sus datos personales; b) Detalle de las políticas y procedimientos institucionales para la protección de la privacidad de datos personales; y, c) Servicio de trámite en línea de las consultas y reclamos en materia de datos personales.

Así, se intenta introducir por vía de una normativa relativa a la garantía de derechos relacionadas con la economía social de los conocimientos, la creatividad, la innovación y la protección de la propiedad intelectual, uno de los principios fundamentales de la protección de datos personales que se denomina transparencia, mediante el cual el titular es informado del uso de los datos y de los mecanismos para su defensa. Si bien esta iniciativa es positiva, nuevamente resulta desarticulada, por cuanto no se establecen mecanismos de incentivo y verificación y, por ende, no suelen ser practicados, ya que no son parte de las obligaciones evaluables y sancionables por parte de ninguna autoridad de control.

Es decir, se introducen equivocadamente criterios y principios que son propios para la protección del derecho fundamental a la protección de datos personales y que, por tanto, ameritan una ley especializada en la cual se puedan garantizar los derechos y libertades individuales y el flujo de información. En este sentido, estas normas deben ser eliminadas, porque no se justifica su existencia en el citado cuerpo normativo, ni aun a título de sectorial.

Finalmente, la disposición general 27ª. dispone que: "Sin perjuicio de las excepciones previstas en la ley, el tratamiento de datos personales que incluya acciones tales como la recopilación, sistematización y almacenamiento de datos personales, requerirá la autorización previa e informada del titular". Si bien en esta parte, la norma coincide con el texto constitucional, resulta desubicada su incorporación en este Código por los criterios antes expuestos. Adicionalmente, este texto agrega que:

> No se requerirá de la autorización del titular cuando el tratamiento sea desarrollado por una institución pública y tenga una finalidad estadística o científica; de protección a la salud o seguridad; o sea realizado como parte de una política pública de garantía de derechos constitucionalmente reconocidos. En este caso deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares. La DINARDAP podrá solicitar que los bancos de datos personales en poder de una persona jurídica privada sean entregados a la misma con la finalidad de cumplir el presente artículo a excepción de los siguientes supuestos: a) si las bases de datos o archivos son de uso exclusivamente personal o doméstico; si las bases de datos y archivos de información son periodísticas y otros contenidos editoriales; y, si las bases contienen datos cuyo uso puede atentar a la privacidad de las personas tales como aquellos que revelen la orientación política, las convicciones religiosas o filosóficas, la pertenencia a organizaciones políticas o sociales.

Esta norma otorga atribuciones a la Dinardap, que podrían llegar a desnaturalizarla a menos que se amplíe su competencia para convertirla en un espacio de análisis de datos con finalidades científicas, estadísticas u otras, ya que la estructura actual del Sinardap

se limita a permitir un intercambio de información controlado a nivel técnico, tecnológico y jurídico. Si se pretende cambiar este diseño, hay que replantear el modelo institucional y hacerlo en la normativa propia de dicha institución y no únicamente mediante una disposición general en una normativa ajena, ya que el hacerlo sin la debida atención y cuidado, podría atentar contra principios como el de seguridad, calidad y finalidad de los datos personales, cuando, sobre todo, no se manejan criterios suficientes de anonimización de la información, sustanciales para el manejo de la información de este tipo.

3.9 Ley Orgánica de Comunicación[46]

El artículo 30 de la Ley Orgánica de Comunicación, respecto de la información de circulación restringida, sostiene que ésta:

> No podrá circular libremente, en especial a través de los medios de comunicación, la siguiente información:
> 1. Aquella que esté protegida expresamente con una cláusula de reserva previamente establecida en la ley;
> 2. La información acerca de datos personales y la que provenga de las comunicaciones personales, cuya difusión no ha sido debidamente autorizada por su titular, por la ley o por juez competente;
> 3. La información producida por la Fiscalía en el marco de una indagación previa; y,
> 4. La información acerca de las niñas, niños y adolescentes que viole sus derechos según lo establecido en el Código de la Niñez y Adolescencia.
>
> La persona que realice la difusión de información establecida en los literales anteriores será sancionada administrativamente por la Superintendencia de Información y Comunicación con una multa de 10 a 20 remuneraciones básicas mínimas unificadas, sin perjuicio de que responda judicialmente, de ser el caso, por la comisión de delitos y/o por los daños causados y por su reparación integral.

Mediante el texto de la Ley de Comunicación, se intenta controlar la divulgación de datos personales. Sin duda es un aporte importante en la construcción de una cultura de protección, en especial de aquellos datos que pertenecen a niños, niñas y adolescentes. Una norma de protección de datos personales se complementaría con el contenido del texto citado, dado que condiciona la actuación de los medios de comunicación en aras de proteger a las personas y sus datos.

La mencionada ley también propone, en el artículo 13 de su correspondiente reglamento, con respecto a la protección de la identidad e imagen, que "no se puede publicar en los medios de comunicación los nombres, fotografías o imágenes o cualquier elemento que permita establecer o insinuar la identidad de niñas, niños y adolescentes que están involucrados de cualquier forma en un hecho posiblemente delictivo o en la investigación y el procesamiento judicial del mismo". Y aclara que "La misma prohibición opera para proteger la identidad e imagen de cualquier persona que haya sido víctima de un delito de violencia sexual o violencia intrafamiliar", con excepción de "los testimonios de personas adultas que voluntaria y explícitamente dan su autorización para que los medios de comunicación cubran sus casos, siempre que esto tenga la finalidad de prevenir el cometimiento de este tipo de infracciones".

Esta norma complementa el sistema que privilegia la protección de datos personales de estos grupos de atención prioritaria y, en consecuencia, es valiosa como mecanismo de salvaguarda de los datos personales en el ámbito de las comunicaciones, si se toma en cuenta que deberán ser supervigiladas por la entidad encargada del control de la comunicación.

3.10 Ley Orgánica de Gestión de la Identidad y Datos Civiles[47]

El artículo 3 de la Ley Orgánica de Gestión de la Identidad y Datos Civiles estipula como objetivos:

1. Asegurar el ejercicio del derecho a la identidad de las personas.

46 Ecuador, *Ley Orgánica de Comunicación*, R.O. Suplem. 22, 25-VI-2013.
47 Ecuador, *Ley Orgánica de Gestión de la Identidad y Datos Civiles*, R.O. Suplem. 684, 4-II-2016.

2. Precautelar la situación jurídica entre el Estado y las personas naturales dentro de sus relaciones de familia.
3. Proteger el registro de los hechos y actos relativos al estado civil de las personas.
4. Proteger la confidencialidad de la información personal.
5. Evitar el subregistro o carencia de datos en registro de una persona.
6. Proteger la información almacenada en archivos y bases de datos de los hechos y actos relativos al estado civil de las personas.
7. Propender a la simplificación, automatización e interoperabilidad de los procesos concernientes a los hechos y actos relativos al estado civil de las personas, de conformidad a la normativa legal vigente para el efecto.

De los varios propósitos en la normativa citada se colige que, por tratarse de un registro público, una ley de protección de datos personales sería directamente aplicable e impactaría en todos los ámbitos y procesos. Por este motivo, se considera necesario un período de gracia para que los actores involucrados puedan adaptarse a su contenido y garantizar el derecho a la protección de datos personales.

3.11 Ley de Seguridad Pública y del Estado[48]

El artículo 19 de la Ley de Seguridad Pública y del Estado señala que los organismos de seguridad y la Secretaría Nacional de Inteligencia pueden realizar la clasificación de la información resultante de las investigaciones o actividades que realicen. La citada clasificación se deberá realizar mediante resolución motivada de la máxima autoridad de la entidad respectiva. Con este objetivo, el reglamento determinará los fundamentos para la clasificación, reclasificación y desclasificación, y los niveles de acceso exclusivos a la información clasificada.

Así, la ley señala que la información y documentación se clasificará como reservada, secreta y secretísima, y que será el reglamento el que determine los criterios para la mentada clasificación. En el artículo 28 del Reglamento a la Ley de Seguridad Pública y del Estado[49], se declarará que un documento o material se considera información reservada, cuando la utilización no autorizada de la información que contiene pudiera perjudicar los intereses de los organismos de seguridad. Será secreto[50], si pudiera ocasionar daño a las instituciones públicas y a los funcionarios que laboran en ellas. Finalmente, se considerará secretísimo, cuando podría incidir en un peligro excepcionalmente grave para la seguridad integral del Estado.

El artículo 29 del Reglamento a la Ley de Seguridad Pública y del Estado determina que "Los servidores públicos, ciudadanos civiles y miembros activos de las Fuerzas Armadas y de la Policía Nacional están prohibidos de divulgar información reservada, secreta y secretísima, aún después de cesar en sus funciones".

El artículo 19 de la Ley de Seguridad Pública y del Estado establece que;

> toda información clasificada como reservada y secreta será de libre acceso luego de transcurridos cinco y diez años, respectivamente; y si es secretísima luego de transcurridos quince años. La información clasificada como secretísima será desclasificada o reclasificada por el Ministerio de Coordinación de Seguridad o quien haga sus veces. De no existir reclasificación, se desclasificará automáticamente una vez cumplido el plazo previsto de quince (15) años.

Por su parte, el artículo 195 del Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público[51] señala que "Los datos personales de servidoras o servidores que forman parte del servicio, así como las actividades u operaciones que se realicen en función de la misión de la entidad, serán calificados de reservada, secreta o secretísima dependiendo del nivel de confidencialidad que se requiera conforme a la normativa jurídica competente".

48 Ecuador: *Ley de Seguridad Pública y del Estado*, R.O. Suplem. 352, 8-IX-2009.
49 Reglamento a la Ley de Seguridad Pública y del Estado, Suplemento del R.O. 336, 27-IX-2018.
50 Reformado por el artículo 15 del D.E. 64, R.O. 36-2S, 14-VII-2017.
51 Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público, R.O. Suplem. 19, 21-VI-2017.

De lo transcrito, se desprende que esta clasificación de los datos se debe coordinar y ser coherente con el principio de confidencialidad, de tal manera que no existan contradicciones y que, por el contrario, la diferente normativa sea armónica, dado que las clasificaciones de reservada, secreta o secretísima no distingue si se trata de datos personales o de datos públicos.

PROPUESTA DE LEY DE PROTECCIÓN DE DATOS PERSONALES

En el mundo existen tres modelos claramente diferenciados para la garantía del derecho o la regulación de los datos personales. El primero, que es de origen europeo, reconoce al derecho a la protección de datos personales como un derecho humano de nacimiento jurisprudencial y con corte constitucional, que permite el desarrollo de la personalidad; por tal motivo concibe los datos de titularidad de cada individuo como un elemento que conforma su personalidad (Conde Ortiz 2005).

El segundo modelo proviene de Estados Unidos y determina la *privacy*, que actualmente se interpreta como la norma que protege los elementos privados de cada persona, incluidos la correspondencia, efectos o enseres, de la intromisión ilegal de un tercero; de ahí surge la necesidad de sentencia judicial para su efectivo ejercicio. Es un modelo de protección asociado a la propiedad privada, desde el derecho a ser dejado en paz, a estar solo[52] y, por ende, al derecho de una persona de que sus datos no puedan ser usados para perturbarlo. Entonces, es contradictorio que tenga que haber un daño para que un titular pueda reclamar, cuando es posible arbitrar medidas que permitan evitar que éste se produzca. Con esta concepción anterior, en la práctica se depositaba en el otro el deber pasivo negativo de no hacer nada para que, sobre la base de la inacción, se pueda asegurar la vigencia de este derecho a la *privacy*. Asimismo, este modelo propone que los datos de carácter personal son patrimonio de un individuo o empresa, no como parte de su identidad, ni de su titularidad, sino como manifestaciones externas que puedan ser objetivadas a tal punto que admiten ser transferidos, cedidos, tratados, en la medida en que conformen bases de datos que logren el intercambio de información y recursos económicos en movimiento. Por ende, como parte de esta visión, se establecen regímenes generales o marcos normativos de regulación que viabilizan su manejo.

Finalmente, el tercer modelo es el latinoamericano, que constituye una postura híbrida entre las dos posiciones antes señaladas; pues, luego de una larga discusión entre intimidad, privacidad y protección de datos personales, admite a este último derecho como autónomo y lo vuelve el centro del sistema de salvaguarda de los datos personales. Además, reconoce la figura del *habeas data* como un mecanismo de justicia constitucional que apuntala la protección de las personas en la sociedad red. Esta corriente también toma en consideración ciertas prácticas norteamericanas, como códigos de conductas, prácticas de buena fe y principios de puerto seguro o escudo de privacidad (Palazzi 2002), con los cuales se establecen mecanismos de regulación que permiten el flujo adecuado de datos personales.

Es importante tener en cuenta estos tres modelos de protección existentes en la medida en que, para realizar una propuesta normativa, hay que identificar: ¿con cuál debe alinearse la futura normativa ecuatoriana?, ¿cuál de ellos es el que se compatibiliza de manera general con las fuentes, derechos y principios rectores de la sociedad ecuatoriana?, y, de forma más específica, ¿qué figuras pueden ser adaptadas a nuestra realidad para aprovechar los mejores elementos de cada modelo en beneficio de los ecuatorianos?

En este sentido, el 19 de septiembre de 2019, se presentó a la Asamblea Nacional un Proyecto de Ley de Protección de Datos Personales que se alinea al modelo latinoamericano, considerado como híbrido porque

52 Bendich, A. M. 1966. "Privacy, Poverty and the Constitution", en: California Law Review. Vol. 54, No. 2: 407-42.

reconoce a la protección de datos personales como un derecho humano y, al mismo tiempo, establece marcos regulatorios que permitan el libre flujo de información personal, siempre que se garantice el respeto a la dignidad humana. Es decir, el proyecto de ley presentado adopta la visión latinoamericana, no solo por la ubicación geográfica del Ecuador sino, sobre todo, porque el artículo 1 de la Constitución dispone que nuestro país es un Estado constitucional de derechos y justicia, social, democrático, soberano, independiente, unitario, intercultural, plurinacional y laico, y, por ende, debe garantizarse en esencia la dignidad de las personas que lo integran.

Entonces, el proyecto de ley desarrolla una propuesta normativa que parte del reconocimiento de la protección de datos personales como derecho fundamental en el artículo 66 numeral 19 de la CRE, así como busca establecer vías administrativas y jurisdiccionales adicionales que contribuyan con la protección de este derecho y de otros relacionados con la manifestación digital de un titular, al tenor de la garantía constitucional del *habeas data*, consagrada en el artículo 92 de la CRE.

Así pues, la propuesta normativa postula a la persona, titular del dato personal, como el centro de la protección; no solo de aquella protección reactiva, a través de acciones constitucionales y ordinarias, sino sobre todo preventiva, mediante normas que orienten, sobre la base de principios, a los responsables del tratamiento, para cumplir sus objetivos de forma que no hagan un uso inadecuado de los datos personales a su cargo. Asimismo, se establece la necesidad de que un órgano de control supervigile las actuaciones de estos responsables del tratamiento para evitar usos indebidos y sancionar en caso de que se hayan producido.

Como se ha analizado, pese a la existencia de una norma constitucional que reconoce el derecho a la protección de datos personales[53] y de la garantía constitucional del *habeas data*[54], es evidente que la falta de normativa legal, de jurisprudencia e incluso de normativa sectorial, mantiene en estado de abandono a los datos personales de los ecuatorianos. Esta afirmación es grave, puesto que los datos personales son parte esencial de un individuo, manifestación de su libertad informativa, de su libre desarrollo de la personalidad, y facultan otros derechos fundamentales y libertades individuales. Por tanto, esta situación de laguna normativa nos retrasa, no solo desde la perspectiva de los emprendimientos, la innovación, la competitividad del país, sino también desde el punto de vista de la protección y salvaguarda de derechos de los titulares y de la construcción de una cultura de protección que permita que la sociedad camine hacia un régimen que garantice el libre flujo de información con respeto a la persona.

La normativa presentada a la Asamblea Nacional responde a las condiciones particulares de este derecho, es decir, el hecho de que es un derecho complejo, porque no tiene un núcleo unívoco. En efecto, está constituido por varios derechos, principios y garantías que, además, siguen en evolución y se complementan en la medida en que la sociedad se desarrolla. Es por este motivo que en su articulado se encuentran recogidos principios, derechos y obligaciones que viabilizan un sistema integral de protección.

La normativa propuesta reconoce, en el artículo relativo al objeto, uno los núcleos primigenios de este derecho, aunque no el único, es decir: la autodeterminación informativa. Ya que las personas pueden decidir qué datos entregan y con qué finalidad, siempre que hayan sido debidamente informadas y que medie su consentimiento para que estos sean tratados y utilizados. Asimismo, en el contenido del proyecto de ley constan varios principios como los de legitimación, finalidad, calidad, seguridad, responsabilidad proactiva, proporcionalidad, limitación del tratamiento; así como derechos: de acceso, rectificación, cancelación, oposición, portabilidad, etc. De tal manera que, de existir un abuso por parte de un responsable del manejo de los datos, la persona puede retirar el consentimiento, cancelar, actualizar u oponerse a la recolección o tratamiento de sus datos personales. En todos estos casos se hace referencia a los derechos ARCO (actualización, rectificación, cancelación u oposición), tal como se denominan en legislaciones de corriente

53 Ecuador, *Constitución de la República del Ecuador*, 2008, art. 66.
54 Ibíd., art. 92.

europea, y que, en otros lugares, especialmente en Latinoamérica, se han reconocido mediante la acción de *habeas data*. Tal acción tutela estos derechos a nivel jurisdiccional por medio de una garantía constitucional que, al consagrarse en una ley de protección de datos personales, permite su efectiva vigencia; ya que, en caso de inobservancia, puede exigirse directamente a los responsables de tratamiento, ante una autoridad de control que supervigile su cumplimiento. De esta manera se abren varias vías de tutela en garantía de los titulares de los datos.

Con todo, hay que insistir en la necesidad de un marco regulatorio que establezca criterios y habilite para una libre circulación de datos personales con la finalidad de que los responsables de tratamiento puedan aprovecharlos positivamente para el desarrollo, la innovación y el fortalecimiento de una sociedad digital que nos permita ir a la par del progreso social, económico, cultural y social del mundo. Este proceso de transformación digital se ha radicalizado en el Ecuador debido a la declaratoria de pandemia de COVID-19 por parte de la Organización Mundial de la Salud, y la consecuente promulgación del estado de excepción en todo el territorio nacional, mediante Decreto Ejecutivo N°. 1017 del 16 de marzo de 2020, por los casos de coronavirus confirmados y las medidas de distanciamiento social impuestas por el COE nacional. Tal situación extrema ha propiciado el uso masivo de tecnologías con la obvia acumulación de datos personales por parte de plataformas que permiten la entrega de bienes, productos y servicios digitales por parte del Estado, en garantía de la implementación de un gobierno electrónico que permita el ejercicio de derechos. Por su parte, muchas entidades privadas facilitan actividades como la teleducación, telemedicina, teletrabajo, etc.; en suma, todas las interrelaciones sociales, económicas y sociales necesarias para la reactivación económica en el actual modelo de economía digital.

Igualmente, el proyecto establece una serie de obligaciones tendientes a garantizar el derecho a la protección de datos personales, de tal manera que se garantice una adecuada actuación de responsables o encargados de bases de datos, sean estos entes públicos o privados, que eviten que se violenten, por acción u omisión, los datos personales sujetos a su tratamiento. De esta forma, el cumplimiento de las obligaciones descritas en el texto propuesto pretende que los responsables de tratamiento procuren una actuación adecuada, diligente y legal en el manejo de los datos personales en todas las fases del ciclo del dato; es decir, en la recogida, almacenamiento, gestión, seguridad, cesión, entre otras, para que no se produzcan daños debido a una incorrecta actuación.

Asimismo, la normativa propuesta establece criterios que permiten el cumplimiento de la obligación de establecer o mantener mecanismos nacionales de supervisión independientes y efectivos, capaces de asegurar la transparencia cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado[55]. Esta obligación se refiere a la creación de una institucionalidad propia, independiente y especializada que pueda realizar actividades de control y vigilancia para el cumplimiento de la normativa que regula un manejo adecuado de los datos personales. También hace alusión a normas, leyes, reglas, procedimientos y prácticas que, con este enfoque de transparencia, se materialicen para la efectiva vigencia de los derechos; y, además, a la utilización de tecnologías, métodos o sistemas que deben implementarse desde el diseño y, por defecto, para proteger los datos personales y, al mismo tiempo, garantizar su tráfico en bienestar de la sociedad.

En el mismo sentido, el proyecto de ley plantea que el Estado debe ser garante del derecho, al establecer el principio de independencia de las actuaciones de una autoridad de control que se encargue de hacer efectivo tal derecho. En efecto, los mecanismos de control y de sanción no tienen como finalidad únicamente la de recuperar recursos a título de multa, sino que su verdadera intención es la de constituirse en elementos disuasivos de la voluntad que eviten futuras transgresiones. Asimismo, un sistema de control y vigilancia del cumplimiento de las obligaciones de los responsables contribuye a establecer un sistema de mejora continua que potencie los mecanismos de resguardo

55 Asamblea General de las ONU, "Resolución A/C.3/68/L.45/Rev.1 sobre el Derecho a la Privacidad en la Era Digital".

y el espíritu preventivo que permita anticipar consecuencias negativas, al mismo tiempo que facilita un uso adecuado y productivo de las innovaciones tecnológicas.

CONCLUSIONES Y RECOMENDACIONES

1. Se han suscitado varios casos de gravedad que demuestran que, en el Ecuador, han existido vulneraciones al derecho a la protección de datos personales de los ecuatorianos.
2. El marco normativo actual es insuficiente, contradictorio y sectorial, de modo que no permite realizar una protección integral de los datos personales de la población ecuatoriana.
3. El proyecto de ley presentado en la Asamblea Nacional se alinea al modelo latinoamericano, considerado como híbrido, ya que reconoce y garantiza el derecho fundamental a la protección de datos personales y establece un marco regulatorio que permite el libre flujo informacional que facilita la innovación y el desarrollo tecnológico, al mismo tiempo que tutela la dignidad del titular del dato personal.
4. Debido al avance en la implementación de las TIC en las actividades de la sociedad ecuatoriana en sus distintas interacciones con el sector público y privado, sobre todo por la actual situación de la pandemia, junto a los riesgos inminentes de un inadecuado tratamiento de los datos personales evidenciado en los graves casos ocurridos en el Ecuador analizados en este trabajo, resulta indispensable que la Asamblea Nacional tramite urgentemente el proyecto de ley de protección de datos personales presentado.

Recomendaciones

La ley de protección de datos personales que la Asamblea Nacional apruebe debe establecer un sistema que garantice la prevención del daño, mediante contenido que clarifique los deberes y responsabilidades de los responsables y encargados de las bases de datos; que empodere a sus titulares con la finalidad de construir en conjunto una sociedad respetuosa de los datos personales y de los derechos individuales de sus titulares. Así mismo, debe permitir, por medio del flujo informacional, el desarrollo social, cultural, económico, tecnológico, la innovación y la competitividad. A la par del desarrollo normativo, y debido a la actual situación de pandemia, es fundamental que el Estado, a través de políticas públicas y aun cuando esté pendiente la aprobación de la normativa, propenda a la construcción de una cultura de protección de datos personales, y que eduque a la ciudadanía y a responsables de tratamiento en cuanto a sus derechos, principios y obligaciones.

BIBLIOGRAFÍA

Acceso no consentido a un sistema informático (base de datos). Proceso N° 170101819110653. Fiscalía de Soluciones Rápidas N° 3. Denunciante DINARDAP, Denunciado Equivida. Quito-Ecuador.

Asamblea General de las Naciones Unidas, "Resolución A/C.3/68/L.45/Rev.1 sobre el Derecho a la Privacidad en la Era Digital".

Bendich, A. M. 1966. "Privacy, Poverty and the Constitution", en: *California Law Review*. Vol. 54, Nº 2: 407-42.

Codificación Superintendencia de Bancos, publicada por Codificación Superintendencia de Bancos n.º 810, R.O. Suplem. 123, 31-X-2017.

Código Orgánico de la Economía Social de los Conocimientos, R.O. Suplem. 899, 9-XII-2016.

Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público, Suplemento del R.O. 19, 21-VI-2017.

Código Orgánico Integral Penal, R.O. Suplem. 180, 10-II-2014.

Código Orgánico Monetario y Financiero, R.O. Suplem. 215, 22-II-2006.

Comisión. N° 5 Especializada Permanente de Soberanía, Integración Relaciones Internacionales y Seguridad Integral de la Asamblea Nacional, Informe para dar cumplimiento a la Resolución del Pleno de la Asamblea Nacional de 17-IX-2019.

Conde Ortiz, Concepción. 2005. *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*. Madrid: Dykinson.

Constitución de la República del Ecuador, 2008.

Corte Constitucional del Ecuador, "Sentencia 001-2014-PJO-CC", Gaceta Constitucional N°. 007, 7-III-2014.

Defensoría del Pueblo. Resolución N.° DPE-DGT-DNAPD-16-2014-DO, CONSEP, Trámite N°. DPE-DGT-DNAPD-133-2013-DO, 22-XII-2014.

Dirección Nacional de Registro y Datos Públicos del Ecuador, "Planificación Estratégica 2015-2017", 2015, http://www.datospublicos.gob.ec/wp-content/uploads/downloads/2016/02/PLANIFICACI%C3%93N-ESTRAT%C3%89GICA-2015-2017.pdf.

Dirección Nacional de Registro y Datos Públicos del Ecuador, Instructivo de clasificación de la información de la Dirección Nacional de Registro de Datos Públicos, Registro de Datos Crediticios y Registros Mercantiles, Resolución 043-NG-DINARDAP-2016 (R.O. 899, 9-XII-2016).

Dirección Nacional de Registro y Datos Públicos del Ecuador, "DINARDAP cuestionó el proyecto de Ley de Protección de los Derechos a la Intimidad que analiza la Asamblea Nacional – DINARDAP". Accedido el 09-VIII-2020: https://www.dinardap.gob.ec/dinardap-cuestiono-el-proyecto-de-ley-de-proteccion-de-los-derechos-a-la-intimidad-que-analiza-la-asamblea-nacional/.

El Comercio, "Gabriela Rivadeneira: 'En ningún momentoleyrestringirádatosdefuncionariospúblicos'", 16-IX-2016, https://www.elcomercio.com/actualidad/gabrielarivadeneira-ley-datospersonales-ecuador-asamblea.html.

El Comercio, "Lenin Moreno denuncia el robo de la base de datos del Plan Toda Una Vida", accedido 25-X-2018, https://www.elcomercio.com/actualidad/leninmoreno-denuncia-robo-basededatos-plan.html.

El Comercio, "BBC revela filtración de datos sensibles de millones de ecuatorianos", accedido 25-IX-2019, https://www.elcomercio.com/tendencias/datos-ecuatorianos-filtracion-reporte-seguridad.html

El Telégrafo, "8.582 conductores portan licencias tipo 'B' ilegales", El Telégrafo, 28-III-2018, https://www.eltelegrafo.com.ec/noticias/judicial/12/conductores-licencias-ilegales.

El Universo, "$ 8'000.000 del Bono de Desarrollo Humano habrían sido cobrados indebidamente; hay siete detenidos", accedido 25-X-2018, https://www.eluniverso.com/noticias/2017/10/31/nota/6459943/8000000-bono-desarrollo-humano-habrian-sido-cobrados-indebidamente.

El Universo, "Ecuador no tiene ley para proteger datos personales", 29-IV-2018, https://www.eluniverso.com/noticias/2018/04/29/nota/6736146/ecuador-no-tiene-ley-proteger-datos-personales.

Expreso.ec, "Débitos no autorizados molestan a los clientes", accedido 24-X-2018, https://www.expreso.ec/economia/debitos-no-autorizados-molestan-a-los-cliente-NAgr_4581611.

Interceptación ilegal de base de datos. Proceso N.° 170101818064001. Fiscalía N° 3 – Unidad para Descubrir Autores, Cómplices y Encubridores. Denunciante DINARDAP, Denunciado Desconocido. Quito-Ecuador.

Ley 0, R.O. Suplem.162, 31-III-2010, Ley del Sistema Nacional de Registro de Datos Públicos.

Ley 67, Ley de Comercio Electrónico, Firmas y Mensajes de Datos, R.O. Suplem.577, 17-IV-2002.

Ley de Seguridad Pública y del Estado, R.O. Suplem. 352, 8-IX-2009.

Ley Orgánica de Comunicación, R.O. Suplem. 22, 25-VI-2013.

Ley Orgánica de Gestión de la Identidad y Datos Civiles, R.O. Suplem. 684, 4-II-2016.

Ley Orgánica de Salud, R.O. Suplem. 353, 23-X-2018.

Ley Orgánica de Telecomunicaciones, R.O. Suplem. 439, 18-II-2015, https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Orgánica-de-Telecomunicaciones.pdf

Ley Orgánica de Transparencia y Acceso a la Información Pública, R.O. Suplem. 337, 18-V-2004.

Ley S/N publicada en el Segundo Suplemento del R.O. 843, 3-XII-2012, que reforma la Ley Orgánica a la Ley del Sistema Nacional de Registro de Datos Públicos.

Palazzi, P. 2002. *La Transmisión Internacional de Datos Personales y la Protección de la Privacidad Argentina, América Latina, Estados Unidos y la Unión Europea*. Buenos Aires: Ad Hoc.

Reglamento a la Ley de Seguridad Pública y del Estado, Suplemento del R.O. 336, 27-IX-2018.

Revelación ilegal de bases de datos. Proceso N° 170101818060469. Fiscalía de Soluciones Rápidas N° 2. Denunciante DINARDAP, Denunciado Desconocido. Quito-Ecuador.

Revelación ilegal de bases de datos. Proceso N° 170101819072102. Fiscalía de Soluciones Rápidas N° 7. Denunciante DINARDAP, Denunciado DataBook. Quito-Ecuador.

Revelación ilegal de bases de datos. Proceso N° 170101819100071. Fiscalía de Soluciones Rápidas N° 3. Denunciante DINARDAP, Denunciado Novaestrat. Quito-Ecuador.