ISSN: 2737-6133

cálamo

Revista de Estudios Jurídicos

Número 13 / Julio 2020

udla | Facultad de Derecho

- Situación de la protección de datos personales en Ecuador
- Transferencia internacional de datos personales en Latinoamérica
- Protección de datos personales en comercios electrónicos B2C
- Modernización del sistema registral ecuatoriano
  Las oportunidades que trae la tecnología *blockchain*
- Psicopolítica, redes sociales y la cuestión criminal
- Cimientos de la libertad de expresión en internet
  Limitaciones desde la esfera civil y penal

REVISTA DE ESTUDIOS JURÍDICOS

CRÉDITOS

UNIVERSIDAD DE LAS AMÉRICAS - ECUADOR
Facultad de Derecho y Ciencias Sociales
Escuela de Derecho

RECTOR
Gonzalo Mendieta

VICERRECTORA ACADÉMICA
Marlena León Mendoza

DECANA
Alexandra Vela

DIRECTOR ACADÉMICO
José Gabriel Terán

DIRECTORA CÁLAMO
Pamela Jijón

COORDINADORA EDITORIAL
Lydia Andrés

COMITÉ EDITORIAL NACIONAL

- José Suing, PhD. Universidad de las Américas
- Richard Ortiz, PhD. Universidad de las Américas
- Pamela Jijón, PhD. Universidad de las Américas
- Wladimir Sierra, PhD. Universidad de Berlín
- Patricia Alvear, PhD. Universidad de las Américas
- Emilio Cerezo, Mg. Universidad de las Américas
- Juan Manuel Alba, PhD. Universidad de las Américas

COMITÉ ASESOR INTERNACIONAL

- Timothy Tambassi, PhD. Università del Piemonte Orientale "Amedeo Avogrado", Italia
- Juan Antón, PhD. Universitat de Barcelona, España
- Ignacio Cremades,PhD. Universidad Complutense de Madrid
- Blanca Rodríguez, PhD. Universidad de Sevilla
- Roberto Bueno, PhD. Universidade Federal de Uberlândia, Brasil
- Gorki Yuri Gonzales, PhD. Universidad Católica del Perú
- Mónica Gonzáles Contró, PhD. Universidad Autónoma de México-Instituto de Investigaciones Jurídicas, México
- Teodoro Yan Guzmán, PhD. Universidad de la Habana, Cuba
- Julio Antonio Fernández, PhD. Centro de Estudios de la Administración Pública, Habana-Cuba
- Patricia Reyes, PhD. Universidad de Valparaíso, Chile
- Martin Aldao, PhD. Universidad de Buenos Aires, Argentina
- Raúl Gustavo Ferreyra, PhD. Universidad de Buenos Aires, Argentina

CORRECCIÓN DE ESTILO
Emilio Cerezo, Mg.

TRADUCCIÓN ESPAÑOL-PORTUGUÉS
Marcella da Fonte Carvalho, PhD.

TRADUCCIÓN ESPAÑOL-INGLÉS
María Helena Carbonell, PhD. (c.)

DISEÑO GRÁFICO E IMPRESIÓN
V&M Gráficas
Contacto: 3201 171

PERIODICIDAD
Semestral

DEPÓSITO LEGAL
Para contribuciones o canje dirigirse a: Universidad de Las Américas. Facultad de Derecho. Sede Norte, instalaciones José Queri. Bloque 6. Quito, Ecuador.

Teléfono +593 (2) 3981000

Envío de artículos, información y suscripción:
calamo@udla.edu.ec

ISSN DIGITAL
2737-6133

Cálamo 13: Los artículos que conforman el número 13 de Cálamo, previo su publicación, han sido evaluados bajo la modalidad de revisión por pares ciegos.

EDITORIAL

Nuestro décimo tercer número de Cálamo surge en un particular momento de conmoción social determinado por la pandemia de Covid-19 que, además de sus nefastas consecuencias para la salud y la economía mundial, ha puesto en evidencia la centralidad de la dimensión informática en nuestras vidas profesionales y privadas. Hoy más que nunca se han acentuado las relaciones en el espacio virtual y generado una organización laboral, política y social en torno a las nuevas tecnologías. En este contexto, pese a la temática libre de la revista, este número 13 reúne, en sus diferentes secciones, contribuciones relacionadas con las innovaciones jurídicas frente al Derecho digital y las TIC.

Así, abrimos nuestro dossier con el artículo de Lorena Naranjo, quien analiza las falencias en la normativa ecuatoriana para la protección de datos personales y hace un llamado a la promulgación de una ley que garantice dicha protección. Este análisis se complementa con el planteado en el artículo de Christian Razza, quien amplía el enfoque a la región latinoamericana y subraya que, pese a existir constitucionalmente el derecho a la protección de datos, éste no se plasma en garantías suficientes, sobre todo en el caso de la transferencia internacional de datos personales. Por su parte, Carolina Sacoto contribuye con este eje específicamente en lo que atañe a los comercios electrónicos B2C, en cuanto a sus obligaciones y avisos legales frente a la protección de datos personales.

Por otro lado, la contribución de Eugenia Novoa y Cristina Escobar se concentra en la aplicación de la tecnología *Blockchain* al sistema registral ecuatoriano y da cuenta de las diversas contribuciones y beneficios que ésta significa frente a la reducción de la brecha tecnológica. Desde el eje de la criminología crítica, Adrián Alvaracín se interesa en el rol del uso de las redes sociales en la criminalización y selección penal de la que son víctimas grupos vulnerables. Por último, nuestro dossier cierra con el artículo de Vicente Vásconez y Edison López, quienes presentan el vínculo que existe entre la libertad de expresión y la democracia deliberativa; tema que es de vital importancia en el delicado momento en que vivimos y que gira en torno al derecho a una comunicación libre y apegada a la verdad.

En esta ocasión, son tres los artículos que conforman nuestra sección de ensayos. Estos complementan el contenido del dossier, primero, con una revisión de lo que son los datos personales y la necesidad de su protección en el caso ecuatoriano, en el aporte de Belén Rivera. Luego, en la contribución de Pablo Espinosa, quien se concentra en las garantías que se deben constituir en el uso de datos personales; en especial la garantía de la ponderación entre la vida privada y la seguridad nacional. Por último, con el texto de Ginna Pasquel, que propone un panorama sobre la libertad de expresión, su dimensión democratizadora y sus restricciones en internet.

La entrevista de este número, realizada por María Helena Carbonell, responde al interés de escuchar de primera mano a Carlos Poveda, abogado ecuatoriano que contribuye en el bufete jurídico presidido por Baltasar Garzón y que es uno de los protagonistas en la defensa de Julian Assange en el caso WikiLeaks. Para terminar, Sofía Fernández nos propone una interesante reseña sobre el libro *Derecho Informático y su aplicación en el Ecuador*, de Janetsky Proenza, editado en 2019 por la Corporación de Estudios y Publicaciones, en Ecuador; texto en el que se reflexiona acerca de un concepto central para nuestra época, el de sociedad de la información.

Quiero agradecer a quienes han contribuido con este número y permitido que, incluso en una situación de emergencia sanitaria, la producción académica no se detenga y continúe creando lazos de intercambio y de reflexión colectiva.

Alexandra Vela Puga
Decana de la Facultad de Derecho
Universidad de Las Américas

ÍNDICE

Dossier

Ensayos

Entrevista

Reseña

DOSSIER

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.

ÍNDICE

TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES EN LATINOAMÉRICA

INTERNATIONAL TRANSFER OF PERSONAL DATA IN LATIN AMERICA

TRANSFERENCIA INTERNACIONAL DE DADOS PESSOAIS NA AMÉRICA LATINA

*Christian Razza**

Recibido: 05/05/2020
Aprobado: 05/06/2020

Resumen

Los datos personales se han tornado a nivel internacional un activo intangible que permite la productividad y competitividad. Por esta razón, es necesario que se regule adecuadamente su tratamiento por medio de una serie de mecanismos, derechos y principios que garanticen el derecho a la protección de datos personales. En Latinoamérica, varios países lo han reconocido constitucionalmente, sin embargo, hasta ahora no se han brindado las garantías suficientes para efectivizar su protección. Aún más grave, en ciertos países no existe regulación respecto a la transferencia internacional de datos personales (TIDP). El presente trabajo abordará el problema de que Latinoamérica no cuenta con un nivel de protección que logre garantizar seguridad y regular adecuadamente la TIDP.

Palabras clave: Privacidad; Protección; Tratamiento; Estándares; Derecho; Garantías; Dato

Summary

On an international level, personal data has become an intangible asset that enables productivity and competitiveness. For this reason, it has been necessary for its treatment to be properly regulated by a series of mechanisms, rights and principles that guarantee the right to the protection of personal data. In Latin America, several countries have recognized constitutionally, however, until now, sufficient guarantees have not been provided to make their protection effective. Even more serious, in certain countries there is no regulation regarding the international transfer of personal data (ITPD). This document raises the problem that Latin America does not have a level of protection that guarantee security and properly regulate the ITPD.

Key words: Privacy; Protection; Treatment; Standards; Right; Guarantee; Data

Resumo

Os dados pessoais passaram a fazer parte de um ativo intangível a nível internacional que permite a produtividade e a competitividade. Por esta razão, é necessário que se regule adequadamente seu tratamento por uma série de mecanismos, direitos e princípios que garantam o direito a proteção de dados pessoais. Na América Latina, vários países os reconhecem constitucionalmente, mas, até agora não se outorgaram as garantias suficientes para tornar efetiva sua proteção. Ainda mais grave, em alguns países não existe regulamentação sobre a transferência internacional de dados pessoais (TIDP). O presente trabalho abordará o problema de que na América Latina não existe um nível de proteção que outorgue a garantia de segurança e a regulamentação adequada da TIDP.

Palavras chave: Privacidade; Proteção; Tratamento; Premissas; Direito; Garantias; Dado

* Abogado por la Universidad de las Américas. Máster en Propiedad Intelectual y Nuevas Tecnologías en la Universidad Internacional de la Rioja (cursando). Consultor en derecho de competencia, laboral, societario, contractual y en nuevas tecnologías, con experiencia en protección de datos y concentraciones económicas. Actualmente, abogado en la Superintendencia de Control de Poder del Mercado.

INTRODUCCIÓN

El incremento de empresas cuyo modelo de negocios se centran en el uso de plataformas digitales durante los últimos años ha sido un fenómeno global que, por un lado, podría llevar al resquebrajamiento de algunos paradigmas del derecho de la competencia y por otro, al aprovechamiento y uso inadecuado de datos personales. Casos como Cambridge Analytica y las investigaciones que se encuentran en curso en Alemania (*Bundeskartellamt*) contra Facebook, en la Unión Europea (UE) con escudo de privacidad UE-Estados Unidos y el Congreso de los Estados Unidos contra Amazon, Facebook, Google y Apple, nos ha hecho reflexionar sobre la importancia que tienen los datos personales en la sociedad actual, pues, es un hecho que la información personal ha permitido construir empresas de miles de millones de dólares.

Los datos personales se han vuelto a nivel internacional un activo intangible que permite la productividad y competitividad. Razón por la cual se ha visto necesario que se regule adecuadamente su tratamiento por una serie de mecanismos, derechos y principios que garanticen el derecho a la protección de datos personales. El tratamiento de datos personales (TDP) debe estar concebido para servir a la humanidad, de ahí que, dentro del Reglamento General de Protección de Datos (por sus siglas en inglés GDPR) de la UE, en el considerando 4, no se concibe al derecho a la protección de datos personales como un derecho absoluto, sino en relación con su función en la sociedad y para mantener el equilibrio con otros derechos.

En Latinoamérica, varios países han reconocido el derecho a la protección de datos personales constitucionalmente, sin embargo, hasta ahora no se han brindado las garantías suficientes para efectivizar su protección. Aún más grave, en ciertos países no existe regulación respecto a la transferencia internacional de datos personales (TIDP), motivo por el cual, si los datos personales de sus ciudadanos son objeto de una de estas transferencias se encontrarían en un total estado de desprotección. La situación anterior, no solo dificulta a los países latinoamericanos su relación con dos de sus más importantes aliados comerciales, Estados Unidos y la UE, sino que además «[...] acentúa las diferencias conceptuales entre los diversos sistemas de derechos humanos, cuya característica fundamental debe residir precisamente en su universalidad» (Maqueo, Moreno y Recio 2017, 93). Históricamente, algunas legislaciones han mostrado una gran preocupación por la protección de datos personales, como es el caso de la UE que, en el 2016, con el GDPR estableció un conjunto de mecanismos para la TIDP. Por esta razón, en la UE se exige un nivel adecuado de protección a terceros países u organizaciones internacionales, a efectos de autorizar una transferencia internacional de datos. Tendencia que se ha seguido a nivel mundial: en EE.UU. con el *Privacy Shield*, la *California Consumer Privacy Act* (CCPA) y la *Stop Hacks and Improve Electronic Data Security Act* (SHIELD); y, en Latinoamérica, con la adopción y aplicación de estándares internacionales en sus legislaciones específicas sobre protección de datos personales.

En el presente trabajo se pretende evidenciar que Latinoamérica no cuenta con un nivel de protección que logre garantizar seguridad y regular adecuadamente TIDP. Para efectos de esta investigación se mencionarán los marcos regulatorios de Argentina, México y Ecuador.

PROTECCIÓN, TRATAMIENTO Y TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

En nuestra época, los avances tecnológicos se han fundido con nuestro diario vivir y prácticamente todas las áreas de la sociedad se ven afectadas por la tecnología. Este panorama ha permitido que el tráfico de información se realice rápidamente y en grandes cantidades; de suerte que, en ocasiones, se constituye

en una herramienta para facilitar el comercio y el desarrollo de las sociedades y, otras veces, en un riesgo para los derechos de las personas (Rebollo y Serrano 2017, 21-3).

Las economías digitales se han convertido en objeto de un sin número de estudios, conferencias, publicaciones, debates legislativos y comentarios de todas las personas. Desde este punto de vista, nos hemos podido dar cuenta de que nuestros datos personales, primero, han sido utilizados para fines que nunca habríamos imaginado y, luego, se han transferido entre cientos de empresas a nivel mundial. En este sentido, también nos dimos cuenta de que las autoridades no han tomado las decisiones apropiadas para evitar que el uso de datos vulnere derechos y concentre poder en manos de unos pocos.

Ahora bien, para luchar contra estos abusos, es necesario que las diferentes ramas del derecho, como el derecho de competencia y el derecho a la protección de datos personales, colaboren; ya vimos que existe una relación y un apoyo entre las agencias de control de cada una de estas ramas, por ej., en el caso de la *Bundeskartellamt* contra Facebook y, al parecer, este es el camino correcto que debemos tomar. El uso de datos sin control, sin normas que impongan límites y principios a seguir, puede, como ha sido noticia, afectar hasta a una elección presidencial. No obstante, para entender mejor qué medidas se deben tomar para proteger los datos personales, empezaremos con los elementos básicos del tema.

1. Datos personales y protección de datos personales

Los datos personales pueden ser tan sencillos como los nombres y apellidos, tan complejos como los datos biométricos, o tan sensibles como los relacionados con la salud. Los datos personales son una lista extensa y abierta que va creciendo, como el número de seguro social, los datos genéticos y hasta nuestros *likes* en Facebook. En realidad, hay miles de formas en las que nuestro propio día a día nos hace identificables (Gil 2016, 45). En este sentido, un dato personal, a simples rasgos es la información que permite identificar concretamente a una persona; específicamente, las Directrices sobre Protección de la Privacidad y Flujo Transfronterizo de Datos Personales de la Organización para la Cooperación y el Desarrollo Económico (OCDE) definen al dato personal como «[...] toda información relativa a un individuo identificado o identificable.».

Al respecto, el Tribunal Europeo de Derechos Humanos, al resolver los casos Leander vs. Suecia (1987), Z vs. Finlandia (1997) y Amann vs. Suiza (2000), señaló que los datos personales son «[...] cualquier información relativa a un individuo identificado o identificable», concepto que el Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE en el Dictamen número 4/2007 y el GDPR en su artículo 4, punto 1 acogen en su definición de dato personal.

La protección de datos personales surge en la década de los años setenta a través del desarrollo tanto legislativo como jurisprudencial de dos sistemas legales contrapuestos, el norteamericano y el europeo (Zaballos 2013, 88). Sus respectivas doctrinas son las bases más relevantes para el desarrollo de la protección de datos personales en todo el mundo.

En estados Unidos, la protección de datos personales, en sus inicios se fundamentó en el derecho a la privacidad, que tiene como origen la doctrina de *Privacy Law* desarrollada por Samuel Warren y Louis Brandeis en 1890. En Europa, en cambio, las ideas norteamericanas fueron sustituidas por la doctrina de la autodeterminación informativa, que consiste en el derecho de cada persona a determinar en qué medida puede comunicar a otros sus datos personales, idea creada por Alan Westin en 1967 (Lucena 2012, 129).

2. Configuración del derecho fundamental a la protección de datos personales

La protección de los derechos fundamentales ha variado a lo largo del tiempo, y no siempre se ha concedido el mismo nivel de protección ni se han reconocido los mismos derechos fundamentales. La Corte Constitucional de Colombia, en la sentencia C-748/11, explica que el derecho a la protección de datos personales partió como una garantía a la vida privada, que luego pasó a ser entendida como el

derecho a la autodeterminación informativa y, finalmente, como un derecho autónomo.

El derecho fundamental a la protección de datos personales comprende un conjunto de derechos que la persona puede ejercer frente a quienes sean poseedores de bases de datos públicos o privados, para conocer el contenido, uso y destino de su información (Guzmán 2013, 114). Asimismo, este derecho tiene un carácter instrumental frente a otros derechos reconocidos. Por un lado, porque el uso indebido de datos personales puede afectar otros derechos, como el de educación o salud; y, por otro, ya que permite a la persona el mantenimiento y desarrollo de su individualidad, la protección de sus derechos, bienes personales, sociales, familiares y patrimoniales (Puccinelli 1999, 68). Por consiguiente, se lo concibe como un mecanismo jurídico que otorga a la persona el control y disposición de todos sus datos (Sanz 2008, 139).

De igual manera, el derecho a la protección de datos personales es un derecho autónomo, pues protege datos de carácter personal de todo tipo y no solo los relativos al ámbito más íntimo de la vida privada. Pero también es un derecho de carácter instrumental; porque, a través de él se garantiza a las personas el pleno ejercicio de varios de sus derechos fundamentales, como el acceso a la educación, vivienda, crédito, entre otros (Villalba 2017, 38). En definitiva, su contenido conlleva una pluralidad de derechos básicos, principios y garantías que lo convierte en un derecho complejo (Valverde 2013, 21).

En este sentido, para que el ejercicio de este derecho sea efectivo, a través de él se debe poder tener acceso, actualizar, rectificar y eliminar mis datos, así como poder oponerse a su tratamiento. De aquí resultan los llamados derechos ARCO, necesarios para un adecuado tratamiento de datos a los que luego, con el GDPR, se suman el derecho a la portabilidad de los datos, la limitación del tratamiento y el derecho al olvido. Ahora, todos ellos en conjunto se denominan derechos AROLPOD. Estas garantías y derechos, en los últimos años se han visto vulnerados. Primero, porque la disparidad existente en la regulación de protección de datos entre países ocasiona una incertidumbre; dado que, debido a las plataformas digitales, las personas interactúan a nivel global y, así, sus datos también se transfieren a distintos puntos del planeta. Segundo, porque ciertos países, como es el caso de Ecuador, no cuentan todavía con una ley de protección de datos personales.

Uno de los casos más recientes e importantes es el de la agencia de competencia de Alemania**,** que impuso a Facebook restricciones de largo alcance en el procesamiento de datos de los usuarios, pues acusa a Facebook de no solo recopilar datos personales que surgen al usar la red social, sino que también reúne datos que los usuarios dejan en WhatsApp, Instagram, Masquerade, Oculus y muchos otros servicios que también pertenecen a Facebook (Bundeskartellamt 2019, 7-8), ocasionando a los usuarios de esta red social una afectación a su autonomía personal y la protección de su derecho a la autodeterminación informativa, que también está protegida por el GDPR. En el contexto de los grandes obstáculos para el cambio que existen para los usuarios de la red (efectos de bloqueo), también representa una explotación de los usuarios que es relevante según la ley antimonopolio, porque la competencia ya no es efectiva debido a la posición dominante de Facebook.

Ahora bien, a pesar de su alcance, el derecho a la protección de datos personales no se puede entender como ilimitado, en vista de que existen diferentes razones, por las que se pueden establecer limitaciones, por ej., las transferencias internacionales. Como bien señala Garriga (2016, 94), «[...] el ciudadano de un Estado social de Derecho no tiene un derecho absoluto e ilimitado sobre sus datos, sino que por ser parte de un conglomerado tiene que aceptar limitaciones en aras del interés superior». La realidad es que los datos son necesarios para realizar varias actividades lícitas, legítimas y de interés general o particular; por ende, el derecho a la protección de datos no es para oponerse a su tratamiento, sino para exigir uno correcto (Remolina, Tenorio y Quintero 2018, 48).

3. Principios rectores

El derecho a la protección de datos personales se garantiza mediante la previsión**,** en la ley, de una serie de mecanismos y elementos dirigidos a asegurar el

control y el dominio sobre los datos. Con el fin de preservar este derecho fundamental se necesita aplicar una serie de criterios específicos para su tratamiento (Sanz 2008, 139). En diferentes instrumentos jurídicos internacionales se han establecido una serie de principios que velan por el respeto a la protección de datos personales. Sin embargo, en el GDPR se han incluido los más importantes, los que la mayoría de las legislaciones sobre protección de datos han tomado como modelo y que, hoy en día, son la base sobre la que el derecho a la protección de datos se efectiviza.

El principio de licitud, lealtad y transparencia exige a los responsables y encargados del tratamiento de datos que solo lo podrán realizar si existe una justificación legal suficiente y que se deberá informar al titular de los datos sobre todo el procedimiento, sin engaño y de la forma en que se indicó (Mendoza 2017, 276). Por otro lado, el principio de limitación de la finalidad establece que el TDP se realizará únicamente en el ámbito de finalidades legítimas, explicitas y determinadas; y sus fines deberán estar determinados con precisión (Ortiz 2002, 134). El de proporcionalidad indica que nada más se deberán tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

De igual forma, los demás principios de exactitud, vigencia, integridad y confidencialidad señalan que los datos deben estar completos, el tiempo por el cual se debe conservar los datos y la seguridad que se debe brindar cuando se está en su posesión. Este andamiaje se refuerza con el principio de responsabilidad proactiva, que obliga a los responsables y encargados del tratamiento a utilizar medidas apropiadas, efectivas y verificables que le permitan probar el correcto cumplimiento de las normas sobre protección de datos (Quesada 2017, 56).

4. Tratamiento de datos personales (TDP) y Transferencia internacional de datos personales (TIDP)

El TDP se ha convertido en una actividad cotidiana y de alta importancia para el Estado, las empresas y los particulares. Todos requieren de información personal para tomar y ejecutar decisiones de diversa naturaleza (económica, seguridad nacional, política, laboral, financiera, comercial, entre otros). La regulación del TDP no se opone al uso de datos sino a su eventual abuso, pues un inadecuado tratamiento de datos puede provocar una vulneración de los derechos humanos de sus titulares (Remolina et al. 2018, 48).

El Art. 4, número 2 del GDPR señala que el tratamiento de datos es:

> [...] Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

De esta definición se puede extraer que el TDP se puede dar de diferentes maneras, puede ser automatizado o no, y tiene la posibilidad de que existan 3 partes en un tratamiento de datos: 1) El interesado, que es la persona física titular de los datos personales; 2) El responsable, que es la persona física o jurídica, de naturaleza pública o privada que, solo o junto con otros, determina los fines y medios del TDP; y 3) El encargado, o es la persona física o jurídica, de naturaleza pública o privada, que lleve a cabo un TDP por cuenta del responsable del TDP. Por otro lado, De Terwangne (2009, 177) explica que**,** en los procesos de integración económica**,** existe la necesidad de exportar e importar datos personales entre las empresas privadas, las personas o las autoridades de los diferentes países. Procesos como el incremento de las relaciones comerciales internacionales y sociales hicieron necesario expedir normas sobre el tratamiento de datos que conciliaran la protección de la privacidad y su eventual transferencia internacional.

A partir del GDPR y de la sentencia Lindqvist vs. Gäta hovärtt., del Tribunal de Justicia de la Unión Europea (TJUE), una TIDP se produce cuando los datos personales que son tratados por un responsable o encargado del tratamiento de datos que se encuentra en el

Espacio Económico Europeo son enviados fuera de dicho territorio a un tercer país u organización internacional. De forma más amplia, es una transmisión realizada por cualquier medio, a través de las fronteras nacionales, de datos personales que sean objeto de un tratamiento de datos o cuando estos se reúnan con el propósito de someterlos al tratamiento que sea (Grande 2016, 59). En definitiva, una TIDP es un proceso de exportación o importación de datos personales contenidos en una base de datos ubicados en un Estado y que son enviados a otro o varios Estados.

La TIDP se puede dar por motivos muy variados, por ej.: «[...] seguridad pública, seguridad nacional, investigaciones contra el terrorismo, labores de inteligencia militar o policial, cooperación judicial, cooperación internacional en general, protección de un interés del titular del dato y controles de inmigración» (Remolina 2010, 376). La TIDP es de vital importancia tanto para el funcionamiento del mercado por su incidencia en el comercio internacional, como para el desarrollo de las actividades de un Estado.

Por las disparidades existentes entre las legislaciones nacionales sobre protección de datos, su transferencia internacional puede poner en riesgo los derechos de las personas. Sin embargo, sin estas transferencias difícilmente se podría dar el comercio mundial (Castellanos 2017, 6). Así pues, para evitar los posibles perjuicios que podría causar una TIDP a la privacidad de las personas y poder garantizar la libre circulación de datos personales, los Estados, así como las Uniones geopolíticas han establecido estándares de protección o convenios para regularlas.[1]

Para que los datos personales puedan ser objeto de TIDP a más de cumplir con los principios rectores para la protección de datos, se debe tomar en consideración los principios de continuidad de la protección y el principio de equivalencia necesarios para poder contar con un nivel adecuado de protección para la TIDP. El principio de continuidad de la protección tiene como propósito que, cuando los datos personales salgan de las fronteras de un Estado y se dirijan a un tercer país u organización, no pierdan el nivel de protección con el que contaban en el país de origen de los datos. Se busca que el nivel de protección del país exportador se garantice en el país importador.

Por otro lado, a nivel internacional, no todos los Estados ofrecen las mismas garantías en cuanto a la protección de datos personales. Por esta falta de uniformidad entre las legislaciones de los países, diferentes instrumentos jurídicos internacionales, como el GDPR, así como la legislación de Argentina o la de México, las Directrices de la OCDE y el *Privacy framework* de la APEC exigen, para autorizar una TIDP, que el país receptor de los datos cuente con un nivel de protección equivalente al que ofrece el país emisor.

El exigir un nivel adecuado de protección para autorizar una TIDP constituye el principio de equivalencia, que tiene como fin, según la sentencia del TJUE de 6 de octubre de 2015, en el caso Schrems, asunto C-362/14, garantizar: «[...] efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en el país emisor de datos personales.».

ESTÁNDARES PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

Por las disparidades existentes entre las legislaciones nacionales sobre protección de datos, la TIDP puede poner en riesgo los derechos de las personas. Sin embargo, como señala Castellanos (2017, 6), sin la TIDP, difícilmente se podría dar el comercio mundial. Así pues, para evitar los posibles perjuicios que a la

1 De las definiciones expuestas, en una transferencia internacional de datos existe la participación de dos partes: el exportador de datos, definido en el Art. 4 literal e) del Decreto N°. 414/009 como «[...] la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realiza una transferencia de datos de carácter personal a un país tercero»; y, el destinatario, que, conforme el Art. 4 del GDPR, es «[...] la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comunican datos personales, se trate o no de un tercero».

privacidad de las personas podría causar una TIDP y poder garantizar la libre circulación de datos personales, los Estados, así como las Uniones geopolíticas (como la UE) han establecido estándares de protección o convenios para regular la TIDP.

1. EE.UU. de América

En EE.UU., el derecho a la protección de datos personales tiene, como antecedente principal, el derecho a la privacidad o *Right to Privacy*. Esta doctrina, construida por Louis Brandeis y Samuel Warren en 1890, aportó una reinterpretación de los precedentes en la materia ya que se comenzó a proteger la privacidad fuera del derecho a la propiedad (Saltor 2013, 275). No obstante, el sistema de protección de datos norteamericano «[...] no reconoce la protección de la privacidad mediante una legislación específica, sino que ello se efectúa a través de normativas sectoriales que, mediante la complementación de reglamentaciones y códigos de adhesión, propician un marco regulador singular» (Castellanos 2017, 14).

En EE.UU., en el siglo XX, se dictaron tres leyes que establecen los principios rectores que configuran el derecho a la privacidad en este país: la *Fredoom of Information Act* (FOIA) de 1966, la *Privacy Act* de 1974 y la *Right to Financial Privacy Act* (RFPA) de 1978. En el siglo XXI aparecieron: el *Safe Harbor* en el 2000, el *Privacy Shield* en 2016 para regular la TIDP con Europa, la *California Consumer Privacy Act* (CCPA) de 2018 y la *Stop Hacks and Improve Electronic Data Security Act* (SHIELD) de 2019, que entraron en vigor respectivamente en enero y marzo de 2020.

2. Del *Safe Harbour* al *Privacy Shield*

El *Safe Harbour* fue un conjunto de principios negociados entre Estados Unidos y la UE, para poder transferir datos personales entre estos territorios. Se constituyó como una institución jurídica que permitía a las empresas la transmisión de datos hacia sociedades en Estados Unidos y, a la vez, exigía el cumplimiento de una serie de principios, tales como: la posibilidad de oposición de los afectados, notificación a los afectados, transferencia ulterior a terceras empresas, integridad de los datos, seguridad, derecho de acceso y la aplicación de mecanismos que garanticen la resolución de conflictos y el cumplimiento de los principios (Ortega 2017, 86).

En el Anexo I de la Decisión, la UE reconoce solo a la *Federal Trade Commission* y al Departamento de Transportes como organismos jurídicos competentes en los Estados Unidos. Pero siempre con arreglo a las competencias que sus propias leyes les otorgan, de manera que el sistema de protección de datos en Estados Unidos es sectorial y no todos los organismos ni materias están incluidos en este acuerdo. Debido a estos problemas, y a pesar de que miles de empresas norteamericanas se adhirieron al acuerdo, en el año 2015, la sentencia del TJUE emitida en el caso Schrems invalidó la Decisión de la CE del año 2000, por la que se aprobaba el acuerdo de *Safe Harbour*, que era el principal marco jurídico que facultaba a las empresas y organizaciones de la UE a realizar TIDP a Estados Unidos (López 2017, 36).

En los fundamentos de hecho de la Sentencia, el señor Maximillian Schrems, de nacionalidad austriaca, que era usuario de la red *Facebook* desde 2008, presentó una reclamación ante el *Data Protection Commissioner* el 25 de junio de 2013, en la cual solicitaba que se prohibiera a *Facebook Ireland* transferir sus datos personales a Estados Unidos, toda vez que este país no garantizaba una protección suficiente de los datos personales conservados en su territorio.

Mediante la Decisión de ejecución (UE) N.º 2016/1250, de la CE, de fecha 12 de julio de 2016, se acordó el *Privacy Shield*, con el que se permitió de nuevo realizar TIDP desde la UE a los Estados Unidos sin necesidad de abordar la autorización de la entidad de control (Castellanos 2017, 26). Su contenido se compone de una serie de principios que vienen consagrados en los Anexos I y II de la Decisión, los cuales, en sentido amplio se estructuran en siete principios generales y dieciséis que los complementan.

Tanto el *Safe Harbour* como el *Privacy Shield* se concibieron como mecanismos para solucionar la ausencia de regulación en los Estados Unidos sobre el TDP y permitir la TIDP con la UE. Estos marcos regulatorios fueron su estándar de protección para realizar la

TIDP con la UE. No obstante, el *Safe Harbour*, que fue el marco regulatorio que más tiempo estuvo vigente, aunque fue acogido por miles de empresa americanas, no era de carácter obligatorio, no estaba en un rango igual que otras leyes americanas y se encontraba desactualizado; tal estatus dificultaba su aplicación y, por ende, tuvo que ser sustituido.

El *Privacy Shield*, si bien pretendía cubrir los vacíos de su antecesor presentó aún los mismos problemas, de suerte que no podía constituirse en un marco regulatorio obligatorio y así, no garantizaba que los Estados Unidos puedan ser considerado un país con un nivel adecuado de protección de datos personales. Por esta razón, el TJUE, en el asunto C-311/18 (Scherms II) declaró que la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-Estados Unidos (*Privacy Shield*) es inválida. Aunque el mismo Tribunal, en esa ocasión, también confirmó que las cláusulas contractuales estándar siguen siendo una herramienta válida para la transferencia de datos personales a procesadores establecidos en terceros países.

En cuanto a las últimas leyes promulgadas, está primero la CCPA, que es una ley de privacidad del consumidor que se aprobó en el Estado de California el 28 de junio de 2018. Desde que se encontraba como proyecto de ley ha sido descrita como el GDPR en los Estados Unidos. De hecho, esta ley es la legislación de privacidad más fuerte promulgada en cualquier Estado hasta el momento. Pues, otorga más poder a los consumidores sobre sus datos privados. Dada la presencia de gigantes tecnológicos con sede en California como Google y Facebook, se piensa que la CCPA está preparada para tener efectos de gran alcance en la privacidad de los datos personales.

Estos efectos se vieron de inmediato, pues casi simultáneamente, el Estado de Nueva York promulgó la ley SHIELD, que modifica la ley actual de notificación de violación de datos del Estado, impone una seguridad de datos más amplia y la notificación de violación de datos requisitos para las empresas, con la esperanza de garantizar una mejor protección para los residentes de Nueva York de las violaciones de datos de su información privada. Por la importancia del tema, se ha señalado que, en los próximos años, otros Estados seguirán el ejemplo de la CCPA y la SHIELD, y se apegarán cada vez más a los estándares de GPDR (Cobb 2019, 18).

3. Unión Europea

En Europa, después de la II Guerra Mundial, se sintió la necesidad y la obligación de defender los derechos humanos y, con la cooperación entre sus países, se creó la primera organización internacional en el continente: el Consejo de Europa (CE) (Cerda 2011, 347). Sobre esta base, a fin de proteger los derechos humanos y promover el Estado de Derecho, el CE adoptó el Convenio Europeo de Derechos Humanos (CEDH), en cuyo Art. 8 consta el derecho a la protección de datos personales.

La regulación sobre protección de datos personales en la UE se ha desarrollado a lo largo del tiempo con gran interés; debido a que, por la evolución de las tecnologías de la información y comunicación (TIC), se pudo realizar un intercambio inmediato de información sin límites físicos. Aquí es donde radica la importancia del derecho a la protección de datos personales, ya que permite proteger en estos intercambios de datos personales los derechos de los titulares de estos datos (Rojas 2014, 110).

En la UE, desde el «Convenio 108» para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981, se han emitido varias normas comunitarias que regulan la protección de datos personales, que prescriben una «protección equivalente» entre los países partes, y buscan una cooperación internacional a través de las autoridades locales de cada país.

De manera conjunta con la normativa comunitaria, los Estados que conforman la UE, en su legislación interna emitieron una serie de leyes que protegían en cierta manera los datos personales; por ejemplo en Alemania, la Ley de Hesse de 1970 y la Ley Federal Alemana de 1977. En Francia la Ley relativa a la informática, los ficheros y las libertades de 1978. Una de

las más significativas es la Ley Federal de Protección de Datos de Austria de 1978, donde se consagra, en el Art. 1, el derecho fundamental de todo ciudadano a la confidencialidad del tratamiento y comunicación de sus datos personales.

De la mano con la regulación normativa sobre protección de datos personales, en la UE hubo un importante desarrollo jurisprudencial. Uno de sus hitos más importantes fue la sentencia 209/83, dictada por el Tribunal Constitucional Federal Alemán el 15 de diciembre de 1983 sobre el censo de 1982. En ella, por primera vez se concibió al derecho a la protección de datos personales como un derecho autónomo e independiente del derecho a la vida privada; fue el primer paso para la construcción y desarrollo del derecho en este ámbito.

Una de las normativas más importantes fue la Directiva 95/46/CE, del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo tocante al TDP y a la libre circulación de estos datos. Los Estados miembros de la UE, a efectos de cumplir con las obligaciones que imponía este Directiva, fueron elevando progresivamente el nivel de protección de los datos personales, de forma que se produjo «[...] un efecto homogeneizador de los medios de protección y de los mecanismos para la eficacia de los derechos» (Rebollo 2008, 105).

Como resultado de este proceso, con la expedición del GDPR, la normativa de la UE en el campo de la protección de los datos se ha constituido como la más exigente del planeta (Guasch 2012, 422).

4. Reglamento General de Protección de Datos (GDPR)

En Europa el 27-IV-2016 se adoptó el Reglamento (UE) 2016/679 del Parlamento y del Consejo, con el que se derogó la Directiva 95/46/CE a fin de reformar la normativa ya existente sobre protección de datos personales y adaptarla al nuevo contexto mundial que, después del caso de *Cambridge Analytica*, cambió notablemente. Con el GDPR, la UE estableció todo un sistema de protección de datos personales que modificó reglas ya existentes, desarrolló aquellas que eran muy básicas y creó otras que eran necesarias. Esta novedad se orienta a una transición hacia una economía centralizada en los datos y la creación de un mercado único digital (Moritz y Gibello 2017, 116).

Respecto a la TIDP, con el GDPR, en la UE se estableció un conjunto de mecanismos para transferir datos a terceros países: decisiones de adecuación, normas contractuales estándar, normas corporativas vinculantes, mecanismos de certificación y códigos de conducta. En la UE, también debido al GDPR, para realizar una TIDP se requiere un nivel adecuado de protección. Razón por la cual, Latinoamérica se encuentra en los últimos años en proceso de adoptar estándares internacionales para la protección de datos personales y Estados Unidos debió implementar el *Privacy Shield* que, ahora, después de declarado invalido, tendrá que proponer algún nuevo escudo de privacidad o promulgar una ley que garantice la protección de datos.

En el GDPR existen tres vías por las cuales se puede realizar una TIDP, las cuales tienen distintos niveles de protección. La vía y el nivel más riguroso es una transferencia basada en una decisión de adecuación en que la Comisión Europea, después de una evaluación global del ordenamiento jurídico de un país, declara que cuenta con un nivel adecuado de protección.

Luego viene la transferencia mediante garantías adecuadas, el establecimiento de normas corporativas vinculantes o certificaciones y, por último, mediante casos excepcionales contemplados en el art. 49 del GDPR, tales como: por razones de interés público, celebración o ejecución de un contrato o cuando haya el interesado dado su consentimiento, siempre y cuando haya sido informado de los riesgos de la TIDP debido a la ausencia de una decisión de adecuación y de garantías adecuadas.

Estas tres vías son el estándar europeo de protección para realizar una TIDP, el cual se diferencia bastante del americano, que solo cuenta con normas corporativas vinculantes para la TIDP y que ofrecen protección a los datos de las personas.

REGULACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES EN AMÉRICA LATINA

En América Latina, la regulación del derecho a la protección de datos personales sigue un ritmo propio y tiene ciertas características que ameritan analizarse.

Recientemente, en las constituciones latinoamericanas se incorporó, como derecho autónomo, la protección de datos personales, frente a la necesidad de dar respuesta al proceso de evolución tecnológica (Ordóñez 2017, 85) y a los peligros de un uso indiscriminado e ilícito de datos por parte de las plataformas digitales. La razón es que los servicios que brindan se comercializan como gratuitos; aunque, en realidad, exigen un pago en forma de datos personales de los clientes que plataformas como *Google* y *Amazon* han usado para perjudicar a sus competidores, de forma que ponen en riesgo la información de las personas.

1. República de Argentina

En el Art. 43 de la Constitución de la República de Argentina se halla consagrado el derecho a la protección de datos personales. De este artículo se deriva la obligación de los organismos públicos de garantizar el acceso a la información, confidencialidad, supresión y rectificación de los datos personales. Pero, donde se encuentra reglamentada la protección de datos personales es en la Ley 25.336, promulgada el 4 de octubre del año 2000. En el Art. 2 de la Ley 25.336 se regula la protección de datos personales, sin hacer una distinción entre el ámbito público y privado.

En el capítulo 2 de la Ley 25.326 se establecen los principios generales en materia de protección de datos personales y las garantías que se deben dar al tratarlos. Allí destaca el principio de licitud para la formación de archivos de datos. También el principio de calidad de datos, que se traduce en que la recolección de datos no puede hacerse por medios desleales y que dichos datos deben ser ciertos y exactos, y su almacenamiento debe permitir el derecho de acceso a su titular. Además el principio de la información, en el sentido de que se debe informar a los titulares para qué serán tratados los datos y quiénes serán sus destinatarios y el principio de responsabilidad demostrada.

En Argentina, conforme el Art. 29, el órgano de control que gozara de autonomía funcional y actuara como órgano descentralizado en el ámbito del ministerio de justicia y Derechos Humanos de la Nación es la Agencia de Acceso a la Información Pública (y específicamente dependiente de esta es la Dirección Nacional de Protección de Datos Personales). Ella es la encargada de supervisar que se cumplan las disposiciones contenidas en la Ley 25.326, en la Ley de Acceso a la Información, y en la Ley del Registro.

Respecto a la transferencia internacional de datos se sigue el modelo europeo para autorizar una TIDP, que el Estado receptor de los datos cuente con un nivel adecuado de protección.

2. Estados Unidos Mexicanos

En México, recién con las reformas constitucionales del año 2007 y 2009 se protegen constitucionalmente los datos personales, se consagra explícitamente el derecho a la protección de los datos personales y se establecen los derechos ARCO como núcleo fundamental de este derecho (Da Cunha 2011, 323). En el año 2010 se adopta la Ley Federal de Protección de Datos en Posesión de los Particulares (LFPDPP), que tiene un ámbito de aplicación únicamente privado. Esta ley se basa en el marco normativo europeo, que apunta hacia la tendencia mundial de regulación jurídica de los datos personales para garantizar el derecho a la vida privada de los individuos, con respecto al TDP.

En la LFPDPP se establece una serie de principios para la protección de datos personales, como son: el de licitud, consentimiento, calidad, finalidad, lealtad, proporcionalidad y responsabilidad. En su capítulo VI se establecen las competencias de la Autoridad reguladora, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Dentro del capítulo IV, en relación con el Reglamento de LDPDPP de 21 diciembre 2011, se regula los derechos ARCO más no los AROLPOD. En el capítulo V se desarrolla la TIDP, pero no se exige un nivel adecuado de protección, sino tan solo consentimiento del titular de los datos y enumera ciertos supuestos que no requieren consentimiento, además no desarrolla las transferencias ulteriores.

El 26 de enero de 2017 se expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), con el fin de regular el ámbito público del TDP. Son sujetos obligados conforme el artículo 1, en el ámbito federal, estatal y municipal: «[...] cualquier autoridad, entidad, órgano y organismo de los poderes ejecutivo, legislativo y judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos». A los particulares, sean personas naturales o jurídicas, no se les aplica esta Ley sino la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En el capítulo I del Título segundo de la LGPDPPSO, en relación con la LDPDPP se aumenta y se desarrolla un conjunto de principios que el responsable del tratamiento debe cumplir cuando recolecta, almacena, usa, circula o realiza cualquier actividad con datos personales, como son los: principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad demostrada en el TDP. De la autoridad de protección de datos personales señala que sigue siendo el INAI. Y en cuanto a la TIDP, en el artículo 68 de la Ley aplicable a los sujetos obligados se señala que:

> [...] El responsable solo podrá transferir o hacer remisión de datos personales fuera del territorio nacional cuando el tercero receptor o el encargado se obliguen a proteger los datos personales conforme a los principios y deberes que establece la presente Ley y las disposiciones que resulten aplicables en la materia.

Así pues, se evidencia que, para autorizar una transferencia internacional de datos se exige el cumplimiento de garantías adecuadas, además de necesitar el responsable del tratamiento, el consentimiento del titular de los datos y la obligación de comunicar al receptor de los datos personales las finalidades, conforme las cuales se tratan los datos personales frente al titular. No obstante, no se requiere un nivel adecuado de protección como en la UE con el GDPR.

3. República del Ecuador

Desde la incorporación y posterior desarrollo de las nuevas tecnologías, el Ecuador ha pasado por una revolución en el manejo de la información. La combinación de estas herramientas tecnológicas con el fenómeno de la globalización trajo consigo múltiples ventajas, por ej.: el desarrollo del comercio electrónico, la implementación de un gobierno en línea, y la virtualización de las relaciones de los ciudadanos, proveedores, consumidores y autoridades (Estrada, Estrada, Rodríguez y Tipantuña 2015, 54).

Todas estas actividades requieren de un TDP o de una TIDP, sin embargo, el Ecuador, en este contexto, no cuenta con una regulación que garantice un nivel adecuado de protección de datos personales. Este particular se evidencia porque la protección de datos personales en el país es incompleta, sectorial, contradictoria y desactualizada. De ahí que sea insuficiente para proteger adecuadamente los derechos de los titulares de datos personales y, además, inexistente respecto a la TIDP.

En el Ecuador se han presentado tres proyectos de ley para regular la protección de datos personales: el primero en el año 2010, por el asambleísta Vethowen Chica; el segundo en el año 2016, por la asambleísta Gabriela Rivadeneira; y el tercero en el año 2019, realizado por la Dirección Nacional de Registros de Datos Públicos (Dinardap) y el Ministerio de Telecomunicaciones. Este último ha realizado una ardua labor para redactar un nuevo proyecto de ley, que busca cumplir con estándares internacionales y ser aplicado a la realidad ecuatoriana. Esta propuesta, con este fin fue socializada con expertos y con la comunidad en general.

Históricamente, en el Ecuador se ha avanzado muy poco en legislación para la protección de datos personales. Recién en la Constitución Política de 1998

se hacía una pequeña referencia al derecho a la intimidad. Recién en el siglo XXI se han emitido algunas normativas que tratan de regular la protección de datos personales. Entre ellas destacan: la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos del 2002; el reconocimiento del derecho a la protección de datos personales en la Constitución del 2008; el desarrollo de la acción jurisdiccional del hábeas data en la Constitución del 2008 y en la Ley de Garantías Jurisdiccionales y Control Constitucional; y, la entrada en vigencia de la Ley del Sistema Nacional de Registro de Datos Públicos en el año 2010.

Si bien la Constitución del Ecuador reconoce el derecho a la protección de datos personales, la normativa interna, aunque regula en varios cuerpos normativos este derecho, no lo hace correctamente, es insuficiente para otorgar una adecuada protección a los titulares de los datos personales. El ordenamiento jurídico ecuatoriano regula esta materia de forma sectorial. Esta medida estaría bien si es que se lo hiciera de forma completa; sin embargo la regulación, al estar desperdigada en varios cuerpos normativos, es incompleta y en muchos casos contradictoria.

Existen algunos parámetros para el TDP de datos públicos, pero no se desarrollan todos los principios necesarios para un adecuado TDP. Así, los derechos de los titulares de los datos se pueden ejercer por el hábeas data, pero no todos, por ej., la limitación al TDP. Además, no se cuenta con una autoridad de control y no existe regulación respecto al TDP en el ámbito privado, y sobre a la TIDP.

En relación con este asunto, la normativa también está desactualizada y en muchos casos es errónea; ya que los conceptos o están mal desarrollados o ya no responden a los avances tecnológicos, como los conceptos de ficheros o de dato personal.

El Ecuador, en comparación con otros países de la región, no cuenta ni con un nivel mínimo de protección de datos personales. Como se mencionó antes, existen tres proyectos de ley sobre protección de datos que se han presentado en el país. No obstante, solo el último de ellos, el presentado en 2019, cumple con los criterios básicos que debe contener una ley de este tipo.

En general, el proyecto de ley realizado por la Dinardap y el Ministerio de Telecomunicaciones, a diferencia de los otros proyectos de ley mejora en la parte de técnica, redacción y fondo. Este proyecto tiene la influencia de normativas sobre datos personales, como el GDPR, la ley uruguaya, mexicana y española, de ahí que cuente con los cambios regulatorios que se han dado a nivel internacional. Sin embargo, aún le falta corregir errores, incluir algunas disposiciones y desarrollar ciertas figuras para lograr regular adecuadamente la protección de datos personales.

4. Comparación entre las regulaciones

Como se ha visto, el derecho a la protección de datos personales se tutela de una manera diferente a nivel mundial, aunque con una tendencia a dirigirse al modelo europeo. Además, debido a los riesgos de la TIDP, se ha marcado una predisposición de los Estados de exigir un nivel adecuado de protección de datos personales para autorizar una TIDP. Así pues, a partir del análisis realizado sobre la regulación de la protección de datos personales, corresponde efectuar una comparación centrada en los temas que son objeto de este trabajo.

Como se puede notar en la tabla 1, Estados Unidos, con el ahora inválido *Privacy Shield*, la CCPA y la SHIELD, y Argentina y México con sus legislaciones, han intentado alinearse al estándar de protección de datos personales que establece la UE con el GDPR. Se resalta la necesidad de contar con autoridades de control autónomas como la AEPD en España o la CNIL en Francia, para un correcto desarrollo de la protección de datos.

En cuanto a la TIDP, de igual manera se sigue la tendencia europea de establecer niveles de protección adecuados que permitan proteger a los titulares de los datos[2]. (véase Tabla 2)

2 Ecuador es un caso aparte, dado que no cuenta con una ley de protección de datos personales y, en las pocas leyes donde se regula algún aspecto sobre la protección de datos, no se hace mención sobre la TIDP.

Tabla 1: Aspectos generales sobre la protección de datos personales

	Argentina	México	Ecuador	EE.UU.	GDPR (UE)
Norma constitucional sobre la protección de datos	✓	✓	✓	X	—
Legislación general sobre protección de datos personales	✓	✓	X	X	✓
Normativa sectorial en cuanto al TDP	✓	X	X	✓	—
Derechos ARCO	✓	✓	✓*	X	✓
Derechos AROLPOD	X	X	X	X	✓
TDP especial para datos personales sensibles	✓	✓	X	✓	✓
Medidas de seguridad	✓	✓	X	X	✓
Autoridad de control independiente	X	✓	X	X	✓
Recursos administrativos y acciones judiciales	✓	✓	X	X	✓
Obligaciones a los responsables y encargados del TDP	✓	✓	X	✓	✓
Principios para el TDP	✓	✓	X	✓	✓
Regulación sobre la TIDP	✓	✓	X	✓	✓
Sanciones	✓	✓	X	✓	✓

Nota: comparación entre las normativas de protección de datos de países latinoamericanos y los estándares de la RIPD.
El símbolo «—» significa que no aplica.
* Por el Hábeas Data se ejercen los derechos ARCO, más no los nuevos derechos, como el de limitación al TDP.

Tabla 2: Aspectos generales respecto a la TIDP

	Argentina	México	Ecuador	GDPR	Privacy Shield
Definición sobre la TIDP	✓	X	X	X	X
Desarrollo de las TIDP ulteriores	X	X	X	✓	✓
Exigencia de un nivel adecuado para la TIDP	✓	X	X	✓	✓
Garantías adecuadas para la TIDP	X	✓	X	✓	X
Normas corporativas vinculantes para la TIDP	X	✓	X	✓	✓
Casos excepcionales para la TIDP	✓	✓	X	✓	✓
Principios propios de la TIDP	X	X	X	✓	X

Nota: comparación de los niveles de protección para realizar una TIDP

CONCLUSIONES Y RECOMENDACIONES

Desde la incorporación y posterior desarrollo de las nuevas tecnologías, Latinoamérica ha pasado por una revolución en el manejo de la información. La combinación de estas herramientas tecnológicas con el fenómeno de la globalización trajo consigo múltiples ventajas, como: el desarrollo del comercio electrónico, la implementación de un gobierno en línea, y la virtualización de las relaciones de los ciudadanos, proveedores, consumidores y autoridades. Todas estas actividades requieren de la TIDP, de ahí la necesidad de buscar armonizar las legislaciones relativas a la protección de datos personales.

A nivel internacional, por los riesgos que implica una TIDP se ha buscado una armonización de criterios respecto a su regulación, de modo que se pueda establecer un nivel mínimo de protección con el que deben contar los países para poder efectuar una TIDP. La UE y Estados Unidos son quienes más han desarrollado este tema, de forma que sus modelos de protección de datos personales son los que a nivel mundial tienen mayor preeminencia. Estados Unidos adopta un enfoque sectorial y de autorregulación que, con los últimos casos que han salido a luz, principalmente en contra de *Facebook* y *Google*, manifiesta sus falencias, mientras que la UE adopta un enfoque fundamentado en una norma general de aplicación extraterritorial, así como la exigencia de contar con autoridades de control independientes y niveles adecuados de protección que han llevado, desde la entrada en aplicación del GDPR, a multar a varias empresas.

En Latinoamérica, si bien son varios los países que regulan la protección de datos personales para proteger los derechos de sus ciudadanos, y desarrollar el comercio internacional y electrónico, aún existen ciertas falencias en la regulación. Por ejemplo, contar con una autoridad de control independiente, regular adecuadamente la TIDP, poder sancionar a los infractores con multas que puedan causar un grado de responsabilidad y actualizar las legislaciones sobre protección de datos. Falta todavía mucho para lograr la protección que brinda el GDPR, pero un paso importante es comenzar a tener una cultura de protección de nuestros datos personales. Por otro lado, debe existir una interrelación entre las agencias de competencia, defensa del consumidor y las de protección de datos, pues de esta forma se podrá controlar que las empresas y todo aquel que trate datos personales comprenda que no puede usarlos sin cumplir con las garantías y estándares básicos de protección.

La promulgación en el Ecuador de una ley de protección de datos personales permitirá regular la forma en que las empresas nacionales y extranjeras, además de los entes públicos utilizan, procesan, conservan y explotan los datos personales de las personas naturales en el Ecuador. El proyecto de ley construido por la Dinardap es la base por la cual se debe construir la ley de protección de datos, dado que su aprobación traería la oportunidad tanto de desarrollar el comercio internacional como de proteger los datos personales de sus ciudadanos. Sin perjuicio de lo anterior, se recomienda la inclusión de ciertas precisiones en el proyecto, como: precisar adecuadamente un tratamiento especial a los datos personales sensibles, establecer una autoridad de control independiente, mejorar ciertos conceptos (como dato personal), no ser repetitivo en la necesidad de consentimiento del titular de los datos, incluir los conceptos de TIDP, exportador e importador de datos, desarrollar las TIDP ulteriores y definir otra forma de cálculo para aplicar las sanciones pecuniarias y corregir los porcentajes del cálculo de estas sanciones.

BIBLIOGRAFÍA

Bundeskartellamt. 2019. "Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing". Consultado el 25-IV-2020. https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4

Castellanos Rodríguez, Albert. 2017. «El régimen jurídico de las transferencias internacionales de datos personales. Especial mención al marco regulatorio Privacy Shield». *ICPS Working Papers* 350: 1-34. Consultado el 15-IV-2020. https://www.icps.cat/archivos/Workingpapers/wp350.pdf?noga=1

Cerda, Alberto. 2011. «El "nivel adecuado de protección" para las transferencias internacionales de datos personales desde la Unión Europea». *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso 36: 327-356*. Consultado el 20-V-2019. https://scielo.conicyt.cl/pdf/rdpucv/n36/a09.pdf

Cobb, Stephen. 2019. «GDPR: ¿el primer paso hacia una ley de privacidad global?». *ESET* 1: 15-19. Consultado el 20-IV-2020. https://empresas.eset-la.com/archivos/novedades/74/Cybersecurity_Trends_2019_v6-ESP.pdf

Da Cunha, Teresa. 2011. «Las recientes reformas en materia de protección de datos personales en México». *Anuario Jurídico y Económico Escurialense* 44: 317-334. Consultado el 29-III-2020. https://webcache.googleusercontent.com/search?q=cache:QvlznE2PZ80J:https://dialnet.unirioja.es/descarga/articulo/3625376.pdf+&cd=1&hl=es&ct=clnk&gl=ec

De Terwangne, Cécile. 2009. «Is a Global Data Protection Regulatory Model Possible?». En *Reinventing data protection?*, editado por S. Gutwirth, Y. Poullet, P. De Hert, C. De Terwangne y S. Nouwt, 175-189. Dordrecht: Springer.

Estrada, José, Estrada, Juan, Rodríguez, Ana, y Tipantuña, Christian. 2015. «Ecuador y la Privacidad en Internet: Una Aproximación Inicial». *Revista Politécnica*, 1. Consultado el 28-III-2020. https://revistapolitecnica.epn.edu.ec/ojs2/index.php/revista_politecnica2/article/view/556.

Foro de Cooperación Económica Asia-Pacífico. 2004. «*Marco de privacidad de la APEC de 2004*». Consultado 18-III-2020. https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf

Garriga, Ana. 2016. *Nuevos retos para la protección de datos personales en la era del Big Data y la computación ubicua*. Madrid: Dykinson.

Gibello, Valentin. y Moritz, Marcel. 2017. «El Reglamento Europeo (UE) 2016/679: análisis de un claroscuro». *Foro 27*: 115-128. Consultado el 25-III-2020. http://repositorio.uasb.edu.ec/bitstream/10644/5948/1/08-TC-Moritz-Gibello.pdf

Gil, Elena. 2016. *Big data, privacidad y protección de datos*. Madrid: Boletín Oficial del Estado.

Gobierno de México. s.f. «*Constitución Política de los Estados Unidos Mexicanos de 5 de febrero de 1917*». Consultado el 10-V-2020. http://www.sct.gob.mx/JURE/doc/cpeum.pdf

Grande, Martha. 2016. «Transferencia internacional de datos personales desde España a países iberoamericanos». *Informática y Derecho* 1: 55-70. Consultado el 10-IV-2020. https://docs.wixstatic.com/ugd/fe8db5_a143e0cda3b44d5998a5c1fe4c70c828.pdf

Guasch Portas, Vicente. 2012. «La transferencia internacional de datos de carácter personal». *Revista de Derecho UNED* 11: 413-453. Consultado el 20-IV-2020 de http://revistas.uned.es/index.php/RDUNED/article/view/11139/10667

Guzmán, María. 2013. «El derecho fundamental a la protección de datos personales en México: análisis desde la influencia del ordenamiento jurídico español». Tesis Doctoral. Universidad Complutense de Madrid. https://eprints.ucm.es/22817/1/T34727.pdf

López, Leticia. 2017. «Las transferencias de datos a EE.UU.: la transición del Safe Harbor al Privacy Shield y un paso más allá». *Actualidad jurídica Uría Menéndez* 45: 36-38. Consultado el 25-III-2020. https://www.uria.com/documentos/publicaciones/5315/documento/art03.pdf?id=6965

Lucena, Isabel. 2012. «La protección de la intimidad en la era tecnológica: hacia una reconceptualización». *Revista Internacional del Pensamiento Político 7*: 117-144. Consultado el 1-IV-2020. http://www.pensamientopolitico.org/Descargas/RIPP07117144.pdf

Maqueo, María, Moreno, Jimena, y Recio, Miguel. 2017. «Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario». *Revista de Derecho Valdivia* 1: 77-96. Consultado el 30-IV-2020. https://scielo.conicyt.cl/pdf/revider/v30n1/art04.pdf

Oficina del Asesor Jurídico de Revisión de la Cámara de Representantes de los Estados Unidos. s.f. «Right to Financial Privacy Act, 12 U.S.C. §§ 3401/342, Ley de libertad de información de 1978». Consultado el 19-IV-2020. http://uscode.house.gov/view.xhtml?path=/prelim@title12/chapter35&edition=prelim

Ordóñez, Luis. 2017. «La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración». Foro 27: 83-114. Consultado el 14-IV-2020. http://repositorio.uasb.edu.ec/bitstream/10644/5947/1/07-TC-Ordo%C3%B1ez.pdf

Organización de Estados Americanos. s.f. «Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales de la OCDE de 1980.» Consultado el 5-IV-2020. http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf

Ortega, Alfonso. 2017. «Transferencia Internacional de Datos de Carácter Personal: del Safe Harbour al Privacy Shield». *Lex Mercatoria*, 4: 85-90. Consultado el 25-III-2019. http://revistas.innovacionumh.es/index.php?journal=lexmercatoria&page=article&op=view&path%5B%5D=1093&path%5B%5D=208

Patterson Belknap. 2018. *California Consumer Privacy (CCPA), Ley de privacidad del consumidor de California*. Consultado el 30-IV-2020. https://www.pbwt.com/content/uploads/2018/06/California-Consumer-Privacy-Act1.pdf

Puccinelli, Oscar. 1999. *El habeas data en Indoiberoamérica*. Bogotá: Temis.

Rebollo, Lucrecio. 2008. *Vida privada y protección de datos en la Unión Europea*. Madrid: Dykinson.

Rebollo, Lucrecio. y Serrano, María. 2017. *Manual de Protección de Datos* (2a. ed.). Madrid: Dykinson.

Remolina, Nelson, Tenorio, Manuel., y Quintero, Gustavo. 2018. *De la responsabilidad demostrada en las funciones misionales de la Registraduría Nacional del Estado Civil: Hacia un programa de gestión de datos personales y la consolidación de un buen gobierno corporativo en el tratamiento de esa clase de información*. Bogotá: Temis.

Remolina, Nelson. 2010. "¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?" *Revista Colombiana de Derecho Internacional*, 16. Consultado el 15-IV-2020. https://revistas.javeriana.edu.co/index.php/internationallaw/article/view/13847

Rojas, Marcela. 2014. "Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales". *Novum Jus*, 8(1). Consultado el 19-IV-2020. https://editorial.ucatolica.edu.co/ojsucatolica/revistas_ucatolica/index.php/Juridica/article/viewFile/652/670

Saltor, Carlos. 2013. «La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina». Tesis doctoral. Universidad Complutense de Madrid. https://eprints.ucm.es/22832/1/T34731.pdf

Sanz, Lourdes. 2008. «Principios de la Protección de Datos». En *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia,* coordinador Carlos Lesmes, 138-162. Valladolid: LEX NOVA.

Valverde, Antonio. 2013. «Protección de datos de carácter personal y derechos de información de los representantes de los trabajadores». *Temas Laborales* 118: 13-54. Consultado el 6-IV-2020. http://www.juntadeandalucia.es/empleo/anexos/ccarl/33_1392_3.pdf

Villalba, Andrea. 2017. «Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa». *Foro 27*: 23-42. Consultado el 18-IV-2019. http://repositorio.uasb.edu.ec/bitstream/10644/5944/1/04-TC-Villalba.pdf

Warren, Samuel. y Brandeis, Louis. 1890. «The Right to Privacy». *Harvard Law Review* 5: 193-220. Consultado el 30-IV-2020. http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

Zaballos, Emilia. 2013. «La Protección de Datos Personales en España: Evolución Normativa y Criterios de Aplicación». Tesis Doctoral. Universidad Complutense de Madrid. https://eprints.ucm.es/22849/1/T34733.pdf

Legislación y jurisprudencia

Asamblea Nacional del Ecuador. s.f. «Proyecto de Ley de Protección a la Intimidad y a los Datos Personales de 2010». Consultado el 12-IV-2020 a http://ppless.asambleanacional.gob.ec/alfresco/d/d/workspace/SpacesStore/1f0a354a-3380-46d8-b828-f912f5dc13cf/Proyecto%20de%20Ley%20de%20Protecci%C3%B3n%20a%20la%20Intimidad%20y%20a%20los%20Datos%20Personales%20Tr.%2025508.pdf

Asamblea Nacional del Ecuador. s.f. «Proyecto de Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales de 2016». Consultado el 12-IV-2020. http://ppless.asambleanacional.gob.ec/alfresco/d/d/workspace/SpacesStore/843473d9-a8b3-4c72-8bd3-7d121aba3e66/Proyecto%20de%20Ley%20Org%C3%A1nica%20de%20la%20Protecci%C3%B3n%20de%20los%20Derechos%20a%20la%20Intimidad%20y%20Privacidad%20sobre%20los%20Datos%20Personales%20Tr.%20254848.pdf

Comisión Europea. 2007. *Dictamen no 4/2007 de 20 de junio de 2007 sobre el concepto de datos personales del Grupo de protección de las personas en lo que respecta al tratamiento de datos personales del artículo 29*. Consultado el 4-IV-2020. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

Constitución de la República del Ecuador, 2008 (Registro Oficial 449 de 20-X-2008).

Constitución Política de la República del Ecuador, 1998 (Registro Oficial 1 de 11 de agosto de 1998).

Corte Constitucional de Colombia. 2011. *Sentencia C-748/11 de la Corte Constitucional de Colombia de 6-X-2011*. Consultado el 16-IV-2020. http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm

Corte Europea de Derechos Humanos. 1987. *Caso Leander vs. Suecia sentencia de 26 de marzo de 1987, asunto 9238/81 del Tribunal Europeo de Derechos Humanos, Corte Chamber*. Consultado el 13-IV-2020. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57519%22]}

Corte Europea de Derechos Humanos. 1997. *Caso Z vs. Finlandia, sentencia de 25 de febrero de 1997, asunto 9/1996/627/811 del Tribunal Europeo de Derechos Humanos*. Consultado el 15-IV-2020. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58033%22]}

Corte Europea de Derechos Humanos. 2000. *Caso Amann vs. Suiza sentencia de 16 de febrero de 2000, asunto 27798/95 del Tribunal Europeo de Derechos Humanos 2000-II*. Consultado el 30-III-2020. https://hudoc.echr.coe.int/spa#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-162541%22]}

Decreto Ejecutivo 2471, de 11 de agosto de 2005, Reglamento a la Ley Orgánica de Transparencia y Consultado a la Información Pública (Registro Oficial 507 de 19-I-2005).

Decreto Ejecutivo 525, de 3-X-2018, Reglamento a la Ley Orgánica de Gestión de la Identidad y Datos Civiles (Registro Oficial 353, de 23-X-2018).

Decreto Ejecutivo 950, de 11 de marzo de 2016, Reglamento a la Ley del Sistema Nacional de Registro de Datos Públicos (Suplemento al Registro Oficial 718, de 23-III-2016).

Departamento de Justicia de los Estados Unidos. 1966. «*Freedom of information Act, 5 U.S.C. § 552ª, Ley de libertad de información de 1966*». Consultado el 27-IV-2020. https://www.justice.gov/oip/freedom-information-act-5-usc-552

Departamento de Seguridad Nacional de los Estados Unidos. 1974. «*Privacy Act, 5 U.S.C. § 552ª, Ley de Privacidad de Estados Unidos de Norteamérica de 1974*». Consultado el 12-IV-2020. https://www.uscis.gov/about-us/freedom-information-and-privacy-act-foia/privacy-act-1974

Derecho Chile. 2016. «*Sentencia 209/83 del Tribunal Constitucional Federal Alemán de 15 de diciembre de 1983, Ley del Censo*». Consultado el 17-IV-2020. http://www.derecho-chile.cl/sentencia-de-15-de-diciembre-de-1983-del-tribunal-constitucional-federal-aleman-ley-del-censo/

Dirección Nacional de Registro de Datos Públicos. 2019. «*Proyecto de la Ley Orgánica de Protección de datos Personales de 19 de septiembre de 2019*». Consultado el 30-IV-2020. https://www.dinardap.gob.ec/wp-content/uploads/downloads/2019/09/PROYECTO-LEY-DE-PROTECCION-DE-DATOS-PERSONALES.pdf

Eur-Lex. 2019. «Caso Lindqvist vs. Gäta hovärtt, sentencia de 6 de noviembre de 2003 del Tribunal de Justicia de la Unión Europea». Consultado el 15-IV-2020. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN

Eur-Lex. 2019. «Caso Schrems vs. Data Protection Commissioner, sentencia de 6-X-2015, asunto C-362/14 del Tribunal de Justicia de la Unión Europea, Gran Sala». Consultado el 18-III-2020. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62014 CJ0362&from=ES

Eur-Lex. 2019. «Decisión de ejecución, Privacy Shield UE-EE. UU 2016/1250 de la Comisión Europea de 12 de julio de 2016». Consultado el 2-V-2019. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D1250&qid=1542660556803&from=EN

Eur-Lex. 2019. «*Decisión de la Comisión 2000/520/CE, Safe Harbor Privacy Principles de la Comisión Europea de 26 de julio de 2000*». Consultado el 2-IV-2020. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32000D0520&from=en

Eur-Lex. 2019. «*Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos de 1995*». Consultado el 4-IV-2020. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN

Eur-Lex. 2019. «*Reglamento General de Protección de datos del Parlamento Europeo y del Consejo UE 2016/679 (GDPR) de 2016.* Consultado el 15-IV-2020. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

Honorable Cámara de Diputados. s.f. «Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México de 2010». Consultado el 30-IV-2020. http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Honorable Cámara de Diputados. s.f. «Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de México de 2017». Consultado el 14-IV-2020. http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Honorable Cámara de Diputados. s.f. «Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México de 2011». Consultado el 10-IV-2020. http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

Infoleg. (s.f.). «Reglamentación de la ley N°. 25.326, relativo a la protección de datos personales de Argentina de 2001, Decreto N°. 1558/2001». Consultado el 25-III-2019. http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/texact.htm

Legisalud. s.f. «Constitución de la Nación Argentina de 23 de agosto de 1994». Consultado el 10-IV-2019. http://test.e-legis-ar.msal.gov.ar/leisref/public/showAct.php?id=877

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, de 2002 (Suplemento al Registro Oficial 557 de 17-IV-2002).

Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, de 2009 (Suplemento al Registro Oficial 52 de 22-X-2009).

Ley Orgánica de Gestión de la Identidad y Datos Civiles, de 2016 (Suplemento al Registro Oficial 684 de 4-II-2016).

Ley Orgánica de Transparencia y Consultado a la Información Pública, de 2004 (Registro Oficial 337 de 18-V-2004.

Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, de 2010 (Suplemento al Registro Oficial 162 de 31-III-2010).

Organización de Estados Americanos. s.f. «Ley de Protección de Datos Personales de Argentina, N°. 25.326 de 2000». Consultado el 25-III-2020. https://www.oas.org/juridico/PDFs/arg_ley25326.pdf

Tribunal Constitucional Español. s.f. «Sentencia 292/2000 del Tribunal Constitucional Español de 30 de noviembre de 2000». Consultado el 16-IV-2019. http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276#complete_resolucion&completa

ÍNDICE

PROTECCIÓN DE DATOS PERSONALES EN COMERCIOS ELECTRÓNICOS B2C

PERSONAL DATA PROTECTION ON E-COMMERCE B2C

PROTEÇÃO DE DADOS PESSOAIS EM COMÉRCIOS ELETRÔNICOS B2C

*Carolina Sacoto**

Recibido: 13/05/2020
Aprobado: 25/06/2020

Resumen

En Ecuador, el crecimiento acelerado de las transacciones comerciales realizadas por internet ya es una realidad. Desafortunadamente, el auge de esta industria se da en un entorno de incertidumbre total ante la inexistencia de una norma adecuada que regule el tratamiento de datos personales. En ese contexto, este artículo pretende señalar las obligaciones y avisos legales esenciales relacionados con la protección de datos personales que los comercios electrónicos B2C deberían tener presente a la hora de operar en el mercado. El análisis se realiza en atención al actual Proyecto de Ley de Protección de Datos Personales, desde una perspectiva legal y, vinculada a ella, una perspectiva técnica y lingüística. Finalmente, se realizan recomendaciones para facilitar al responsable el cumplimiento de los parámetros revisados en este documento.

Palabras clave: Privacidad en internet; Tratamiento de datos; Seguridad de datos; Procesamiento de datos; Contratación electrónica

Summary

In Ecuador, the accelerated growth of commercial transactions made through internet is already a reality. Unfortunately, its rise is taking place in conditions of total uncertainty caused by the absence of legal regulations regarding data protection and its processing. In this context, this article aims to cover the main obligations and legal notices related to personal data protection that B2C electronic commerce should consider when operating. The analysis is based on the personal data protection bill of Ecuador from a legal perspective, and linked to it, a technical and linguistic perspective; finally, this work provides recommendations to guide organizations with the compliance of the requirements reviewed in this document.

Key words: Internet privacy; Data treatment; Data security; Data processing; Electronic contracting

Resumo

No Equador, o crescimento acelerado das transações comerciais realizadas por internet já é uma realidade. Infelizmente, o auge desta indústria está acontecendo ao redor de uma incerteza total diante da inexistência de uma norma adequada que regule o tratamento dos dados pessoais. Nesse contexto, este artigo pretende indicar as obrigações e avisos legais essenciais relacionados com a proteção de dados pessoais que os comércios eletrônicos B2C deveriam observar na hora de entrar no mercado. A análise se realiza em compatibilidade com o atual Projeto de Lei de Dados Pessoais, desde uma perspectiva legal e, vinculada a ela, uma perspectiva técnica e linguística. Finalmente, se realizam recomendações para facilitar ao responsável o cumprimento de parâmetros revisados neste documento.

Palavras chave: Privacidade na internet; Tratamento de dados; Segurança de dados; Processamento de dados; Contratação eletrônica

* Abogada por la Universidad Técnica Particular de Loja, Ecuador; Ingeniera comercial por la Universidad del Azuay, Ecuador; Magíster (c) en Propiedad intelectual y nuevas tecnologías por la Universidad Internacional de La Rioja, España. Tiene experiencia en comercio electrónico y es abogada en libre ejercicio profesional. Correo electrónico: carolina.sacoto94@gmail.com

INTRODUCCIÓN

El constante desarrollo tecnológico ha permitido la creación y rápida expansión de un nuevo modelo de negocio que gira en torno a la compra y venta de bienes y servicios por internet a través de relaciones contractuales por medios electrónicos. Este es un canal de ventas que, mediante el uso de herramientas tecnológicas, obtiene gran cantidad de información sobre los internautas, la cual, tratada en diverso modo y por diferentes prestadores de servicios, consigue, además de prestar el servicio de compra y venta en línea, mejorar la experiencia del usuario al navegar por una página web.

En este sentido, y si bien las acciones de procesamiento de datos están encaminadas a potenciar las ventajas que un *e-commerce* ofrece, en la misma o mayor medida representan una amenaza latente para la privacidad de las personas, quienes, además, no tienen ningún poder de negociación con los comercios. Esta situación ha llamado la atención del legislador de cada país, quien ha tenido la difícil tarea de crear la normativa adecuada para tutelar un derecho fundamental de la persona, obviamente sin impedir el desarrollo del comercio electrónico.

Lamentablemente en Ecuador, si bien existe un Proyecto de Ley Orgánica de Protección de Datos Personales, a la fecha, el marco jurídico es insuficiente; pues, con o sin norma que regule este derecho, es de gran importancia que el comercio electrónico cumpla con parámetros adecuados de protección de datos personales. Por tal motivo, este artículo hará una revisión de los requisitos fundamentales que los *e-commerce* B2C deberían tener en Ecuador, al momento de salir al mercado. Para lograr una visión integral del asunto, se abordarán estos puntos desde el ámbito legal y, vinculadas este, las perspectivas técnica y lingüística.

NOCIONES IMPORTANTES SOBRE EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL MARCO DEL COMERCIO ELECTRÓNICO

1. Una mirada a la evolución del derecho a la protección de datos personales

La aparición de las primeras normativas que regulaban la protección de datos se remonta a los años 70 (Frosini 1998). Estas formaban parte de *la primera generación de protección de datos* y nacieron como una reacción a la "informatización progresiva de la sociedad y también, a la incertidumbre acerca de sus implicaciones inmediatas, así como de las medidas precisas que debían tomarse" (Lazpita 1994, 404).

A partir de esa base, surgió una variada legislación a nivel internacional. Esta se distinguió, por un lado, por ordenamientos jurídicos que se decantan por el impulso del desarrollo económico, como es el caso de Estados Unidos. Por otro lado -línea que pretende seguir Ecuador- se hallan aquellos otros que han implementado un sistema jurídico con un nivel alto de protección de datos personales, al que confieren un rango de derecho fundamental independiente, como es el caso de la Unión Europea. Con tal aporte a la doctrina se inició "una nueva etapa, que se basa en la consideración de la protección de datos de carácter personal como un verdadero derecho fundamental autónomo e independiente del derecho a la intimidad" (Piñar 2003, 29).

La explicación a esta evolución conceptual, que sitúa el derecho a la protección de datos personales en la 3.ª generación de derechos fundamentales, viene dada por el crecimiento preponderante que ha tenido el uso de la tecnología en todos los ámbitos de la vida diaria. Y "la protección de datos personales constituye una respuesta jurídica frente al fenómeno de la sociedad de la información para frenar la potencial amenaza que el desarrollo tecnológico representa para los derechos y libertades de las personas" (Herrán 2003, 15).

Finalmente, y en respuesta a las crecientes exigencias que la era digital ha traído, en el año 2012 se inició en Europa la elaboración del más moderno instrumento que se tiene en la materia, el RGPD[1]. Esta normativa es un modelo nuevo que, por los principios, derechos y obligaciones que incorpora, pretende lograr un uso ético y responsable de la información. Además, intenta armonizar dos objetivos importantísimos: por un lado, la protección de datos y, por otro, libre circulación en el mercado para no limitar de forma injustificada la innovación. En Ecuador, el nuevo proyecto de ley en la materia sigue casi en su totalidad los preceptos legales contenidos en el mencionado Reglamento.

Nuestro país no es uno de los que ha respondido con rapidez a la era digital. Como consecuencia, la ley para la protección de datos personales en Ecuador aún no es una realidad, y lo único que tenemos son preceptos legales dispersos en diversas normas que no son ni suficientes, ni claros, ni completos para regular eficientemente el tratamiento de los datos personales en instituciones públicas y privadas. Sin embargo, no deja de ser una normativa vigente y plenamente aplicable para el caso concreto; y, por esta razón, la revisamos brevemente a continuación.

La Constitución del Ecuador, en su art. 66 numeral 19 establece que se reconoce y garantiza a las personas el acceso, la decisión y protección sobre información y datos de carácter personal que le concierne, de forma que su tratamiento requerirá la autorización del titular o el mandato de la ley; y el art. 92 de la misma norma posee un sentido similar. Luego, tenemos la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, que principalmente contiene una definición bastante básica sobre lo que se considera dato personal, regula la contratación electrónica; y dedica su art. 9 a la protección de datos, en el que pone énfasis en el consentimiento y el mandato legal como base para el tratamiento de datos. También establece que el procesamiento de los datos debe responder a los derechos de privacidad, intimidad y confidencialidad. En definitiva, esta ley sí recoge algunos preceptos importantes en la materia, pero sin una estructura clara y adecuada que resulte eficiente.

2. ¿Qué se considera dato personal?

El art. 5 del proyecto de Ley Orgánica de Protección Datos Personales, recoge una definición que tiene en cuenta todo dato que concierne a una persona, cuya identidad es evidente (identificada) o puede establecerse y llegar a serlo, directa o indirectamente, a partir de la combinación de unos datos con otra información (identificable). Esta identificación requiere obligatoriamente, elementos que describan de forma clara a una persona de tal modo que no se la confunda con otra.

Además, hace énfasis en la posibilidad de que un dato se haga identificable en el "presente o en el futuro" como un anticipo a las novedades que tecnologías inexistentes hoy en día podrían traer. Este es un concepto más adecuado en comparación con la única e incompleta definición disponible en el ordenamiento jurídico ecuatoriano a la fecha, que está prevista en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y que textualmente dice**:** "son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley" (Disposición general 9.ª, glosario de términos).

Para entender de mejor manera esta definición es preciso mencionar unos cuantos ejemplos, con datos que permiten identificar directamente a una persona, su nombre o número de identificación; asimismo permitirán identificarla indirectamente, mediante información como su dirección o número de celular. A estos clásicos datos personales, se suman aquellos que provienen del uso de la tecnología y que también hacen posible la identificación, los cuales usualmente son recogidos cuando la persona navega por internet en una web, por ejemplo, la dirección IP.

Finalmente, en ese concepto se evidencia que la persona objeto de protección es una persona física.

3. Características de los comercios electrónicos B2C

Pues bien, para comprender las obligaciones legales en materia de protección de datos personales que se

1 Reglamento General de Protección de Datos, vigente para su aplicación desde el 25-V-2018.

abordarán más adelante hay que tener claro algunas cuestiones importantes sobre los *e-commerce*.

Desde el surgimiento del comercio electrónico en los años 90 hasta la fecha, las plataformas digitales han atravesar varias etapas para poder llegar a su actual estado: un modelo de negocio que incluye el uso de herramientas tecnológicas de seguridad, funcionalidades que permiten personalización del servicio, elementos de publicidad, campañas de marketing masivas integradas, etc. Es decir, es un modelo de negocio capaz de incorporar todo tipo de tecnologías para el tratamiento de datos personales, y estos rasgos lo han posicionado como el canal de ventas más importante a nivel mundial.

Existen tantas definiciones de comercio electrónico como autores; sin embargo, resultan más acertadas aquellas que ya tienen presente la distribución de información que se genera en las transacciones comerciales por internet.[2] Así mismo, existen varias formas de clasificar al comercio electrónico. La que nos interesa es aquella que tiene en cuenta a quiénes participan en la transacción electrónica; particularmente, el modelo B2C (*business to consumer*), en el que interviene, por un lado una empresa, y por otro el consumidor final hacia el que la compañía dirige sus esfuerzos de venta.

Este modelo de negocio no sería tan atractivo de no contar con innumerables ventajas tanto para consumidores como para empresarios. Entre las más valoradas están: comodidad, variedad de productos, precios competitivos, atención continua al público, acceso a un mercado global y, una de las más importantes, la personalización del servicio.

Ahora bien, para que las transacciones de un *e-commerce* sean posibles, es necesario que se realicen con otros proveedores de soluciones electrónicas. Los servicios que casi siempre son requeridos son: servidores en la nube para el almacenamiento de datos, pasarelas de pago, herramientas para publicidad, etc. Procesos en los que existe un importante intercambio de datos personales, sin los cuales no sería posible prestar el servicio. Adicionalmente, el éxito de una página de comercio electrónico está ligado claramente a la eficiencia del servicio; pero, sobre todo, a la estrategia de marketing que se utilice para hacerle apreciar al cliente las ventajas de comprar en su tienda. Y tanto el servicio como los esfuerzos comunicacionales para lograr ese objetivo necesitan de información valiosa de los compradores.

4. Contratación electrónica

En vista de que la dinámica del negocio requiere una importante cantidad de datos personales para que se logre el nivel de eficiencia deseado, ¿cómo hacen los comercios para conseguir toda esa información y poder tratarla de una forma lícita? La respuesta es mediante una contratación electrónica que utilice, como base legal, el consentimiento dado por el internauta.

Para la mayoría de propósitos, cuando no ha existido una relación contractual previa, los comercios electrónicos requieren del consentimiento del titular de los datos personales para tratar su información, que se exterioriza con la aceptación de contratos electrónicos. Ellos son básicamente los Términos y Condiciones, las Políticas de Privacidad y los Avisos sobre. Más adelante abordaremos el contenido sugerido para estos contratos.

En este punto se revisará qué se entiende por consentimiento. Nos remitimos nuevamente a la definición que pretende el proyecto de Ley Orgánica de Protección de Datos Personales en Ecuador[3], que lo define como "manifestación de la **voluntad libre, previa, específica, expresa informada e inequívoca**[4] por la que el titular de los datos personales autoriza al responsable del tratamiento de datos personales a tratar los mismos".

Así, en ella se entiende que existen requisitos para que el consentimiento en materia de protección de datos sea válido: primero, la voluntad libre; y solo se considera que es libre el consentimiento que se ha dado

2 Ver, en este sentido: Anteportamlatinam 2014.
3 Proyecto de Ley Orgánica de Protección de Datos Personales, artículo 5.
4 Negrita de la autora.

sin que exista violencia, error, coacción, o temor de consecuencias negativas. Luego, el consentimiento debe ser previo, es decir, tiene que conseguirse antes de tratar los datos personales. También debe ser específico: debe describirse claramente y en términos inequívocos el fin para el que se recogen ciertos datos, de modo que los consentimientos genéricos aplicados a un contexto ilimitado no son válidos.

Después, la norma refiere que el consentimiento debe ser expreso, es decir, manifiesto, cierto y explícito (Albaladejo 2002); además debe ser informado, pues el interesado debe contar con la información suficiente que le permita tener conciencia y comprensión clara y amplia de las consecuencias de dar su consentimiento o de no darlo; y, por tanto, el responsable debe proporcionar una descripción específica y completa de toda la información que permita al titular comprender las implicaciones de su actuar. Finalmente, se dice que debe ser inequívoco ya que no debe caber duda alguna de que el titular quería exteriorizar su voluntad de admitir el tratamiento de sus datos.

En consecuencia, el silencio, por regla general, y al menos en el ámbito de contratación electrónica, no puede considerarse expresión de la voluntad, toda vez que "nadie puede imponer a otro que el silencio sea signo de declaración" (Flume 1998, 94). Se trata, más bien, de una falta de expresión, y considerarla como aceptación de una oferta resultaría abusivo; tampoco podrá entenderse que una oferta ha sido aceptada por el solo hecho de visitar un determinado sitio web.

En el caso particular de las páginas web, la manifestación de la voluntad se da cuando se selecciona la casilla en donde se debería poder visualizar el contrato y se pulsa clic en el botón "aceptar"; razón por la cual, las casillas ya marcadas que llevan a una inacción del sujeto no deben constituir consentimiento.

En cuanto a los contratos electrónicos, existe acuerdo en que es posible la formación del consentimiento por cualquier medio electrónico. Puesto que, "si la voluntad puede declararse por gestos, y aun por silencios, cómo no se va a poder declarar por medio de un ordenador" (Rodríguez 2000, 356). No hay discusión al respecto, debido a que la contratación electrónica cumple con los elementos esenciales de la contratación común, regulada en materia civil; y, si bien incluye el uso de medios telemáticos y presenta particularidades que han sido desarrolladas para generar mayor seguridad jurídica, no aporta novedades relevantes que lleven a un debate sobre el asunto. Asimismo, tampoco parece existir problema jurídico alguno en el uso de las nuevas tecnologías o de internet para expresar el consentimiento.

En el mismo sentido, La Ley de Comercio Electrónico, Firmas y Mensajes de Datos de Ecuador, en su artículo 45, establece la validez de los contratos electrónicos e indica que "no se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos"; además, regula el consentimiento para el uso de medios electrónicos.

OBLIGACIONES LEGALES EN MATERIA DE PROTECCIÓN DE DATOS RELACIONADAS AL COMERCIO ELECTRÓNICO

En este punto es importante entender que la finalidad de la norma no es impedir a los comercios el uso de datos personales, sino evitar conductas indebidas en el tratamiento de estos datos, a fin de precautelar un derecho fundamental de la persona. Ahora, que las empresas estén preparadas para dar cumplimiento a lo dispuesto en una futura ley en la materia, así como para iniciar operaciones comerciales con otros países que exigen el mismo nivel de protección de datos personales que ellos ofrecen, será indispensable al menos considerar los puntos que se explican a continuación.

El comercio debe cumplir el principio de licitud, lealtad y transparencia, en virtud del cual se exige que el tratamiento de datos personales tenga un fundamento legal. En el caso de los *e-commerce*, como ya se indicó, hay que tener en cuenta principalmente el consentimiento

como base para el procesamiento legal de datos personales, tratamiento que ha de ser ético. Además, la empresa debe proporcionar al usuario suficiente información relativa a sus datos personales. En todo caso, ha de existir un esfuerzo honesto de usar todos los medios disponibles para mantener al interesado informado antes, durante y después de cualquier proceso relacionado al tratamiento de los datos personales.

También hay que tener presente que la finalidad del tratamiento de los datos debe delimitarse correctamente, de modo que resulte específica y clara. De igual manera, el responsable debe identificar cuáles son los datos mínimos que requiere para cumplir con su propósito legal, de modo que no resulten excesivos e inadecuados; así se dará cumplimiento a los principios de limitación de la finalidad y de minimización.

Y, en concordancia con el principio de limitación de almacenamiento, los datos personales deben conservarse únicamente por el tiempo que sea necesario para cumplir el fin para el que se recogieron. Transcurrido ese periodo deben eliminarse, o pueden mantenerse, pero siempre que se vuelvan anónimos, de manera que no se identifique al titular.

El responsable del tratamiento garantizará razonablemente que los datos sean exactos y precisos, que se han actualizado, y que todo dato falso o engañoso se ha rectificado o eliminado sin dilaciones. Asimismo, el responsable debe implementar medidas técnicas y organizativas, de forma que se minimice el riesgo de actos fraudulentos vinculados con los datos del interesado, sin importar que estén vinculados al su uso, acceso, divulgación, pérdida o destrucción no autorizado, accidental o deliberado. Los comercios deben asegurarse de evitar cualquier tipo de consecuencia desfavorable para el interesado que vulnere sus derechos y libertades; porque, en virtud del principio de seguridad, se tiene que garantizar una protección apropiada de la información.

Por otro lado, íntimamente relacionados a estas obligaciones que tienen los responsables del tratamiento, los derechos de las personas usuarias de estas plataformas digitales. La exigencia de informar al usuario para obtener su consentimiento es un derecho específico del interesado: el de tener a su disposición toda la información respecto del tratamiento sus datos personales. Su contenido depende de si los datos se recogen directamente del individuo o si se los consiguió de otra fuente; y, por lo general, los datos que se deben compartir incluyen:

- Información completa del responsable del tratamiento de los datos o su encargado: nombre, datos de contacto, de registro, etc.

- Propósitos del procesamiento de los datos personales vinculados a la base legal correspondiente, incluido el interés legítimo que pudiera tener el comercio, sobre todo relacionados a marketing, publicidad, seguridad, etc.

- Los destinatarios de los datos personales. Más en concreto, al usuario se le debe poner al tanto acerca de los prestadores de servicios de la sociedad de la información involucrados en cada caso, así como de las medidas de seguridad que se tomarán para precautelar la integridad y confidencialidad de la información en estas transferencias. También, los destinarios de los datos se deben corresponder con los propósitos del procesamiento.

- El tiempo que se pretende almacenar los datos del internauta, que está ligado a la finalidad para la cual se recogió la información.

- Los derechos del usuario en relación con sus datos personales.

- Igualmente, los comercios han de tener en cuenta que no basta con colocar la información en la web, sino que, además, **la información ha de ser concisa, transparente, inteligible y de fácil acceso**[5].

- Entre los derechos que pueden ser ejercidos por el interesado y que, por tanto, se han de tener presentes en la plataforma web están: el derecho de acceso, por el que el interesado puede requerir una confir-

5 Negrita de la autora.

mación de si se están tratando o no sus datos, y obtener una copia de estos; el de rectificación, por el que el interesado tiene derecho a corregir o completar sus datos personales cuando estos sean inexactos o estén incompletos; el de supresión[6] o derecho al olvido, que faculta al interesado a pedir al comercio que elimine sus datos personales tanto del sistema activo como del de respaldo; el de limitación del tratamiento, que otorga a cada persona el derecho de restringir temporalmente el procesamiento de sus datos personales. Para cumplir con esta exigencia se puede considerar mover temporalmente los datos a otro sistema de procesamiento, evitar que estén disponibles para los usuarios o eliminarlos temporalmente del sitio web. En todo caso, el responsable, durante este tiempo, no puede usarlos en ninguna forma.

Similar al anterior es el derecho de oposición al tratamiento del total o de una parte de sus datos personales. La valoración de la aplicabilidad de este derecho depende de las circunstancias particulares, sobre todo, del objetivo del procesamiento y de la base legal que lo justifica. Sin embargo, en el caso del procesamiento de datos personales con fines de marketing directo, este derecho es absoluto e inmediato.

Luego, el derecho a la portabilidad de los datos permite a las personas solicitar al responsable del tratamiento, los datos personales que le corresponden y que le ha proporcionado al comercio; también es posible que se le pida que los datos sean transmitidos directamente a otro responsable, y esta obligación se extiende a la información que la empresa haya podido recabar mediante el análisis de las actividades que realiza la persona en internet. Los datos deben proporcionarse en un formato estructurado, comúnmente utilizado y legible para una máquina.

Además, se debe dar a conocer al internauta si el comercio, ya sea directamente o por medio de terceros, toma decisiones automatizadas con el uso de herramientas netamente tecnológicas o elabora perfiles a partir de estos procedimientos para evaluar aspectos personales de un usuario. Al respecto, está prohibido usar estas herramientas para tomar decisiones que produzcan efectos jurídicos o tengan consecuencias adveras similares para el interesado, debido a que afectan a aspectos importantes en su vida relacionados con otros derechos o libertades fundamentales. Para los demás asuntos, el responsable debería poner a disposición del interesado información significativa sobre el razonamiento que se usa en estas herramientas automáticas y que, en todo momento, puede ser objeto de alegación por parte del interesado.

En caso de que no se haya atendido el requerimiento del interesado, se debe justificar razonadamente por qué no se ha dado una respuesta, y poner en conocimiento del solicitante las acciones legales o administrativas que puede ejecutar. Adicionalmente, estos derechos serán gratuitos a menos que sean excesivos o infundados; en cuyo caso, el comercio puede fijar un precio para cumplir con la solicitud. Para el caso de los *e-commerce*, lo ideal es proporcionar al usuario un mecanismo para realizar estas solicitudes por vía electrónica, preferiblemente desde la propia web.

También es relevante el hecho de que el responsable del tratamiento de datos debe ser capaz de demostrar, de forma efectiva y en todo momento, tanto a los interesados como a las autoridades y al público, que viene ejecutando adecuadamente las obligaciones a ellos impuestas en virtud del principio de responsabilidad proactiva.

1. Accesibilidad técnica y lingüística

Ya se ha visto como la norma pretende incidir de forma importante en las transacciones electrónicas que se llevan a cabo mediante una plataforma web, al regular estas con una serie de obligaciones que el comercio deberá cumplir. Sin embargo, los límites anotados tampoco son suficientes para cumplir eficientemente el espíritu de la norma, ya que dejan abierto un abanico de posibilidades sobre cómo estas obligaciones han de ser cumplidas. Por ej., aunque con el pasar del tiempo los comercios cumplan la normativa, en ocasiones lo hacen mediante la publicación de políticas y términos de muy difícil acceso dentro de la plataforma; o

6 En este punto es interesante la sentencia del CJEU, C-131/12, Google Spain SL, Google Inc. versus la Agencia Española de Protección de Datos (AEPD).

efectivamente permiten el ejercicio de los derechos del usuario, pero mediante procesos tan complejos, que al final resultan inútiles. Puede pasar también que estos términos y políticas están presentes en extensiones poco razonables, de modo que no habrá manera de que el usuario las lea; menos aún, cuando la comodidad es una ventaja muy valorada en este tipo de modelo de negocio y, dado que leer políticas extremadamente largas, con tecnicismos o incomprensibles, no resultaría nada cómodo para un internauta.

Este es justamente el gran problema al que nos enfrentaremos en un futuro cercano, pues si los avisos legales no fueron de fácil acceso, si el usuario ni siquiera los notó, o si estuvieron presentes, pero en una extensión tal que era casi imposible que el internauta los lea, sería adecuado dudar de si el usuario ha dado su consentimiento informado. Y evidentemente no sería así, porque la información que se dé al usuario ha de ser concisa, transparente, inteligible y de fácil acceso.

Pues bien, para entender a qué se refiere la accesibilidad técnica es necesario comprender que no solo es importante colocar toda la información en el sitio web, sino que, además, esta debe ser de fácil acceso; pues, de otra manera, poco se lograría con tener los datos completos en la web si un usuario medio es incapaz de identificarlos dada la complejidad de diferenciarlos de los otros elementos.

Este aspecto forma parte integrante del cumplimiento de las obligaciones legales en materia de protección de datos. Aquí ya no se aborda el qué se debe cumplir, sino el cómo; y, para hacerlo operativo, es esencial desarrollar procesos intuitivos que permitan llegar hasta los avisos legales, formularios y otros elementos que garanticen el efectivo cumplimiento de las obligaciones antes descritas; esto. Tal procedimiento debe ser posible para un internauta sin que este sea un experto en el uso de plataformas digitales. Así, se entiende que las herramientas puestas a disposición de los individuos deben ser de uso sencillo e idealmente amigables.

En suma, el comercio no usará las herramientas tecnológicas de las que dispone solo para mejorar la experiencia del usuario o para inducirlo a la compra, sino también para conseguir una plataforma web en la que, por los elementos que incorpora, la persona sienta confianza al usarla, y perciba que efectivamente la empresa ha puesto esfuerzo en dejar a la vista las condiciones bajo las cuales prestará su consentimiento. Este proceder, sin lugar a duda generará un impacto positivo en el potencial comprador, quien no temerá que el comercio pretende ocultar información.

Para lograrlo habrá que tener en cuenta los requerimientos siguientes:

- Los avisos legales deberán estar disponibles en todo momento durante la navegación de la página web.
- Los procesos no han de ser complicados en el sentido de que obliguen al usuario a adelantar y retroceder en las páginas para conseguir información.
- El despliegue de los avisos debe evitar interrumpir la navegabilidad del usuario; y, en este sentido, es recomendable el uso de ventanas tipo *pop-up*.
- Los avisos legales deben ser fáciles de distinguir y, para conseguirlo, hay que cuidar la ubicación, el tipo y el tamaño de la letra.
- Idealmente, el formato de los avisos legales debe permitir archivarlos.
- Los avisos legales deben ser accesibles desde cualquier dispositivo móvil.
- Los procedimientos para retirar el consentimiento o ejercer los derechos también deben estar técnicamente optimizados, de modo que sean igual de sencillos que los que se usan para conseguirlo.
- No se pueden usar, en ningún caso, casillas ya marcadas.

Luego, y en relación con la accesibilidad lingüística, ha de considerarse que los textos que se ponen a disposición del interesado han de proporcionar, en su conjunto, un mensaje inteligible; y, por ende, usar términos que faciliten el entendimiento de los avisos legales para los internautas. También, en este aspecto se debe considerar que la extensión de los avisos legales

debe ser razonable y, de preferencia, debe incorporar diagramas, ejemplos u otros elementos que ayuden al lector a comprender el mensaje; para lograrlo se deberían tener presentes los siguientes puntos:

- La información que se facilita debe ser concisa, y debe transmitirse con un lenguaje claro y sencillo, a fin de evitar el uso de tecnicismos.
- La información debe estructurarse razonadamente en párrafos breves y, en su conjunto, el mensaje debe ser fácil de comprender.
- La tecnología permite la implementación de elementos gráficos que facilitan la comprensión del texto y, por consiguiente, es recomendable usarlos.

AVISOS LEGALES EN LA WEB Y COMUNICACIONES COMERCIALES

Una vez que hemos visto las obligaciones, así como los aspectos que validan y apoyan en gran medida su cumplimiento, en este apartado se revisarán los puntos que usualmente se recogen en cada aviso legal.

1. Contrato de términos y condiciones

Usualmente, el contrato de términos y condiciones de la web cumplirá con el objetivo de informar al usuario sobre los datos del comercio, así como sobre la dinámica y proceso de compra dentro de la web. Respecto a este asunto se abordan las políticas de devolución, las garantías del usuario en el correcto manejo de la plataforma y se definen las responsabilidades de las partes. También se hace referencia a la protección de datos personales, a la política de *cookies* y también en el apartado de legislación y fuero; asimismo se suele hacer mención a los códigos de ética a los que el comercio esté adherido. Lamentablemente, en Ecuador no existe ningún tipo de iniciativa para la creación de códigos en esta rama, situación que se espera cambie con la expedición de la Ley Orgánica de Protección de Datos Personales, pues son especialmente necesarios para establecer pautas a seguir y para la resolución de conflictos.

2. Política de privacidad

En concreto, esta es la política en la que quedarán recogidas las obligaciones y derechos que se han explicado. Generalmente, una política adecuada empieza por informar al internauta quien es el responsable del tratamiento de los datos personales, y proporciona su información completa. Luego, explica cuáles son las finalidades por las cuales se recogen los datos personales y relaciona esta información con la base legal del tratamiento. Después, se suele informar sobre el tipo de datos que se recogen y cómo, habitualmente existen datos que el usuario proporciona al comercio. Hay datos que la empresa los recoge cuando el internauta navega en la web, otros vendrán de redes sociales o incluso de medios, tales como llamadas telefónicas, mensajes de texto o correos electrónicos y, en plataformas más modernas, de llamadas al robot de la página web.

Además, se informa sobre los terceros con quienes se comparten los datos personales: qué información se les proporciona, con qué fin y en qué condiciones. Hay que considerar que las empresas prestadoras de servicios de *hosting*, de publicidad online y de transporte, comúnmente tienen acceso a datos personales de los clientes de la empresa. También se debe hacer referencia al tiempo que se pretende mantener la información y a las medidas de seguridad que se han implementado en la web.

Finalmente, y de modo fundamental, deben explicarse al usuario los derechos que le corresponden y la forma en que puede ejercitarlos; una política responsable no hace solo una mera lista de estos, sino que los explica en términos sencillos y pone a disposición de la persona vías fáciles para elevar las correspondientes solicitudes al comercio.

3. Política de *cookies*

Este aviso legal es el más duro de comprender para los usuarios, dado el tecnicismo de algunos términos

y, así, representa un reto para el comercio en cuanto a la forma en la que se proporciona la información al usuario. Para empezar, hay que explicar en palabras sencillas qué es una *cookie* y cuáles son los tipos de *cookies* que se usan en el sitio web. Esta herramienta es en extremo versátil y útil, pues permite entre otras cosas: el uso de los carritos de compra, personalizar la página web para el usuario en una segunda visita, almacenar información relacionada a la forma de pago del cliente, analizar y segmentar a los visitantes del sitio, así como enviar y presentar publicidad. Esta tecnología es de vital importancia para lograr el cometido de una plataforma web. Por esta razón, ni bien el internauta aterriza en la página de inicio, el comercio ya pide su consentimiento para usar *cookies*.

Al efecto, es especialmente recomendable usar tablas, paneles u otros elementos que permitan mostrar la relación entre la cookie que se implementa, su finalidad, su propiedad, su descripción y la vigencia, de modo que el internauta no se sienta abrumado por términos técnicos o exceso de texto y termine por rechazar el uso de *cookies*. Asimismo, es indispensable que se informe al usuario del sitio cómo puede configurar el uso de cookies o, en su caso, deshabilitarlas y nuevamente recordar que, en virtud de los principios revisados, solo se debe recoger la información necesaria para los propósitos explicados al internauta.

4. Comunicaciones comerciales

Por último, se debe tener presente que, en toda transacción por internet, la comunicación electrónica digital ocupa un papel primordial. En la actualidad, una de las herramientas más comunes que usan los comercios en línea para comunicar sus promociones y productos son las campañas de *mailing*.

Para usarlas se ha de tener presente que estas comunicaciones deben, en primer lugar, tener clara identificación de la persona que las envía. En el caso de promociones, ofertas o concursos, la información que se ofrezca debe ser inequívoca y sugerir con claridad las condiciones de acceso. Además, pueden ser enviadas solo si el interesado lo ha consentido de forma expresa (*opt-in*[7]) o si ya existe una relación contractual previa.

En todo caso, se debe ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos para fines promocionales mediante un proceso que sea sencillo y gratuito. Este, además de estar presente en el momento de la recogida de los datos, debe constar en cada comunicación comercial, acompañado de una dirección de correo mediante la que el usuario pueda ejercitar su derecho. De no ser así, estas comunicaciones quedan prohibidas.

Nuestra legislación[8] hace referencia a la publicidad y promoción por redes electrónicas, y hace énfasis en que el consumidor debe tener acceso a toda la información disponible relacionada al bien o al servicio del que se trate; igualmente exige que se facilite un medio sencillo para que el destinatario de las comunicaciones comerciales pueda solicitar la exclusión de listados con objetivos de marketing y publicidad.

CONCLUSIONES Y RECOMENDACIONES

La situación que vivimos hoy en día ha hecho que comprar por internet no sea solo una opción sino una necesidad. Si antes de esta emergencia el papel protagónico que tenía el *e-commerce* era innegable, de aquí en adelante advertiremos un crecimiento exponencial de transacciones electrónicas. La gran mayoría de las empresas ecuatorianas, sean estas pequeñas, medianas o grandes, se encuentran en proceso de trasladar su negocio físico a internet, y lo están haciendo sin que exista normativa adecuada que alcance a regular eficientemente la cantidad de negocios que tenemos por delante con los nuevos hábitos de compra.

7 Acción mediante la cual, el internauta acepta recibir información sobre la empresa, usualmente vía correo electrónico.
8 *Ley de Comercio Electrónico, Firmas y Mensajes de Datos*, artículo 50.

Además, toda persona tiene derecho a conocer el propósito con el que se tratan sus datos y a controlar la forma en la que estos se emplearán, de forma que el uso indiscriminado de datos personales con fines económicos u otros que resulten poco éticos y causen daño al titular de la información están prohibidos.

A fin de evitar que los avisos legales por medio de los cuales se recaba el consentimiento del internauta para tratar datos personales resulten abusivos, los comercios deberían limitar sus acciones de tal manera que respeten las obligaciones en la materia. Hacerlo, a más de preparar al comercio para el cumplimiento de una ley a corto o mediano plazo que le faculte para operar lícitamente en el tráfico mercantil, le permitirá cumplir las expectativas de sus potenciales clientes y ganar credibilidad frente a estos. Hoy en día es fácil para el usuario comparar y verificar el nivel de responsabilidad, transparencia y esfuerzo puesto por otros comercios respecto del tratamiento de datos personales.

Con lo expuesto, es urgente que Ecuador cuente con una ley de protección de datos personales que salvaguarde derechos fundamentales de los ecuatorianos por diversas razones. Por un lado, debe existir una norma completa y suficiente capaz de garantizar a la persona un derecho sobre el uso y empleo de sus datos personales y de equiparar el desequilibrio entre comercios y usuarios, de modo que se reduzca la posición preferente en la que se encuentra una empresa con sus avisos legales frente al usuario del servicio que no tiene ninguna capacidad de negociación. Por otro lado, también se necesita una normativa que promueva el desarrollo del *e-commerce* en nuestro país, y que haga factible el intercambio comercial con otros territorios que exigen niveles mínimos de protección de datos para realizar negociaciones. Ahora bien, esta normativa debe estar a la altura de las exigencias de otros países y tendría que ocuparse no solo sobre qué se debe informar o qué derechos le asisten al internauta, sino que también debería dar pautas sobre cómo deben cumplirse las obligaciones que le sean aplicables al comercio. En relación con este punto, es esencial tener en cuenta aspectos técnicos y lingüísticos, de suerte que se asegure que el consentimiento sea efectivamente una manifestación de voluntad libre, inequívoca, específica e informada. De la mano de una nueva ley debería promoverse la creación de entidades de certificación con códigos de conducta propios que sin duda impulsarán buenas prácticas entre los comercios más relevantes que se posicionen en Ecuador. Es claro que la norma, por su propia naturaleza, que ha de ser flexible para poder adaptarse a los nuevos retos del ámbito tecnológico, no puede ahondar en cuestiones tan específicas sobre el cómo cumplir las obligaciones en la materia, pero sí que lo puede hacer una entidad de certificación.

Finalmente, es importante decir que estas medidas no deben ser una razón para creer que el internauta va a restringir demasiado las posibles acciones de los comercios en relación con el tratamiento de sus datos personales; de facto, los usuarios aceptan compartir su información para recibir ciertos servicios y lo harán más aún si sienten esa confianza que genera el hecho de que puedan identificar prácticas responsables por parte de la empresa[9]. Además de que, como ya se explicó, hacerlo les permitirá participar lícitamente de la dimensión internacional de este tipo de comercio.

Recomendaciones

Antes de implementar cualquier herramienta para recolección de datos en la web, es recomendable, en primer lugar, definir con precisión los propósitos del tratamiento de datos personales, que deben estar relacionados con la actividad de la empresa. Asimismo, se debe identificar la base legal que respalde el tratamiento de los datos personales para ese fin y, luego, analizar cuidadosamente cuáles son los datos estrictamente necesarios para el cumplimiento de dichos fines. Con este análisis podremos ya escoger las herramientas tecnológicas más apropiadas para recolectar y tratar la información sin que se recojan datos irrelevantes y excesivos. En el proceso de recabar el consentimiento del usuario es recomendable que el *e-commerce* incorpore una página de visualización obligatoria del aviso legal antes de que el internauta pueda marcar la casilla de aceptación; así se presume que la persona ha dado su consentimiento informado.

9 Estudio realizado por la compañía *Accenture Interactive* denominado *Pulse Check 2018 Making it Personal.*

También es recomendable que, una vez implementada la web, junto con las pruebas en las que se verifique la experiencia del usuario, se compruebe la accesibilidad técnica. El usuario debería ser capaz de ubicar los avisos legales sin dificultad y de ejecutar órdenes sencillas que validen la facilidad de los procesos relacionados a la protección de datos personales.

Finalmente, se debe comprobar que se han tenido en cuenta todos los puntos mencionados en este documento, y, para conseguirlo, nada mejor que una lista de verificación en la que se anote si se cumple o no con cada parámetro, de modo que sea posible cuantificar el nivel de cumplimiento. No estará por demás hacer este control con cada actualización del sitio web.

Estas recomendaciones no son más que una parte de un proceso de planificación para una mejora continua que, de cumplirse, dará a la empresa una ventaja competitiva sobre aquellas que no lo hagan.

BIBLIOGRAFÍA

Accenture Interactive. 2018. "Making it Personal. Why brands must move from communication to conversation for greater personalization. Pulse Check 2018." Acceso el 15-IV-2020. https://www.accenture.com/_acnmedia/PDF-83/Accenture-Making-Personal.pdf#zoom=50

Adelola, Tiwalade. Dawson, Ray y Batmaz, Firat. 2015. "Privacy and data Protection in e-commerce in developing nations: evaluation of different data protection approaches". Journal for Digital Society 6: 950-959. Acceso el 10-IV-2020. https://pdfs.semanticscholar.org/ae95/5ceae73996d0d59ba1a55afaad101405744b.pdf%20 https://www.omicsonline.org/open-access/data-privacy-issues-and-possible-solutions-in-ecommerce-2168-9601-1000294-104325.html

Albaladejo, Manuel. 2002. *Derecho Civil. Introducción y Parte General*. Barcelona: Librería Bosch S.L.

Alonso Conde, Ana. 2004. Comercio electrónico: antecedentes, fundamentos y estado actual. Madrid: Dykinson. https://bv.unir.net:3555/es/ereader/unir/60875

Anteportamlatinam Valero, José. 2014. Relevancia del e-commerce para la empresa actual. Tesis de Licenciatura en Administración y Dirección de Empresas. Universidad de Valladolid.

Brkan, Maja y Psychogiopoulou, Evangelia. 2017. *Courts, Privacy and Data Protection in the Digital Environment*. Cheltenham: Eward Elgar Publising Limited.

European Union Agency for Fundamental Rights and Council of Europe. 2018. *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union.

Frosini, Vittorio. 1988. *Informática y Derecho*. Bogotá: Editorial Temis.

Flume, Werner. 1998. *El Negocio Jurídico*. Madrid: Editorial Fundación Cultural del Notariado.

Herrán, Ana. 2003. *El derecho a la protección de datos personales en la sociedad de la información: Cuadernos Deusto de derechos humanos*. Bilbao: Universidad de Deusto.

Illescas Ortiz, Rafael. 2019. *Derecho de la contratación electrónica*. Pamplona: Editorial Civitas.

Information Commissioner's Office. 2018. "Guide to the General Data Protection". Acceso el 25-IV-2020. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Lazpita, María. 1994. "Análisis comparado de las legislaciones sobre protección de datos de los Estados miembros de la Comunidad Europea". *Informática y Derecho* 6-7: 397-420. Acceso el 3-IV-2020. https://dialnet.unirioja.es/servlet/articulo?codigo=248383

Lodder, Arno y Murray, Andrew. 2017. *EU Regulation of e-commerce*. Cheltenham: Edward Elgar Publishing Limited.

Martín Bernal, José. 2001. "Internet y Virtualización del Derecho en General y del Derecho Civil en Particular". *Revista Actualidad Civil* 2: 443-459. Acceso el 20-IV-2020. http://actualidadcivil.laley.es

Pinochet, Ruperto. 2004. "La Formación del Consentimiento a Través de las Nuevas Tecnologías de la Información". *Ius et Praxis* 10: 267-320. Acceso el 2-IV-2020. https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-00122004000200009#nota46

Rodríguez Adrados, Antonio. 2000. "El Documento Negocial Informático". *Notariado y Contratación Electrónica, editado por Consejo General del Notariado*, 353-74. Madrid: Colegios Notariales España.

Seoane, Eloy. 2005. *La nueva era del comercio electrónico*. Madrid: Ed. Ideaspropias.

Singh, Avinash. 2018. "E-Commerce interfering with Privacy: Perceived Risks and Security issues with Techno-policy outcomes". En *Digital Transformation Strategies and trends in E- learning* 1: 802-23. Acceso el 10-IV-2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3298224

Piñar Mañas, José. 2003. "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas". *Cuadernos de Derecho Público* 19-20: 45-90. Acceso el 15-IV-2020. https://core.ac.uk/download/pdf/61482627.pdf

Vega Clemente, Virginia. 2013. "COMERCIO ELECTRÓNICO Y PROTECCIÓN DE DATOS". *Revista de Estudios Económicos y Empresariales* 25: 205-244. Acceso el 11-IV-2020. https://core.ac.uk/download/pdf/72044528.pdf

Legislación

Carta de los Derechos Fundamentales de la Unión Europea (Parlamento, Consejo y Comisión Europea, 7-XII-2000).

Constitución de la República (Ecuador, Registro Oficial No. 449, 20-X-2008).

Convenio No. 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de datos de Carácter Personal (Consejo de Europa, 28-I-1981).

Directiva 95/46/CE. Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Parlamento Europeo y del Consejo, 24-X-1995).

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ecuador, Registro Oficial No. 557, 17-IV-2002).

Proyecto de Ley Orgánica de Datos Personales (Ecuador, Memorando No. PAN-CLC-2019-0184, 19-IX-2019).

Reglamento General de Protección de Datos de la Unión Europea (Parlamento y Consejo de la Unión Europea, Reglamento (UE) 2016/679, 27-IV-2016).

MODERNIZACIÓN DEL SISTEMA REGISTRAL ECUATORIANO
Las oportunidades que trae la tecnología *blockchain*

MODERNIZATION OF THE ECUADORIAN REGISTRY SYSTEM
The opportunities given by blockchain technology

MODERNIZAÇÃO DO SISTEMA DE REGISTRO EQUATORIANO
As oportunidades que traz a tecnologia *blockchain*

Eugenia Novoa* y Cristina Escobar**

Recibido: 10/05/2020
Aprobado: 23/06/2020

Resumen

La modernización del sistema registral ecuatoriano con el uso de tecnología *blockchain* presenta oportunidades de diversas índoles. Destacan los beneficios de crear un sistema de auditoria inmutable, que abarque mayor control sobre los negocios entre los ciudadanos respecto de los predios y bienes inmuebles. Esta técnica tendría un efecto directo en la eliminación de los conflictos continuos del sistema registral actual, tales como la destrucción, deterioro y alteración fraudulenta de varios archivos físicos. Evidentemente, esta opción para el sistema registral también brinda alternativas frente a la situación mundial presentada por el COVID–19, ya que promueve la eliminación paulatina de la brecha tecnológica, así como el avance del país en vías del desarrollo sostenible y consecución de los Objetivos de Desarrollo Sostenible y la Agenda 2030 de Naciones Unidas.

Palabras clave: *Blockchain*; Registros de datos; Modernización registral; Nuevas tecnologías; Era digital

Summary

The modernization of the Ecuadorian registry system via blockchain technology bring many opportunities. One of the main benefits is to create a fix audit system that allows an ampler control over business regarding land and real state. Blockchain technology could eliminate the continuous conflicts of the registry system as we know it, such as the destruction, deterioration and fraudulent modifications of the physical archive. It is clear that this is an option in circumstances such as the COVID-19 emergency, because it promotes a sustainable development and the achievements of the sustainable development goals and the 2030 Agenda for Sustainable Development.

Key words: Blockchain; Data registry; Registry modernization; New technologies; Digital era

Resumo

A modernização do sistema de registro equatoriano com o uso da tecnologia blockchain apresenta oportunidades de diversos tipos. Destaca-se, entre estas, os benefícios de criar um sistema de auditoria imutável, que abarque maior controle sobre os negócios entre os cidadãos relativos aos prédios e bens imóveis. Esta técnica terá um efeito direto na eliminação dos conflitos contínuos do sistema de registro atual, tais como a destruição, deterioração e alteração fraudulenta de vários arquivos físicos. Evidentemente, esta opção para o sistema de registro também proporciona alternativas diante da situação mundial apresentada pelo COVID–19, já que promove a eliminação paulatina do abismo tecnológico, assim como o avance do país rumo ao desenvolvimento sustentável y consecução de seus Objetivos de Desenvolvimento Sustentável na Agenda 2030 das Nações Unidas.

Palavras chave: Blockchain; Registros de dados; Modernização do sistema de registro; Novas tecnologias; Era digital

* LLM por Tulane University. Se desempeña como docente en la Universidad Central del Ecuador. Es coordinadora de UNCTAD Youth Action Hub Ecuador y fundadora de Digital Basis. Tiene experiencia en el trabajo coordinado con la Conferencia de Comercio y Desarrollo de Naciones Unidas para iniciativas juveniles fomentando el desarrollo sostenible y trabajo como voluntario para la Agenda 2030 y la era digital. Ha liderado proyectos regulatorios pertenecientes al sistema registral ecuatoriano, protección de datos e interoperabilidad. Fue asistente de investigación de Guiguo Wang en Tulane University. Ha publicado varios artículos promoviendo la economía digital y el multilateralismo. Correo electrónico: epnovoa@uce.edu.ec

** Estudiante Suma Cum Laude de la Facultad de Jurisprudencia de la Universidad Central del Ecuador. Involucrada en proyectos de vinculación social y con particular interés en el desarrollo de nuevas tecnologías aplicadas al Derecho. Correo electrónico: criis.isabel@gmail.com

INTRODUCCIÓN

En la última década, y debido al desarrollo inminente de las nuevas tecnologías a nivel mundial, se ha reflexionado respecto a la redefinición y necesidad de modernizar el sistema registral ecuatoriano. Desde la promulgación de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos en el 2010, dichas reflexiones han aumentado paulatinamente.

A esta nueva conciencia se suma la complejidad del sistema registral ecuatoriano, particularmente en lo referente a registros de la propiedad. Los cuestionamientos y preocupaciones se han incrementado, y la tecnología presenta soluciones eminentes que vale la pena considerar para avanzar en el contexto Post Covid 19.

Con la modernización de un sistema registral con el uso de tecnología *blockchain* destacan los beneficios de crear un sistema de auditoría inmutable, que abarque mayor control sobre los negocios entre los ciudadanos respecto de los predios y bienes inmuebles. La nueva tecnología tendría efecto directo en la eliminación de muchos conflictos continuos del sistema registral actual tales como destrucción, deterioro y alteración fraudulenta de varios archivos físicos. Esta opción promovería también la eliminación paulatina de la brecha tecnológica y generaría desarrollo para el país.

El presente trabajo, entonces, comenzará por introducir brevemente el sistema registral ecuatoriano, su actual funcionamiento y forma de manejo, para entender las problemáticas nacionales inmersas en la modernización del sistema registral. Posteriormente, se presentará el uso de tecnología *blockchain* o *distributed ledger tecnology*, así como casos internacionales en los que esta se encuentra en desarrollo. Finalmente se busca establecer la necesidad del Estado ecuatoriano de modernizar el sistema registral, con miras a buscar la implementación de tecnologías *distributed ledger* para facilitar este proceso.

EL SISTEMA REGISTRAL ECUATORIANO Y LA LEY ORGÁNICA DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS

1. Generalidades del sistema registral en Ecuador

En el Ecuador, el sistema registral está regulado en la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos (en adelante Ley SINARDAP), expedida el 24 de marzo del 2010 y publicada en el Registro Oficial Suplemento Nº. 162, de fecha 31 de marzo de ese año. Esta ley regula de manera general todo el sistema 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" (Ley SINARDAP, art. 13). Históricamente, los registros de datos en Ecuador han sido físicos. Esta ley busca promover el desarrollo de la actividad registral, con "medios tecnológicos normados y estandarizados (...)" (Ley SINARDAP, art. 13).

Los registros en el Ecuador son "dependencias públicas, desconcentrados, con autonomía registral y administrativa" y están "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" (Ley SINARDAP, art. 13).

El sistema registral ecuatoriano se complementa con el contenido de la Ley de Registro, expedida en el año 1966 y publicada en Registro Oficial N.º 150 de 28 de octubre de 1966. Dicho cuerpo normativo se modificó

en gran parte una vez expedida la Ley del Sistema Nacional de Registro de Datos Públicos; sin embargo, hasta la presente fecha regula los requisitos para ser registrador, sus obligaciones y responsabilidades, el mecanismo para repertorio, los registros e índices; los títulos, actos y documentos que se deben registrar; el procedimiento, forma y solemnidad de las inscripciones, la variación de estas y su cancelación, entre otros aspectos (Ley de Registro, arts. 18-25).

El sistema registral ecuatoriano es bastante diverso y complejo de entender por diversas razones. Por un lado, la división territorial del Ecuador implica que existan registros muy pequeños; además, el clima, tiempo y movilización de registros repercute en la destrucción y deterioro de varios archivos físicos. Finalmente, para impulsar la modernización registral, es importante considerar la brecha tecnológica y las limitaciones de acceso al internet en varios lugares del país.

2. El Sistema Nacional de Datos Públicos

La Ley del SINARDAP crea el Sistema Nacional de Datos Públicos (en adelante SINARDAP), que cumple la finalidad de "proteger los derechos constituidos, los que se constituyan, modifiquen, extingan y publiciten por efectos de la inscripción de los hechos, actos y/o contratos" (Ley SINARDAP, art. 28), determinados por la respectiva normativa registral nacional. Asimismo, el sistema unificado de registros cumple el objeto de "coordinar el intercambio de información de los registros de datos públicos" (Ley SINARDAP, art. 28).

El ente encargado de presidir el SINARDAP es la Dirección Nacional de Registro de Datos Públicos (en adelante DINARDAP), como un organismo autónomo, con personaría jurídica, de derecho privado y adscrito al Ministerio de Telecomunicaciones (Ley SINARDAP, art. 30).

Los numerales 1, 2, 4, 5 y 6 del artículo 31 de la Ley Orgánica de Registro de Datos Públicos establecen como facultades de la Dirección Nacional de Registro de Datos Públicos las de:

> 1. Presidir el Sistema Nacional de Registro de Datos Públicos, cumpliendo y haciendo cumplir sus finalidades y objetivos; 2. Dictar las resoluciones y normas necesarias para la organización y funcionamiento del sistema; (...) 4. Promover, dictar y ejecutar a través de los diferentes registros, las políticas públicas a las que se refiere esta Ley, así como normas generales para el seguimiento y control de las mismas; 5. 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; 6. Definir los programas informáticos y los demás aspectos técnicos que todas las dependencias de registro de datos públicos deberán implementar para el sistema interconectado y control cruzado de datos, y mantenerlo en correcto funcionamiento. (Ley SINARDAP, art. 30)

Así pues, es competencia de la Dirección Nacional la de definir programas informáticos para implementar el sistema interconectado y control cruzado de datos. Es decir, cualquier proceso de implementación para cambiar o mejorar el actual sistema registral ecuatoriano deberá ser liderado por esta institución, especialmente aquellos que cumplan el fin de brindar una plataforma tecnológica para coordinar el intercambio de información de entre distintos registros de datos públicos.

El SINARDAP también abarca un conjunto de registros de datos que, por disposición legal, administran información registral de carácter público. Entre los entes que conforman el SINARDAP están los registros: civil, mercantil, de la propiedad, vehicular, societario, entre otros (Ley SINARDAP, art. 30).

Estos sistemas registrales, sean de la naturaleza que sean, tienen como finalidad brindar seguridad sobre los datos personales, patrimoniales, contractuales y su conservación. Para fines de la presente investigación nos enfocaremos en detallar la operatividad de los registros mercantiles y de la propiedad en el Ecuador.

INTEROPERABILIDAD Y UNIFICACIÓN DE SISTEMAS REGISTRALES EN ECUADOR

La finalidad y objeto de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, por un lado es el de crear y regular "el sistema de registro de datos públicos y su acceso, en entidades públicas o privadas que administren dichas bases o registros" y, por el otro, el de "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" (Ley SINARDAP, art. 1).

El objetivo y finalidad tanto de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, como de la DINARDAP, deben cumplirse a fin de observar el mandato de la Constitución de la República del Ecuador.

Tenemos el artículo 66 numeral 25, que garantiza el derecho de los y las ecuatorianos de "acceder a bienes y servicios públicos y privados de calidad, con eficiencia, eficacia y buen trato, así como a recibir información adecuada y veraz sobre su contenido y características" (Constitución de la República del Ecuador, art. 66 Nº. 25).

Para posibilitar dicho mandato en Ecuador, también debe observarse el contenido del artículo 227, que establece como principios rectores de la administración pública "eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación" (Constitución de la República del Ecuador, art. 227).

De conformidad con el artículo 13 de la Ley Orgánica de Registro Nacional de Datos Públicos, los registros están 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 (...)" (Ley SINARDAP, art. 13).

Respecto al sistema informático para el funcionamiento e interconexión de registros, este es "es de propiedad estatal y del mismo se podrán conceder licencias de uso limitadas a las entidades públicas y privadas que correspondan, con las limitaciones previstas en la Ley (...)" (Ley SINARDAP, art. 23).

La Disposición Transitoria Cuarta de la Ley Orgánica de Registro de Datos Públicos establece que "los Registros de la Propiedad, Societario, Civil y Mercantil que mantengan digitalizados sus registros, deberán mudar sus bases de datos al nuevo sistema, para lo cual la Dirección Nacional asignará los fondos para la creación y unificación del sistema informático nacional de registro de datos públicos".

La Dirección Nacional de Registro de Datos Públicos, por lo tanto, es competente para implementar un sistema informático que estandarice procesos entre los distintos Registros mercantiles y de la propiedad a nivel nacional, competencias que le han sido establecidas en su Ley de Registro de Datos Públicos, conforme lo señalado en párrafos previos.

1. Sistema Nacional de registros mercantiles en Ecuador

Los Registros Mercantiles en el país están organizados y administrados por la Función Ejecutiva a través de la Dirección Nacional de Registro de Datos Públicos, ente a cargo de dictar las normas técnicas y ejercer las demás atribuciones ley para la conformación e integración al sistema (Ley SINARDAP, art. 23).

Al momento, todos los registros mercantiles del país se hallan operativos a través de un sistema electrónico unificado llamado Sistema Nacional de Registro Mercantil (SNRM), que se creó con fecha 14 de septiembre de 2012, mediante Resolución Nº. 15-NG-DINARDAP-2012 de la DINARDAP. A partir de dicha fecha, los distintos Registros mercantiles a nivel nacional pasaron a implementar este sistema, en

observancia de los manuales especificados en el artículo 4 de la Resolución antedicha.

En los últimos años se han evidenciado en la DINARDAP continuas fallas y necesidades en el sistema SNRM, que han llevado a la institución a crear un Comité de Gestión de Cambios (Informe de Auditoría de Tecnologías de la Información DINARDAP, 0004-DATI-2015) para mitigar los riesgos del manejo informático de las plataformas. Este proceso ha llevado a la institución a plantearse, como solución estructural, la de generar un sistema más amplio que permita el óptimo funcionamiento de la plataforma virtual, de modo que facilite la inscripción de actos y contratos en el registro mercantil.

2. Sistemas de registros de la propiedad del Ecuador

La Constitución de la República del Ecuador, en su artículo 265, establece la concurrencia en la administración del sistema público de registro de la propiedad entre el Ejecutivo y las municipalidades (Constitución de la República del Ecuador, art. 265). Dicha concurrencia ha sido normada tanto en la Ley del SINARDAP, como en el Código Orgánico de Organización Territorial, Autonomía y Descentralización (en adelante COOTAD), con el fin de esclarecer la aplicación de la normativa en posibles conflictos de interpretación.

El COOTAD, en su artículo 142, define la competencia de los Gobiernos Autónomos Descentralizados Municipales (en adelante GAD) en la administración de los registros de la propiedad bajo los siguientes parámetros:

> (...) La administración de los registros de la propiedad de cada cantón corresponde a los gobiernos autónomos descentralizados municipales. El sistema público nacional de registro de la propiedad corresponde al gobierno central, y su administración se ejercerá de manera concurrente con los gobiernos autónomos descentralizados municipales de acuerdo con lo que disponga la ley que organice este registro. Los parámetros y tarifas de los servicios se fijarán por parte de los respectivos gobiernos municipales. (COOTAD, art. 142)

Por su lado, la Ley del SINARDAP, especifica en su artículo 19, la operatividad de la administración conjunta entre las municipalidades y gobierno central:

> (...) el Municipio de cada cantón o Distrito Metropolitano se encargará de la estructuración administrativa del registro y su coordinación con el catastro. La Dirección Nacional dictará las normas que regularán su funcionamiento a nivel nacional. Los Registros de la Propiedad asumirán las funciones y facultades del Registro Mercantil, en los cantones en los que estos últimos no existan y hasta tanto la Dirección Nacional de Registro de Datos Públicos disponga su creación y funcionamiento. (Ley SINARDAP, art. 19)

Cabe señalar que en aquellos casos de registros de la propiedad de cantones pequeños en los que aún no existan registros mercantiles, los registradores de la propiedad serán quienes cumplan tales funciones. Ejemplos de estos casos son variados, como el registro de Quevedo o de Cevallos. Dichos registros, igualmente estarán controlados por la DINARDAP, con sus respectivas competencias en materia mercantil y como registro de la propiedad inmobiliaria.

No se ha logrado hasta el momento estandarizar un sistema informático que permita el control cruzado de información para los distintos registros de la propiedad a nivel nacional, conforme requieren las especificidades de los artículos 23 y 24 de la Ley del SINARDAP. En el intento de lograrlo, la DINARDAP, en el año 2013 emitió la Resolución 019-NG-DINARDAP-2013, mediante la cual crea el Sistema Nacional de Registro de la Propiedad, que ha sido adoptado por pocos registros a nivel nacional.

Existen varios municipios que han invertido considerables cantidades en optimizar su sistema registral electrónico. Un ejemplo es el Sistema Integrado de Registros de la Propiedad y Mercantiles del Ecuador (en adelante SIRE) desarrollado por la municipalidad de Guayaquil. Otros ejemplos son los casos de

Ambato y Quito. A pesar de varios intentos fallidos, al momento, en Ecuador no se ha implementado un sistema unificado para el manejo de información y datos de los distintos registros de la propiedad existentes.

3. Interoperabilidad del sistema registral ecuatoriano en el marco del COVID 19

La llegada del coronavirus al Ecuador ha presentado una serie de problemáticas a nivel gubernamental, tanto económicas, como de salud y educación, entre otras. Al tener que tomar medidas para evitar las aglomeraciones de personas en un determinado lugar para evitar los contagios, la ejecución de muchos trámites burocráticos que se realizaban en los registros se vio directamente afectada, razón por la cual se detuvo una gran cantidad de acciones de las personas y empresas, al no poder salir la gente de sus casas para realizar los trámites.

Los registros de la propiedad, mercantil y los que fungen las veces de registros mixtos se vieron en la necesidad de implementar nuevos servicios de trámites en línea. Por la necesidad de que los tramites no se paralicen, a través de las resoluciones N.º 008-NG-DINARDAP-2020 y N.º 009-NG-DINARDAP-2020, del 11 y 30 de abril respectivamente, la DINARDAP regula todos los procedimientos necesarios para que los trámites más comunes, tanto en los registros mercantiles, los de la propiedad y los registros de la propiedad que ejercen funciones de mercantiles, se realicen en línea. Estos trámites, tal como lo establecen dichas resoluciones, se efectuarán a través de la plataforma GOB.EC, u otras TICs que puedan cumplir con la misma finalidad.

Todos los trámites ciudadanos se los llevará a cabo a través de formularios prestablecidos en línea, y la integración de cada registro dentro de la plataforma GOB.EC es responsabilidad cada registro. Los registros tienen a su cargo la realización de las gestiones necesarias en el Ministerio de Telecomunicación para integrarse a la plataforma gubernamental y publicar sus trámites, y para diseñar los formularios. Igualmente, "corresponde a los Registros de la Propiedad y Registros de la Propiedad con funciones y facultades de Registro Mercantil que no tengan autonomía realizar las gestiones correspondientes ante los Gobiernos Autónomos Descentralizados Municipales o Metropolitano para la habilitación del Registro en la plataforma GOB.EC (Resolución 009 DINARDAP 2020, art. 10).

A la fecha ya existe un amplio catálogo de trámites que se pueden realizar en la plataforma GOB.EC. En materia mercantil encontramos: inscripción de nombramientos, cancelación de Contratos de Prenda Industrial o Prenda Especial de Comercio, Arrendamiento Mercantil o Contrato de Reserva de Dominio, Gravamen de Compraventa Agrícola, Inscripción de Compraventa con Reserva de Dominio, Certificación de Gravámenes de Vehículos o Bienes Muebles, entre otros (DINARDAP 2020).

Cabe destacar que estos sistemas se implementaron a partir de la cuarentena dictada para evitar contagios del COVID-19. Lamentablemente, el progreso solo se ha alcanzado con la coyuntura de la emergencia sanitaria. La necesidad de actualizar los sistemas registrales, como se ha detallado previamente, era palpable hace ya algunos años. Ahora es emergente evolucionar como Estado, a fin de fomentar la innovación y disrupción digital, no solo para trámites registrales, sino para la administración pública en general. El gobierno electrónico es una necesidad urgente para el Ecuador y para todos los Estados, frente a la coyuntura social que ha presentado la situación mundial del COVID-19.

4. Necesidad de unificar e interoperar sistemas registrales en Ecuador

Los registros de la propiedad y mercantiles tienen la finalidad de contribuir al buen funcionamiento de la sociedad, con el propósito de brindar seguridad a las personas que adquieren bienes muebles o inmuebles. La relevancia de estos entes se palpa claramente en el desarrollo económico de la sociedad; la transabilidad y los negocios son más ágiles cuando existe un sistema registral consolidado que brinde servicios de calidad a sus ciudadanos.

Para lograr servicios registrales eficaces y eficientes es evidente la necesidad no solo de controlar la actividad

de los distintos registros en el país; sino de ofrecer opciones tecnológicas que simplifiquen y agilicen los procesos de cada institución.

La DINARDAP en sujeción al artículo 15 de su ley ha expedido varios actos normativos con el objeto de estandarizar el sistema de registros de la propiedad y mercantil. Esta normativa interna debe ser tomada en cuenta para la modernización del sistema registral del país. En este sentido, es importante enumerar las normas internas a las que se debe adaptar el nuevo sistema, como también enunciar aquellas que impedirían su buen desarrollo y, por ende, deberían ser reformadas o directamente derogadas.

Tabla Nº. 1: Normativa interna de la DINARDAP relevante para la modernización del sistema registral

No.	NOMBRE NORMATIVA	RESOLUCIÓN
1	Instructivo separación libros registrales actos propiedad mercantil	Resolución 006-NG-DINARDAP-2012
2	Norma regula procedimiento sistema de notificaciones electrónicas	Resolución 009-NG-DINARDAP-2014
3	Norma que regula interoperación de registros mercantiles y propiedad	Resolución 012-NG-DINARDAP-2014
4	Crea el sistema nacional de registro de la propiedad	Resolución 019-NG-DINARDAP-2013
5	Instructivo de transferencia documental de registradores mercantiles	Resolución 025-NG-DINARDAP-2011
6	Instructivo de control y vigilancia registros mercantiles, propiedad	Resolución 038-NG-DINARDAP-2016
7	Información actos y contratos inscritos registro mercantil propiedad	Resolución 039-NG-DINARDAP-2015
8	Crea el sistema nacional de registro mercantil	Resolución 15-NG-DINARDAP-2012
9	Norma de digitalización de documentos de la DINARDAP	Resolución 15-NG-DINARDAP-2012
10	Norma regula uso del sistema de envío y depuración de la información	Resolución 0007-NG-DINARDAP-2017

La Dirección Nacional de Registro de Datos Públicos, con el fin de facilitar la modernización del sistema registral ecuatoriano tendría que observar la normativa enunciada, puesto que esta define procesos elementales que podrían coartar los procesos automáticos que ofrece un sistema de *blockchain* para un registro de datos públicos.

También es importante mencionar que varios doctrinarios y expertos en materia registral nacional han identificado como la principal problemática, para la unificación, interoperabilidad y modernización del sistema registral ecuatoriano, la falta de claridad y vacíos legales existentes en el actual marco regulatorio registral del país (Orna 2013, 71).

Sin embargo, la presente sección simplemente busca poner de manifiesto los distintos obstáculos de carácter normativo que el sistema registral podría presentar al momento de buscar una modernización del mismo.

USO DE TECNOLOGÍA *BLOCKCHAIN* PARA LA MODERNIZACIÓN DE SISTEMAS REGISTRALES

Los sistemas registrales son una suerte de garantía existente del derecho a la propiedad de las personas. El 70% de la población mundial no tiene acceso a un sistema formal de registro de tierras (Weizsäcker, Eggler y Atarim 2019, 1). Debido a que los registros públicos ofrecen constancia de los títulos, facilitan las transacciones y previenen el fraude, cumplen un rol esencial para el desarrollo de los países, en la medida en que incentivan la inversión en el sector inmobiliario y, así, generan un desarrollo económico y social beneficioso. En cuanto a los habitantes de una nación, el estatus de los derechos de propiedad puede afectar a sus oportunidades económicas, mientras que, respecto a los gobiernos, dichos registros son esenciales para el cobro de impuestos, provisión de servicios y establecimiento territorial de autoridades (Benbunan-Fich y Castellanos 2018, 4).

La seguridad de los derechos de propiedad, sobre bienes muebles e inmuebles, es un elemento esencial para promover el crecimiento económico, identificar las inequidades económicas, aliviar la solución de conflictos y apoyar los procesos de gobernanza local. Los países en vías de desarrollo, por lo general, aún cuentan únicamente con registros físicos y archivos en papel, que no solo presentan dificultades de acceso, sino que también existe vulnerabilidad de los registros ante desastres naturales, e inseguridad en las actuaciones de cualquier persona que tenga acceso a los archivos físicos.

La búsqueda de seguridad de la información va encaminada a garantizar no solo la veracidad contenida en los archivos de registros con el objeto de evitar alteraciones arbitrarias, sino que también busca la rapidez de los procesos de inscripción, la transparencia en actuaciones y la confianza en el sistema de registral de un país. La corrupción, la falta de legalización de ciertos predios y las condiciones de vulnerabilidad, entre otras causas, son las que legitiman un cambio de sistema de registro con miras a que este garantice una mayor seguridad, y en este contexto resalta el valor del sistema de *blockchain*, también conocido como *distributed ledger technology* (en adelante DLT), como una alternativa positiva para innovar y dar el paso a la era digital que es ahora la que define la economía y el mundo.

A continuación, presentamos una explicación detallada de los sistemas *blockchain* para registros públicos y de las novedosas alternativas que ofrece este avance tecnológico a países como el Ecuador.

1. El sistema *blockchain*

En palabras sencillas, un *blockchain* o cadena de bloques, es una base de datos tecnológica. Es una forma o sistema de registro de cuentas distribuido o descentralizado, al que pueden acceder y también actualizar una multiplicidad de usuarios (Ledger Insights, 2019).

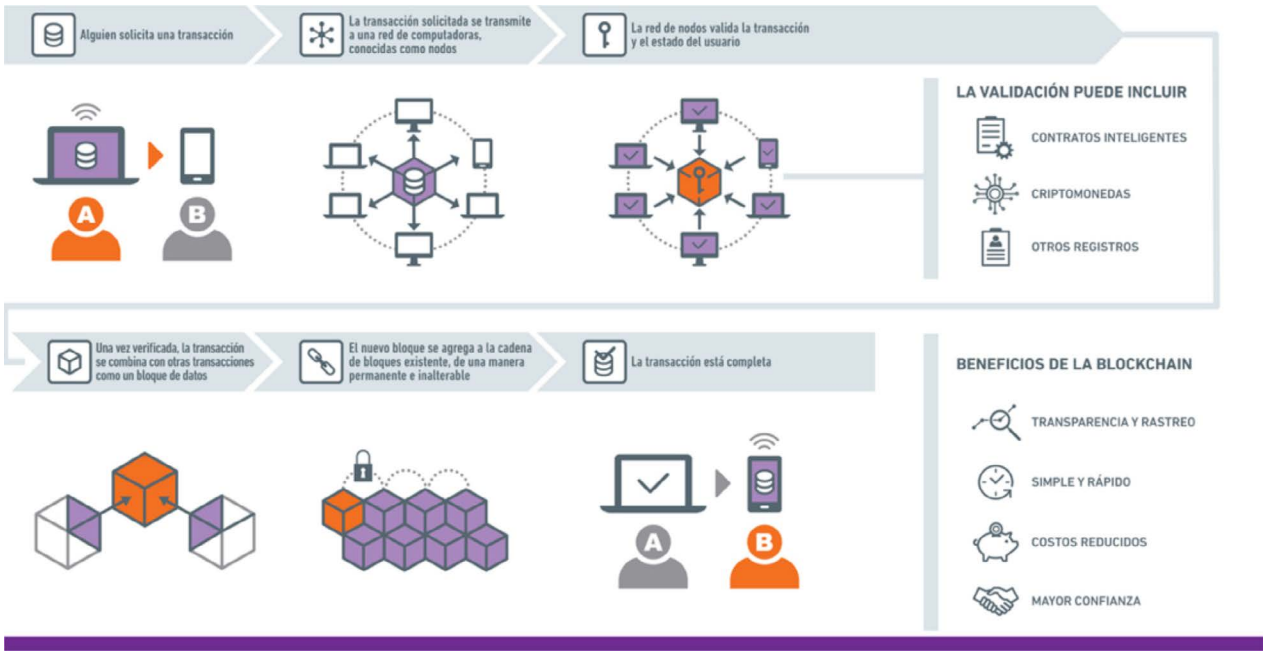
El *blockchain* es una "lista creciente de registros que se guardan en bloques, que son criptográficamente seguros y se vinculan a través de una red de computadoras. Incluso si el 99% de computadoras de esa red están desactivadas, los registros se mantendrán disponibles y seguros en otra parte de la red" (Weizsäcker, Eggler y Atarim 2019, 2).

Los integrantes de una red de *blockchain,* de manera colectiva, validan la nueva información ingresada. La validación se hace a través de algoritmos consensuales y ésta añade la información a *blocks* (en español bloques). Dichos bloques están enlazados o conectados de manera criptográfica a una *chain* o cadena (United Nations Conference of Trade and Development 2019, 6). De ahí deviene el nombre de *blockchain*, que en español sería: cadena de bloques.

Una vez que la transacción ha sido aprobada por la red, y se ha añadido al *blockchain*, la transferencia de dominio, un acto inmutable, se registra en el sistema, que se convierte en un punto único de confianza que impide la corrupción o adulteración de las transferencias (United Nations Conference of Trade and Development 2019, 6).

Como resultado de dicho proceso, esta red descentralizada permite crear un registro, en base a acuerdos, acerca del tiempo y origen de cada entrada, que se almacenará en varias computadoras. Por esta razón, consideramos que el sistema de *blockchain* ofrece beneficios inigualables para validar transacciones en cualquier campo al que se aplique (bancos, empresas, o sistemas de almacenamiento de registros gubernamentales); por sus características, es un sistema muy complejo de hackear, engañar o manipular. A continuación, en la Fig. Nº. 1 presentamos una ilustración de la funcionalidad del sistema *blockchain*.

Figura Nº. 1: Funcionalidad del sistema *blockchain*
(Pro Universitarios 2018)



El sistema *blockchain* se caracteriza por la seguridad que brinda a sus usuarios, las transacciones que se llaman "bloques" se validan en cadena, en una sucesión de computadoras, y no se almacenan en un único servidor; por el contrario, estas se verifican en una variedad de nodos o red de computadores. Este sistema democratiza y da transparencia a las transacciones, y permite a los usuarios rastrear procesos en tiempo real, debido a la arquitectura distributiva que posee y a los protocolos de entrada propios del sistema (Kraft 2019).

El sistema de *blockchain* puede desarrollarse en distintas formas de acuerdo con las necesidades de sus usuarios (Benbunan-Fich y Castellanos 2018, 7). Particularmente existe la división primordial entre sistema de *blockchain* público y el sistema de *blockchain* privado.

El sistema de *blockchain* público encarna la idea de descentralización, pues no existe un actor único que tenga control sobre la red. Este modelo asegura que la información no sea alterada una vez que se validó. En otras palabras, cualquier persona, en cualquier lugar puede usar un sistema de *blockchain* público para ingresar transacciones e información mientras esté conectada a la red. En el sistema de *blockchain* privado, en cambio, los permisos para crear los registros se centralizan en determinadas entidades determinadas por los desarrolladores, es decir existe un acceso restringido a los usuarios que participan en dicha red de validación transaccional (ITU News 2018).

Por lo pronto los usos que se han dado a los sistemas de *blockchains* se han limitado al ámbito de la creación de *tokens* redituables para las empresas y en el desarrollo de criptomonedas (ITU News 2018). Empero, las

características propias de este sistema permiten que él se pueda introducir en una escala más amplia de aplicaciones, para incrementar la transparencia y mejorar la gobernanza. Existen factores que propenden a que el desarrollo del *blockchain* en los derechos de propiedad sea exitoso. Entre los factores estratégicos están el diseño de consenso y el rastro que deja (Lantmäteriet, y otros 2016, 15); mientras que encontramos factores operacionales que se resumen en la transferibilidad de los derechos.

2. Los *smart contracts*

Para el efectivo funcionamiento de un sistema de *blockchain* atado a la actividad registral, es necesario que se utilice la figura de los *smart contracts,* conocidos en español como contratos inteligentes o virtuales. Los contratos de esta clase permiten a los programadores codificar las aplicaciones de varios usuarios, incluir su identidad digital e, incluso, un activo intercambio automático de los datos que forman parte de la cadena de bloques (Eder 2019, 2-3).

Tales "contratos inteligentes" implican la transferencia de dominio en sí misma. Este proceso involucra digitalizar por completo los registros para legalmente efectuar un contrato de compraventa de propiedades de punto-a-punto (*peer-to-peer*), que permite eliminar a intermediarios del proceso como los bancos, notarías y las oficinas públicas de registro (Muller y Seifert 2019, 7-8). Es decir, estos contratos significan un libro de registro público, digitalmente formado por las partes y que transfiere de manera automática el título de propiedad tras el pago. El proceso de los *smart contracts* se resumen en la Fig. Nº. 2 (Ameer 2016).

Figura Nº. 2: *Smart contracts*

Este sistema de contratos inteligentes, que no requieren la comparecencia física de las partes contratantes, bastaría con sus firmas electrónicas a través de *tokens*[1]. Es decir, para implementar un sistema de *blockchain* con contratos inteligentes en Ecuador, el régimen legal necesitará especificar la figura de los contratos de este tipo, mediante reformas al marco regulatorio en materia de contractual civil y comercial, además de plantear las reformas al sistema registral especificadas en capítulos anteriores.

Los contratos inteligentes representan una suerte de modelos genéricos para todos los casos, de manera que, en su contenido, no reflejarían acuerdos extracontractuales, los cuales quedarían fuera del *blockchain*. Sin embargo, la tecnología ha avanzado de tal forma que ofrece una solución para esta particularidad, los *oracles* (Panfil, Mellon y Robustelli 2019, 2) u oráculos, sistemas que cumplen la función de adecuar el *blockchain* a la vida real, con vistas a proveer la información sobre estos agentes externos para la ejecución de los contratos inteligentes.

La idea de basar el registro de propiedades en una sofisticada solución a través de contratos inteligentes trae una complejidad de problemas legales que son desafiantes al momento de implementarlas. Doctrinarios y especialistas internacionales recomiendan un entorno regulatorio amplio y general que permita la paulatina definición de particularidades en el uso de *smart contracts* basadas en la práctica y necesidades diarias de cada país. A la final, el derecho siempre va detrás de la tecnología y no podría adelantarse a definir la inmensidad de circunstancias excepcionales que podrían presentar estos sistemas" (Weizsäcker, Eggler y Atarim 2019, 5).

3. Ventajas y desafíos de aplicar el sistema de *blockchain* en el sistema registral

La solución en base al sistema de *blockchain*, se centra en que la cadena de transacciones no se controla de manera unilateral, o por un solo actor. La información pasa y es validada por una multiplicidad de usuarios, una circunstancia que disminuye las posibilidades de manipulación de registros, acaparamiento de tierras o estafas. Esta situación genera, entre otras, las siguientes ventajas:

1. Control descentralizado de distintos usuarios, como ya se mencionó; todos esos usuarios trabajan para verificar esa la información a través del consenso y toda la información está conectada como una única huella o fingerprint para asegurar la integridad de la información.

2. Permite seguir el rastro de manera real de cualquier cambio de dueño de un bien mueble o inmueble, al igual que la transparencia en el estado en el que se encuentra una propiedad, de forma que se elimina la posibilidad de una manipulación de títulos.

3. Los sistemas de este tipo son remotamente accesibles para los usuarios, evitan ciertos escenarios de corrupción al fomentar la transparencia de actuaciones, mejoran la calidad de la información y la confianza en el almacenamiento. La tecnología *blockchain* destaca por su inmutabilidad y resiliencia. Otro aspecto trascendental, previamente mencionado, es la descentralización de la información, que se almacena en varios servidores gracias a la conjunción del *cloud computing*.

Este sistema implementado al registro de bienes muebles e inmuebles de un país puede eventualmente aumentar la eficiencia de la administración, disminuir los costos de los registros, los intermediarios y los usuarios finales. Incluso repercute en la transparencia y confianza que este sistema presenta (Bloch 2018, 4).

Frente a esta multiplicidad de beneficios, también encontramos problemáticas al momento de evaluar la necesidad de modernizar un sistema registral a la hora de implementar la tecnología *blockchain*. Entre las desventajas se pueden mencionar las siguientes:

1. Como todo avance tecnológico, el sistema *blockchain* no estará siempre a la vanguardia

1 Ya existentes en Ecuador con la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

de los avances tecnológicos a futuro, es decir, eventualmente puede dejar de tener vigencia. Sin embargo, cualquier sistema distributivo en cadena descentralizada es menos propenso a fallar durante su vigencia, en la medida en que depende en varios e independientes componentes y nodos para validar transacciones.

2. Las limitaciones legales y tecnológicas para la estructuración de los contratos inteligentes antes mencionadas. Este obstáculo acarrea inseguridad respecto a los títulos de propiedad de bienes muebles e inmuebles y las obligaciones de las partes contratantes. Sin embargo, la interpretación de los contratos siempre ha causado conflictos legales, con medios físicos o digitales.
   La complejidad de la legislación contractual deberá entonces ser sustentada estar bien estructurada en el desarrollo de los contratos inteligentes para las transacciones en *blockchain*. Esta exigencia no solo implica introducir cambios en la normativa nacional, sino también un desarrollo de cultura digital y capacitación continua, para disminuir la brecha digital.

3. Otra desventaja es la falta de madurez o desarrollo de la tecnología de *blockchain* en el campo registral (DiCamillo 2019, 1). La tecnología DLT es emergente y, en los últimos años, ha iniciado su implementación para el espectro de sistemas registrales. Será entonces necesario aceptar el riesgo y el desafío tanto de esta migración de la información como de la puesta en marcha de esta nueva tecnología.

Específicamente destacan los beneficios de crear un sistema de auditoria inmutable, que abarque mayor control sobre los negocios entre los ciudadanos respecto de los predios y bienes inmuebles.

4. Lineamientos para un buen funcionamiento e implementación de un sistema registral con la tecnología *blockchain*

Si bien la tecnología *blockchain* en un primer momento es alentadora, también presenta limitaciones muy evidentes al momento de su implementación. Para el buen funcionamiento del sistema es importante asumir retos iniciales que inciden en el cambio de procesos gubernamentales, el aprovechamiento de nuevas tecnologías y el desarrollo de cultura digital, como ha sucedido en la experiencia de otros países. Para la implementación de sistemas de este tipo deberá tomarse en cuenta lineamientos como: incluir un sistema de identificación funcional, registros precisos y digitalizados, y una comunidad entrenada para el cambio de paradigma.

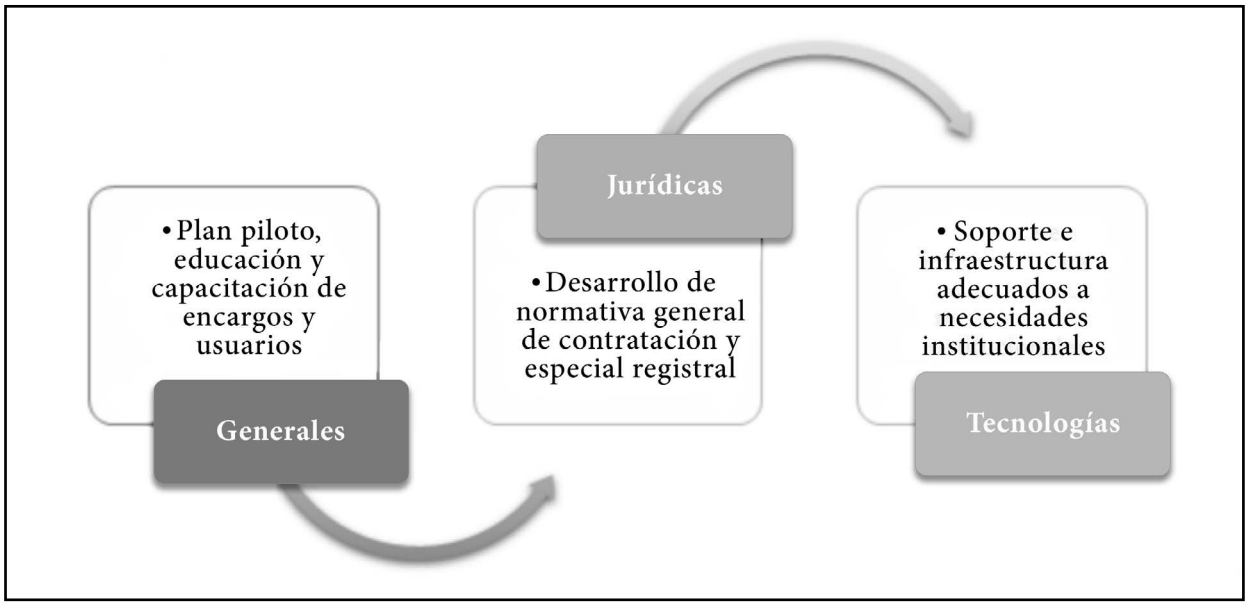
El caso exitoso de implementación de tecnología *blockchain* en Georgia presenta un buen ejemplo de los requisitos a considerar. Inicialmente se desarrolló por etapas una habituación de la sociedad a este tipo de trámites (International Business Times UK 2017). Tal sensibilización incluso incidió en cambios de cultura política que nacen de una iniciativa externa para atraer inversores internaciones y frenar la corrupción (Eder 2019, 5). Como resultado de este proyecto se mejoró notablemente la eficiencia gubernamental a fin de reconstruir la confianza pública en las agencias nacionales. Hasta el 2018 se reportó un total de 1.5 millones de registros de títulos de propiedad de predios en Georgia realizadas y verificadas a través de transacciones DLT (Shang y Price 2018, 77).

La implementación de la tecnología *blockchain* en sistemas registrales como el ecuatoriano debe igualmente considerar distintos factores. En principio, es necesario generar un plan de trabajo e iniciar con un MPV (*Mínimum Viable Product*) en pequeñas muestras territoriales. La ejecución de tal plan piloto debe tomar en cuenta la educación y la capacitación, tanto de servidores públicos como de usuarios (VectorITC 2018, 21). Es elemental considerar los aspectos jurídicos de las transacciones y desarrollar una normativa abierta que contemple la validez de los contratos inteligentes dentro de todo el régimen civil y mercantil ecuatoriano. También será preciso definir, mediante normativa especializada, los actos y contratos que podrán ser materia de registro una vez implementados sistemas de *blockchain*.

Dentro del aspecto tecnológico hay varias consideraciones que se deben contemplar: La madurez de la organización para pasar al ámbito digital, el equipo

sólido de soporte para una adecuada gestión de plataformas, la seguridad de la información, y la fiabilidad de los sistemas tecnológicos a ser implementados (Clohessy y Acton 2018, 73). Los aspectos a tener en cuenta para implementar el sistema *blockchain* se especifican en la siguiente figura.

Figura Nº. 3: Consideraciones para implementación del sistema *Blockchain*



Fuente: Clohessy y Acton (2018).
Elaboración: Novoa Eugenia y Escobar Cristina.

La implantación de sistemas DTL, evidentemente presenta sus retos iniciales, pero las ventajas son innumerables si se siguen ciertos lineamientos para su buen funcionamiento. El escenario perfecto para probar la efectividad de estos procesos es el combate contra las prácticas fraudulentas y corruptas, particularmente las que se relacionen con el fraude de documentos, las ventas duplicadas, o el riesgo de que actores maliciosos confabulados con funcionarios sobornables de ciertas instituciones gubernamentales confisquen los predios. Es elemental, para el buen funcionamiento e implementación de *blockchain* en sistemas registrales, la educación continua de servidores públicos y usuarios durante el proceso de implementación (World Economic Forum s.f.). En general, cualquier cambio en los procesos gubernamentales, implica o requiere una combinación de experticia tecnológica, preparación de infraestructura y mecanismos para superar la resistencia cultural (Ledger Insights, 2019).

LA MODERNIZACIÓN DEL SISTEMA REGISTRAL ECUATORIANO Y APLICACIÓN DE TECNOLOGÍAS *BLOCKCHAIN*

La consecución de los Objetivos de Desarrollo Sostenible de la Agenda 2030 implica la promoción y refuerzo en el uso de estas tecnologías. De ahí que sea necesario, tanto en el Informe sobre la Economía Digital del año 2019 (United Nations Conference of Trade and Development 2019, 3) como en el "Informe E-Government" realizado por la ONU en el año 2018, la prioridad de instituir políticas estatales para promover una transformación digital (Department of Economic and Social Affairs of the United Nations Secretariat

2019). El Ministerio de Telecomunicaciones, en su Libro Blanco de la Sociedad de la Información y del Conocimiento establece, como objetivo de Programa de implementación para la digitalización de las empresas hacia la Transformación Digital, el "Mejorar la productividad y la competitividad de las industrias del país, a través de la Transformación Digital" (Ministerio de Telecomunicaciones del Ecuador 2019, 68). Este programa tiene como líneas de acción "facilitar el entorno hacia la transformación digital en las empresas, fomentar el uso de comercio electrónico, promover el emprendimiento e innovación de base tecnológica, y generar acciones para el desarrollo de la Industria TIC" (Ibid.). Aquí se evidencia la importancia que tiene para el gobierno central el impulso de la economía digital en el Ecuador.

El Ministerio de Telecomunicaciones también fomenta el uso de tecnologías emergentes y, entre sus líneas de acción, busca promover el uso de servicios de analítica de grandes volúmenes de datos, impulsar la transformación de los GAD hacia ciudades inteligentes o *smart villages*, e incluso traer nuevas tecnologías disruptivas, por ej. *blockchain*, como mecanismo de validación descentralizada de la información (Ministerio de Telecomunicaciones del Ecuador 2019, 35). Estos objetivos son sin duda alentadores, resta entonces transformar las palabras en acciones y transformarlas en línea con la era digital.

El Plan de la Sociedad de la Información y del Conocimiento (PSIC), para el período 2018-2021 busca propiciar el desarrollo nacional a través de programas y proyectos que permitirán alcanzar objetivos trazados en la Política Nacional de Telecomunicaciones y de la Sociedad de la Información, elaborada para el período 2017-2021 (Ministerio de Telecomunicaciones y de la Sociedad de Información 2017, 10). El PSIC, en su objetivo 4.3.3 busca la implementación de la tecnología de Registros Distribuidos (*Distributed Ledger Technology* o *blockchain*) (Ministerio de Telecomunicaciones y de la Sociedad de Información 2017, 30).

Para posibilitar el objetivo 4.3.3. del PSIC se ha planteado el "*Proyecto 3. Fomentar el uso de la Tecnología de Registros Distribuidos–Distributed Ledger Technology (Blockchain)*" dentro del que se plantea incrementar DLT en el 30% de los procesos registrales en materia mercantil y en el 10% de los procesos registrales en materia de la propiedad; con un punto de partida del 0% de los procesos registrales en materia mercantil y de la propiedad que utilizan DLT (Ministerio de Telecomunicaciones y de la Sociedad de Información 2017, 30).

Entre las acciones que se han planteado para alcanzar los objetivos se establecen: (i) el desarrollo de la herramienta que permitirá asegurar la información de procesos registrales mercantiles y de la propiedad con DLT; y (ii) el fomento del uso de DLT en el Ecuador enfocado a los desarrolladores y usuarios de aplicaciones. Para conseguirlo se precisa de campañas de difusión, webinars, seminarios, concursos, etc. (Ministerio de Telecomunicaciones y de la Sociedad de Información 2017, 31).

Los entes responsables de posibilitar este proyecto son: la Subsecretaría de Fomento de la Sociedad de la Información y Gobierno en Línea y la Dirección Nacional de Registros de Datos Públicos. Las entidades que estarán directamente involucradas son: el Ministerio de Telecomunicaciones y de la Sociedad de la Información, los Registros Mercantiles y Registros de la Propiedad, así como los proveedores y consumidores de información del SINARDAP (Ministerio de Telecomunicaciones y de la Sociedad de Información 2017, 32).

También cabe mencionar la necesidad de involucrar a la academia, a organismos internacionales y organizaciones de la sociedad civil. Estas alianzas permitirán posibilitar la ejecución de proyectos de este tipo. De esta manera se posicionará al país a nivel internacional por los avances en sus sistemas de registro, que a su vez implicarían mejoras en la dinamización de la economía y del sistema gubernamental, así como en el aumento de la confianza de los ciudadanos. Es elemental generar alianzas estratégicas para traer a Ecuador la evolución de la era digital.

De acuerdo con los datos del Instituto Nacional de Estadística Censos (INEC), el gasto total en ACTI (Actividades de Ciencia, Tecnología e Innovación) entre el 2009 al 2014 se incrementó en un 88,92%

(Instituto Nacional de Estadística y Censos 2014, 15). El ACTI está conformado por Investigación y Desarrollo Agregado, Otras Actividades de Ciencia y Tecnología, y Otras actividades de Innovación.

Igualmente, el gasto en Ciencia y Tecnología creció en un 122% entre los años 2009 y 2014. En la misma línea, el gasto en innovación durante el periodo 2012–2014 en un 74,47% representa financiamiento del sector privado y asciende a $3.175,27 millones de dólares (Instituto Nacional de Estadística y Censos 2014, 18).

En el país existe efectivamente inversión en innovación y tecnología. Estos fondos podrían ser asignados en gran parte a la modernización del sistema registral, que a su vez dinamizaría la economía nacional y atraería inversión extranjera, junto con la confianza de un sistema más fiable para sus usuarios.

Gradualmente, el ámbito lo virtual va más allá de la soberanía de los países y elimina fronteras. Es deber de cada Estado, entonces, impulsar el uso de TIC para el desarrollo global de su sociedad, así como velar por el progreso de su economía mediante la creación de oportunidades que se hallan acordes con la realidad de la cuarta revolución industrial y de la era globalizada.

Dentro de esta tendencia se ubica la Política 5.6 del Objetivo 5, Eje 2: Economía al Servicio de la Sociedad del Plan Nacional de Desarrollo 2017-2021 (Secretaría Nacional de Planificación y Desarrollo 2017, 83). Ecuador podría aprovechar las inversiones en ingenio a nivel nacional para desarrollar software y hardware destinados a la modernización del sistema registral con el uso de tecnología *blockchain*. También podría aplicar a fondos extranjeros y beneficiarse del apoyo de gigantes compañías internacionales que buscan invertir en nuevos modelos de registros. Así, seguiría la senda del exitoso caso de Georgia.

La necesidad de implementar mecanismos tecnológicos para operar los sistemas registrales de varios países se volvió mucho más evidente con la llegada de la pandemia por COVID-19, situación en la que ya no es posible hacer trámites físicos. Ahora es emergente contar con medios tecnológicos que permitan desarrollar trámites de administración pública por medios electrónicos. Incluso tras la etapa de COVID-19, la humanidad no estará lista para regresar a sistemas obsoletos; es decir, la implementación de nuevas tecnologías debe ser progresiva. En este contexto, el *blockchain* presenta una gran opción para manejo de sistemas registrales.

Es hora de apostar a la modernización del sistema registral, promover la inversión internacional, repensar las alternativas actuales y crear nuevas coyunturas diferenciadoras que ubiquen a Ecuador como un país pionero, no solo en Latinoamérica, sino a nivel mundial, en el cual se priorice la promoción de los objetivos de desarrollo y Agenda 2030, sobre la base de nuevas tecnologías. No podemos cerrarnos a las oportunidades, debemos crearlas.

CONCLUSIONES

La principal problemática para la unificación, interoperabilidad y modernización del sistema registral ecuatoriano es la falta de claridad y vacíos legales existentes en el actual marco regulatorio registral del país (Orna 2013, 81).

En Ecuador es preciso dar el paso a la modernización del sistema registral con el uso de tecnologías *blockchain* con el que se validen y verifiquen los actos registrales mediante procesos completamente electrónicos, para evitar la destrucción, deterioro y alteración fraudulenta de varios archivos físicos. Se necesita eliminar la brecha tecnológica, así como el avance del país en vías del desarrollo sostenible y consecución de los Objetivos de Desarrollo Sostenible y la Agenda 2030 de Naciones Unidas, a fin de aprovechar oportunidades de inversión nacional e internacional que fomenten la era digital, de forma que se dé respuesta a las nuevas necesidades que resultan palpables en la actual situación mundial presentada con el COVID 19.

ANEXO: DEFINICIONES

Blockchain	Lista creciente de registros que se guardan en bloques criptográficamente seguros, que se vinculan a través de una red de computadoras, también denominada cadena de bloques (Weizsäcker, Eggler y Atarim 2019, 2).
Distributed Ledger Technology (DLT)	Es una base de datos descentralizada, distribuida en varios ordenadores o nodos. Cada nodo mantendrá el libro y, si ocurre algún cambio en los datos, el libro se actualiza de forma independiente en cada nodo. El *blockchain* es una clase de DLT.
Interoperabilidad	Capacidad de los sistemas informáticos de compartir datos y operar coordinadamente que posibilita el intercambio y validación de información entre distintos actores.
Oracles	Sistemas que cumplen la función de adecuar el *blockchain* a la vida real, para proveer la información de estos agentes externos en la ejecución de los contratos inteligentes. (Panfil, Mellon y Robustelli 2019, 2)
Smart contract	Acuerdo legal en forma de algoritmo, que se ejecuta parcial o totalmente de forma automática por medios digitales. (Giuffrida 2018, 760)

BIBLIOGRAFÍA

Ameer, Rosic. 2016. "Smart Contracts: The Blockchain Technology That Will Replace Lawyers". Consultado: noviembre 2019. https://blockgeeks.com/guides/smart-contracts/

Bastardo, Julio. 2018. "Gobierno de Colombia presenta piloto de registro de tierras en Ethereum" Obtenido de Criptonoticias. Acceso: noviembre 2019. https://www.criptonoticias.com/seguridad-bitcoin/certificacion/gobierno-colombia-presenta-piloto-registro-tierras-ethereum/

Benbunan-Fich, R., y Castellanos, A. 2018. «Digitalization of Land Records: From Paper to Blockchain.» *Tristy Ninth International Conference on Information Systems*: 1-9.

Bloch, Daniel. 2018. "Blockchain Powered Land Registry in Ghana with BenBen Big Chain DB". Consultado: noviembre 2019. https://www.bigchaindb.com/usecases/government/benben/

Department of Economic and Social Affairs of the United Nations Secretariat. 2019. «United Nations E-Government Survey.» Consultado: noviembre 2019. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Governmentt%20Survey%202018_FINAL%20for%20web.pdf

DiCamillo, Nathan. 2019. "Inter-American Development Bank to Pilot Land Registries on Blockchain". Consultado: noviembre 2019. https://www.coindesk.com/inter-american-development-bank-to-pilot-land-registries-on-blockchain

Eder, George. 2019 "Digital Transformation: Blockchain and land titles." *OECD*. Consultado: noviembre 2019. http://www.oecd.org/corruption/integrity-forum/academic-papers/Georg%20Eder-%20Blockchain%20-%20Ghana_verified.pdf

Herweijer, C., y J. Swanborough. 2018. "8 ways blockchain can be an environmental game-changer". Consultado: noviembre 2019. https://www.weforum.org/agenda/2018/09/8-ways-blockchain-can-be-an-environmental-game-changer/.

International Business Times UK. 2017. "Bitfury Trumpets Blockchain Land Registry with Republic of Georgia at Harvard and UN". Consultado: noviembre 2019. https://www.ibtimes.co.uk/bitfurytrumpets-Blockchain-land-registryrepublic-georgia-harvard-un-1646616

ITU News. 2018. "Distributed Ledger Technology: ITU to provide guidance to blockchain adopters". Consultado: noviembre 2019. https://news.itu.int/guidance-to-blockchain-adopters/

Kraft, Jess 2019. "Blockchain and Property Rights". Consultado: noviembre 2019. https://www.newamerica.org/future-property-rights/reports/proprightstech-primers/blockchain-and-property-rights/

Lantmäteriet, Telia Company, ChromaWay, y Kairos Future. 2016. "The Land Registry in the blockchain". Consultado: noviembre 2019. http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf

Ledger Insights. 2019. "Inter-American Development Bank contracts ChromaWay for blockchain land registry". Consultado: nov. 2019. https://www.ledgerinsights.com/inter-american-development-bank-idb-blockchain-land-registry-chromway/.

Ledger Insights. 2019. "UAE to store land registry documents on blockchain". Consultado: noviembre 2019. https://www.ledgerinsights.com/uae-land-registry-blockchain/

Muller, Hartmut y Markus Seifert 2019. "Blockchain, a feasible technology for land administration?" Consultado: 22-IV-2019 https://www.fig.net/resources/proceedings/fig_proceedings/fig2019/papers/ts01i/TS01I_seifert_mueller_10110.pdf

Oprunenco, A., y C. Akmeemana. 2018. "Using blockchain to make land registry more reliable in India". Consultado: noviembre 2019. https://www.undp.org/content/undp/en/home/blog/2018/Using-blockchain-to-make-land-registry-more-reliable-in-India.html.

Orna, Nelson 2013. "Folio real informático: sus implicaciones técnico-jurídicas a la luz de la Ley de Registro de 1966." Tesis de grado para la obtención del título de abogado de los tribunales y juzgados de la República. Universidad Internacional del Ecuador.

Panfil, Yuliya; Mellon, Christopher y Robustelli, Tim. 2019. "PropRightsTech Primers: How New and Emerging Technologies Can be Harnessed for Property Rights". New America. Consultado: noviembre 2019 https://www.newamerica.org/future-property-rights/reports/proprightstech-primers/

ProUniversitarios. 2018. "Cómo funciona Blockchain". Consultado: noviembre 2019. https://prouniversitarios.com/como-funciona-blockchain/.

Price, Allison. 2018. "A blockchain based land titling project in the Republic of Georgia". *Revista Innovation*: 72-78.

United Nations Conference of Trade and Development. 2019. *Digital Economy Report*. NY: UNCTAD.

Weizsäcker, F., S. Eggler, y E. Atarim. 2019. "Land registries on a distributed ledger" GIZ. Consultado: noviembre 2019. https://www.giz.de/en/downloads/giz2019-en-distributed-land-registry.pdf.

World Economic Forum. 2019. *Shaping the Future of Technology Governance: Blockchain and Distributed Ledger Technologies*. Consultado: noviembre 2019. https://www.weforum.org/platforms/shaping-the-future-of-technology-governance-blockchain-and-distributed-ledger-technologies.

Legislación

Asamblea Nacional del Ecuador. Ley de Registro. 1966. Publicado en Registro Oficial [= R.O.] no. 150. Quito, 28-X-1966.

CRE. Asamblea Nacional del Ecuador. Constitución de la República. 2008. Publicado en R.O. 449 de 20-X- 2008.

Ley SINARDAP. Asamblea Nacional del Ecuador. Ley del Sistema Nacional de Registro de Datos Públicos. 2010. Publicado en R.O., Suplemento Nº. 162. Quito, 31-III-2010.

COOTAD. Asamblea Nacional del Ecuador. Código Orgánico de Organización Territorial, Autonomía y Descentralización. 2010. Publicado en Registro Oficial. R.O. Suplemento. 303 de 19-X-2010.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. Plan Nacional De Telecomunicaciones y Tecnologías de Información del Ecuador 2016-2021. Quito, 2016.

Ministerio de Telecomunicaciones y de la Sociedad de Información. Políticas Públicas del Sector de las Telecomunicaciones y de la Sociedad de la Información 2017–2021, en R.O. N°. 15. Quito, 15-VI-2017.

Presidencia de la República. Decreto Ejecutivo 372. 2018. Publicado en R.O., Suplemento Nº. 234. Quito, 4-V-2018.

Asamblea Nacional del Ecuador. Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos. 2018. Publicado en R.O., Suplemento Nº. 353. Quito, 23-X-2018.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. Plan de Servicio Universal 2018-2021. Quito, 2018.

Ministerio de Telecomunicaciones y de la Sociedad de Información. Plan de la Sociedad de la Información y de Conocimiento 2018-2021. Quito, 2018.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. Plan Nacional de Gobierno Electrónico 2018-2021. Quito, 2018.

Ministerio de Telecomunicaciones y de la Sociedad de Información. Acuerdo Ministerial Nº. 015-2019. Quito, 18-VII-019.

Dirección Nacional de Registro de Datos Públicos. Resolución Nº. 008-NG-DINARDAP-2020. Quito, 11-IV-2020.

Dirección Nacional de Registro de Datos Públicos. Resolución Nº. 009-NG-DINARDAP-2020. Quito, 30-IV-2020.

PSICOPOLÍTICA, REDES SOCIALES Y LA CUESTIÓN CRIMINAL

PSYCHOPOLITICS, SOCIAL MEDIA AND THE CRIMINAL AFFAIR

PSICOPOLÍTICA, REDES SOCIAIS E A QUESTÃO CRIMINAL

*Adrián Alvaracín**

Recibido: 10/05/2020
Aprobado: 25/06/2020

Resumen

La presente tarea investigativa analiza los procesos de ciminalización desarrollados a través de redes sociales. A partir del estudio de un caso concreto acontecido en el Ecuador, se identifica el proceso de criminalización llevado a cabo en dichas plataformas digitales. La justificación del presente trabajo se encuentra en la necesidad de incorporar nuevas técnicas de control social al estudio del saber criminológico. De esta manera, desde los aportes de la Criminología Crítica, se analizan los efectos y las consecuencias del uso de redes sociales desde la técnica de poder denominada *psicopolítica*, para dar cuenta de la criminalización y la selectividad penal destinada a ciertos grupos vulnerables. En las conclusiones se entregan puntos de apoyo para la construcción de un saber criminológico que incorpore estos nuevos paradigmas del control social, a fin de contener el poder punitivo desplegado contra sectores excluidos.

Palabras clave: Criminología crítica; Control social; Selectividad penal; Psicopolítica; Redes sociales

Summary

This research analyzes the criminalization process developed through social media. From the study of a particular case, the criminalization process carried out on said digital platforms is identified. The rationale of this work is found in the need to incorporate new techniques of social control to the study of criminological knowledge. From the contributions of Critical Criminology, the effects and consequences of the use of social media are analyzed from the power technique called psychopolitics, to account for the criminalization and criminal selectivity for certain target vulnerable groups. The conclusions support the construction of a criminological knowledge that incorporate these new paradigms of social control in order to contain the punitive power deployed against exclusive sectors.

Key words: Critical criminology; Social Control; Criminal Selectivity; Psychopolitics; Social Media

Resumo

A presente pesquisa analisa os processos de criminalização desenvolvidos nas redes sociais. A partir do estudo de um caso concreto ocorrido no Equador, se identifica o processo de criminalização levado a cabo nas plataformas digitais. O presente trabalho se justifica pela necessidade de incorporar novas técnicas de controle social ao estudo do saber criminológico. Desta maneira, con os aportes da Criminologia Crítica, se analisam os efeitos e as consequências do uso das redes sociais com o uso da técnica de poder denominada psicopolítica, para que nos demos conta da criminalização e da seletividade penal destinada a certos grupos vulneráveis. Nas conclusões se entregam pontos de apoio para a construção de um saber criminológico que incorpore estes novos paradigmas de controle social, a fim de conter o poder punitivo destinado aos setores excluídos.

Palavras chave: Criminologia crítica; Controle social; Seletividade penal; Psicopolítica; Redes sociais

* Adrián Alvaracín Jarrín es Especialista Superior y Magíster en Derecho Penal por la Universidad Andina Simón Bolívar. Investigador de Sociología Criminal. Se ha desempeñado como Coordinador de Indultos de la Presidencia de la República y formador de jueces de garantías penitenciarias. Es autor de varios artículos sobre Criminología, Política Criminal y Derecho Constitucional; y ponente en varios congresos de Derecho Penal y Criminología. Correo electrónico: adrianalvaracinj@gmail.com

"Se escribe siempre para dar vida, para
liberar la vida allí donde esté presa,
para trazar líneas de fuga"
Gilles Deleuze

INTRODUCCIÓN

La Criminología en esta investigación es vista desde un enfoque interdisciplinario, cuya función se centra en la parte del control social que conduce a procesos de criminalización, razón por la cual se trata de evidenciar una forma de criminalización de personas excluidas a través de redes sociales. Este fenómeno no ocurre por una simple causalidad, como tampoco bajo un determinismo. Existen técnicas digitales de manipulación de conducta que construyen estos procesos de criminalización, y es importante comprenderlos. Por tanto, se estudia una innovadora técnica desarrollada por la ideología neoliberal denominada psicopolítica, la cual manipula, condiciona y controla la psique de los individuos en una sociedad.

A partir de una triangulación teorética entre biopolítica, psicopolítica (redes sociales) y sistema penal se llega a conclusiones que aportan una mejor comprensión de nuevos fenómenos para el estudio de la cuestión criminal. No se pierde de vista la realidad actual de nuestra región, que constituye una de las más violentas del mundo, donde se invierte la tesis foucaultiana de un soberano que "hace vivir y deja morir", por el de "hace morir y demasiado poco deja vivir" (Codino y Alagia 2019, 478). Es preciso aclarar que, en esta contribución académica, se entiende como redes sociales a un espacio virtual en el cual interactúan millones de personas en el planeta y que genera formas de socialización a través de las así llamadas "aldeas globales" (Aguilar Rodríguez y Said Hung 2012, 192).

La presente investigación teórica se desarrolla bajo el enfoque cualitativo con alcance descriptivo. En ella se usa el método inductivo, que permite "[…] construir teoremas desde situaciones particulares y casos concretos, establecer regularidades, generalizar y pautar conclusiones" (Villabella 2015, 938). Este método recorre el camino de lo particular a lo general, ya que toma en cuenta situaciones específicas, de las cuales se inducen regularidades que se aplican a casos similares. En esta línea, dentro de la metodología aplicada, con un discurso argumentativo se efectúa un análisis de un acontecimiento que, por su particularidad y relevancia en el contexto nacional e internacional, guarda relación fáctica con lo explicado por la teoría. En suma, se efectúa un ejercicio inductivo–deductivo para emitir las conclusiones del presente trabajo. Esta investigación es emergente y exploratoria, porque, dado el fenómeno que se estudia y la escasa bibliografía al respecto, se toma en consideración que el conocimiento sobre el mundo social se construye poco a poco, de modo que se originan nuevas preguntas para transformar el problema original (Downes y Rock 2011, 283).

La pregunta que guía el presente trabajo es la siguiente: ¿cómo las redes sociales inciden en el proceso de criminalización dirigido contra personas excluidas?.

Bajo esta interrogante se desarrollan tres partes de análisis dentro del trabajo investigativo. En la primera parte se introduce el contexto mediante un ejercicio intelectivo: un hecho relevante sucedido en Ecuador que nos permite explorar el cambio de paradigma respecto de las tesis foucaultianas de la sociedad disciplinaria a la tesis líquida de la sociedad psicopolítica. Aquí se aborda el cambio de paradigma que necesariamente debe revisarse desde la crítica criminológica.

En la segunda parte del trabajo, se analiza el fenómeno de la psicopolítica y su funcionalidad para los procesos de criminalización. Este punto desarrolla, conjuntamente con el caso enunciado en la primera parte, las premisas teóricas y el fenómeno en nuestra realidad actual.

En tercer lugar, se advierte sobre la necesidad de incorporar a la crítica criminológica la forma en que las

redes sociales criminalizan a sectores excluidos, para indicar algunos aspectos relevantes que podrían coadyuvar a la contención del poder punitivo.

Por consiguiente, este trabajo pretende evidenciar cómo las redes sociales impulsan procesos de criminalización hacia los extraños; en este caso se analizarán estos procesos en referencia a la migración forzada.

Es un aporte a la comprensión de la teoría del control social y sus efectos sobre los procesos de criminalización.

EL SABER CRIMINOLÓGICO Y LA PSICOPOLÍTICA

Se torna imprescindible tener en cuenta los criterios de inclusión en torno al caso de criminalización de la migración forzada que se presenta a continuación y que sirve de apoyo metodológico para el desarrollo de la investigación. En primer lugar, se evidencian rasgos esenciales de los procesos de criminalización, como el estereotipo de inmigrante inferiorizado, la selectividad penal y la exclusión social. En segundo lugar, se aborda el manejo de las redes sociales destinadas a criminalizar a este grupo vulnerable, pues es notorio su uso para tal efecto y, por último, se escogió tal caso dada la relevancia nacional e internacional que adquirió este acontecimiento.

La noche del sábado 19 de enero de 2019**,** en pleno centro de la ciudad de Ibarra, ubicada al norte de Ecuador, un joven asesina a su pareja tras propinarle varias puñaladas, luego de retenerla por más de una hora y conducirla por las cuadras de la ciudad, mientras amenazaba con apuñalarla. Luego de ese tránsito por las calles de la ciudad, a las 22:40, el joven de 22 años, al encontrarse acorralado por la policía, mata a su pareja ante la mirada enardecida de los espectadores que, con sus cámaras de celular, filmaban lo acontecido (El Universo 2019). Esta noticia incluyó dos componentes que abordarían la mayor cantidad de diarios nacionales, reportajes y redes sociales. La primera, que la mujer tenía cuatro meses de gestación; la segunda, que su conviviente era de origen venezolano, un extranjero (El Telégrafo 2019).

Los diarios más importantes se hacían eco de la transmisión de dicho evento en redes sociales, y determinaban que este se viralizó (El Universo 2019); e incluso en varios *tweets* donde se daba a conocer el asesinato, se usaba el *hashtag* #venezolano (La República 2019).

Nueve días más tarde, el New York Times redactaba un artículo con el título "La xenofobia en Ecuador empuja a migrantes venezolanos a salir del país" (The New York Times 2019). Este artículo relata la experiencia vivida por los ciudadanos venezolanos en la ciudad de Ibarra, el día 20 de enero de 2019, un día después del asesinato ocurrido en las calles de la ciudad. Una turba enardecida pretendía desalojar de sus hogares a toda persona que tuviera la apariencia de venezolano o a quienes confundía con extranjeros latinos.

Cerca de mil personas se tomaron las calles de la ciudad de Ibarra con este propósito. Invasiones de residencias, departamentos, residenciales y pequeños hogares fueron abatidos por los manifestantes. Tumbaron portones y puertas. Con griteríos se referían a los venezolanos, llamados despectivamente de esa manera, y con algunas frases soeces e intimidantes como "sáquenlos para quemarlos". La notica no deja pasar un aspecto importante de toda esta agresión vindicativa: "[…] la filmación se propagó en redes sociales con un detalle incendiario: el asesino era venezolano" (The New York Times 2019).

¿Qué implicaciones traen para la Criminología estos fenómenos que se producen en la realidad mediante el uso de redes sociales? El objeto de estudio del saber criminológico ha devenido en diversos paradigmas durante el transcurso de su desarrollo epistemológico. La criminología aparece con el estudio etiológico de los demonólogos sobre el mal (siglos XII al XVII), para luego pasar al estudio del sistema penal por parte de los iluministas (siglo XVIII). El positivismo biologista regresó a la etiología, pero esta vez fundada en el colonialismo que inferiorizaba a los involucionados (siglo XIX) (Zaffaroni 2010, 11).

Hasta la intervención de la sociología norteamerciana en el campo criminológico**,** a mediados de la primera mitad del siglo XX, el estudio del delito y del delincuente giraban en torno al análisis positivista con base científica que observaba a los fenómenos sociales de forma neutral y objetiva, cuya herramienta era la estadística; pero que siempre recaía sobre el sujeto delincuente como producto patológico, de manera que se convertía en una ciencia causal–explicativa del delito (Zaffaroni 2012, 6–8). Esta etiología del delito y el delincuente, cuyas raíces se encuentran en el positivismo biológico–racista, arrastraba problemas irresolubles en cuanto a la prevención del delito y a la víctima, pues tal enfoque se centraba en explicar qué incentivaba a una persona a cometer un delito, como la forma de su cráneo para Lombroso o la inclinación delictual por el nivel de melanina en la piel, aunque no indagaba las causas subyacentes del hecho ilícito y mucho menos se ocupaba de examinar los procesos de criminalización impuestos desde el poder.

Entonces, a mediados del siglo XX, se produjo una disrupción en el saber criminológico con investigaciones que provenían del interaccionismo simbólico y que asestó un golpe letal al sistema penal proveniente de la teoría del etiquetamiento o *labeling approach* de Howard Becker (Becker 2014). En efecto, este demostraba la ínsita selectividad del sistema penal dirigida hacia los más desfavorecidos; en otras palabras, con la teoría del etiquetamiento –también llamada "de la rotulación"– se descubría que "[…] la desviación es provocada, porque hay una empresa moral que hace las reglas, y porque no se estudia a los fabricantes de las reglas (empresarios morales) sino a las personas a quienes se les aplica la etiqueta que las deja afuera (*outsiders*)" (Zaffaroni 2013, 150). Esta teoría demolía cualquier intento de legitimación del sistema penal como un ente que opera de forma igualitaria ante el delito, dado que las agencias policiales ejercen el poder punitivo de manera selectiva y arbitraria. Esta teoría explicaba dicha rotulación y ayuda a rectificar teorías más complejas. De igual manera, la nueva criminología de Taylor, Walton y Young, en la primera Escuela de Chicago, redirigía el foco de la explicación del delito ya no hacia una etiología individual del sujeto sino hacia un estudio más profundo de las causas con la teoría de las subculturas[1], cargada de una etiología de la pobreza.

Bajo estos antecedentes se produjo un giro copernicano en torno de la cuestión criminal, pues fue el momento de la aparición de la Criminología Crítica o de la "reacción social". Así, se propiciaron dos vertientes de esta criminología: la radical y la liberal. Por un lado, la criminología crítica hacía un enjuiciamiento radical al sistema penal y, por tanto, al poder en general, que llegaba a distintos niveles del poder social. Mientras tanto, la criminología crítica liberal realizaba una crítica a los sistemas penales sin llegar al poder general, es decir que se mantenía dentro de los límites de las agencias del sistema penal (Zaffaroni 2013, 148–54). Ambas dejaban de lado al delincuente patógeno del positivismo ciminológico como sujeto de estudio, puesto que iban más allá de la comprensión de la criminalidad en las culturas subordinadas.

Dicha criminología miraba como objeto de estudio al control social, e incorporaba en su campo de análisis al sistema penal y al poder punitivo. La Criminología Crítica en versión latinoamericana llamaba a comprender el fenómeno criminal y los procesos de criminalización desde una visión social y política. Así, "la atención sobre los procesos de criminalización, antes que en la vida del 'delincuente' han sido una fuente rica para poner en evidencia los procesos de selectividad, que hacen que utilicemos preferentemente los recursos violentos del Estado (no otra cosa es la pena) sobre sectores ya de por sí desfavorecidos, vulnerables, simplemente pobres" (Pardo Angles 2012, 13). Este nuevo enfoque provocó que "el objeto de la Criminología Crítica fuera el estudio del control social, formal o informal" (Aniyar de Castro 2010, 58), y asumió el rol de una criminología que controla los controles.

La vertiente radical de esta Criminología basaba sus premisas, en parte, en los estudios antropológicos de Michel Foucault, el cual estableció el término

1 Al respecto ver: Taylor, Ian, Walton, Paúl y Young Jock. 1997. *La nueva criminología. Contribución a una teoría social de la conducta desviada*. Buenos Aires: Amorrortu.

Biopolítica para describir la sociedad disciplinaria y vigilante, que se explicaba a través de la estructura ideada por Jeremy Bentham: el panóptico. Para Foucault, la sociedad del panóptico benthamiano controla los cuerpos a través del disciplinamiento y el castigo; así, el control social se vuelve contra el cuerpo del sujeto, donde "el poder se ejerce por entero, de acuerdo con una figura jerárquica continua, en el que cada individuo está constantemente localizado, examinado y distribuido […], todo esto constituye un modelo compacto del dispositivo disciplinario" (Foucault 2002, 229). Para ilustrar la tesis antedicha, imaginemos una cárcel, una fábrica o un manicomio; en todas estas instituciones se normaliza al individuo mediante el deber guiado por la moral o la biopolítica.

En la Criminología Crítica, la incidencia del pensamiento de Foucault y su biopolítica es evidente, debido a que ayudó a comprender que los dispositivos de poder para disciplinar –entre ellos, el sistema penal– no solamente son funcionales para mantener a cierta población recluida, sino que actúan como poder positivo configurador de la vigilancia total. En otras palabras, la importancia de los sistemas penales no radica en el mero poder de encerrar a un grupo de la población, sino que su poder juega un rol políticamente relevante: la vigilancia de todos los que estamos sueltos (Zaffaroni 2013, 70).

A su vez, la teoría elaborada por Foucault pertenece a una sociedad distinta a la que se desarrolla en este momento de poder planetario. Si se analiza cualquier espacio de interacción social, encontramos que en él se halla un aparato que deviene esencial: el *Smartphone*. El celular invade el espacio social e interactivo de nuestra sociedad, y se ha convertido en un aparato necesario para cualquier individuo. Mediante este aparato, las personas construyen vidas paralelas digitales, donde aplicaciones como *Whatsapp*, *Facebook* o *Twitter* se presentan como no–lugares de una realidad virtual que ocasiona la pérdida de la percepción del mundo real. Es claro que el aparente mundo real diseñado en el ámbito virtual no guarda similitud con la realidad en sí, sino que constituye tan solo un fragmento de una realidad, acomodada para usar la libertad como instrumento de dominación y control (Alvaracín 2019, 20).

La actual realidad se explica desde una modernidad líquida[2], donde lo sólido de la sociedad disciplinaria que regía mediante el deber, las instituciones totales, las prohibiciones y la vigilancia, necesitan de una fluidez que permita desplegar todo el poder neoliberal en un mundo globalizado (Alvaracín 2019, 49). En lugar de condicionar con el deber, se transita ahora a la sociedad del "poderlo–todo" (Han B. C. 2014, 124), donde el foco de interés se pone en la explotación de las emociones. Cada *like*, *tweet* o reacción cuentan como elementos para algoritmos que llegan a leer y evaluar nuestros pensamientos conscientes e inconscientes. "Hoy, el globo entero se desarrolla en pos de formar un gran panóptico. […] Google y las redes sociales, que se presentan como espacios de la libertad, adoptan formas panópticas. […] Cada uno se entrega *voluntariamente* a la mirada panóptica. A sabiendas, *contribuimos* al panóptico digital, en la medida en que nos desnudamos y exponemos" (Han 2013, 94–5). Ahí está la dialéctica de la libertad que se transforma en control.

Si echamos mano de la metáfora del topo y la serpiente desarrollada por Byung–Chul Han, se puede comprender en mejor medida el paso de lo sólido a lo líquido, de la sociedad biopolítica a la sociedad psicopolítica. El topo representa lo sólido, el poder disciplinario, es el sujeto sometido. La serpiente representa la fluidez de lo líquido, es un proyecto, en la medida en que genera espacio a partir de su movimiento. El topo, como es conocido, se mueve en espacios reducidos y cerrados en los cuales se desenvuelve, y representa al sujeto disciplinado. La serpiente, por otro lado, no tiene un límite espacial, sino que genera su propio espacio de movimiento. La serpiente es un empresario, con sus deudas y sus culpas, y simboliza el régimen neoliberal. En este entramado neoliberal, cada sujeto se convierte en su propio amo y esclavo, explotador y explotado a la vez, al instituir una rivalidad interminable entre los sujetos a modo de competición (Han 2016, 117). La aplicación UBER es una clara muestra de la disolución de la dialéctica hegeliana del amo y esclavo,

2 Al respecto véase: Zygmunt, Bauman. 2005. *Modernidad líquida*. Buenos Aires: Grafinor.

en vista de que cada sujeto, mediante esta aplicación, sumado a un automóvil, puede ser su propio jefe y empleado a la vez (Alvaracín 2019, 20). Fenomenos como este convierten al neoliberalismo en una forma de dominación inteligente.

Todo este poder que fluye se despliega a través de la psicopolítica, que es una "[…] técnica de dominación que estabiliza y reproduce el sistema dominante por medio de una programación y control psicológicos" (Han 2016, 117). Es la concepción de un nuevo poder, además de una nueva forma de dominación neoliberal, que se produce por los medios y plataformas tecnológicas, por medio de la cual, el poder "atraviesa, produce cosas, induce placer, forma saber, produce discursos" (Foucault 1979, 182), y que hoy es esencialmente seductor (Alvaracín 2019, 21). A esta técnica se suman herramientas como el *Big Data*, que permite pronosticar el comportamiento humano a través de un cúmulo de datos que son fácilmente apropiables por parte de quienes diseñan políticas públicas, entre ellas, la política criminal. La sociedad capitalista descrita por Foucault llena de coacciones disciplinarias, cede ante el "capitalismo del me gusta"[3].

Todo funciona dentro de un "apóptico" que segrega y excluye. Se trata de una "construcción basada en una «óptica excluyente» que identifica como indeseadas y excluye por tales a las personas enemigas del sistema o no aptas para él" (Han 2018, 29). Dentro de este apóptico se generan depresivos y fracasados que no logran alcanzar el éxito vendido por la publicidad en redes sociales; como consecuencia, surge en cada sujeto el miedo por sí mismo que provoca en la búsqueda de un enemigo que le provea identidad. Se observa**,** en muchos lugares, la frustración de quienes piensan que todo objeto del deseo que se publicita en redes sociales es el ideal al que deben acceder, para luego caer mortificados ante la impotencia de una realidad que se lo impide. En este punto es donde surge el sujeto del rendimiento que se autoexplota hasta obtener el éxito fundado en la publicidad. Es así que "el sujeto del rendimiento se explota hasta quedar abrasado (quemado) (*burnout*)" (Han 2014, 21); ante esa frustración, el sujeto que se cree libre, trata de conducir su violencia contra el exterior y, al seguir esta dinámica, encuentra enemigos en el afuera de su mundo virtual, sean estos "inmigrantes, refugiados o grupos sociales ´inferiores', declarados así debido a la raza, la etnia, la sexualidad o la religión" (Santos 2018, 29). Ante esta violencia contra sí mismo, se abre la opción de fabricar enemigos de la sociedad, que se vuelven funcionales al ejercicio del poder punitivo; enemigos que, dicho sea de paso, calman las frustraciones y el miedo del yo. Se excluye al ajeno, diferente, que causa conmoción y reacción desfavorable en el mundo en red.

Ante un control social de esta magnitud, la Criminología debe evaluar las consecuencias que produce ese control social en los procesos de criminalización y en la selectividad o procesos selectivos dentro de la cuestión criminal, de modo que se torna fundamental estudiar el control social actual que ha transmutado de la disciplina y vigilancia biopolítica hacia un control social sutil mediante la psicopolítica, cuyo efecto más claro es la exclusión.

LOS PROCESOS DE CRIMINALIZACIÓN SECUNDARIA A TRAVÉS DE LA PSICOPOLÍTICA

La realidad descrita en párrafos anteriores se comprende en nuestra sociedad ecuatoriana a grandes rasgos, como se aprecia en el caso descrito al principio de este trabajo. Este fenómeno no es casual, pues nuestro país se encuentra en una de las regiones más inequitativas del mundo (Banco Mundial, s. f.), y se localiza entre las más peligrosas del planeta[4].En estas sociedades, al igual que en muchas otras del Sur

3 Al respecto véase: Han, Byung–Chul. 2016. *Psicopolítica. Neoliberalismo y nuevas técnicas de poder*. Barcelona: Herder. En esta obra, el autor surcoreano desarrolla la diferencia sustancial entre el neoliberalismo actual y el capitalismo del siglo XIX.

4 Revisar el índice de homicidios en la región en: Instituto Igarapé. 2017. https://igarape.org.br/venas–abiertas–homicidios–en–america–latina/. Acceso el 16–IV–2020.

global, comparecen relaciones de poder entre incluidos–excluidos; pues la actual polarización de riqueza dentro del "totalitarismo financiero" hace que "pierda importancia la relación entre explotador y explotado (dialéctica propia del capitalismo productivo: no hay explotador sin explotado)" (Zaffaroni y Dias dos Santos 2019, 51). Esta nueva relación incluido–excluido (que no es dialéctica como tal, porque el incluido no necesita del excluido), se lleva a cabo, como vimos *ut supra*, mediante las plataformas digitales dentro de la técnica psicopolítica que excluye y segrega, de manera que invisibiliza la dominación y el control. Acerca de este panorama, es preciso traer a colación el caso acontecido en la ciudad de Ibarra–Ecuador, en razón de que este entrega insumos valiosos para comprender el fenómeno que se estudia, por reflejar aspectos claros sobre la criminalidad y el control social de la psicopolítica, de manera concisa con la migración forzada, como se explica a continuación.

En el relato se puede apreciar que, tras un hecho delictivo aislado, se creó un potenciador imparable del miedo y de la xenofobia y, por tanto, del enemigo a eliminar. Antes de empezar con el análisis de este conflicto social, se debe tener presente que internet y las redes sociales pueden ser un instrumento muy potente de emancipación. No obstante, nuestras sociedades plagadas de violencia e inequidad pueden revertir fácilmente esa realidad transformadora a la que pueden llevarnos las plataformas digitales, dado que el efecto negativo de las redes sociales recae sobre los individuos más débiles física y psicológicamente, e incrementa la probabilidad de actos violentos (Beristain y Neuman 2004, 66). Este mecanismo socio–tecnológico monta un escenario que se debe prevenir para evitar que el poder punitivo se desborde.

En este contexto, es necesario señalar que, para Lola Aniyar de Castro, existen cuatro tipos de sistemas penales, entre los que se encuentra el "sistema penal del otro" (Aniyar de Castro 2010, 97). La diferenciación de este con los demás sistemas penales es esencial, debido a que este parte de la creación del enemigo para sustentar su operatividad real. Sobre la base de un enemigo identificado, previamente esteriotipado e inferiorizado, se encauza el poder punitivo contra aquél, en un proceso de criminalización secundaria, que consiste en "la acción punitiva ejercida sobre personas concretas, [y] es el acto del poder punitivo por el que este recae sobre una persona como autora de un delito" (Zaffaroni, Alagia, y Slokar 2008, 12).

Antes de que la sociedad imagine un enemigo que canaliza venganza pública, es necesario que el miedo se imponga. Este efecto, lo logran los poderes a través de emergencias que se desarrollan de acuerdo a los eventos de la dinámica social. Para llevar a cabo este proceso de criminalización, la sociedad debe operar automáticamente aquella primera categoría para la identificación de enemigos. En primer lugar, crea estereotipos sobre la base de prejuicios (racistas, xenófobos, clasistas, sexistas) que configuran poco a poco, en el imaginario colectivo, la fisonomía de un delincuente con rostro e incluso con nacionalidad. Este delincuente es potenciado por los medios de comunicación que construyen esa figura delictiva; y, de tal forma, la realidad virtual, creada con la técnica psicopolítica, se traslada a la realidad en forma de poder punitivo selectivo.

A este proceso se suma que el poder punitivo actúa como ente simbólico a través del derecho penal que, en el imaginario colectivo, opera como solución de conflictos. Dicha interpretación constituye una falacia que trae graves consecuencias en el plano de la democracia y de los derechos humanos. Estas condicionantes convierten al sistema penal en un aparato de reproducción de la desigualdad y de la exclusión social (Hulsman y Bernat de Celis 1984, 62).

En esta línea, el castigo se muestra necesario ante los enemigos en la emergencia. La fe ciega en la omnipotencia del castigo es otro ingrediente necesario para que los mensajes de las redes sociales calen hondo en el imaginario colectivo. La idea de que el castigo civiliza fue desmontada por Marcel Mauss en 1925. Así, derrumbaba la idea de que la agresión es inmanente al hombre y a la mujer, de manera que debe imponerse el monopolio de la violencia estatal para solucionar conflictos (Codino y Alagia 2019, 446) y la población insiste en depositar su confianza en la agresión vindicativa. Así, la visión del inmigrante como enemigo por ser un potencial delincuente se funda en la emergencia producida a través de redes sociales, que se ve

como merecedor del castigo respectivo, tal como lo demuestran las brutales acciones emprendidas contra sectores inmigrantes en la ciudad de Ibarra.

Luego, está el paso a la inferiorización del autor del hecho y de aquellos que pertenecen a su origen o se asemejan a su fisonomía. La inferiorización que permite la venganza pública y el castigo proviene de la migración forzada desde una perspectiva de la aporofobia –el inmigrante excluido que molesta–. Esta realidad se explica desde la técnica psicopolítica que, en la sociedad del "poderlo–todo", inventa enemigos para reducir la mortificante autoexplotación que conlleva el rendimiento. Por consiguiente, esa ocupación mortificante del sujeto consigo mismo deviene en la creación de enemigos imaginarios donde se exterioriza la violencia interna. La xenofobia de hoy en día remite a esa instancia imaginaria (Han 2014, 76). La migración forzada es una oportunidad para criminalizar al Otro. La inferiorización a base de prejuicios xenófobos se cumple en el proceso de criminalización secundaria a través de redes sociales.

La siguiente categoría dentro del proceso de criminalización secundaria se funda en la selectividad del sistema penal. El día en que la *notitia criminis* se hizo viral en redes sociales se produjeron otros hechos con mayor contenido lesivo para la sociedad ecuatoriana en su conjunto y que no generaron igual impacto en redes sociales. Por ejemplo, en el 2019 se registró la pobreza más alta de los últimos cinco años (Cobos 2019), así como más de doscientas mil personas a abril de 2019 perdieron su empleo adecuado (El Comercio 2019) y, los datos de UNICEF revelaban ese año que uno de cada cuatro niños en Ecuador sufrían de desnutrición crónica, situación que era aún más grave para los niños indígenas, entre quienes uno de cada dos la padecían (UNICEF, s. f.). El día en que las redes sociales fijaron su atención en develar el pasaporte del asesino más que fijarse en la muerte por razones misóginas o por relaciones de poder derivadas en un femicidio, se presentaban situaciones que frustraban proyectos existenciales de miles de adultos y niños, las cuales, en muchas ocasiones, derivan en actos violentos. Así, debe admitirse que el ejercicio de poder del sistema penal "se orienta a la contención de grupos bien determinados y no a la 'represión del delito'" (Zaffaroni 2005, 44). De esta manera se demuestra que la privación de libertad de inmigrantes corresponde más a un "encarcelamiento de diferenciación" que a un "encarcelamiento de seguridad" (Wacquant 2004, 113–6).

La selectividad del poder punitivo es una característica estructural e inmanente al mismo (Kropotkin 2001, 10). La selectividad es estructural, por cuanto se dirige contra determinados grupos de la población bien identificados a través de procesos de ciminalización, donde los medios de comunicación incitan a las agencias ejecutivas del poder punitivo –policía– a actuar conforme a los estereotipos que se proyectan en la pantalla. Esta realidad se potencia con la llegada de las redes sociales, que responden a la opinión pública previamente manipulada –el enemigo inferiorizado–. Entonces, los procesos de criminalización se sostienen con la manipulación digital de conducta mediante la técnica psicopolítica como parte del poder neoliberal, donde las redes sociales juegan un rol fundamental en el objetivo de montar un aparato represivo violento para contener a los excluidos de la sociedad. Así se conformó un aparato represivo contra la población migrante latina en nuestro territorio.

UN NUEVO ELEMENTO PARA LA CRÍTICA CRIMINOLÓGICA

La dependencia entre control social y delito es inequívoca. El mantenimiento del primero depende de la funcionalidad del segundo y viceversa. De esta forma, los procesos de criminalización se diseñan en una mixtura que permite mantener vigente al control social y al delito, para mantener a la población excluida controlada. En otras palabras, el poder punitivo se convierte en la punta de lanza para controlar a los sectores excluidos de la población, conforme los procesos de criminalización que se analizó para la migración forzada. Alessandro Baratta reclamaba una ciencia que no se limite a la tecnócrata tarea de analizar

la desigualdad tan solo desde el ámbito normativo –la ley penal–, sino que permita la comprensión del funcionamiento y de la operatividad real del sistema penal en una sociedad tardo–capitalista. Ahora que se da una sociedad de incluidos–excluidos, que utiliza técnicas sofisticadas como la psicopolítica, donde surge una sociedad de la transparencia, el giro parece ser significativo.

No se pueden obviar los procesos de criminalización, pues hacerlo implicaría el retorno a viejos paradigmas positivistas, cuyas consecuencias derivan en la comprensión del delito bajo posiciones racistas o xenófobas. Como se evidencia, la criminalidad resulta de procesos sociales mucho más complejos. El estudio debe enfocarse desde una perspectiva interdisciplinaria, donde se analicen no solo a quienes cumplen con el rol introyectado por la etiqueta impuesta desde las esferas del poder y reproducido por las redes sociales, sino también a quienes fabrican esa etiqueta. En este desarrollo juega un papel importante la reacción de la sociedad y de las agencias del sistema penal –tribunales, policía– ante el delito viralizado en redes sociales. Una justicia penal que se acerque al ideal del Estado de Derecho es una que contenga al poder punitivo dentro de los límites razonables.

La Criminología Crítica, al observar estos nuevos fenómenos en los procesos de criminalización, debe emprender la tarea de incorporarlos y estudiarlos de manera interdisciplinaria, porque la función de una criminología de los controles es tratar al delito desde una perspectiva interdisciplinaria. Esta es la necesidad de comprender e integrar al control social represivo en todas las otras formas de control social, de modo que se contemple el contexto del ejercicio de ese poder.

Así la cuestión, se hace patente la desintegración de la otredad; pues filmar con cámaras de celulares un acontecimiento de homicidio doloso, como en el caso estudiado, demuestra la pérdida total del reconocimiento respetuoso que cada quien hace del otro. Además, estos actos impiden conformar un diálogo simétrico conforme el diseño de una sociedad incluyente y solidaria. El poder punitivo se presenta inescindible de estos procesos de exclusión. El viraje hacia procesos más humanos fundados en la solidaridad pasa por un programa racional de minimalismo penal que acuda, en conjunto con otros saberes, a la transformación social. Hay que dar el paso del castigo al respeto de los derechos humanos fundamentales y a la sociedad que incluya las voces de los sectores excluidos, que por ahora son reprimidos y contenidos por procesos de criminalización que los etiqueta como el mal a eliminar.

La Criminología del siglo XXI debe ofrecer puntos de apoyo al Derecho Penal, para que "su contenido sirva programáticamente a reducir la violencia institucional vindicativa y a prevenir la pulsión genocida que alimenta toda ley penal: destruir la vida para salvar la vida" (Codino y Alagia 2019, 379). Esta propuesta parte de comprender a la Criminología como la ciencia del ser, que aporta los insumos de la realidad a la construcción del Derecho Penal como un deber ser que llegaría a ser si y solo si sus leyes se fundamentan en datos de la realidad.

Por tal motivo, resulta indispensable conformar estrategias que contrarresten los efectos de la psicopolítica en los procesos de criminalización. En consecuencia, es momento de fijarse objetivos que impidan el sometimiento de nuestras sociedades ante renovadas técnicas neoliberales de exclusión. Se puede empezar con introducir un discurso diferente y no violento (Zaffaroni 2005, 181) que neutralice la propaganda vindicativa expuesta en redes sociales.

En esa línea, es relevante construir una hermenéutica diatópica, como la denomina Boaventura de Sousa Santos, que consiste en romper la imposición hegemónica de un único mensaje o saber, para dar paso a la construcción emancipadora a través de diversos saberes, donde la luz de experiencias ocultas de los sectores excluidos crean una racionalidad comprensiva y liberadora. Este proceso comprende que la globalización no es más que un localismo globalizado, donde una cultura se traga a las demás (Santos 2003, 32), y así sucede también con los mensajes introducidos en redes sociales. Esta estrategia de traducción de saberes no se impone, sino que se propone dentro de un marco de respeto donde se origine un diálogo simétrico con los sectores afectados por procesos de criminalización.

La senda de la crítica criminológica no debe apartarse de estas manifestaciones del control social, pues siempre ha sido claro que controlar el delito es controlar a la sociedad. Por ende, en una sociedad donde las redes sociales inciden en los procesos de criminalización, se torna una tarea inaplazable para la Criminología Latinoamericana incorporar a su estudio las nuevas técnicas de control social, sin perder de vista todo el bagaje histórico y potencial de los siglos anteriores, para desentrañar el verdadero efecto que produce en nuestros pueblos la concepción de estos nuevos paradigmas de control y dominación.

CONCLUSIONES Y RECOMENDACIONES

La sociedad disciplinada del panóptico benthamiano**,** que usaba el deber como imperativo de dominio, pasa ahora a una versión más sutil de dominación**,** que se genera a través de la psicopolítica como técnica neoliberal, la cual trae herramientas funcionales a la exclusión, como son las redes sociales.

En la cuestión criminal, esta realidad ofrece algunos fenómenos que se despliegan en los procesos de criminalización dentro de un sistema penal del Otro. A través del mundo virtual, en redes sociales, se crean enemigos y se selecciona a las personas contra quienes se dirige el poder punitivo; pero también controlamos y se nos controla mediante las plataformas digitales. El poder configurador de vigilancia que forma la psicopolítica con el poder punitivo se potencia más allá de la sociedad disciplinaria.

Se comprende que los procesos de criminalización se abordan desde el estudio del control social represivo, pero siempre inscritos en un control social más amplio. El poder punitivo es usado como instrumento de exclusión contra la población desfavorecida. Se genera un miedo, una emergencia –como la migración forzada–, luego se identifica al enemigo mediante redes sociales que implantan la idea vindicativa con el objeto de lograrlo, se usa cualquier noticia con componentes de violencia elevados–, se inferioriza a toda la población –los parecidos al individuo del hecho delictivo por estereotipo y/o nacionalidad–; para, al final, criminalizar a todo sujeto que cargue con el estigma prefabricado por la psicopolítica, cuya pantalla son las redes sociales.

Recomendaciones

Se recomienda analizar, mediante estudios teóricos y empíricos, otras manifestaciones de la psicopolítica en la cuestión criminal, a fin de evaluar sus alcances y efectos. Luego, a partir de ese bagaje de estudios teóricos y empíricos, se procedería a conformar un diálogo con los excluidos, como herramienta esencial para la generación de contra–mensajes, donde su voz entregue saberes ocultados por los mensajes vindicativos en redes sociales. Este aporte sería el eje programático para la construcción de una Criminología que visualice la realidad de los sectores desfavorecidos y que sea la fuente real para la construcción de una crítica criminológica renovada, en favor del respeto a la dignidad de toda la población.

BIBLIOGRAFÍA

Aguilar Rodríguez, Daniel, y Elías Said Hung. 2012. "Identidad y subjetividad en las redes sociales virtuales: caso Facebook". Recuperado en: https://www.redalyc.org/pdf/853/85316155013.pdf

Alvaracín, Adrián Alejandro. 2019. "Psicopolítica en el sistema penal: en busca de una política criminal racional". Quito: Universidad Andina Simón Bolívar.

Aniyar de Castro, Lola. 2010. *Criminología de los Derechos Humanos. Criminología Axiológica como Política Criminal*. Buenos Aires: Editores del Puerto.

Banco Mundial. s. f. "Índice de Gini–Ecuador". Recuperado en: https://datos.bancomundial.org/indicador/SI.POV.GINI?locations=EC&view=map%20Este%20%C3%ADndice%20muestra%20que%20los

Bauman, Zygmunt. 2005. *Modernidad Líquida*. Buenos Aires: Grafinor.

Becker, Howard. 2014. *Outsiders: hacia una sociología de la desviación*. Buenos Aires: Siglo Veintiuno.

Beristain, Antonio, y Elias Neuman. 2004. *Criminología y Dignidad Humana: diálogos*. Buenos Aires: Universidad

Cobos, Eduardo. 2019. "La pobreza más alta de los últimos cinco años". En: *Gestión Digital*. Recuperado en: https://www.revistagestion.ec/sociedad–analisis/la–pobreza–mas–alta–de–los–ultimos–cinco–anos

Codino, Rodrigo, y Alejandro Alagia. 2019. *La descolonización de la criminología en América*. Buenos Aires: EDIAR.

Downes, David, y Paúl Rock. 2011. *Sociología de la desviación*. Barcelona: Gedisa.

El Comercio. 2019. "261767 personas perdieron su empleo adecuado en el último año, según INEC". Recuperado en: https://www.elcomercio.com/actualidad/inec–desempleo–subempleo–ecuador–marzo.html

El Telégrafo. 2019. "Ministra del Interior condena asesinato de joven en Ibarra". Recuperado en: https://www.eltelegrafo.com.ec/noticias/judicial/12/ministra–interior–condena–asesinato–joven–ibarra

El Universo. 2019. "Fallece mujer embarazada, tras recibir varias puñaladas de su pareja; ocurrió en Ibarra". Recuperado en: https://www.eluniverso.com/noticias/2019/01/20/nota/7147622/hombre–asesino–su–pareja–que–tenia–cuatro–meses–embarazo–ocurrio

Foucault, Michel. 1979. *Microfísica del poder*. Madrid: Las ediciones de la piqueta.

_____. 2002. *Vigilar y castigar: Nacimiento de la prisión*. Buenos Aires: Siglo Veintiuno.

Han, Byung Chul. 2018. *La expulsión de lo distinto. Percepción y comunicación en la sociedad actual*. Barcelona: Herder.

_____. 2016. *Psicopolítica. Neoliberalismo y nuevas técnicas de poder*. Barcelona: Herder.

_____. 2014. *Topología de la violencia*. Barcelona: Herder.

_____. 2013. *La sociedad de la transparencia*. Barcelona: Herder.

Hulsman, Louk, y Jacqueline Bernat de Celis. 1984. *Sistema penal y seguridad ciudadana: hacia una alternativa*. Barcelona: Ariel.

Instituto Igarapé. 2017. "Venas abiertas: homicidios en América Latina". Recuperado en: https://igarape.org.br/venas–abiertas–homicidios–en–america–latina/

Kropotkin, Pedro. 2001. "Las prisiones". Recuperado en: https://www.inventati.org/ingobernables/textos/anarquistas/kropotkin_lasprisiones.pdf

La República. 2019. "Mujer es apuñalada en pleno centro de Ibarra por hombre que la tomó como rehén". Recuperado en: https://www.larepublica.ec/blog/sociedad/2019/01/19/presunto–venezolano–toma–como–rehen–mujer–ibarra–apunala/

Pardo Angles, Renato. 2012. *Criminología. Un enfoque crítico actual*. Cochabamba: J.V. Editora.

Santos, Boaventura de Sousa. 2018. *Izquierdas del mundo, ¡uníos!* Barcelona: Ed. Icaria.

_____. 2003. *Crítica de la razón indolente. Contra el desperdicio de la experiencia*. España: Desclée de Brouwer.

Taylor, Ian, Paul Walton, y Jock Young. 1997. *La nueva criminología. Contribución a una teoría social de la conducta desviada*. Buenos Aires: Líquida.

The New York Times. 2019. "La xenofobia en Ecuador empuja a migrantes venezolanos a salir del país". recuperado en: https://www.nytimes.com/es/2019/01/28/espanol/ecuador–ibarra–venezolanos.html

UNICEF. s. f. "Desnutrición". recuperado en: https://www.unicef.org/ecuador/desnutrici%C3%B3n

Villabella, Carlos Manuel. 2015. "Los métodos en la investigación jurídica. Algunas precisiones". Recuperado en: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3983/46.pdf

Wacquant, Loïc. 2004. *Las cárceles de la miseria*. Buenos Aires: Manantial.

Zaffaroni, Eugenio. 2013. *La cuestión criminal*. Bogotá: Ibáñez.

_____. 2012. *Criminología. Aproximación desde un margen*. Buenos Aires: Librex.

_____. 2010. "Masacre: larvas y semillas. Lineamientos para un replanteo criminológico". En: *Instituto de Investigaciones*.

_____. 2005. *En busca de las penas perdidas. Deslegitimación y dogmática jurídico–penal*. Buenos Aires: EDIAR.

Zaffaroni, Eugenio, Alejandro Alagia, y Alejandro Slokar. 2008. *Manual de Derecho Penal*. Buenos Aires: EDIAR.

Zaffaroni, Eugenio, y Ílison Dias dos Santos. 2019. *La nueva crítica criminológica. Criminología en tiempos de totalitarismo financiero*. Quito: El Siglo.

CIMIENTOS DE LA LIBERTAD DE EXPRESIÓN EN INTERNET
Limitaciones desde la esfera civil y penal

THE FOUNDATIONS OF FREEDOM OF EXPRESSION ON THE INTERNET.
Limitations from the civil and criminal sphere

CIMENTOS DA LIBERDADE DE EXPRESSÃO NA INTERNET.
Limitações desde a esfera civil e penal

Vicente Vásconez y Edison López***

Recibido: 30/04/2020
Aprobado: 04/06/2020

Resumen

La presente investigación, en primer lugar, pone sobre la escena el reconocimiento nacional e internacional que recibe el derecho a la libertad de expresión y más importante todavía, resalta que el fundamento de su existencia tiene un estrecho vínculo con la idea de una democracia deliberativa. Finalmente, en esta investigación se logra identificar los límites y consecuencias jurídicas que recaen sobre el ejercicio abusivo del derecho a la libertad de expresión, tanto desde la esfera del Derecho civil, como también a la luz del Derecho penal.

Palabras clave: Democracia; Honra; Indemnización; Libertad de expresión; Poder punitivo

Summary

This work, in the first place, puts on the scene the national and international recognition of the right to freedom of expression, and more importantly, highlights that the bedrock of its existence has a close link with the idea of a deliberative democracy. Finally, in this investigation it is possible to identify the limits and legal consequences that fall on the abusive exercise of the right to freedom of expression, both from the sphere of civil law and criminal law.

Key words: Democracy; Honor; Compensation; Freedom of expression; Punitive power

Resumo

A presente pesquisa, em primeiro lugar, põe no centro do debate o reconhecimento nacional e internacional do direito à liberdade de expressão e destaca que o fundamento de sua existência possui um estreito vínculo com a ideia de uma democracia deliberativa. Finalmente, nesta pesquisa se permite identificar os limites e consequências jurídicas que recaem sobre o exercício abusivo do direito à liberdade de expressão, tanto nas esferas do direito civil quanto na esfera penal.

Palavras chave: Democracia; Honra; Indenização; Liberdade de expressão; Poder punitivo

* Abogado por la Universidad Católica del Ecuador, sede Ibarra. Diplomado en igualdad y no discriminación por la Universidad de Buenos Aires. Especialista en Derecho penal por la Universidad de Belgrano, Buenos Aires, Argentina. Máster (c) en Derecho con orientación en Derecho penal por la Universidad de Palermo, Buenos Aires, Argentina. PhD (c) en Derecho por la Universidad de Palermo, Buenos Aires, Argentina. Investigador independiente. Correo electrónico: vvasconez@hotmail.es

** Abogado por la Universidad Central del Ecuador. Máster en Derecho Privado Patrimonial por la Universidad de Salamanca y la Universidad Pública de Navarra, Salamanca, España. Abogado en libre ejercicio profesional e investigador independiente. Correo electrónico: edisonisraellopez@gmail.com

INTRODUCCIÓN

En términos históricos, pese a los primeros indicios del Derecho ateniense y romano, la discusión sobre los Derechos humanos es un tema relativamente nuevo, debido a que solo fue puesto en escena de forma expresa en el año 1215, con la firma de la Carta Magna inglesa, y de ahí en adelante fue exiguamente discutido según la conveniencia de quienes ostentaban el poder. En particular, sobre el derecho a la libertad de expresión, puede verse con mayor claridad que la discusión sobre los Derechos humanos no es un tema que ha recibido la importancia que merece, pues esta cuestión recién saltó a primer plano después de la Gloriosa Revolución Inglesa**,** que trajo como consecuencia la proclamación del *Bill Of Rights* en el año de 1689.

De ahí en adelante, el derecho a la libertad de expresión fue reconocido por los pueblos estadounidense, español, italiano, y gran parte del resto de pueblos europeos, hasta alcanzar como punto de referencia mundial su reconocimiento en la Declaración Universal de los Derechos Humanos de1948. Para el día de hoy, este derecho no solo se encuentra consagrado en distintos pactos internacionales y forma parte de la jurisprudencia de los más importantes tribunales de justicia internacional, sino que, incluso, cuenta con una relatoría especial que se encarga de sentar sus principales bases y alcances. Sin embargo, no es coincidencia que haya alcanzado tal grado de desarrollo y reconocimiento en los últimos años, dado que es un derecho preponderante y *sine qua non* para nuestra convivencia en democracia; por tal motivo se dedicará un capítulo para destacar el lazo inquebrantable entre la libertad de expresión y el mantenimiento de la democracia.

Asimismo, es ostensible que la segunda modernidad en la que nos encontramos trae aparejado un sinnúmero de retos para la vigencia y respeto del derecho a la libertad de expresión; así pues, resulta de vital importancia efectuar un análisis crítico sobre el fundamento de su existencia a la luz de los principales instrumentos internacionales que lo reconocen, por supuesto, también a partir de la norma constitucional ecuatoriana. Solo a raíz de esta base teórica será posible identificar su alcance y limitaciones. En efecto, como es de conocimiento público, ningún derecho es absoluto; y, por tanto, nuestra tarea consiste principalmente en resaltar su verdadero contenido y, en consecuencia, determinar de forma taxativa las limitaciones del derecho a la libertad de expresión en Internet, desde las esferas del Derecho civil y del Derecho penal.

EL FUNDAMENTO Y RECONOCIMIENTO CONSTITUCIONAL Y CONVENCIONAL DEL DERECHO A LA LIBERTAD DE EXPRESIÓN VÍA INTERNET

El legislador constituyente en el Ecuador, en armonía con los tratados internacionales de la materia, fue acertado en prescribir taxativamente el derecho a la libertad de expresión en la parte dogmática de la Constitución Nacional del año 2008. Puede verse dicho reconocimiento en el artículo 66, numeral 6, en el cual se plasma expresamente el derecho de todo ciudadano a opinar y expresar su pensamiento libremente, y en todas las formas y manifestaciones. En suma, a más del reconocimiento taxativo, bien se podría sostener que este derecho guarda un reconocimiento tácito a partir de la proclamación de igualdad formal y material para todos los ciudadanos; puesto que, si un individuo tiene la posibilidad de expresar sus pensamientos, por el principio de igualdad, lo lógico sería que todos los demás gocen del mismo derecho por su sola condición de persona.

Y si los argumentos aludidos no son suficientes para denotar su existencia y dotarle de contenido a la libertad de expresión, con plena seguridad la noción de libertad en sentido amplio sí está en condiciones de

hacerlo. Al respecto, en esta investigación no se defiende cualquier concepción de libertad, sino una libertad entendida en términos de no dominación, de manera que el ciudadano debe tolerar restricciones impuestas por el gobierno únicamente en los casos en que estas sean prescritas en una norma jurídica legítima, es decir, fruto de un proceso democrático. En este sentido, sobre esta forma de entender a la libertad, Philip Pettit emite el siguiente argumento clarificador:

> (…) bajo la concepción de la libertad como no-dominación, la dominación es necesaria y suficiente para una reducción de la libertad. Yeso significa que, si no hay dominación involucrada, la libertad no se reduce en presencia de interferencia o frustración. (…) Sugiere que, si las personas gobernadas por un estado controlan la interferencia practicada por el gobierno, si controlan las leyes impuestas, las políticas perseguidas, los impuestos aplicados, entonces no pueden sufrir la dominación a manos de sus gobernantes y pueden continuar disfrutando de sus responsabilidades. La libertad en relación con el estado. Un estado que fuera controlado adecuadamente sería legítimo en el sentido requerido de no ejercer dominio sobre su gente. Desde luego, practicaría la interferencia, piense en lo frustrantes que pueden ser las leyes y los impuestos, pero solo interferirá con ellos en sus términos, no por voluntad propia o por placer. (Pettit 2012, 152-3)

Entonces, ya tenemos el primer indicador de que, si la intención de un gobierno es pretender restringir la libertad de los ciudadanos, en cuanto a la libertad de expresión, solo podría hacerlo en términos excepcionales y en base a un estricto test de legitimidad democrática. Ahora bien, respecto del alcance del derecho a la libertad de expresión en el Ecuador, de la misma norma constitucional se desprende que no es un derecho absoluto, y en el artículo 18 puede verse cómo el legislador prescribió algunas limitaciones. En efecto, si bien se reconoce que todo individuo tiene el derecho a buscar, recibir, intercambiar y producir información sin censura previa, esta información tiene que ser veraz, verificada, oportuna, contextualizada y plural. Es decir, en el Ecuador se fomenta que cualquier ciudadano pueda producir información, pero esta debe estar sujeta a un estándar de calidad para que tenga pleno reconocimiento.

Por otro lado, dado el marco jurídico internacional, en La Declaración de Principios sobre Libertad de Expresión emitido por la CIDH, se prevé, en el numeral 7, que condicionamientos previos tales como veracidad, oportunidad o imparcialidad por parte de los Estados son incompatibles con el derecho a la libertad de expresión reconocido en los instrumentos internacionales. En consecuencia, por control de convencionalidad, la restricción a la libertad de expresión plasmada en el artículo 18 de la Constitución Nacional perdería fuerza, debido a que el instrumento internacional aludido reconoce derechos más amplios en esa materia. La amplitud del derecho a la libertad de expresión recogida en la declaración de la CIDH guarda plena armonía con las aseveraciones argüidas por Ronald Dworkin, en el sentido que a continuación se expresa:

> La afirmación de que los ciudadanos tienen derecho a la libertad de expresión debe implicar que estaría mal que el Gobierno les impidiese usar de ella, aun cuando el Gobierno crea que lo que han de decir causará más mal que bien. (Dworkin 1989, 284)

Es más, para reafirmar el amplio reconocimiento internacional del derecho a la libertad de expresión, hay que sumar lo prescrito en el artículo 4 de la Declaración Americana de los Derechos y Deberes del Hombre, donde se establece que "Toda persona tiene derecho a la libertad de investigación, de opinión y de expresión y difusión del pensamiento por cualquier medio" (Declaración Americana de Derechos y Deberes del Hombre 1948). Asimismo, la Convención Americana de Derechos Humanos prevé en su artículo 13 que:

> 1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:
   a) el respeto a los derechos o a la reputación de los demás, o
   b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas. (Convención Americana de Derechos Humanos 1969)

Como se ve, el derecho a la libertad de expresión no solo tiene reconocimiento doctrinal y constitucional, sino que, más importante aún, tiene un reconocimiento amplio y expreso en tratados y convenciones internacionales a los que se ha adherido el Ecuador. Sin embargo, pese al gran alcance que le reconoce tanto la CIDH como la Declaración Americana de Derechos y Deberes del hombre, puede verse que la Convención Americana de Derechos humanos ya nos ofrece un primer indicio sobre las limitaciones que tiene este derecho; pues se pone sobre la mesa la posible responsabilidad *ex post* de las declaraciones que puedan menoscabar la reputación de los demás y las que pongan en juego la seguridad nacional, el orden público, salud o moral pública. Es decir, parece haber una colisión de criterios no solo puertas adentro, sino también en el Derecho internacional, ya que existe un vaivén de criterios sobre el alcance de la libertad de expresión.

Según nuestra forma de ver la situación, la jurisprudencia de la Corte Interamericana de Derechos Humanos da en el clavo sobre el alcance y posibles limitaciones al derecho de la libertad de expresión, ya que, por ejemplo, en el caso Kimel vs Argentina, se dejó establecido que:

> (…) la libertad de expresión no es un derecho absoluto. El artículo 13.2 de la Convención, que prohíbe la censura previa, también prevé la posibilidad de exigir responsabilidades ulteriores por el ejercicio abusivo de este derecho. Estas restricciones tienen carácter excepcional y no deben limitar, más allá de lo estrictamente necesario, el pleno ejercicio de la libertad de expresión y convertirse en un mecanismo directo o indirecto de censura previa. (Corte IDH, párrafo 54)

En el mismo sentido, la Relatoría Especial para la Libertad de Expresión de la CIDH (en adelante RELE) se suma a la jurisprudencia de la Corte y expresa, en el informe especial sobre la libertad de expresión para el Estado de Honduras**,** que todas las restricciones al derecho a la libertad de expresión deben satisfacer un estricto test tripartito en los siguientes términos:

- Estar definidas en forma precisa y clara a través de una ley formal y material preexistente;

- Estar orientadas al logro de objetivos legítimos bajo el derecho internacional;

- Ser necesarias en una sociedad democrática para el logro de los fines que se buscan, estrictamente proporcionadas a la finalidad perseguida, e idóneas para obtener el objetivo que pretenden lograr. (RELE 2018, 5)

En tal circunstancia, sea desde el fuero civil como también en la esfera penal, la restricción a la libertad de expresión únicamente puede darse en los términos aludidos, y solo cuando concurran todos ellos. Ahora bien, puede notarse que la normativa interna y el Derecho Internacional amparan a la libertad de expresión en cualquiera de sus formas, inclusive las expresiones y manifestaciones que se realicen a través de medios telemáticos, redes sociales o en el Internet en general.

Por esta causa, en la sección tercera de la Constitucional Nacional relativa a la comunicación e información, se tiene prescrito, en el numeral 1 del artículo 16, el derecho de toda persona a una comunicación libre, diversa, participativa, y por cualquier medio y forma. En el siguiente numeral, se resalta el derecho al acceso universal a la tecnología, que no es un derecho menor ni mucho menos, pues constituiría la precondición necesaria para que ese derecho a la libertad de expresión a través del Internet pueda materializarse. Es decir, la tarea del gobierno no solo consiste en un reconocimiento formal y expreso de los derechos, sino que, además, tiene que obtener los medios y recursos necesarios para que los derechos puedan practicarse

ontológicamente; y las carencias en este ámbito, como es de conocimiento público, constituyen una falencia generalizada sobre todo en los países en vías de desarrollo.

LA LIBERTAD DE EXPRESIÓN COMO BASE FUNDAMENTAL DE UNA DEMOCRACIA DELIBERATIVA

Es conveniente echar una mirada a la realidad antes de adentrarnos en el tratamiento del fondo de este apartado. Los presidentes Lenín Moreno en Ecuador, Donald Trump en Estados Unidos, Alberto Fernández en Argentina, Martín Vizcarra en Perú, y muchos otros mandatarios, han adoptado la costumbre de tener como principal medio de difusión de sus decisiones a la red social Twitter, y solo subsidiariamente utilizan la televisión y la radio. Así se pone en evidencia que, si bien los medios de comunicación tradicionales todavía son utilizados para fines de información, hoy todo gira en torno al Internet. Es decir, solo quienes tengan acceso a la Internet estarán en condiciones de recibir información ágil y oportuna. El resultado es que solo estas personas pueden participar de forma activa en el control de las decisiones adoptadas por el poder.

Ahora bien, el ejercicio del derecho a la libertad de expresión parece tener dos niveles de intensidad**;** debido a que sí es posible observar una serie de restricciones impuestas para la relación entre privados, es decir**:** cuando las expresiones o manifestaciones tienen un contenido injurioso, cabe abiertamente la posibilidad de imponer sanciones jurídicas ulteriores. En cambio, la intensidad que adorna a este derecho en el plano público, que se traduce en la posibilidad que tienen los ciudadanos para criticar las decisiones que adoptan las personas que ostentan cargos públicos, tiene un reconocimiento mayor y, en consecuencia, las restricciones en este ámbito deben ser prácticamente inexistentes.

En el mismo sentido, La Declaración de Principios sobre Libertad de Expresión de la CIDH prevé, en su artículo 11, que los funcionarios públicos están sujetos a un mayor escrutinio por parte de la sociedad y, por consiguiente, "Las leyes que penalizan la expresión ofensiva dirigida a funcionarios públicos generalmente conocidas como 'leyes de desacato' atentan contra la libertad de expresión y el derecho a la información" (Declaración de Principios sobre Libertad de Expresión 2000, art. 11). En todo caso, según parámetros de la misma CIDH, la utilización del Derecho Penal resulta abiertamente desproporcional para sancionar a las personas que se excedan en el ejercicio de su derecho a la libertad de expresión en contra de funcionarios públicos y sus decisiones. En tal circunstancia, a lo sumo debería admitirse sanciones en el plano del Derecho Civil, y siempre que se corrobore de manera estricta la concurrencia de los tres elementos del test de necesidad propuesto por la RELE.

¿Pero por qué se da tanta importancia al derecho a la libertad de expresión? Dar una respuesta convincente a esta pregunta ayudará a entender el motivo por el que la comunidad internacional y el derecho interno le confieren un reconocimiento y alcance tan profuso. Sin lugar a dudas, la respuesta intuitiva sería que este derecho permite que los ciudadanos interactuemos y, de esa forma, se hace posible nuestra convivencia; pero realmente, este derecho tiene un tinte fuertemente político y no en el sentido partidista, sino en el sentido de participación ciudadana en todos los escenarios de relevancia pública.

De esta manera, solo se puede entender la verdadera importancia del derecho a la libertad de expresión en la esfera pública, siempre que se tome como punto de partida un concepto acertado de democracia. En efecto, del contenido que se dé a ésta dependerá en gran medida el alcance del derecho a expresarse de forma libre. Así pues, si la noción de democracia que nos resulta acertada es meramente participativa, es decir, el solo reconocimiento formal de que todos los ciudadanos tienen el derecho a elegir a sus representantes y nada más, lo más probable es que el derecho a la libertad de crítica a las autoridades públicas sea muy restringido; ya que, en esa noción de democracia, la

tarea del ciudadano termina en el depósito del voto en las urnas y, de ese modo, estaría plenamente justificado que se sancione cualquier expresión ulterior desagradable en contra del poder.

Por tal motivo, desde nuestra concepción de democracia, estamos plenamente convencidos de que ésta no es meramente participativa, sino que su esencia es que sea de carácter deliberativa y, de esta suerte, no es legítima la imposición de restricciones a la libertad de expresión. Al respecto, sobre la democracia deliberativa, Roberto Gargarella ha escrito lo siguiente:

> De acuerdo con esta visión, en una democracia deliberativa, i) todos los potencialmente afectados por una cierta norma intervienen en su creación; y ii) el proceso de toma de decisiones que lleva a dicha creación se caracteriza fundamentalmente por una amplia discusión colectiva; iii) organizada bajo condiciones de igualdad. (Gargarella 2015, 102)

Es decir, el compromiso de la ciudadanía debe extenderse al control de cualquier decisión que se adopte desde el poder y, en especial, sobre la elaboración de las normas. Así también lo entiende Sunstein, quien manifiesta que la participación política de los ciudadanos "no deberá efectuarse en un sentido meramente instrumental, sino que, deberá entenderse como un canal para el ejercicio de la ciudadanía en donde primará la empatía, la virtud y el compromiso con el sentido de la comunidad" (Sunstein 2004, 160-1). Sin embargo, para lograr esta anhelada participación ciudadana, necesariamente se requiere de un aparataje jurídico permisivo y una tendencia política que no sea represiva con las voces disonantes. Además, de nada sirve tener políticos abiertos a recibir críticas y un sistema jurídico permisivo, si el gobierno no se ocupa de proveer las vías necesarias para que el ciudadano haga llegar su voz crítica.

Por ejemplo, digamos que un Estado hace gala de un paraíso normativo en el cual se reconocen ampliamente todos los derechos, y además los políticos, funcionarios públicos y cualquier persona que se desenvuelva en el sector público, son ciudadanos abiertos a ser criticados y fiscalizados por su pueblo. Sin embargo, pese a darse todas las condiciones de forma, digamos que la pobreza del pueblo es tal, que un gran número de ciudadanos no tiene acceso a la Internet; en consecuencia, materialmente no habría esa posibilidad de ejercer control y crítica a las decisiones de las funciones del Estado.

Dicho de otra manera, si no se dan los medios necesarios para que el pueblo pueda ejercer su derecho constitucional a expresarse libremente y de esa manera controlar las decisiones del poder, lo más seguro será que los actos de corrupción proliferen exponencialmente, pues solo si se vigila al vigilante es posible contener cualquier desbordamiento en las actividades públicas. Finalmente, la experiencia enseña que, ante situaciones de emergencia, sea que estas sean reales o creadas artificialmente por un gobierno para legitimarse, el derecho a la libertad de expresión corre mayor peligro de ser censurado y, paradójicamente, en esos momentos es cuando resulta de mayor importancia su ejercicio para ejercer el control de los actos de gobierno.

LÍMITES A LA LIBERTAD DE EXPRESIÓN EN INTERNET DESDE LA ESFERA JURÍDICO-CIVIL

En el capítulo segundo de esta investigación se puso de manifiesto que el derecho a la libertad de expresión, como cualquier otro, puede ser sujeto a limitaciones.

Al respecto se hizo una breve descripción del estado de la cuestión en el Derecho internacional y también en el Derecho nacional; sin embargo, todavía no se ha dado una explicación del motivo por el que puede limitarse este derecho.

En este tema, nos parece que le asiste la razón a Robert Alexy al argüir que la norma constitucional que reconoce un derecho debe recibir el tratamiento de un

principio jurídico y, en consecuencia, su ejercicio solo puede practicarse hasta donde las posibilidades jurídicas existentes así lo permitan. Es decir, en la medida en que existen normas civiles y penales que ponen un dique de contención al ejercicio pleno de este derecho, solo en armonía con esas normas jurídicas podrá practicarse la libertad de expresión. Para profundizar en el pensamiento de Alexy sobre el tratamiento que debe recibir un principio, veamos a continuación un extracto de su obra titulada *Teoría de los Derechos Fundamentales*.

> El punto decisivo para la distinción entre reglas y principios es que los principios son normas que ordenan que algo sea realizado en la mayor medida posible, dentro de las posibilidades jurídicas reales existentes. Por tanto, los principios son mandatos de optimización que están caracterizados por el hecho de que pueden ser cumplidos en diferente grado y que la medida debida de su cumplimiento no sólo depende de las posibilidades reales, sino también de las jurídicas. (Alexy 1993, 86)

En este sentido, tal como se plantea en la Convención Americana de Derechos Humanos, los límites de la libertad de expresión están marcados por el respeto a los derechos de terceros. De ahí que el Derecho Civil moderno se ha encargado de establecer ciertos límites a las libertades individuales a fin de proteger derechos civilmente tutelables. Por consiguiente, en el estudio que nos ocupa cabe plantearse cuáles son estos derechos que merecen protección ante el ejercicio abusivo de la libertad de expresión en entornos digitales.

Tras el establecimiento de una Web interactiva y de fácil acceso se han originado diversos ambientes virtuales en los que se ejerce la libertad de expresión en su máximo esplendor, puesto que cualquier cibernauta puede verter sus opiniones sin necesidad de revelar su identidad o proporcionar datos verificables, en cualquier momento y en cualquier lugar. Estas circunstancias han sido la clave del rotundo éxito de plataformas digitales como foros, blogs y redes sociales. Sin embargo, precisamente estas cuestiones hacen que los ciudadanos se extralimiten en el ejercicio de su libre expresión sin consideración de los derechos ajenos. Esta situación deja en evidente vulnerabilidad, en especial, a los bienes jurídicos de carácter personal, mejor conocidos como derechos de la personalidad.

> Según se desprende de la doctrina, los derechos de la personalidad son el conjunto de derechos subjetivos por los que se otorgan a su titular las facultades de goce, protección y disposición de los atributos intrínsecos inherentes a su persona. (Díez-Picazo y Gullón 2012, 325)

De manera específica, dentro de la categoría de derechos de la personalidad, se encuentran el derecho al honor, el derecho a la intimidad y el derecho a la imagen. Estos han sido considerados de suma importancia para el libre desarrollo de la personalidad de los ciudadanos y, por ende, tienen el más alto reconocimiento a nivel constitucional en la mayoría de los ordenamientos jurídicos. En el caso de Ecuador, están reconocidos en el art. 66, numerales 18 y 20, de la Constitución.

> En términos jurídico-civiles, el honor debe ser entendido como aquel derecho que protege la buena reputación de una persona, que preserva frente a expresiones de descrédito. Los doctrinarios contemporáneos han entendido que el derecho al honor se halla articulado por dos aspectos esenciales: el subjetivo, que se refiere a la estima que tiene una persona de sí mismo; y el objetivo, que contempla la consideración que los demás hacen de la dignidad de su dignidad. (Herrera 2017, 18)

Por su parte, el derecho a la intimidad ha sido definido de manera solvente por la jurisprudencia constitucional española en los siguientes términos:

> El derecho fundamental a la intimidad (…) tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona, frente a la acción y el conocimiento de los demás, sean éstos poderes públicos o simples particulares. (Tribunal Constitucional de España, 2000)

Mientras que el derecho a la imagen conlleva la facultad de su titular de hacer pública su propia imagen o rasgos identificados o identificables y, por tanto, su

derecho a impedir su reproducción cuando no medie autorización alguna (Sánchez 2017, 125).

La función limitadora de estos derechos radica en que, al tener el mismo rango que la libertad de expresión, el ejercicio de esta última no puede suponer vulneración o intromisión ilegítima en el honor, intimidad o imagen de los demás ciudadanos. No obstante, este criterio se ve matizado por el hecho de que puede prevalecer la libertad de expresión en supuestos en los que exista un interés general relevante, que puede ser de índole histórico, científico o cultural; así también en los casos en que la información tenga relevancia pública, siempre que se enmarque en la veracidad del hecho y que la opinión vertida se encuentre acorde a los usos sociales, sin la utilización de expresiones injuriosas o denigrantes.

Estos criterios de preponderancia de la libertad de expresión han sido establecidos en leyes especiales que se encargan de regular la protección civil de los derechos de la personalidad, como sucede en México y en España. Tales criterios han sido desarrollados por la jurisprudencia. Sin embargo, el marco normativo ecuatoriano no contempla de manera expresa una norma específica de índole civil que determine circunstancias que legitimen la extralimitación de las opiniones en el ejercicio de la libre expresión. Por tanto, al juez le corresponde hacer juicios de ponderación de derechos en atención a las circunstancias de cada caso en concreto, según el interés general que pueda conllevar determinada opinión o información y el grado de afectación moral que haya sufrido la víctima.

De comprobarse una vulneración ilegítima de los derechos de la personalidad, se debe acudir a las normas de responsabilidad civil extracontractual recogidas en el Código Civil ecuatoriano. Para el caso en que el honor se vea afectado por expresiones atentatorias resulta aplicable el artículo 2231, que, textualmente, determina que: "Las imputaciones injuriosas contra la honra o el crédito de una persona dan derecho para demandar indemnización pecuniaria, no sólo si se prueba daño emergente o lucro cesante, sino también perjuicio moral" (Código Civil, 2005).

Mientras que, por su lado, frente a la vulneración del derecho a la intimidad y a la imagen, se debe aplicar el régimen de responsabilidad establecido en el artículo 2232 del mismo cuerpo legal, en el que se reconoce el derecho de demandar una indemnización pecuniaria para quien hubiera sufrido daños meramente morales, siempre que exista una gravedad particular del perjuicio sufrido, es decir cuando el daño tenga suficiente intensidad como para que se tenga que resarcir pecuniariamente.

En tal virtud, según el Derecho Civil ecuatoriano, el ejercicio temerario de la libertad de expresión conlleva responsabilidad civil derivada del daño moral ocasionado por la lesión del derecho al honor, intimidad o imagen. En suma, desde la perspectiva civil, la libertad de expresión en los entornos digitales encuentra su límite en los derechos de la personalidad del resto de individuos, esencialmente en los derechos al honor, a la intimidad y a la propia imagen. Por tanto, en vista de que las libertades y derechos están en constante colisión, solo pueden ser indemnizadas aquellas vulneraciones en las que el ejercicio extralimitado de la libertad de expresión no pueda ser justificado con criterios de veracidad o interés legítimo, de carácter general y público.

LÍMITES A LA LIBERTAD DE EXPRESIÓN VÍA INTERNET DESDE LA ESFERA JURÍDICO-PENAL

Se ha visto que la RELE ha recomendado trazar un test tripartito cuyo cumplimiento haría que una restricción a la libertad de expresión alcance cierto grado de razonabilidad y consecuente legitimidad. Además, también ha dicho la RELE que la restricción al derecho de expresarse libremente desde la esfera penal sería abiertamente desproporcional, pues las consecuencias jurídico-penales por incumplimiento de normas resultan ser muy severas y, por tal causa, se ha recomendado su derogación cuando las aseveraciones

vayan dirigidas a funcionarios públicos. Al respecto, Muñoz Conde y García Arán señalan que "[e]l poder punitivo del Estado debe estar regido y limitado por el principio de intervención mínima. Con esto quiero decir que el Derecho penal sólo debe intervenir en los casos de ataques muy graves a los bienes jurídicos más importantes" (Muñoz Conde y García Arán 2010, 72).

Bajo esta perspectiva, no es coincidencia que la intervención del poder punitivo sea pospuesta como último recurso y para los casos estrictamente necesarios. Sin embargo, el legislador ecuatoriano ha tomado la decisión política criminal de tipificar algunos delitos que pueden cercenar la posibilidad de expresarse libremente, y esta decisión política solo puede explicarse a raíz de un ejercicio de ponderación en el cual la honra individual, la moral privada y la seguridad del Estado, en determinadas circunstancias están por encima del derecho a la libertad de expresión.

Entonces, y de acuerdo con las aseveraciones del capítulo III en el sentido de que el derecho a la libertad de expresión tiene por lo menos dos intensidades, es decir, un reconocimiento más amplio para las aseveraciones o manifestaciones con relevancia pública y un alcance más restrictivo para los supuestos entre privados, lo más conveniente en términos metodológico es que, en este capítulo, se efectúe un examen diferencial. Con miras a lograrlo, se trabajará con un supuesto fáctico acaecido en 2014 y, de esa manera, también se busca ganar en claridad argumental.

Como aclaración preliminar, las reglas y criterios para analizar el alcance de la libertad de expresión son idénticas para supuestos en los que el medio utilizado sea el Internet o, alternativamente, se utilice cualquier medio tradicional como la prensa, la telefonía o alguna forma de exteriorización de las ideas y pensamientos. Con el objeto de analizar este tema, en primer lugar, se analizará el tratamiento jurídico penal que debe darse al derecho a la libertad de expresión, cuando la finalidad de este derecho se encamine a la crítica del poder y en consecuencia tenga relevancia pública.

Entonces, para concretizar todos los conceptos y analizarlos en un caso real acaecido en el Ecuador, pensemos en la causa judicial Nro. 172942015011486G**,** que fue propuesta por la Confederación Nacional Afroecuatoriana (CNA) en contra del caricaturista Xavier Bonilla (Bonil), debido a que este último**,** supuestamente habría cometido el delito de discriminación en contra del asambleísta por Alianza País Agustín Delgado (ex-futbolista). Los hechos fueron los siguientes: Bonil, en calidad de caricaturista del Diario el Universo, publicó**,** en agosto del 2014**,** una caricatura en la que destacaba la falta de preparación académica de ese político, pues, en días anteriores, Delgado había intervenido en el seno de la Asamblea Nacional con un discurso por demás defectuoso.

Posteriormente, la CNA interpuso una denuncia en contra de Bonil, quien se defendió a través de su abogado, con el siguiente argumento: "el objetivo (…) al dibujar la caricatura del asambleísta Agustín Delgado (Alianza PAIS), publicada el pasado 5 de agosto en EL UNIVERSO, no fue la de discriminar, sino reflejar la falta de preparación del oficialista" (El Universo 2015). Ventajosamente para Bonil, finalmente esta denuncia fue archivada.

Ahora bien, ¿procedieron bien las autoridades judiciales en esta causa? Seguramente, la respuesta no puede ser otra que sí, como se explica por los siguientes argumentos: habíamos resaltado la importancia del derecho a la libertad de expresión como base de una democracia deliberativa y, además, se dejó claro que la persona que decida ponerse voluntariamente en un escenario público, sea que haya accedido por elección popular, por concurso o por decisión de alguna autoridad, necesariamente tiene que someterse a un escrutinio serio por parte de la sociedad, pues la base de un modelo de gobierno republicano exige una constante rendición de cuentas y explicación de cualquier intervención o decisión que se tome por parte de los funcionarios públicos. Entonces, es impensable la comisión de una discriminación por criticar, de cualquier forma, la deficiencia intelectual de un asambleísta, pues tal acción constituye no solo un derecho, sino, además, un deber cívico de desnudar la incompetencia de quienes toman las decisiones por nosotros los ciudadanos.

Pero entonces, ¿las aseveraciones o cualquier forma de libertad de expresión con contenido de interés público

no tienen límites? No se ha afirmado tal cosa: los límites existen y estos se dan en un marco de excepcionalidad. Así pues, conviene traer a cuento los criterios fijados por la Corte Suprema de los Estados Unidos en la doctrina de la real malicia a propósito del *leading case* "New York Times vs Sullivan". En efecto, esta línea jurisprudencial, que luego tuvo un amplio desarrollo por la doctrina, prevé la posibilidad de responsabilizar penalmente al emisor de una información de contenido público cuando se comprueben los siguientes requisitos:

a) La prueba por el accionante de una manifestación difamatoria;
b) la prueba por el accionante sobre la inexactitud de la expresión;
c) la prueba del accionante de que la emisión de la expresión fue hecha en base al conocimiento de que era falsa (dolo directo) o con una temeraria despreocupación acerca de su verdad o falsedad (dolo eventual), como expresión de una indiferencia egoísta de la producción del hecho lesivo. (Donna 1999, 317)

En tal circunstancia, si bien esta doctrina fue emitida en un contexto en el que una empresa destinada a informar (New York Times) había emitido información cuestionable sobre el proceder de un comisionado de policía, es completamente admisible su utilización para cualquier supuesto en que una persona critique el proceder de un funcionario público, ya sea un medio de comunicación o cualquier ciudadano. Y el fondo de este asunto es que solo es admisible restringir el derecho a la libertad de expresión en situaciones excepcionales debido a su preponderancia para la continuación del sistema democrático.

Pues bien, para redondear la idea de la real malicia, únicamente cuando una persona haga uso abusivo de su derecho a la libertad de expresión con un desprecio absoluto o potencial sobre la veracidad de los hechos, será admisible una persecución criminal. Sin embargo, ¿Qué hubiese pasado si Bonil hacía una caricatura en la que exponían las falencias intelectuales de un particular? *Prima facie* ya podría pensarse que, en estos casos**,** sí existiría la perpetración de alguna infracción, pues habría que tomar en cuenta que la persona caricaturizada no es ningún funcionario público y seguramente una caricatura de esas características generaría su descrédito social, acompañado de aflicción psíquica a raíz de las burlas en su contra. Sin embargo, para dar una respuesta convincente a esta pregunta, de aquí en adelante haremos una exposición doctrinal del estado de la cuestión sobre infracciones contra el honor.

Los profesores Murillo y Serrano González, al parafrasear al maestro alemán Maurach, sostenían que, "el honor es el bien jurídico más sutil, el más difícil de aprehender con los toscos guantes del Derecho penal y por tanto el menos eficazmente protegido" (Murillo y Serrano González 1993, 27). De modo que la utilización del Derecho Penal para sancionar un exceso de libertad de expresión no es ni siquiera idónea, de modo que, de entrada, podríamos afirmar que cualquier conducta tipificada como delito por el legislador tiene serios inconvenientes de legitimidad, en términos del test tripartito sugerido por la RELE.

Con todo, en el artículo 182 del Código Orgánico Integral Penal se ha prescrito el delito de calumnia. Y en el artículo 396 del mismo cuerpo legal se prevé la contravención de injurias. Por su parte, el artículo 229 se refiere al delito de revelación ilegal de base de datos, y el cajón de sastre del gobierno cuando quiere cercenar la libertad de expresión consta en el artículo 180, referido al delito de difusión de información de circulación restringida. Estos tipos penales pueden lesionar el derecho a la libertad de expresión en el caso de que su interpretación por las autoridades judiciales sea errada. Sin embargo, para efectos de exponer el tratamiento que debería darse a la conducta de Bonil en el supuesto planteado de la caricatura dirigida a un particular, únicamente se estudiará la contravención de injurias.

Entonces, el legislador ecuatoriano ha prescrito que comete la infracción de injurias aquella persona que profiera expresiones en descrédito o deshonra de otra; consecuentemente, en primer lugar, corresponde examinar el contenido del término "honra" para arribar a conclusiones válidas. Con miras a desarrollar este punto, a continuación, se expondrán sus principales características, pese a que ya fue definido desde la

esfera del Derecho Civil en el capítulo anterior. Así pues, enseña Donna que:

> Honor es la suma de todas las cualidades, incluido no solo los atributos morales sino también los valores jurídicos, sociales y profesionales valiosos para la comunidad, que se pueden atribuir los individuos a sí mismos o la buena opinión y fama que tienen los terceros respecto de uno mismo. (Donna 1999, 306)

De esta manera, es posible aseverar que el honor puede tener dos dimensiones: un aspecto meramente subjetivo correspondiente a la propia apreciación que tenga el individuo sobre sí mismo, y, en segundo lugar, un aspecto objetivo que tiene como base la reputación que se tenga. En consecuencia, el delito de injurias se puede configurar cuando exista un menoscabo tanto en la faz subjetiva como también en la objetiva.

En el caso planteado de Bonil, de comprobarse que, como producto de la publicación de la caricatura, se ocasionó un menoscabo en alguna de las facetas de la honra, pese a que no sea legítimo por ineficaz sancionar penalmente a una persona por excederse en el ejercicio de su derecho a expresarse libremente, parecería que es completamente legal una condena en este supuesto, debido a que el particular no tiene la carga que sí tiene un funcionario público de soportar cualquier tipo de crítica, y el mismo análisis y conclusiones correspondería para los supuestos en los que se utilice al Internet como medio para proferir la injuria.

CONCLUSIONES Y RECOMENDACIONES

- El derecho a la libertad de expresión tiene reconocimiento a nivel interno, es decir, en la Constitución Nacional del Ecuador, y así también lo tiene a nivel foráneo en diversos tratados y convenios internacionales. Además, existe un importante desarrollo jurisprudencial proveniente de la Corte IDH y las recomendaciones emitidas desde la Relatoría Especial de la CIDH tendiente a identificar el alcance del derecho a la libertad de expresión por Internet; dado que, al día de hoy, éste constituye el principal medio de difusión de ideas.

- Existe consenso nacional e internacional acerca de que el derecho a la libertad de expresión tiene algunas limitaciones, y en el fallo Kimel vs Argentina de la Corte IDH es en donde mejor se advierte esta situación, puesto que se prevé responsabilidades ulteriores en el caso de abusar de este derecho, sea por lesionar la honra o reputación de los demás, sea por una cuestión de seguridad nacional y orden público. Por supuesto que las limitaciones aludidas están dirigidas a las formas tradicionales de libertad de expresión y también para su ejercicio a través medios digitales. Los parámetros de legitimidad para sancionar jurídicamente un abuso del derecho a la libertad de expresión en sentido amplio son los siguientes: la sanción jurídica debe estar prevista en una ley formal y material preexistente, debe estar direccionada a un objetivo legítimo y ser necesaria e idónea para conseguir el objetivo propuesto.

- El derecho a expresarse libremente puede hacerse por cualquier medio y constituye la base de un modelo republicano de gobierno en el que las autoridades deben rendir cuentas constantemente. Solo puede ser así, siempre que se parta de un concepto de democracia deliberativa en donde constituye un derecho de los ciudadanos criticar y controlar cualquier situación de interés público, y es un deber del Estado proveer los medios necesarios para que efectivamente se materialice ese derecho. En este sentido, una condición necesaria para ejercer plenamente el derecho a la libertad de expresión es el acceso a Internet, pues, dada la vertiginosidad con la que cambia nuestra vida en sociedad, solo a través de este medio es posible adquirir información oportuna y diversa. En tal circunstancia, cualquier gobierno que diga ser amante de la libertad de expresión, tendrá como deber fundamental trabajar para que hasta el pueblo más remoto tenga acceso a Internet.

- El derecho a expresarse libremente tiene dos intensidades. Una de ellas se da el marco de las relaciones entre privados, en las cuales existe un alcance más restringido de este derecho. La otra intensidad, mucho más amplia, se da en el marco de asuntos de interés público, porque allí las restricciones a la libertad de expresión son prácticamente inexistentes; salvo que se compruebe que las aseveraciones fueron falaces y el emisor de dicha información lo conocía, o tal vez tuvo una despreocupación absoluta por conocer la verdad.

- Desde una mirada del Derecho Civil, la libertad de expresión en los entornos digitales encuentra su límite en los derechos de la personalidad de los demás, esencialmente en el derecho al honor, a la intimidad y a la propia imagen. Entonces, ya que las libertades y derechos generalmente entran en colisión, solo pueden ser indemnizadas aquellas vulneraciones en las que el ejercicio extralimitado de la libertad de expresión no pueda ser justificado con criterios de veracidad e interés legítimo.

- La utilización del Derecho Penal es abiertamente desproporcional y por ende ilegítima para sancionar conductas que abusen del derecho a expresarse libremente; no obstante, el legislador ecuatoriano ha previsto una serie de delitos y contravenciones para sancionarlas.

Recomendaciones

Cualquier propuesta de restringir el derecho a la libertad de expresión es una seria amenaza a la democracia de un Estado. Nuestra tarea como ciudadanos es defenderla y fomentar la libertad de expresión en cada espacio que sea posible y si para conseguirlo es necesario acudir a instancias judiciales, que así sea. Un ejercicio pleno del derecho a la libertad de expresión, en conjugación con una toma de conciencia del ciudadano de que tiene amplios derechos de escrutinio a cualquier decisión que se adopte desde el poder, es el camino indicado para erradicar los actos de corrupción; pues, así como el hambre y la pobreza vuelven trabajadores a los hombres, una vigilancia permanente de los gobernantes seguramente los vuelva correctos en sus quehaceres públicos.

BIBLIOGRAFÍA

Alexy, Robert. 1993. *Teoría de los derechos fundamentales*. Madrid: Centro de Estudios Constitucionales.

CIDH. 2018. *Informe especial de la Relatoría Especial para la libertad de expresión*. Honduras.

Díez-Picazo, Luis y Gullón, Antonio. 2012. *Sistema de derecho civil*, vol. I, Madrid: Tecnos.

Donna, Edgardo. 1999. *Derecho penal parte especial*, tomo I. Bs. As.: Rubinzal Culzoni.

Dworkin, Ronald. 1989. *Los Derechos en serio*. Barcelona: editorial Ariel.

El Universo. 2015. "Objetivo de caricatura de Agustín Delgado fue reflejar falta de preparación del asambleísta, dice defensa de Bonil". Acceso el 8-IV-2020. Recuperado de: https://www.eluniverso.com/noticias/2015/02/11/nota/4546866/objetivo-caricatura-agustin-delgado-fue-reflejar-falta-preparacion.

Gargarella, Roberto. 2015. "Mano dura sobre el castigo. Autogobierno y comunidad (II)", en *Revista jurídica de la Universidad de Palermo*. Bs. As.

Herrera, Ramón.2017. *Responsabilidad civil por vulneración del derecho al honor en las redes sociales*. Madrid: Reus.

Muñoz Conde, Francisco y García Arán, Mercedes. 2010. *Derecho penal parte general.* Valencia: Tirant lo Blanch.

Murillo, Alfonso y Serrano González, José.1993. *Protección penal del honor.* Madrid: Universidad de Extremadura

Pettit, Philip. 2012. *On the People´s Terms. A Republican Theory and Model of Democracy.* NY: Cambridge.

Sánchez, María. 2017. *Honor, intimidad y propia imagen.* Lisboa: Juruá.

Sunstein, Cass. 2004. "Más allá del resurgimiento republicano", en *Nuevas ideas republicanas: Autogobierno y Libertad.* Barcelona: Paidós.

Legislación y jurisprudencia

Convención Americana de Derechos Humanos, 1969

Corte IDH. 2008. caso *Kimel vs Argentina.* Fondo, reparaciones y costas. Sentencia del 2-V-2008. Serie C No. 177

Declaración Americana de Derechos y Deberes del Hombre, 1948

Ecuador. *Código Civil.* Registro oficial 46, 24-VI-2005.

Ecuador. *Constitución de la República del Ecuador*. Registro oficinal 449, 20-X-2009.

La Declaración de Principios sobre Libertad de Expresión emitido por la CIDH. 2000

Tribunal Constitucional de España. Sentencia de 15 de mayo de 2000.

Unidad Judicial Penal. 2015. Caso *Confederación Nacional de Afroamericanos y otros. Vs Bonilla Zapata Rodrigo Xavier y Pérez Barriga Carlos Eduardo representante de Diario El Universo,* número de causa: 172942015011486G.

ENSAYOS

LA IMPORTANCIA DE LA PROTECCIÓN DE DATOS Y LA SITUACIÓN ACTUAL DEL ECUADOR

THE IMPORTANCE OF DATA PROTECTION AND THE CURRENT SITUATION IN ECUADOR

A IMPORTÂNCIA DA PROTEÇÃO DE DADOS E A SITUAÇÃO ATUAL DO EQUADOR

*Belén Rivera**

Recibido: 03/05/2020
Aprobado: 13/06/2020

Resumen

Los múltiples avances tecnológicos han traído consigo grandes beneficios a la vida de los individuos, pues facilitan las rutinas diarias y permiten el acceso casi inmediato a la información y al conocimiento. Si bien este gigantesco desarrollo ha revolucionado la forma de vivir y de hacer las cosas; para lograrlo, ha sido necesario crear un mundo digital paralelo, lleno de datos e información que se ha utilizado durante muchos años, sin ningún control. Tal es el caso del Ecuador, donde todavía no existe una Ley de Protección de Datos que permita garantizar el derecho ciudadano a disponer y decidir libremente sobre ellos. El conocimiento que existe sobre esta materia es escaso, y tal situación promueve posibles infracciones. Este ensayo pretende explicar qué son los datos personales y su protección. Además, se enfoca en analizar la realidad ecuatoriana, así como las normas que han desarrollado otras jurisdicciones para proteger a sus ciudadanos. De igual forma se explican cuáles son las consecuencias reales de un posible mal uso, en conexión con el potencial de la Inteligencia Artificial, el Aprendizaje Automático y el Aprendizaje Profundo.

Palabras clave: Protección; Datos; Inteligencia artificial; Aprendizaje automático; Aprendizaje profundo

Summary

The multiple technological developments have brought great benefits to our lives, making daily routines easier and allowing immediate access to information and knowledge. Although this gigantic progress has revolutionized our way of living and how things are done. To achieve this, it has been necessary to create a parallel digital world, full of data and information that have been managed without any control for many years. Such is the case of Ecuador, where there is still no Data Protection Law that allows citizens to freely establish and decide over their data. The knowledge that individuals have on this matter is scarce and this situation promotes possible breaches. This article explains what personal data is and how it is protected. It also analyses the Ecuadorian reality, as well as the legal regulations developed by other countries to protect their citizens. In the same way, it explains the real consequences of the misuse of data, especially when it is connected with the potential of Artificial Intelligence, Machine Learning and Deep Learning.

Key words: Protection; Data; Artificial Intelligence; Machine Learning; Deep Learning

Resumo

Os múltiplos avanços tecnológicos vêm trazendo grandes benefícios na vida dos indivíduos, pois facilitam as rotinas diárias e permitem o acesso quase imediato a informação e ao conhecimento. Ainda que este gigantesco desenvolvimento vem revolucionando a forma de viver e de como sao feitas as coisas; para consegui-lo, foi

* Abogada de los Tribunales de Justicia y Licenciada en Derecho por la Pontificia Universidad Católica del Ecuador; Master of Laws por Leibniz Universität Hannover. Secretaria Adjunta de la Academia Americana de Derecho Internacional CAIL – 2018. Es miembro de la Asociación Internacional de Profesionales de Privacidad, docente de la cátedra de Herramientas Informáticas y Bases de Datos Aplicadas al Derecho de la Universidad Tecnológica Equinoccial y Jefe del Departamento de Litigios Marcarios de Bermeo & Bermeo Abogados. Correo electrónico: mbrivera12@gmail.com

necessário criar um mundo digital paralelo, cheio de dados e informações que se utilizaram durante muitos anos sem nenhum controle. Tal é o caso do Equador, onde ainda não existe uma Lei de Proteção de Dados que permita garantir o direito cidadão para dispor e decidir livremente sobre eles. O conhecimento que existe sobre a matéria é escasso, e tal situação promove possíveis infrações. Este artigo pretende explicar o que são os dados pessoais e sua proteção. Ademais, se concentra em analisar a realidade equatoriana, assim como as normas que vem sendo desenvolvidas por outras jurisdições para proteger os seus cidadãos. Da mesma forma se explicam quais são as consequências reais de um possível uso indevido, em conexão com o potencial da Inteligência Artificial, a Aprendizagem Automática e a Aprendizagem Aprofundada.

Palavras chave: Proteção; Dados; Inteligência Artificial; Aprendizagem Automática; Aprendizagem Aprofundada

ECUADOR Y LA PROTECCIÓN DE DATOS

El Ecuador no cuenta con una Ley de Protección de Datos Personales que regule su tratamiento. Sin embargo, la falta de reglamentación no implica la inexistencia de un marco jurídico mínimo que proteja al individuo y a sus datos (El Universo 2018). Así pues, la Constitución de la República del Ecuador, en su artículo 66 numeral 19, dentro del Capítulo Sexto relativo a los Derechos de Libertad, reconoce y garantiza a las personas: "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley."

De tal manera que el país reconoce la protección de datos personales como un derecho constitucional. Existe una obligación por parte del Estado, sus instituciones y todas aquellas compañías o personas que procesen datos, de protegerlos y recolectarlos, previa autorización expresa de su titular, siempre que su tratamiento se realice en cualquier parte del territorio nacional. A pesar de este mandato constitucional, el derecho no ha podido ser plenamente garantizado, debido a la falta de normativa técnica, y también a la falta de que la autoridad competente sea provista de capacidad para controlar y sancionar su uso inadecuado. Así se discutió en la "Mesa de Diálogo acerca del Órgano Rector en Acceso a la Información y Protección de Datos", organizada por Fundamedios, donde se analizó la importancia de contar con un organismo autónomo, capaz de regular estos temas de manera independiente (DINARDAP 2020).

Debido a esta coyuntura, hay que realizar un análisis de la situación actual de la protección de datos en el Ecuador; así como, entender cuál es la percepción del ciudadano común sobre este tema. Además, para determinar la relevancia del tratamiento de datos personales en la vida de los individuos, es conveniente revisar qué es un dato personal y qué significa inteligencia artificial, en paralelo con la normativa que se aplica en otras jurisdicciones.

Todos estos logros nos permitirán obtener una mejor perspectiva, para entender por qué es necesario contar con una regulación que permita procesar los datos de manera adecuada, a fin de proteger los derechos del ciudadano e incentivar el desarrollo tecnológico.

TOLERANCIA EN EL PROCESAMIENTO DE DATOS

La falta de regulación y control en esta materia ha permitido que el acceso a los datos personales de los ecuatorianos se convierta en una práctica tolerada; la cual, hasta cierto punto ha sido justificada por comerciantes y vendedores, quienes utilizan estos datos so pretexto de mejorar sus ofertas, segmentar sus preferencias, tratar al cliente por su nombre e inclusive ofrecer descuentos y ventajas accesibles desde su

ubicación (Lavin 2006). Sin embargo, ¿cuán importante es cuidar esta información? ¿realmente podría afectar a una persona que un tercero recolecte los datos de su localización, estilo de compra o preferencias si, en definitiva, con esa información le brindan un mejor servicio y le permiten acceder de manera más rápida a sus preferencias?

Para una sociedad que está acostumbrada a proporcionar su nombre, número de cédula, teléfono, dirección y correo electrónico cada vez que realiza una compra[1]; o que, entrega su documento de identidad para entrar a cualquier edificio u oficina, ¿el uso de sus datos personales es realmente percibido como una violación a la privacidad?, ¿se podría afirmar que el ecuatoriano considera estos actos como un atentado a su derecho constitucional de disponer y decidir sobre los datos de carácter personal o, por el contrario, lo considera como algo normal y beneficioso?

La sociedad ecuatoriana todavía no es consciente del uso que se puede dar a esta información. Llenar formularios y aportar datos sobre su etnia, tipo de sangre o nivel de ingresos económicos para simplemente obtener una tarjeta de crédito o inscribirse en un sorteo, se ve como algo aceptable y muchas veces necesario, para tener acceso a determinados servicios o calificar para ciertos créditos. Si un tercero solicita esta información es porque así lo requiere o porque forma parte de la "política" de dicha institución.

Son tantas las acciones y omisiones que se estarían cometiendo a la hora de procesar datos de carácter personal, que no es cuantificable el mal manejo que se hace de una base de datos o de la transferencia de los mismos. Sin embargo, cuesta afirmar que este mal manejo sea producto de una mala intención; cuando, en la sociedad ecuatoriana, de hecho, prima el desconocimiento.

Por este motivo es fundamental fomentar una cultura de respeto a los datos personales, y habrá que empezar por educar sobre qué significa un dato y cuáles serían las reales afectaciones que podrían ocurrir en caso de su mal manejo. El construir este marco de respeto, no solo motivará que exista un procesamiento responsable de datos, sino que va a evitar que casos como el de "Novaestrat" se vuelvan a repetir.

1. Caso Novaestrat

La consultora y analista de datos ecuatoriana Novaestrat, alojaba en Miami un servidor con datos personales y sensibles de aproximadamente 20 millones de ecuatorianos (Yeung 2019). Esta base incluía información de 7 millones de menores de edad y otros tantos millones de personas fallecidas. A pesar de que en la actualidad existen casi 17 millones de habitantes en Ecuador, la consultora poseía datos de 20 millones de ciudadanos, debido a que almacenaba la información de difuntos sin justificación alguna.

Los datos que habrían sido develados correspondían a nombres completos, fecha y ciudad de nacimiento, dirección domiciliaria, correo electrónico, cédula de identidad, Registro Único de Contribuyentes, información del Instituto Ecuatoriano de Seguridad Social, estado de cuenta bancaria, balances crediticios y tipo de crédito al que el ciudadano tenía acceso (Yeung 2019). Si bien hubo una respuesta inmediata por parte del Ministerio de Telecomunicaciones, los datos ya fueron expuestos y posiblemente vendidos, sin poder cuantificar el perjuicio que se generó para todos los ecuatorianos.

El representante legal de la compañía fue detenido para investigaciones por un presunto delito de violación a la intimidad, sin que hasta el momento exista una fórmula de juicio o sentencia en el caso (Vanessa Silva, 2019). Hasta la fecha, Novaestrat Compañía de Responsabilidad Limitada consta como una empresa activa, que ha cumplido sus obligaciones societarias y de existencia legal, de acuerdo con la información contenida en la página de la Superintendencia de Compañías, y únicamente figura un nuevo representante legal.

Debido a este sonado escándalo, que inclusive tuvo resonancia a nivel internacional, el 19 de septiembre de 2019, el Presidente del República Lenin Moreno

1 Así lo exige el Sistema de Rentas Internas.

remitió el Proyecto de Ley Orgánica de Protección de Datos Personales a la Asamblea Nacional (GK 2019). Al momento, el Proyecto se encuentra pendiente de primer debate**,** de acuerdo con la información de la página de la Asamblea Nacional.

Este Proyecto fue desarrollado en base a las necesidades y la realidad ecuatoriana; y fue inspirado en el Reglamento General a la Protección de Datos adoptado por la Unión Europa en 2016, que entró en vigor el 2018, de cuya evolución se hablará a continuación.

2. Normativa relativa a la protección de datos

Las leyes adoptadas por la Unión Europea (UE) para la protección de datos personales han sido siempre un marco de referencia para varias legislaciones, incluidas las de países latinoamericanos, tal como se lee en la página web oficial de la Autoridad de Protección de Datos de la Unión Europea (European Data Protection Supervisor 2018). Los valores comunes contenidos en los Tratados de Integración fomentaron la libre circulación de mercancías y personas (Unión Europea 2020). Este objetivo común, fuertemente perseguido por los Estados Miembros, implicó un gran movimiento de datos entre los países integrantes. El Parlamento y Consejo de la Unión Europea**,** preocupados por esta realidad, deciden emitir el 24 de octubre de 1995, la Directiva 95/46/EC, relativa a la "Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos".

Esta Directiva fue formulada en una época donde el número de usuarios de internet a nivel mundial alcanzaba apenas el 0.4% de toda la población existente (Internet World Stats 2020). Por esta razón, si bien la Directiva era innovadora para su tiempo, pues definía conceptos y regulaba de manera adecuada la transferencia de datos; pronto quedaría obsoleta por la rápida evolución de la tecnología, por cuyas dinámicas aparecieron sistemas y funcionalidades que se consideraban imposibles para ese momento.

En el año 2012, la Comisión Europea propuso una reforma a la Directiva 95/46/EC para reforzar los derechos de privacidad en línea e impulsar la economía digital de Europa. Desde entonces se empezó a trabajar en el Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés).

El 12 de marzo de 2014, el Parlamento de la Unión Europea apoyó la implementación del RGPD con 621 votos a favor. Dicho Parlamento, el Consejo y la Comisión Europea llegaron a un acuerdo sobre el RGPD el 15 de diciembre de 2015, cuando fue finalmente publicado bajo la forma de regulación oficial el 27 de abril de 2016 (European Data Protection Supervisor, 2018). Sin embargo, el Art. 99 del RGPD, relativo a su entrada en vigor y aplicación, estableció que: "1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea"; y, "2. Será aplicable a partir del 25 de mayo de 2018." De manera que, si bien la norma fue aprobada en el año 2016, esta empezó a ser aplicable dos años después de su publicación.

El legislador europeo otorgó estos dos años de plazo para que las instituciones, organizaciones y empresas de los Países Miembros se pusieran a tono con las disposiciones contenidas en el Reglamento, a fin de que elaboraran protocolos, auditaran la cantidad de datos que manejan y eliminaran todos los componentes previos que no fueran absolutamente necesarios. La entrada en vigor del RGPD no solo puso en vilo a toda Europa, sino que exigió que países de fuera de la Unión que procesen datos de ciudadanos europeos acoplaran sus estándares a los exigidos por el RGPD (Goddard 2017, 704).

Todo esto se debió a la disposición de territorialidad contenida en el artículo 3 del RGPD que señala que "el Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, **independientemente de que el tratamiento tenga lugar en la Unión o no**"[2]. Por lo tanto, la normativa sería aplicable incluso fuera de los Estados Miembros, de modo que muchos países han tenido que revisar su legislación y adaptar su normativa al estándar de la Unión Europea (Albrecht 2016, 287).

2 La negrilla es de la autora.

Tal es el caso del Ecuador, que ha utilizado al RGPD como marco de referencia para generar su propia legislación nacional, y se ha adaptado a parámetros internacionales que le permitan calificarse como un país que garantice un nivel adecuado de protección de datos personales.

Al momento, el Proyecto de Ley Orgánica de Protección de Datos del Ecuador sigue siendo ampliamente impulsado para su discusión y aprobación; y se encuentra a cargo de la Comisión de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral de la Asamblea Nacional (PrensaEC 2020).

3. ¿Qué se entiende por dato personal y cuándo es objeto de protección?

Ahora bien, es preciso entender qué es un dato personal y cuáles son los parámetros que permiten determinar si cierta información es susceptible de protección o no.

El RGPD clasifica a los datos en cuatro categorías más una categoría especial, mientras que el Proyecto de Ley ecuatoriano los divide en seis tipos. Si bien las definiciones dadas por el RGPD y el Proyecto difieren en número, estas son muy cercanas en contenido y guardan las mismas características.

Art. 4. Reglamento General de Protección de Datos	Art. 5 Proyecto de Ley de Protección de Datos ecuatoriana
"Datos personales: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;	**"Datos personales:** Dato que identifica o hace identificable a una persona natural, directa o indirectamente, en el presente o futuro. Los datos inocuos, metadatos o fragmentos de datos que identifiquen o hagan identificable al ser humano, forma parte de este concepto.
Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;	**Dato genético:** Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobra la fisiología o salud de un individuo; generalmente se analizan a través de las biológicas."
Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;	**Dato biométrico:** Dato personal único obtenido a partir de un tratamiento técnico-específico, relativo a las características físicas, fisiológicas o conductuales de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros.

Art. 4. Reglamento General de Protección de Datos	Art. 5 Proyecto de Ley de Protección de Datos ecuatoriana
Art. 9 Categorías especiales de datos personales: Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.	**Datos sensibles:** Se consideran datos sensibles los relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos humanos o la dignidad e integridad de las personas. La Autoridad de Protección de Datos podrá determinar otras categorías de datos sensibles.
Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud".	El Proyecto de Ley de Protección de Datos incluye a los datos relativos a la salud dentro de datos sensibles.
El RGPD no define los datos personales crediticios de manera específica, sin embargo, su concepto calza dentro de la definición de datos personales.	**Datos personales crediticios:** Datos que integran el comportamiento de personas naturales para analizar su capacidad de pago y financiera.
El RGPD no define los datos personales registrables de manera específica, sin embargo, su concepto calza dentro de la definición de datos personales.	**Datos personales registrables**: Datos personales que**,** conforme al ordenamiento jurídico**,** deben estar contenidos en Registros Públicos.

Del cuadro comparativo se observa que la legislación ecuatoriana agregó dos definiciones adicionales al RGPD, el dato crediticio y el dato registrable. Dichos conceptos nacieron como un reflejo de la realidad ecuatoriana, donde todos los ciudadanos mayores de edad poseen un perfil crediticio que es ampliamente manejado y consultado por instituciones bancarias y de crédito en el Ecuador. Esta información identifica directamente a su titular, razón por la cual es necesario que exista un control y supervisión respecto al acceso de los datos personales crediticios.

De igual forma, en el Ecuador existe una gran cantidad de información que posee el gobierno de sus ciudadanos, almacenada en registros públicos por mandato de ley. A este tipo de dato se lo conoce como dato personal registrable, el cual, a pesar de ser personal, puede ser procesado y almacenado siempre y cuando exista una disposición legal que así lo permita.

De todas estas definiciones se destacan ciertas características comunes, que son las que limitan el alcance de un dato personal y le permiten diferenciarse del resto de información que no cuenta con protección.

Persona natural*:* Para que un dato sea protegido, el generador de dicha información debe ser una persona

natural. Los datos que provienen de una persona jurídica no son materia de esta legislación.

El objetivo final de la protección de datos personales es proteger al individuo y limitar el uso de la información que emana de este. Esta información podría llegar a perjudicar particularmente su libertad y dignidad según sea su contenido. La Protección de Datos no pretende regular la información o datos todo tipo, al contrario, se circunscribe únicamente al ser humano (Voss, 2016).

Identificada o identificable de manera directa o indirecta: si la cantidad de información contenida en el dato o conjunto de datos permite identificar de manera directa o indirecta al titular de la información, por medios razonables, entonces se convierte en dato personal. Puede ser que el dato procesado no contenga el nombre del individuo o que su contenido corresponda a un dato aislado; mas, si permite identificar al individuo entonces es materia de protección (Sophos 2011).

Identificación sensible: Si los datos identifican a una persona de manera directa o indirecta, entonces son objeto de protección. Sin embargo, existen ciertos datos que podrían poner en riesgo o pueden atentar contra derechos humanos, la dignidad o integridad de las personas, y que pueden ser usados como base de discriminación. Por definición**,** estos datos no deben ser procesados, debido al alto riesgo que podría existir en caso de un mal uso. Sin embargo, el legislador contempla excepciones específicas en las que se autoriza su tratamiento.

Con estas definiciones, se entiende de mejor manera qué es un dato personal y se deja por sentado que no solamente los datos que evidentemente identifican a la persona, como el nombre, la edad o la fecha de nacimiento, pueden ser considerados como objeto de protección. Al contrario, existe una gran cantidad de información, como la geolocalización, afiliación política o historia clínica que, aun siendo anonimizadas, podrían asociarse al individuo con facilidad.

Con estas aclaraciones, nos preguntamos, ¿cuál es el verdadero riesgo de que estos datos sean procesados?, ¿realmente existe una afectación a los derechos del individuo, si se permite que terceros procesen su información personal?

Cada día es más frecuente que decisiones que afectan al individuo de manera directa sean tomadas en función de sus datos personales. El poder de decisión ya no recae en la deliberación de los seres humanos, sino que la decisión es tomada por Inteligencia Artificial. Máquinas y algoritmos son ahora los encargados de decidir si es que alguien puede acceder a un préstamo o ayuda financiera. Además, seleccionan de manera independiente a lo que un individuo puede acceder, ya sea en sus búsquedas o en sus redes sociales, de acuerdo con los datos personales recolectados por estos (Matheson 2017).

Estas decisiones**,** generalmente no son apelables y los algoritmos que las toman son prácticamente ininteligibles. El ciudadano común no tiene por qué tener un conocimiento avanzado sobre cómo funciona la inteligencia artificial o cómo se creó el algoritmo. Por este motivo existen cada vez más discusiones respecto de la necesidad de que tanto los algoritmos como sus resultados sean más transparentes y puedan ser corregidos en caso de un error. Al Estado le corresponde establecer regulaciones y derechos mínimos que deban ser respetados por quienes procesan los datos, para que exista un buen uso de estos y se proteja el bienestar de los individuos (Smith 2016).

4. ¿Qué se entiende por Inteligencia Artificial?

El concepto fue acuñado en 1956 por John McCarthy, y se desarrollaron tres acepciones, de acuerdo con el enfoque que se le dio al término. La primera acepción se enfocaba en el comportamiento de la máquina y se entendía a la Inteligencia Artificial como "programar computadoras para comportarse de una manera inteligente o "astuta". El enfoque cognitivo hacía referencia a "intentar recrear el proceso de razonamiento humano para entender la mente de mejor manera" y, finalmente, el enfoque robótico no se limitaba a la programación, sino que se refería a la acción de "construir la máquina" (Trappl 1985).

Una definición más actual señala a la Inteligencia Artificial como "la capacidad de las computadoras

o programas para operar de manera que se cree que imitan los procesos de pensamiento humano, como el razonamiento y el aprendizaje" (Saffiong 2020). Justamente esta capacidad es la que ha permitido que la máquina reemplace ciertas funciones que antes eran realizadas por el ser humano. El resultado ha sido que las decisiones sean mucho más precisas y tomadas en cuestión de segundos o fracciones de estos.

Gracias a la Inteligencia Artificial, las máquinas pueden a emular el pensamiento humano. Pero ¿cómo aprenden las computadoras? ¿cómo adquieren la capacidad de razonar?

Hay dos técnicas que forman parte de la Inteligencia Artificial y permiten "enseñarle a pensar" a la máquina, el Aprendizaje Automático o *Machine Learning* y el Aprendizaje Profundo o *Deep Learning*.

El Aprendizaje Automático es la capacidad que tiene la computadora de aprender nuevas habilidades sin ser programada continuamente. Consiste en un conjunto de técnicas y herramientas que permiten que la computadora interactúe activamente con datos acumulados, a través de un conjunto de algoritmos (Borgese, Newman y Norris 2019). Tales datos provienen generalmente del procesamiento de datos personales. El *Big Data* es utilizado para entrenar a los algoritmos que van a ser utilizados en el *Machine Learning*. Con este entrenamiento, el sistema puede razonar de manera independiente del aporte humano y puede por sí solo crear nuevos algoritmos (DATATILSYNET 2018).

Es decir, con el Aprendizaje Automático se le enseña a la computadora a "pensar" de cierta manera, gracias al uso de algoritmos. Los algoritmos fueron previamente entrenados para generar experiencia y enseñarle a la computadora cómo actuar. Una vez que la computadora ha aprendido a identificar los mismos patrones, tendencias y relación de datos, se le puede aportar nuevos datos para que por sí sola, ya sin entrenamiento ni ayuda humana, pueda actuar de la forma en la que se le enseñó, respecto de esos nuevos datos.

Por su parte, el Aprendizaje Profundo, que es una derivación del Aprendizaje Automático, permite a la computadora construir conceptos complejos a partir de conceptos simples. Consiste en capas anidadas de nodos interconectados. Después de cada nueva experiencia, aprende al reacomodar las conexiones entre los nodos (Banafa 2016). Estas capas procuran asimilarse al uso de redes neuronales, que crean conexiones y generan mayor conocimiento.

Para que la máquina "aprenda" necesita una exuberante cantidad de información que es recolectada a través del procesamiento de datos, incluidos los personales. La máquina los analiza y empieza a identificar patrones y similitudes. Estos patrones son los que se utilizan para enseñar a la máquina, en base a los cuales crea modelos que le permitirán actuar de tal o cual forma, si es que encuentra información similar a la previamente aprendida.

Por ejemplo, una aplicación de música recolecta grandes cantidades de información de sus usuarios, especialmente su selección musical. Esta información es procesada para identificar patrones de conducta similares y arroja como resultado un modelo de conducta identificable, con ellos se alimenta el algoritmo para que aprenda a distinguir dicho modelo. Una vez que la maquina ha aprendido a identificarlo, puede programarse para que, cuando identifique que el usuario concuerda con el patrón enseñado, le prediga que canción podría ser compatible con sus gustos, tras un análisis de su historial musical. Así, con la Inteligencia Artificial la máquina aprende de toda la información que recibe, se ajusta a la nueva información y responde casi de manera inmediata, sin que exista intervención humana (DATATILSYNET 2018).

Si bien estas innovaciones pueden facilitarnos la vida, ¿Hasta qué punto podemos aceptar que "recomendaciones" de este tipo puedan ser legítimas y consideradas de buena fe? ¿Qué evita que la información obtenida no sea direccionada por intereses propios de la empresa? ¿Cómo se puede estar seguro de que la recomendación a la que un individuo tiene acceso solo se apega a su gusto musical y no es el resultado de una sugerencia patrocinada sin su aprobación? Si algo tan intrascendente como las preferencias musicales de un individuo pueden ser analizadas y luego influenciadas por estos algoritmos, ¿Qué garantiza que no se utilice

el mismo tipo de comportamiento cuando se trate de elecciones presidenciales, cuando se solicite una visa o se aplique a asistencia social gubernamental?

Con el análisis anterior no se pretende desconectar a la sociedad de los avances tecnológicos. Sería descabellado pensar que puede detenerse el progreso de la tecnología y oponerse de manera absoluta al tratamiento de datos. Una actitud como esta solo retrasaría investigaciones y convertiría al individuo o a la sociedad respectiva en analfabetos digitales, y limitaría su acceso a posibles curas para enfermedades catastróficas como el cáncer, o a desarrollos tecnológicos tan increíbles como prótesis robóticas en interacción con el cuerpo. No obstante, tampoco se puede aceptar un tratamiento irresponsable o irrestricto de los datos. Resulta fundamental que exista una legislación que permita garantizar un apropiado tratamiento de datos personales, y que respete los derechos del ciudadano de conocer y decidir el fin que se va a dar a dicha información. Es indispensable que se reduzca al mínimo la cantidad de datos recolectados, y que se los guarde únicamente por el tiempo estrictamente necesario. Cada vez crece más la necesidad de llegar a un equilibrio, donde las empresas y el gobierno puedan utilizar los datos personales de manera responsable, de forma que respeten los derechos de sus usuarios.

CONCLUSIONES Y RECOMENDACIONES

El uso y alcance que se puede dar a los datos es todavía desconocido, por lo que es adecuado contar con una normativa que controle su procesamiento y que prevea futuros desmedros o abusos; tal y como lo han hecho un gran porcentaje de países, incluidos varios estados latinoamericanos (Leite 2016).

El Ecuador no puede ser ajeno a una realidad en la que ya está inmerso, de modo que se vuelve primordial adoptar medidas de protección que limiten la recolección, el procesamiento y el uso indiscriminado de datos personales. Resulta fundamental fomentar el uso responsable de datos personales. Se debe evitar que terceros utilicen esta información de forma inadecuada y que, como consecuencia, se desconozca el propósito que se les da. Es importante no olvidar que la información que almacena una computadora, muchas veces es sensible, y que debe ser procesada con absoluto cuidado, debido a las graves consecuencias que puede traer la divulgación de temas delicados como preferencias sexuales, religiosas, políticas, entre otras.

El Proyecto de Ley de Protección de Datos Personales es, sin lugar a dudas, una norma necesaria y fundamental que no solo permitirá alcanzar los estándares internacionales adecuados que facilitará recibir y transferir información de manera segura, sino que coadyuvará a estar a tono con los avances que la tecnología genera.

El contar con un marco jurídico adecuado no solo permitirá que el país cumpla con sus deberes internacionales, sino que otorgará seguridad jurídica a empresas que pretenden hacer negocios digitales en el país, y, así, promoverá un mayor desarrollo económico. Además, el incentivar que la Inteligencia Artificial sea utilizada de una manera transparente permitirá que los avances tecnológicos sean de amplio beneficio para el ser humano. Se ha demostrado que el hecho de enseñar a pensar a una máquina puede traer desarrollos y ventajas que antes eran inimaginables. Sin embargo, no podemos olvidar que los derechos del ciudadano están por sobre cualquier descubrimiento e interés particulares de las empresas.

Finalmente, hay que educar a la población respecto a la importancia de conservar y limitar el acceso a sus datos personales, dado que esta información define al ciudadano. Es necesario inculcar el valor de estos, para que el individuo tome decisiones en libertad, sin verse influenciado por recomendaciones o sugerencias que responden a intereses de terceros. El ciudadano debe poder ejercer su derecho de conocer el uso de sus datos y pedir su eliminación de forma absolutamente voluntaria.

BIBLIOGRAFÍA

Albrecht, Jan Philipp. 2016. "How the GDPR will change the World". *European Data Protection Law Review*, Volume 2 (2016), Issue 3, Pages 287 – 9. DOI https://doi.org/10.21552/EDPL/2016/3/4

Banafa A. 2016. "Qué es el aprendizaje profundo?". *OpenMind BBVA*, 7-VIII-2016. Consultado el 7-III-2020. https://www.bbvaopenmind.com/tecnologia/mundo-digital/que-es-el-aprendijaze-profundo/

Borgese A., Newman J. Y A. Norris. 2019. "AI, Machine Learning & Big Data 2019". *Australia, Global Legal Group*. 41. Acceso el 7-IV-2020. https://iapp.org/media/pdf/resource_center/ai_machinelearning_bigdata_2019_gli.pdf

DINARDAP. "Dinardap participó en la Mesa de Diálogo acerca del Órgano Rector en Acceso a la Información y Protección de Datos". Consultado el 25-IV-2020. https://www.dinardap.gob.ec/dinardap-participo-en-la-mesa-de-dialogo-acerca-del-organo-rector-en-acceso-a-la-informacion-y-proteccion-de-datos/

Directiva 95/46/EC del Parlamento Europeo y del Consejo de 24 de octubre de 1195 relativa a la "Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos. Consultado el 30-III-2020. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=EN

El Universo. "Lorena Naranjo: Protección de la información es un derecho", El Universo, 29-IV-2018. Consultado el 2-V-2020. https://www.eluniverso.com/noticias/2018/04/29/nota/6736137/proteccion-informacion-es-derecho

European Data Protection Supervisor. 2018. "The History of the General Data Protection Regulation". Consultado el 23-II-2020. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

GK. 2019. "La información de millones de ecuatorianos fue expuesta en línea". GK, 17-IX-2019. Consultado el 6-II-2020. https://gk.city/2019/09/16/filtran-datos-de-ecuatorianos/

Goddard, Michelle. 2017. "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact". *International Journal of Market Research* Vol. 59 Issue 6: 703-5. DOI: 10.2501/IJMR-2017-050

Internet World Stats. 2020. "Internet Growth Stadistics". Consultado el 24-III-2020. https://www.internetworldstats.com/emarketing.htm

Lavin, Marilyn. 2006. "Cookies: What do consumers know and what can they learn? *Journal of Targetting, Measurement and Analysis for Marketing* Vol 14, 4, 279-288. Consultado el 24-III-2020. https://link.springer.com/content/pdf/10.1057/palgrave.jt.5740188.pdf

Leite, R. 2016. "Data Protection Law in Latin América–an overview". *International Association of Privacy Professionals*, Consultado el 30-III-2020. file:///C:/Users/brivera/Documents/PERSONAL/Propuesta%20Articulo/Data%20protection%20laws%20in%20Latin%20America%20–%20an%20overview.pdf

Mathenson, Lee. 2017. "WP29 releases guidelines on profiling under the GDPR". *International Association of Privacy Professionals*, 18-X-2017. Consultado el 25-III-2020. https://iapp.org/news/a/wp29-releases-guidelines-on-profiling-under-the-gdpr/

Saffiong, K.. 2020. "Artificial Intelligence Applied Computer Science", CSI 3106 *African Virtual University*, 14. Consultado el 12/III/2020 .https://oer.avu.org/bitstream/handle/123456789/669/CSI%203106_EN%20Artificial%20Intelligence1.pdf?sequence=1&isAllowed=y

Servicio de Rentas Internas. "Facturación física, formatos". Consultado el 18-III-2020. https://www.sri.gob.ec/web/guest/facturacion-fisica

Silva, Vanessa. 2019. "La Policía arresta a gerente de Novaestrat, por supuesta filtración de datos de ecuatorianos", 16 de septiembre de 2019. Consultado el 7-II-2020. https://www.elcomercio.com/actualidad/policia-arresto-gerente-novaestrat-filtracion.html

Smith, Lauren. 2016. "Algorithmic transparency: Examining from within and without", 28-I-2016. Consultado el 25-II-2020. https://iapp.org/news/a/algorithmic-transparency-examining-from-within-and-without/

Sophos White Paper. 2011. "Protecting personally identifiable information: What data is at risk at what you can do about it". *Sophos White Paper*, octubre 2011. Consultado el 23-III-2020. https://www.sophos.com/es-es/medialibrary/PDFs/other/sophosprotectingPII.pdf

Trappl, R. 1985. "Impact of Artificial Intelligence". *Elsevier Science Publishers B.V*. 6-7. Consultado el 30-III-2020. http://pure.iiasa.ac.at/id/eprint/2758/1/XB-86-001.pdf#page=13

Unión Europea. 2020. "Tratados de la EU". Consultado el 23-IV-2020 https://europa.eu/european-union/law/treaties_es

Voss, W. Gregory. 2016. "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting". *The Business Lawyer*, 72(1), 221-234. doi:10.2307/26419118

Yeung, Jessie. 2019. "Almost entire population of Ecuador has data leaked". CNN WORLD, 17-IX-2019. Consultado el 16-II-2020. https://edition.cnn.com/2019/09/17/americas/ecuador-data-leak-intl-hnk-scli/index.html"

DATATILSYNET. 2018. "Artificial intelligence an privacy", The Norwegian Data Protection Authority, 6 -7. Consultado el 30-IV-2020. https://iapp.org/media/pdf/resource_center/ai-and-privacy.pdf

VIGILANCIA MASIVA
Conflicto entre seguridad nacional, derecho a la protección de datos personales y vida privada

MASS SURVEILLANCE
Conflict between national security, right to data protection and private life

VIGILÂNCIA MASIVA
Conflito entre segurança nacional, direito a proteção de dados pessoais e vida privada

*Pablo Espinosa**

Recibido: 15/05/2020
Aprobado: 20/06/2020

Resumen

La revolución tecnológica ha generado profundos cambios sociales y ha convertido a los datos en materia prima de herramientas para incontables fines. Los programas de vigilancia masiva permiten la captura indiscriminada de enormes cantidades de datos, razón por la cual, su uso con fines de investigación y prevención criminal es cada vez mayor en todo el mundo. Estas actividades constituyen una injerencia en la vida privada y en los derechos de las personas. En este artículo, se analizan las garantías para que dicha intromisión sea legítima y justificada, así como la ponderación entre vida privada, protección de datos y seguridad nacional.

Palabras clave: Derecho a la vida privada; Programas vigilancia masiva; Big Brother; Big data; Defensa Nacional

Summary

Technological revolution has brought deep social changes and has turned data into a tool with countless uses. Mass surveillance programs allow the indiscriminate capture of enormous amounts of data. Therefore, the use of this data for criminal investigation and prevention purposes has globally expanded. These activities are a violation of people's private life and rights. This article analyzes the guarantees for such interference to be legitimate and justified as well as the balance among private life, data protection and national security.

Key words: Right to privacy; Mass surveillance programs; Big Brother; Big data; Homeland Defense

Resumo

A revolução tecnológica gerou profundas mudanças sociais convertendo os dados em matéria prima como ferramentas para incontáveis fins. Os programas de vigilância massivas permitem a captura indiscriminada de enormes quantidades de dados, razão porque, seu uso com fins de pesquisa e prevenção criminal é cada vez maior em todo o mundo. Estas atividades constituem uma ingerência na vida privada e nos direitos das pessoas. Nesse artigo, se analisam as garantias para que esta intromissão seja legítima e justificada; assim como a ponderação entre a vida privada, proteção de dados e segurança nacional.

Palavras chave: Direito à vida privada; Programas vigilância massiva; Big Brother; Big data; Defesa Nacional

* Máster en Justicia Criminal por la Universidad Carlos III de Madrid. LL.M. Máster en Derecho con Especialización en Litigación Oral por California Western School of Law. Experto en Derecho y Compliance TIC, por la Universidad Camilo José Cela. Doctorando Investigador en el Programa de Derecho Penal y Nuevas Tecnologías, de la Universidad Carlos III de Madrid. Correo electrónico: pabloespinosap@outlook.com

INTRODUCCIÓN

Desde fines de los años 90 del siglo XX hasta el día de hoy, vivimos en una sociedad inmersa en una revolución digital de las tecnologías de la información y las comunicaciones (TIC), con las que se crea una base para el libre flujo de información, ideas y conocimientos en todo el planeta. En esta sociedad, conocida como Sociedad de la Información, la información pasa a convertirse en el factor decisivo de la organización económica, como consecuencia de la nueva tecnología digital, y genera cambios profundos en todos los ámbitos de la vida: culturales, políticos y sociales; sobre todo, aquellos determinados por la transformación de las condiciones en las interacciones entre los miembros la sociedad.

No es novedad que el vivir en la época de las nuevas tecnologías, en los años dorados del internet y la conectividad, nos ha llevado a estar abocados a vivir rodeados de información. Hoy en día facilitamos nuestra información casi en todo momento, entregamos datos cuando mantenemos una conversación con alguien mediante teléfono o mediante alguna aplicación de mensajería, lo hacemos al compartir publicaciones en las redes sociales; también cuando queremos adquirir algún producto o servicio en línea, y, en esos casos, no dudamos en facilitar nuestros datos bancarios y nuestros datos de domicilio, para que el bien deseado llegue a nuestras manos.

Pero este punto no es lo realmente relevante, pues el transferir nuestros datos es una acción que no podemos más que realizar, sin lo cual nos mantendríamos en una especie de aislamiento informacional. La cuestión es: ¿cuál es el tratamiento que se hace con esos datos? y ¿para qué fines las empresas privadas requieren esta información de nosotros? A partir de estas preguntas entra en juego el concepto de vigilancia masiva, en base al cual nos damos cuenta de que los datos que aportamos sirven para algo más que para simples fines comerciales.

En este contexto nacen los sistemas masivos de datos (*Big Data*), sistemas capaces de recoger, almacenar y tratar grandes cantidades de datos procedentes del entorno de las personas. El poder sobre la información que confieren estos nuevos sistemas ha sido el causante de que grandes empresas privadas, así como instituciones públicas, entre las que se encuentran las agencias de inteligencia de los Estados, los hayan situado en el centro de su inversión. Como consecuencia, se han creado centros de datos, en los que, según el tipo de entidad que los dirija, el uso de los datos obtenidos y analizados se puede destinar, entre otros, a fines u objetivos culturales, administrativos, o, como nos interesa aquí, para la investigación y la defensa estatal.

Y es que en un contexto social donde está presente la amenaza del terrorismo y la criminalidad, tanto nacional como internacional, en la práctica, la totalidad de los países del mundo y las agencias de inteligencia de los grandes Estados han aprovechado las ventajas que ofrecen estos sistemas de tratamiento masivo de datos para desarrollar los llamados "programas de vigilancia masiva" (PVM en adelante), sobre los que hablaremos más adelante y cuyo propósito inicial es la defensa de la seguridad nacional. No obstante, dado el secretismo y la escasa información que existe sobre ellos, así como la insuficiente regulación establecida a nivel nacional, estos programas entrañan numerosos riesgos para los derechos más elementales de los ciudadanos.

Por vigilancia masiva debemos entender aquella red de vigilancia que se ejerce sobre una importante parte de la población. Puede ser llevada a cabo por Estados, empresas privadas u organizaciones no gubernamentales, aunque el Estado suele ser el principal responsable. Las empresas, en ocasiones, desarrollan la vigilancia en nombre del Estado, aunque también pueden hacerlo por iniciativa propia. De acuerdo a las leyes de cada nación y sus sistemas judiciales, la legalidad, alcance y el tipo de vigilancia masiva varía. Puesto que existen muchos tipos de vigilancia, desde la que se da a conversaciones telefónicas, pasando por las imágenes que pueden ser captadas por un circuito cerrado o la utilización de los datos que hemos facilitado a una empresa, hasta las muy novedosas

aplicaciones de rastreo que incluso se pretenden normalizar por la actual pandemia ocasionada por la Covid-19. La utilización de esta información puede suponer un choque contra el derecho a la privacidad, intimidad, derecho a la protección de datos y al secreto de las comunicaciones.

Las preguntas más importantes son: ¿cómo afecta esta práctica a nuestra vida? y ¿estamos realmente sufriendo una violación del derecho a la vida privada al facilitar información? Hemos empezado a ser realmente conscientes, tanto la sociedad como los órganos jurisdiccionales, de la posible vulneración de nuestros derechos y de que estábamos siendo más vigilados de lo que pensábamos. A partir de las filtraciones de Edward Snowden, los tribunales han empezado a pronunciarse, aunque no siempre en el sentido que se podría intuir o en aquel que valoraba más el derecho a la intimidad que las posibles acciones terroristas. También se han llegado a desarrollar normativas completas (tratados, acuerdos y protocolos) en relación a la transmisión de informaciones entre países, o de empresas a gobiernos; como es el caso de los distintos acuerdos en relación al tratamiento de los nombres de pasajeros[1] y del Reglamento General de Protección de Datos (en adelante RGPD), que es una manera de dotar de ciertas garantías y de acabar por introducir la legitimidad de ciertas formas de vigilancia masiva.

VIGILANCIA MASIVA

1- Origen de la vigilancia masiva

El uso de tecnología para recopilar información no es reciente. La agencia de inteligencia de Reino Unido, en la II Guerra Mundial, se valió de Alan Turing y su equipo de capacidad innovadora informática para descifrar los códigos encriptados de los alemanes (Oppenheimer 2013). De modo que el uso de la tecnología como medio de vigilancia y espionaje, se podría rastrear desde su creación y uso en objetivos militares.

Los inicios de la vigilancia a gran escala se pueden remontar a los años 40, con la suscripción del Acuerdo entre Estados Unidos y Reino Unido, llamado UKUSA, que se firmó entre estos dos países en 1946. Esta alianza entre agencias de seguridad e inteligencia estadounidenses y británicas, se amplió en los años siguientes incorporando otros países, en especial Australia, Canadá y Nueva Zelanda, países con los cuales se formó lo que se denominó el *Five eyes*, grupo que duró más de 70 años en la confidencialidad y que llevó a cabo vigilancia de índole militar y diplomática en el marco de la guerra fría. Cada uno de sus Estados integrantes realizaba actividades de interceptación, colección, análisis y descifrado en su respectiva jurisdicción geográfica y luego la compartía con los demás. También se estableció en el acuerdo un centro de operaciones donde se reunirían los operativos de las agencias de inteligencia (González Porras 2015).

La Agencia Nacional de Seguridad estadounidense (en adelante NSA, por sus siglas en inglés) fue creada en 1952 por el presidente Harry Truman, teniendo como precedente la *Black Chamber*, que operó de 1919 a 1929. En 1960, el *Federal Bureau of Investigation* (FBI, por sus siglas en inglés), bajo el mandato de J. Edgar Hooveer, se dedicó a la recolección de información privada de dirigentes sindicales, políticos y activistas, por medio de escuchas telefónicas. A raíz del escándalo conocido como *Watergate,* se condujo una investigación por parte del Senado de los Estados Unidos, en la cual se llegó a la conclusión de que las agencias de inteligencia habían vulnerado los derechos constitucionales de los ciudadanos norteamericanos. Pero recién en 1978, después que se revelara esta conclusión, se creó la Ley de Vigilancia Extranjera, por la que se organizó un tribunal para administrar solicitudes de vigilancia, especialmente de vigilancia interna hacia extranjeros.

1 Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

2. Vigilancia masiva en la actualidad

Después del trágico atentado terrorista del 11 de septiembre de 2001, el Consejo de Seguridad de la ONU señaló que estos ataques son una amenaza para la paz y seguridad globales y adoptó la Resolución 1373 (2001), que motivaba a los Estados a tomar parte de la lucha contra el terrorismo con medidas para la prevención de comisión de actos terroristas, y les daba libertad para realizar operaciones subrepticias, que han originado vulneraciones a garantías fundamentales (Serra Cristóbal 2015).

Muchos Estados aprobaron leyes con la finalidad de legitimar estas intervenciones, como Reino Unido, que aprobó la ley antiterrorista en 2001, y Estados Unidos, que aprobó la Ley Patriota, que trajo muchas dudas sobre la constitucionalidad del uso excesivo de medidas adoptadas para la prevención de ataques. Muchos otros países crearon programas antiterroristas y permitieron el uso de espacios aéreos para el traslado y entrega de terroristas capturados a Estados Unidos.

Uno de los escándalos más recientes que atrajo la atención de la prensa y de la sociedad en general hacia la vigilancia masiva, fue la revelación de información por Edward Snowden. Este ex agente de la NSA hizo revelaciones al diario *The Guardian*, que publicó la primera de las denuncias sobre la recolección de información de usuarios de la compañía americana de telefonía celular Verizon por parte de la NSA (Greenwald 2013).

Estas noticias fueron polémicas y tuvieron relevancia de carácter global. Snowden empezó a ser perseguido por el gobierno estadounidense y se emitió una orden de extradición en su contra. Él fundamentó sus denuncias en documentos que extrajo de la NSA de manera clandestina, y se convirtió en fugitivo internacional. El gobierno de los Estados Unidos justificó su accionar por considerarlo necesario para proteger la vida de los ciudadanos, y con sustento en la *Protect America Act* (PAA) (González Porras 2015). Se puede decir que estas revelaciones abrieron los ojos de la sociedad en lo relativo al poder de la vigilancia masiva en internet y por medio de la tecnología en general, ya que se iniciaron litigios internacionales y demandas contra el gobierno estadounidense y el gobierno británico.

3. Principales programas de vigilancia masiva

Una de las principales características de estos programas es su confidencialidad estricta, lo que dificulta que se tenga información sobre el alcance real de estos programas. Así, lo poco que se conoce hasta el momento es la información que se ha logrado filtrar.

La información filtrada por Edward Snowden en sus entrevistas a los periódicos *The Guardian* y *The Washington Post*, mostraba el programa que utiliza la NSA desde el 2007 para esta vigilancia. Este programa de la NSA, llamado en clave PRISM, fue legalizado en los Estados Unidos a través de la Ley de Servicios de Inteligencia Extranjera (*Foreign Intelligence Service Act*, FISA), y es capaz, según las diapositivas de la NSA filtradas, de acceder e interceptar información de los *Data Centers* de empresas tan conocidas como Google, Microsoft, Facebook, Skype o Apple. Concretamente, es capaz de interceptar correos electrónicos, videos, fotos, chats (de video y voz), transferencias de archivos, notificaciones de actividad (cuando se ha conectado o desconectado una persona) y detalles de las redes sociales de los usuarios (Gonzáles Monje 2017). Y existen indicios claros de que el *Government Communications Headquarters* (GCHQ, por su siglas en inglés) de Reino Unido, tuvo acceso a este programa desde el año 2010.

Menos conocido, pero igual de intrusivo, es el PVM, conocido como XKeyScore (Mejías Alonso 2018), también de la NSA, que es mucho más complejo que el PRISM. El PVM es capaz no solo de interceptar y recolectar datos como lo hace el PRISM, sino también de almacenar información proveniente de otros sistemas y programas, con usos varios como: espionaje de diplomáticos y líderes políticos extranjeros; interceptación de datos de satélites y datos procedentes de servicios de telecomunicaciones, como Vodafone. Este programa permite, además de acceder al contenido de los correos electrónicos, leer el contenido íntegro de todos los mensajes y chats de Facebook. Para lograrlo,

el agente solo necesita introducir el nombre del usuario objetivo y un intervalo de fechas.

Por otro lado, el GCHQ británico controla el PVM TEMPORA, una versión mejorada del XkeyScore, capaz de nutrirse de toda la información que pasa a través de fibra óptica en diferentes países y en todo el tráfico telefónico. Tiene las mismas funcionalidades (grabaciones de llamadas, contenido de correos electrónicos, chats de Facebook, historial de acceso a páginas web de cualquier usuario) que los anteriores programas, pero a mayor nivel. Este programa no discrimina objetivos, es decir que almacena información de usuarios sin ningún fundamento de sospecha previo, y se ejecuta sin la necesidad de que se imponga alguna orden o permiso gubernamental (Gonzáles Porras 2015). La ley que autoriza la utilización de estos programas en Reino Unido es la *Regulation of Investigatory Powers Act 2000*.

No se puede dejar de mencionar a ECHELON. Este PVM es considerado por algunos expertos como la mayor red de espionaje de la historia de PVM. Cuerda Arnau describe su funcionamiento:

> "En sus numerosas estaciones de interceptación captura las conversaciones y, después, cada estación selecciona dicha información pasada por el tamiz de lo que podría denominarse «diccionarios de palabras clave» (sospechosas o peligrosas) diseñados por los Estados en función de los concretos intereses que cada uno pueda tener en ese particular momento. Posteriormente, la referida información o bien se transcribe y registra o bien se elimina, que es, al parecer, lo que sucede con la mayoría ante las dificultades para hacer frente a su almacenamiento y procesamiento" (Cuerda Arnau 2013,109).

4. Vulneración a los derechos fundamentales

Al respecto de este sistema, el Parlamento Europeo ya realizó un informe redactado por una Comisión temporal[2] que fue creada para investigarlo. El informe señaló que sólo se permitirían intervenciones de espionaje en los casos en que estuviere en peligro la seguridad nacional, y siempre y cuando esta injerencia a la privacidad se halle prevista en el derecho interno del país, sea accesible su conocimiento a todas las personas y se indique claramente en qué circunstancias se realizaría. Estas operaciones deben ser equilibradas, razón por lo que la cual se debe establecer una simetría con los derechos en juego, de acuerdo a la jurisprudencia del Tribunal Europeo de Derechos Humanos (en adelante TEDH). Estas medidas no sólo deben ser necesarias, sino también estar legitimadas y ser compatibles con los derechos fundamentales, de modo que deben observarse con medios de control estatales previamente designados (González Monje 2017).

Una vez revisada esta información parcial sobre el alcance de estos programas, parece lógico que el "Informe Moraes", de la Unión Europea (en adelante UE), haya determinado que estos programas son una vulneración sistemática de los derechos fundamentales de todos los ciudadanos, y que no es posible garantizar, ni a las instituciones públicas de la UE, ni a sus ciudadanos, que su seguridad o intimidad informática puedan ser protegidas de los ataques de intrusos bien equipados. Además, pone en entredicho que los fines de estas operaciones de vigilancia masiva respondan únicamente al fin de la lucha contra el terrorismo y la defensa de la seguridad nacional, y les llega a atribuir otros fines como el "espionaje político y económico", o la elaboración de perfiles de ciudadanos, a quienes trata como potenciales sospechosos[3]. En consecuencia, este informe concluye con la petición a las autoridades de los Estados Unidos y a los Estados miembros de la UE, que decidan la prohibición inmediata de las actividades de vigilancia masiva generalizada.

La amplia gama de programas documentada por diferentes Estados, y con diferentes propósitos, que abarcan desde espionaje de actividad en línea en tiempo real hasta descifrado de claves de transacciones bancarias,

2 *Informe Moraes* de 21-II-2014. En: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7- 2014-0139+0+DOC+XML+V0//ES

3 En este sentido, este informe señala en su conclusión 12ª, que estos programas "constituyen un paso más hacia el establecimiento de un estado preventivo de pleno derecho".

es muy preocupante, ya que nos muestra la dimensión a la que han llegado los Estados partícipes en el uso de estos programas. Esta vigilancia debe ser vista como una injerencia altamente intrusiva a la privacidad, que revela la tendencia al aumento de redes y programas de vigilancia masiva, incluso más allá de las fronteras de los países, en gran parte debido a los acuerdos que realizan los Estados, en los que se benefician mutuamente por la información recolectada unos de otros.

Se cree que es imposible que cualquier agencia pueda ser capaz de leer y analizar toda la información, correos electrónicos, metadatos y llamadas que colectan con su actividad a lo largo del mundo. Pero, sin duda provocan en la sociedad una sensación de vigilancia extrema, que causa que las personas se sientan todo el tiempo controladas, para así asegurar la reducción en el cometimiento de delitos y actos terroristas. Aunque este proceder puede ser muy efectivo para aumentar el cumplimiento de la ley o prevenir actos terroristas, es una vulneración grave a las garantías fundamentales de una sociedad democrática.

5. Derecho a la protección de datos personales y vigilancia masiva

El primer gran desafío en cuanto a tratamiento de datos personales, por su dimensión y primicia, ocurrió en 1935. Cuando el presidente norteamericano Franklin D. Roosevelt aprobó la Ley de Seguridad Social (en inglés, *Social Security Act*), con el objetivo de alcanzar los beneficios propios del Estado del bienestar, mediante el tratamiento de datos. Mediante esta ley se procuraba la actualización de los datos personales que concernían a la clase trabajadora, por ejemplo, en materia de pensiones.

El TEDH ha manifestado que la protección de los datos personales está dentro del ámbito de aplicación del artículo 8 de la Convención Europea de Derechos Humanos (en adelante, CEDH). En el Caso S. y Marper contra Reino Unido, señala que el simple acto de memorizar datos de la vida privada de una persona es una injerencia al artículo 8 del convenio, se utilice o no esta información en un futuro. También resalta que, para determinar si la información de carácter personal conservada por las autoridades hace que entre en juego algún aspecto de la vida privada, el Tribunal tendrá debidamente en cuenta el contexto particular en el que ha sido recogida y conservada la información, el carácter de los datos consignados, la manera en la que son utilizados y tratados, así como los resultados que pueden extraerse de ellos[4].

El Tribunal indica que información como huellas dactilares y ADN son datos personales, ya que se refieren a personas identificables. También considera como injerencia la conservación de datos relativos a la vida personal de un individuo por parte de una autoridad, así sea con motivos de seguridad nacional. De la misma forma, se entienden como datos personales: la compilación o análisis de datos médicos, llamadas telefónicas, localización por GPS, movimientos de tren y avión en bases de datos policiales, y antecedentes de un individuo (Salamanca Aguado 2014).

El derecho a la protección de datos personales está reconocido también en la Constitución ecuatoriana, en el artículo 66 numeral 19, en el que se reconoce y garantiza a las personas este derecho. Sin embargo, hasta el día de hoy no se ha logrado trasponer este mandato constitucional en legislación sobre este ámbito, siendo hasta el momento el intento más prometedor el Proyecto de Ley Orgánica de Protección de Datos Personales, presentado el 19 de septiembre de 2019. Este proyecto de ley lleva una clara y acertada inspiración en el RGPD europeo, que hasta ahora es la más vanguardista legislación a nivel mundial en protección de datos personales.

La gran concreción a nivel normativo y práctico del derecho de protección de datos personales, se materializa en el Reglamento General de Protección de Datos 679/ 2016 de la Unión Europea. Éste tiene como finalidad establecer un nivel coherente de protección de los datos de las personas físicas en toda la UE, así como proporcionar seguridad jurídica y transparencia a los operadores económicos. Se atribuye la titularidad del derecho únicamente a las personas físicas, independientemente de su nacionalidad o lugar de residencia.

4 Sentencia TEDH de 4-XII-2008, S. y Marper c. UK. Sentencia de 4-XII-2008, apartados (en adelante, *apdo*.) 67-69.

Se define como dato personal en el RGPD, art. 4.1:

> "toda información sobre una persona física identificada o identificable; se considerará persona identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular un identificador, como por ej. un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

De esta manera, la información recolectada por los PVM está plenamente considerada como datos personales. Una aportación muy valiosa que hace el RGPD es la concreción de los principios relativos al tratamiento de datos, los cuales son transversales a todo manejo de datos personales. Los datos deberán ser tratados de manera lícita, leal y transparente en relación con el interesado (principio de licitud, lealtad y transparencia); serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines (principio de limitación de la finalidad); deberán ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (principio de minimización de datos). También deberán ser exactos y actualizados (principio de exactitud); mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales (principio de limitación del plazo de conservación); tratados de tal manera que se garantice una seguridad adecuada de los datos personales (principio de integridad y confidencialidad); y el responsable y encargado del tratamiento serán responsables del tratamiento y capaces de demostrarlo (principio de responsabilidad proactiva)[5].

Estos principios deberán ser mandatorios en todo tipo de tratamiento de datos, como confirma la Directiva (UE) 2016/680, de protección de las personas en cuanto al tratamiento de sus datos personales por las autoridades policiales y de justicia penal, y a la libre circulación de estos datos. Esta es la normativa legal que se aplicaría en los PVM, que señala los principios concretados por el RGPD, como obligatorios en el tratamiento de datos con fines de investigación criminal.

El *Big Data* es uno de los métodos mediante los cuales los PMV recopilan información y la analizan. Lamentablemente, el RGPD, más que proporcionar soluciones específicas para abordar los problemas planteados por el nuevo paradigma de gestión de la información, sólo es un punto de partida para una reflexión más amplia (Mantelero 2017). El marco regulador de la Unión Europea, a partir de las primeras leyes sobre protección de datos, se basa en el presupuesto según el cual las personas son capaces de conocer los métodos y los fines del tratamiento y de entenderlos en términos de posibles consecuencias. Sin embargo, en el contexto del *Big data*, la complejidad del tratamiento agrava los límites ya conocidos a la autodeterminación real de la persona. Así mismo, existen dificultades en la aplicación de los principios de minimización y de finalidad del tratamiento.

Los programas de vigilancia masiva claramente realizarían un tratamiento de datos personales. Por este motivo, y a primera vista, se pensaba que el RGPD sería un freno al uso de estos programas. Pero no ha sido así, ya que el reglamento, dentro de su ámbito de aplicación material, excluye el tratamiento por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención[6].

Así las cosas, nuevamente se ve limitada la protección a derechos como el derecho a la intimidad o a la protección de datos personales, sobre la ponderación con otros como la seguridad nacional; por lo tanto, es pertinente revisar el choque, justificación y legitimación a nivel internacional de esta limitación.

5 Para más información sobre el Reglamento Europeo General de Protección de Datos, ver: Rebollo Delgado L. y M. Serrano Pérez. 2019. *Manual de Protección de Datos*. Madrid: Dykinson.

6 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27-IV-2016 relativo a la protección de las personas físicas respecto al tratamiento de datos personales y a la libre circulación de estos datos, artículo 2.2.

EL DERECHO A LA VIDA PRIVADA FRENTE A LA DEFENSA DE LA SEGURIDAD NACIONAL

1. Derecho a la vida privada

El derecho a la vida privada se halla regulado en el artículo 12 de la Declaración Universal de Derechos Humanos, el cual establece que: "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Este derecho está reconocido también en instrumentos internacionales regionales que Ecuador ha adoptado, como la Declaración Americana de los Derechos y Deberes del hombre de 1948 y la Convención Americana sobre Derechos Humanos de 1969, donde se señala el derecho de las personas a la protección de una vida privada sin injerencias arbitrarias o abusivas.

La Constitución del Ecuador reconoce y protege el derecho a la intimidad en la vida personal y familiar, así como el derecho a la inviolabilidad y al secreto de la correspondencia física o virtual, en su artículo 66 numerales 20 y 21 respectivamente. En el mismo sentido protector de este derecho, la legislación ecuatoriana tipifica la violación a la intimidad en el art. 178 del Código Orgánico Integral Penal (en adelante COIP), dentro de los delitos contra el derecho a la intimidad personal y familiar. En este precepto se sanciona toda conducta que implique el acceso, difusión o divulgación no consentida de información privada, y se castiga de manera amplia conductas que afecten a la intimidad y privacidad.

En el art. 476 del COIP, dentro de las actuaciones especiales de investigación, se enmarca la interceptación de las comunicaciones o datos informáticos. Hay que señalar que esta diligencia solamente podrá efectuarse previa solicitud de la Fiscalía, después de otorgada la orden judicial, cuando existan indicios relevantes a los fines de la investigación. Su alcance serán las comunicaciones del investigado o procesado y de aquellos con los cuales éste se comunique. Para solicitar la interceptación por parte de un fiscal, debe existir una investigación previa o una instrucción fiscal. Aquí se empiezan a notar las diferencias entre esta diligencia de investigación y los PVM, ya que estos efectúan interceptaciones generales sin previos indicios o investigaciones específicas, no dentro de una instrucción fiscal, sino buscando indicios de delitos que muchas veces aún no se han cometido, como ataques terroristas. Además, su alcance no está limitado a ciertas personas investigadas identificadas, sino que se da una interceptación de telecomunicaciones de carácter amplio, masivo y general.

De igual manera, en los requisitos señalados en el art. 476, se señala el plazo de duración de la interceptación, así como la necesaria autorización judicial correspondiente para la ampliación de esta medida; diferenciándose del secretismo y la falta de especificación temporal de utilización de los PVM.

Por su parte, el CEDH regula en su artículo 8 el derecho al respeto de la vida privada y familiar. Y manifiesta que:

> "no podrá haber injerencia de la autoridad en el ejercicio de este derecho sino en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás" (CEDH, artículo 8, apartado 2).

El TEDH ha interpretado que los términos "vida privada" y "correspondencia" abarcan las comunicaciones por teléfono[7], fax o correo electrónico. Incluye también aquí toda la información derivada del

7 STEDH de 29-VI-2006, Weber y Saravia c. Alemania. Apdo. 77.

seguimiento del uso personal de internet, el almacenamiento en un registro secreto y la comunicación de datos relativos a la vida privada de un individuo (Salamanca Aguado 2014).

Por otro lado, en el apartado 2° vemos que, en cuanto no nos encontremos ante un derecho absoluto, se permiten injerencias o limitaciones sobre este derecho, que aquí se regulan mediante una serie de requisitos con los que cualquier injerencia sobre este derecho quedaría justificada. Estos requisitos son: la previsión por la ley de la injerencia; que dicha injerencia responda a un fin legítimo (por ejemplo, la seguridad nacional); y, por último, que sea necesaria en una sociedad democrática para conseguir tal fin.

2. Gravedad de la injerencia de los PVM sobre el derecho a la vida privada

En cuanto a la gravedad de la injerencia, la podemos medir según dos criterios:

1. La calidad del ámbito material afectado por la intromisión. Donde el cuerpo, el domicilio y las comunicaciones personales conforman una intimidad de calidad máxima. Mientras los datos o información privada del sujeto que más relación guardan con el exterior constituyen una intimidad de calidad mínima.

2. El medio por el cual se accede al conocimiento de los datos o informaciones. Mas, al haber una amplia variedad de medios, la gravedad de la injerencia dependerá del carácter ocasional o permanente de la vigilancia, y de que ella se dirija contra persona determinada o contra un grupo; o que sea visible o se desarrolle subrepticiamente, de suerte que pasa inadvertida para el interesado.

En base a estos dos criterios, podemos determinar que los PVM producen una injerencia en el derecho a la intimidad de los ciudadanos con un grado de lesividad máximo, toda vez que, con estos programas, se puede acceder a datos estrechamente vinculados con el libre desenvolvimiento de la personalidad.

Respecto al argumento de que mucha de la información recopilada por los PVM nunca llegará a ser examinada, debemos traer a colación la Sentencia del Tribunal Europeo de Derechos Humanos (en adelante, STEDH) de 29 de junio de 2006, Weber y Saravia c. Alemania, en cuyo apartado 78º, el tribunal señala que la mera existencia de una legislación que permita un sistema para el monitoreo secreto de las comunicaciones conlleva una amenaza de vigilancia para todos aquellos a quienes se les pueda aplicar tal medida. Esta amenaza necesariamente afecta a la libertad de comunicación entre los usuarios y, por lo tanto, equivale a una injerencia en el ejercicio de los derechos recogidos en el art. 8 de la CEDH. Este fenómeno se encuentra ligado al "efecto panóptico", por el cual un poder es capaz de imponer conductas al conjunto de la población a partir de la idea de que estamos siendo vigilados, de acuerdo con la teoría del panóptico de Michel Foucault[8].

Otro argumento esgrimido por los Estados a la hora de atenuar el grado de injerencia de estos programas de vigilancia en la intimidad de los ciudadanos, es que algunos programas de vigilancia únicamente almacenan metadatos, sobre la información recolectada, y no su contenido propiamente dicho. Al respecto, la European Digital Rights, argumentó ante el TEDH, en el caso Big Brother Watch vs. United Kingdom, que, en la actualidad, los metadatos pueden proporcionar una imagen más detallada e íntima sobre la persona investigada, así como sobre las personas con las que se relaciona, que el propio contenido de la información. En suma, esta agrupación internacional concluye que no se debe otorgar un grado diferente de protección a los datos personales, basados en la distinción irrelevante entre el contenido y los metadatos[9]. Por tanto, los metadatos aportan información más rápida, precisa, fácil de analizar y mucho más operativa sobre cada individuo y su entorno social, especialmente para vigilancias prospectivas y sin destinatario específico (De

8 Para más información sobre el tema, ver en web: https://psicologiaymente.com/social/teoria-panoptico-michel-foucault
9 Apdo. 301º de la STEDH, de 13-IX-2018, Big Brother Watch vs. The United Kingdom.

Prada 2016). Se recalca así el grado máximo de injerencia de los PVM sobre los derechos de las personas.

3. Defensa de la seguridad nacional

No existe un consenso a nivel internacional sobre lo que constituye y abarca el concepto de Seguridad Nacional; debido a factores como la delimitación del término "seguridad", que es extensamente amplio, o la idea de amenaza, que genera la necesidad de seguridad y está en constante evolución. Este concepto respondía, en un principio, a amenazas en términos militares, pero que, con el paso del tiempo, han dado lugar a nuevas formas de amenazas no militarizadas, como pueden ser el ciberterrorismo o los problemas medioambientales. La Seguridad Nacional es una materia de competencia nacional, por lo que la UE no tiene competencia regulatoria alguna sobre ella, sino únicamente en la seguridad interna de la UE[10].

Parece claro que, entre los fines de la Seguridad Nacional, se encuentra la lucha contra el terrorismo, la criminalidad y delincuencia organizada. No obstante, debemos reiterar que uno de los principales aspectos controvertidos y criticados de los PVM es el uso de estos con propósitos distintos a los amparados por la Seguridad Nacional, ya sean fines políticos, económicos, de espionaje de autoridades, o, incluso, un fin delictual, como puede ser la extorsión a personas de interés (grandes empresarios, autoridades).

A la luz del precedente análisis, vemos que la defensa de la seguridad nacional responde a un interés general, el bienestar común de toda una sociedad, un derecho colectivo. Parece pues razonable que éste prevalezca frente a una serie de requisitos asociados al derecho a la intimidad, toda vez que éste responde a un interés individual. Como se desprende del apartado segundo del art. 8 de la CEDH, al señalar a la seguridad nacional como uno de los fines legítimos que justifica la injerencia en este derecho. Pero, en el caso de los PVM, donde su utilización aparentemente produce una violación del derecho a la intimidad de forma sistemática y masiva, no se puede hablar de un interés individual en conflicto con un interés general, sino de un conflicto entre dos intereses generales o colectivos.

No obstante, y pese a dicho enfrentamiento entre estos dos intereses, vemos que la seguridad y la intimidad o privacidad, no son conceptos antagónicos. Desde los Principios de Siracusa sobre las disposiciones de limitación y derogación del Pacto Internacional de Derechos Civiles y Políticos, en su cláusula 22º, se dispone que "la violación sistemática de los derechos humanos socaba la seguridad nacional y puede poner peligro la paz y la seguridad internacional". Vemos, por tanto, que la seguridad y el derecho fundamental a la intimidad y privacidad, se encuentran relacionados y son dependientes.

Llegados a este punto, dar una respuesta clara y genérica para este dilema es complicado. Por tal motivo, analizaremos cada uno de los requisitos que deben cumplir los Estados en la aplicación y utilización de los PVM, para que cualquier injerencia de estos sobre el derecho a la vida privada y familiar de los ciudadanos sea lo menos lesiva y pueda justificarse de acuerdo con lo estipulado en la CEDH. En este sentido, nos será de mucha ayuda la reciente STEDH de 13 de septiembre de 2018, Big Brother Watch vs. The United Kingdom, en la que nos apoyaremos más adelante para dar una respuesta a la compatibilización de ambos derechos.

4. Compatibilidad de los programas de vigilancia masiva con el CEDH

En el actual marco constitucional ecuatoriano se resuelve el conflicto entre derechos a partir de la ponderación de derechos, es decir: sopesar los principios que han entrado en colisión en el caso concreto para determinar cuál de ellos tiene un peso mayor en las circunstancias específicas y, por tanto, cuál de ellos determina la solución para el caso concreto. El núcleo de la ponderación consiste en una relación que se denomina ley de la ponderación y que se puede formular así: "Cuando mayor sea el grado de no satisfacción o restricción de uno de los principios, tanto mayor deberá ser el grado de la importancia de

10 Extraído del postulado de la seguridad nacional y la inteligencia del Informe sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU. Informe Moraes", p. 52.

la satisfacción del otro"[11]. Existe una tendencia de la Corte Constitucional ecuatoriana, en sus sentencias, a aplicar el principio de proporcionalidad como criterio para examinar la constitucionalidad de las intervenciones en los derechos fundamentales, y la ponderación como método para la solución de conflictos entre derechos, valores o principios.

Esta se diferencia del TEDH, en que el tribunal europeo concentra, *prima facie,* su valoración en revisar si se ha vulnerado o no algún derecho protegido por el convenio. Sin embargo, el TEDH ha dejado claro en su jurisprudencia que no todos los derechos son absolutos. Por este motivo, utiliza también la ponderación y especialmente la proporcionalidad para verificar si la injerencia en un derecho es apegada a los requisitos señalados por el convenio. Las pruebas de necesidad y proporcionalidad son aplicadas por el TEDH dentro del requisito para legitimar una injerencia, que analizaremos posteriormente, conocido como "medida necesaria en una sociedad democrática".

Como hemos analizado, los PVM son un instrumento de control de la población en general, con un alto grado de injerencia en el derecho a la intimidad de todos los ciudadanos, y, por lo tanto, afectan a un interés colectivo. No obstante, parece razonable que, en situaciones donde la seguridad del Estado se encuentra comprometida, cuando existe peligro para la nación, su territorio o la independencia política, se puedan emplear estos programas como fórmula de defensa y prevención contra todas las amenazas que hemos señalado.

En todo caso, cualquier tipo de excepción que permita la disminución de garantías fundamentales en un Estado, como, en este caso, el acopio de información que consta en el apartado segundo del art. 8 de la CEDH, debe ser informada, de acuerdo de una serie de principios y conforme a la legalidad, a fin de evitar siempre cualquier limitación arbitraria, imprevisible o irrazonable.

De acuerdo con estas premisas, la visión del TEDH sobre los PVM se aleja de la afirmación de que cualquier sistema de interceptación masiva constituye una violación de la CEDH. Esta visión queda reflejada en la STEDH Big Brother Watch vs. United Kingdom, que establece, conforme al apartado segundo del art. 8 de la CEDH, los principios y requisitos a los que se deben someter estos programas, para salvaguardar y respetar los derechos fundamentales garantizados por el convenio. Para que la injerencia ocasionada por los PVM en el derecho a la intimidad del art. 8 de la CEDH quede justificada, deben concurrir los requisitos que se detallan en el siguiente apartado.

REQUISITOS PARA JUSTIFICAR LA INJERENCIA

1. Finalidad u objetivo legítimo

La seguridad nacional es uno de los objetivos legítimos recogidos en el apartado segundo del art. 8 de la CEDH. Al respecto, el tribunal europeo entiende que las autoridades nacionales disfrutan de un amplio margen a la hora de lograr tal objetivo. Señala que los PVM entran dentro de ese margen de apreciación y que constituyen un mecanismo adecuado en la consecución de este objetivo, porque en la actualidad las amenazas que atentan contra la seguridad de los Estados, como el terrorismo, el narcotráfico, la trata de seres humanos o ciertos delitos informáticos, se encuentran agravadas por el desarrollo tecnológico. Esta situación facilita la comisión delictiva dada la amplia variedad de canales y medios de comunicación (alto grado de imprevisibilidad), y, en consecuencia, dificulta su prevención y detención[12].

Esta prerrogativa dada a los Estados a la hora de poder elegir el mecanismo con el cual garantizar este objetivo legítimo, se ve contrarrestado por un mayor

11 Sentencia N°. 002-009-SAN-CC (Caso 0055-089-AN) del 2-IV-2009.
12 En este sentido, ver el apdo. 106 de su STEDH de 29-VI-2006, Weber y Saravia c. Alemania.

número de requisitos que hagan lo suficientemente previsibles estos regímenes de interceptación, de tal forma que se minimice el riesgo de abusos de poder por parte de los Estados.

2. Previsión legal

La previsión legal va a ser fundamental a la hora de que los Estados utilicen los PVM. La utilización de estos programas de interceptación masiva deberá estar regulada en el ordenamiento jurídico del país en una norma con fuerza de ley. Además, dicha ley deberá ser accesible y previsible para las personas interesadas en cuanto a sus efectos.

En cuanto a la previsibilidad, su grado de exigencia en el contexto de los PVM, dada su naturaleza subrepticia, no puede ser el mismo que en otros campos. En este sentido, el TEDH reitera, en esta sentencia, lo dispuesto en el apartado 93 de la STEDH Weber y Saravia c. Alemania; allí señala que la previsibilidad no significa que una persona pueda prever cuándo es probable que las autoridades intercepten sus comunicaciones, para adaptar su comportamiento en consecuencia, sino que para evitar la arbitrariedad y el abuso del Estado, lo esencial es que la legislación nacional sea lo suficientemente clara para dar a los ciudadanos una indicación adecuada de las circunstancias y las condiciones en que las autoridades están facultadas para recurrir a tales medidas. A la luz de esta jurisprudencia, el Tribunal reseña los seis requisitos mínimos que debe haber en la ley para la interceptación de comunicaciones en procesos penales, que son también de aplicación para estos programas, para así poder evitar abusos de poder.

En un análisis de la reiterada jurisprudencia sobre la intervención de las comunicaciones individuales, el TEDH ha establecido garantías mínimas que deben estar definidas en la ley, como son: la naturaleza de las infracciones que puedan dar lugar a una orden de interceptación, la especificación de las categorías de personas susceptibles de sufrir vigilancia telefónica judicial, los límites a la duración de la ejecución de la medida, el procedimiento que deberá seguirse para el uso y conservación de los datos obtenidos, las precauciones necesarias para comunicar los datos a otras organizaciones y las circunstancias en las que se puede o se debe realizar el borrado o la destrucción de la información.

Adicionalmente, para los PVM también se tendrán en cuenta los acuerdos para supervisar la aplicación de las medidas de vigilancia secreta, los mecanismos de notificación y los recursos previstos a tal efecto[13].

3. Medida necesaria en una sociedad democrática para lograr el fin legítimo

Por último, la utilización de los PVM, además de responder a un fin legítimo y estar prevista en una ley con las características anteriormente descritas, debe constituir una medida necesaria en una sociedad democrática para lograr tal fin, en este caso la seguridad nacional.

Por tanto, con miras a determinar si se cumple este requisito, se deberá hacer un test de necesidad y otro de proporcionalidad (Salamanca Aguado 2014). Es decir que se deberá establecer que los medios sean necesarios para lograr el fin, y que, de entre las medidas disponibles para dicho fin, la elegida sea la menos perjudicial para el derecho a la intimidad.

En la STEDH Big Brother Watch vs. The United Kingdom, el tribunal, tras analizar una gran cantidad de material e informes, concluyó que la intercepción masiva de información, que incluye los PVM, es necesaria y proporcional en una sociedad democrática, en base a los argumentos que se expondrán a continuación[14].

Dadas las circunstancias sociales actuales, la sociedad se ve gravemente amenazada por terroristas y grupos criminales que cuentan con medios cada vez más sofisticados para llevar a cabo sus fines ilícitos y que escapan al control de los medios de detección tradicionales. Además, como ya se dijo, la utilización

13 Apdo. 308 de la STEDH Big Brother Watch v. The United Kingdom.
14 Información extraída del apdo. 384º de la STEDH Big Brother Watch vs. UK.

de internet proporciona acceso a una amplia variedad de canales de comunicación, de manera que se hace impredecible la ruta de comunicación empleada para preparar los actos delictivos.

No existe otra alternativa o alternativas que logren equipararse al poder y efectividad de intercepción del que se dispone por medio de los PVM, para lograr la preservación de la seguridad nacional.

Aunque se reconocen los riesgos para los derechos individuales de los ciudadanos que entraña la intercepción masiva, se ha reconocido la utilidad de estos programas para las operaciones de seguridad. Dado que permite a los Estados adoptar un enfoque proactivo frente al problema, así como detectar focos de peligro hasta ahora desconocidos.

En cuanto al régimen de intercambio de información entre las agencias de inteligencia, el TEDH entiende que, dada la particular complejidad inherente a las redes terroristas globales, es proporcional y legítimo el intercambio de información entre las agencias. Este permite prevenir la perpetración de actos violentos que ponen en peligro la vida de miles de ciudadanos inocentes. Pero esto es así siempre que lo prevea el legislador nacional y que se cumpla con las garantías en caso de abuso por parte de las autoridades, de forma que este modo de actuar sea plenamente compatible con el art. 8 de la CEDH.

CONCLUSIONES

- La utilización de los programas de vigilancia masiva por las agencias de inteligencia, sumada a la colaboración de las grandes empresas relacionadas con internet (Facebook, Google, Microsoft) y una mala praxis en el uso de las redes por los ciudadanos, nos han llevado a una situación en la que las autoridades pueden tener acceso a prácticamente cualquier información, inclusive datos personales sensibles. Este problema conduce, si no se adoptan las medidas y garantías necesarias, a una vulneración sistemática y masiva de un derecho tan importante para el sostenimiento del Estado de Derecho, como el derecho a la intimidad y a la vida privada de los ciudadanos.

- Ha quedado claro que tal grado de injerencia estaría justificado en aras de garantizar la defensa de la seguridad nacional. Este es, sin duda, uno de los fines de los PVM, y ello adquiere más fuerza en el contexto social actual, en el que todas las naciones del mundo se encuentran bajo amenaza terrorista y bajo el yugo de grandes organizaciones criminales. En este sentido, el desarrollo tecnológico ha facilitado la comisión de estas actividades delictivas, de modo que es necesaria la implementación y utilización de los PVM para prevenirlas y combatirlas, toda vez que los mecanismos de investigación tradicionales han resultado ser ineficaces.

- Nos encontramos en una era completamente digital, en la que el derecho al respeto a la vida privada o a la protección de datos necesitan ser entendidos de una forma completamente distinta y mucho más amplia. Hay que tener en cuenta que las injerencias que se oponen a este derecho pueden venir de otros Estados, y ésta sería posiblemente la forma más grave en la que se puede presentar tal intervención. Aunque parezcan suficientes, es necesario dotar de más garantías a todos los procesos que puedan suponer un medio para la vigilancia masiva, y asegurar que la intromisión que se va a dar en los derechos de una persona siempre será la mínima necesaria y justificada.

- A la luz de la jurisprudencia del TEDH, resulta esencial para la utilización de estos medios, una legislación nacional previsible y clara para los ciudadanos, que les proporcione suficientes garantías en los casos en que haya abusos. Este es el requisito más controvertido, dada la ausencia de una regulación armonizada al respecto. Es necesario que los aparatos legislativos de cada Estado trabajen con especial empeño en este requisito.

- En conclusión, queda un largo camino por recorrer a la hora de compatibilizar el uso de los PVM para

la defensa de la seguridad nacional con una adecuada protección de los derechos fundamentales de los ciudadanos. No obstante, y en base a los argumentos del TEDH, podemos afirmar que los PVM sí pueden ser compatibles con los derechos fundamentales de los ciudadanos, siempre que se cumpla con las exigencias y requisitos analizados. La clave será concretar el equilibrio y la cooperación, tanto entre autoridades como entre Estados, para que se respeten los derechos a la vida privada y a la protección de los datos personales.

ANEXO: ABREVIATURAS

CEDH: Convención Europea de Derechos Humanos.

DM: Decisión Marco.

FD: Fundamento de Derecho.

GCHQ: Cuartel General de Comunicaciones del Reino Unido.

LIBE: Comisión de Libertades Civiles, Justicia y Asuntos de Interior.

NSA: Agencia de Seguridad Nacional estadounidense.

PVM: Programas de vigilancia masiva.

RGPD: Reglamento General de Protección de Datos.

RIPA: Regulation of Investigatory Powers Act 2000.

STEDH: Sentencia del Tribunal Europeo de Derechos Humanos.

TEDH: Tribunal Europeo de Derechos Humanos.

UE: Unión Europea.

BIBLIOGRAFÍA

Cuerda Arnau, María. 2013. «Intervenciones prospectivas y secreto de las comunicaciones. Cuestiones pendientes». En: González Cussac y Arnau Cuerda (Eds.). *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación*. Valencia: Tirant lo Blanch.

De Prada, Eirene. 2016. «Vigilancia masiva y derecho a la privacidad». En: *Revista Jueces para la Democracia 87*: 19-27. Acceso el 5-IV-2020. http://www.juecesdemocracia.es/wp-content/uploads/2017/05/revista-87-noviembre-2016.pdf

González Monje, Alicia. 2017. «Amenazas A La Seguridad Y Privacidad: La Dificultad Del Equilibrio Perfecto». En: *Revista Europea de Derechos Fundamentales* 29: 267-94. Acceso 18-IV-2020. https://dialnet.unirioja.es/descarga/articulo/6144011.pdf.

González Porras, Andrés José. 2015. «Privacidad en internet: Los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica. La vigilancia Masiva». Tesis doctoral. Universidad de Castilla-La Mancha. https://ruidera.uclm.es/xmlui/handle/10578/10092

Greenwald, Gleen. 2013. «NSA collecting phone records of millions of Verizon customers daily». En: *The Guardian*, 5 de junio de 2013. Acceso 7-IV-2020. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Mantelero, Alessandro. 2017. «From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era». En: Taylor, L., Van der Sloot, B. y L. Floridi (Eds.). *Group Privacy: New Challenges of Data Technologies*. Springer International Publishing.

Mejías Alonso, Eva. 2018. «La vigilancia y el control de la población a través de la gestión, la conversación y la explotación de datos masivos». Tesis de posgrado. Universidad Autónoma de Barcelona. https://ddd.uab.cat/pub/trerecpro/2017/hdl_2072_271333/Treball_de_recerca_3_.pdf

Oppenheimer, Walter. 2013. «Turing, condenado por gay, recibe el perdón real 60 años después de su muerte». En: *El País*, 24-XII-2013. Acceso 10-IV-2020. https://elpais.com/internacional/2013/12/24/actualidad/1387873660_129481.html

Salamanca Aguado, Esther. 2014. «El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones». En: *Revista del Instituto Español de Estudios Estratégicos* 4: 6-32. Acceso 25-IV-2020. https://dialnet.unirioja.es/servlet/articulo?codigo=4900470

Serra Cristobal, Rosario. 2015. «La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional». En: *Revista de Derecho Político* 92: enero-abril 2015,73-118. Acceso el 2-IV-2020. https://dialnet.unirioja.es/servlet/articulo?codigo=5050060

ÍNDICE

EJERCICIO DEL DERECHO A LA LIBERTAD DE EXPRESIÓN EN INTERNET

THE EXERCISE OF THE FREEDOM OF EXPRESSION THROUGH THE INTERNET

EXERCÍCIO DO DIREITO A LIBERDADE DE EXPRESSÃO NA INTERNET

*Ginna Pasquel**

Recibido: 25/04/2020
Aprobado: 03/06/2020

Resumen

El presente ensayo analiza el derecho a la libertad de expresión a la luz de los instrumentos internacionales de derechos humanos, con relación al uso de internet como una herramienta global que conecta a diversas sociedades dentro de los ámbitos de comunicación y acceso a la información.

Teniendo en cuenta que internet es una herramienta relativamente nueva, resulta imprescindible el estudio de la libertad de expresión dentro de un marco normativo naciente, que regula las relaciones sociales que surgen a partir de dicho medio. En tal sentido, esta contribución propone elementos orientadores para la comprensión de este fenómeno, en consideración de la importancia que tiene el ejercicio del derecho a la libertad de expresión, su potencial democratizador y sus posibles restricciones en internet, dentro del margen de la legalidad, necesidad y proporcionalidad.

Palabras clave: Universalidad; Democratización; Libre acceso; Restricción de derechos; No discriminación; Regulación

Summary

This article analyses the right to freedom of expression in the light of International Human Rights instruments, in relation to the use of the Internet as a global tool connecting diverse societies within the fields of communication and access to information.

Given that the Internet is a relatively new tool, it is essential to study freedom of expression within an emerging normative framework that regulates the social relations that arise from this medium. In this sense, this article proposes guiding elements for the understanding of this phenomenon, considering the importance of the exercise of the right to freedom of expression, its democratizing potential; and, its possible restrictions on the Internet within the margin of legality, necessity and proportionality.

Key words: Universality; Democratization; Free access; Restriction of rights; Non-discrimination; Regulation

Resumo

O presente artigo analisa o direito à liberdade de expressão à luz dos instrumentos internacionais de direitos humanos, em relação ao uso da internet como uma ferramenta global que conecta a diversas sociedades dentro dos âmbitos de comunicação e acesso a informação.

Dado que a internet é uma ferramenta relativamente nova, resultado imprescindível é o estudo da liberdade de expressão dentro da estrutura normativa nascente, que regula as relações sociais que surgem a partir deste meio. Nesse sentido, este artigo propõe elementos que orientam a compreensão deste fenômeno, considerando a importância do exercício ao direito de liberdade de expressão, seu potencial democrata, e, suas possíveis restrições na internet dentro da margem da legalidade, necessidade e proporcionalidade.

Palavras chave: Universalidade; Democratizar; Livre acesso; Restrição de direitos; Não discriminação; Regulação

* Abogada por la Pontificia Universidad Católica del Ecuador; Máster en investigación con especialización en Desarrollo Sostenible de Países del Sur por la Universidad Sorbona de Paris IV; Estudios sobre libertad de expresión en el Centro Knight para el Periodismo en las Américas, de la Universidad de Texas; Experiencia profesional en Derechos Humanos, Derecho Internacional Público y Derecho Penal. Campos de en investigación dentro del Derecho y las ciencias sociales y humanas. Correo electrónico: ginnapasquelandrade@hotmail.com

Desde su inicio, internet ha servido como una herramienta de alcance global para democratizar la información y el conocimiento. A través de ella se ha estimulado la universalización de opiniones y discusiones en el entorno digital. En este sentido, la UNESCO define al internet como "un sistema global de dispositivos interconectados (…) para dar servicio a varios miles de millones de usuarios en todo el mundo" (UNESCO 2013, 2); y, tal como lo señala la Organización de Naciones Unidas (en adelante ONU), internet incluye de manera ineludible y fundamental las relaciones sociales de quienes interactúan dentro del mundo digital (Asamblea General de la ONU 2011).

Dentro de este marco, la libertad de expresión ha encontrado en internet un instrumento nunca antes visto para incrementar su ejercicio en las diversas sociedades globales, "Internet, como ningún medio de comunicación antes, ha permitido a los individuos comunicarse instantáneamente y a bajo costo, y ha tenido un impacto dramático en el periodismo y en la forma en que compartimos y accedemos a la información y las ideas" (Asamblea General de la ONU 2011). Por tal razón, internet tiene un potencial democratizador de la información y acceso universal al conocimiento.

Este carácter universal evidentemente confirma su apertura global; la cual procura y promueve un acceso e intercambio mundial de información, de forma que evita mantenerse restringido a ciertas minorías. Dentro de este marco existen amplias ventajas como recursos educativos, información diversa, flujo plural de opiniones, datos accesibles, entre muchos otros. Pero, al mismo tiempo, puede presentar problemas como: vigilancia oculta a grupos poblacionales, una aparente democratización del conocimiento sin llegar a serlo realmente, y una herramienta para el cometimiento de delitos, entre otros.

En efecto, la universalidad de internet no abarca solo su análisis tecnológico, sino también tiene una dimensión social entendida a través del análisis de uso por los usuarios. Sobre la base de este planteamiento, ¿es necesario reglamentar la utilización de internet?, ¿debe ser universal esta reglamentación? ¿Quién o quiénes tienen el deber de regular su uso? A través del desarrollo de este ensayo se responderán preguntas planteadas mediante el análisis de la naturaleza del internet, la universalidad como su característica esencial, un acercamiento al concepto del derecho a la libertad de expresión, sus características fundamentales, sus dimensiones: individual y colectiva; y su íntima relación con el uso de internet. Posteriormente se estudiará la regulación del ejercicio a la libertad de expresión dentro del marco de la utilización de internet, las normas sobre las cuales se fundan actualmente las regulaciones, y los Estados como sujetos llamados a garantizar la libertad de expresión, con ciertas restricciones a este derecho fundamentadas sobre la base del derecho internacional de los derechos humanos.

El Informe del Relator Especial sobre la promoción y protección del Derecho a la Libertad de Opinión y de Expresión declaró que Internet es uno de los instrumentos más potentes del siglo XXI para aumentar la transparencia en la conducta de los poderosos, el acceso a la información y para facilitar la participación activa de los ciudadanos en la creación de sociedades democráticas (2011, 4).

En el mismo sentido, la UNESCO ha desarrollado un concepto que gira en torno a su principal característica: la universalidad; y sobre esa base ha distinguido cuatro normas fundamentales para ejercer una regulación activa y al mismo tiempo garantista, respecto del uso de internet:

> "(i) internet está basada en los Derechos Humanos, lo que en este documento significa una "Internet libre"; (ii) internet es "Abierta"; (iii) (…) es accesible para todos; y (iv), (…) se sustenta en la Participación de múltiples partes interesadas. Las cuatro normas pueden resumirse en el acrónimo nemotécnico D – A – A – M (Derechos, Apertura, Accesibilidad, Múltiples partes interesadas)" (UNESCO 2013, 1).

Efectivamente, reconocer la característica de la universalidad en internet es fundamental para acercarnos a un marco regulatorio efectivo y coherente. Dentro de este marco, al posicionar una herramienta como universal frente a una realidad social diversa, resulta

indispensable normar su uso a la luz de las normas de derechos humanos, las cuales son de aplicación general y fundadas sobre la base del respeto a la dignidad humana. Sin embargo, el mero análisis del carácter universal de internet resulta ampliamente complejo. En efecto, mientras que internet cada vez se integra de forma más amplia a los usuarios, a cada individuo le resulta difícil calcular la integralidad mundial de esta herramienta, es decir, su atributo de ser uno solo. Cada persona realiza actividades diversas cuando utiliza esta herramienta, al percibirla de manera fragmentaria y adaptada a su propia realidad, la cual puede resultar totalmente diferente a la de otros usuarios; mientras que individualmente no da cuenta de la totalidad de internet, que, si bien es heterogénea, resulta que se encuentra interconectada.

Para comprender este fenómeno se podría plantear la metáfora del espejo. Si imaginamos que un espejo gigante se rompe en miles de pedazos, y cada persona que se halla en diferente ubicación espacial toma alguno de ellos, cada uno podrá afirmar poseer parte de este, lo cual resulta cierto; pero también es verdad que ninguno de ellos tiene el espejo integro. A través de esta metáfora es posible comprender como cada individuo percibe internet de forma individual y acorde a su realidad. Sin embargo, este punto de vista resultaría restrictivo, si es que no se considera que también internet se configura como una herramienta de amplio alcance, de manera que, una minúscula parte es aprovechada por cada usuario individual. La comprensión de la universalidad del internet es un elemento clave para analizar su regulación.

Es comprensible, entonces, que internet sea una herramienta modificadora de conductas sociales, ya que ha innovado y reformado la manera en la cual se desenvuelven las actividades humanas. En este contexto se ubica el ejercicio del derecho a la libertad de expresión a través de la utilización de una herramienta de amplio alcance global que no conoce fronteras.

La universalidad de internet presenta la necesidad, para las sociedades modernas, de estudiar y comprender el vínculo entre los derechos humanos con esta herramienta global y, más en concreto, el derecho a la libertad de expresión y a la intimidad, a la seguridad y al acceso a la información, entre otros, que resultan ser complementarios**:** "una internet que no respete a los derechos humanos estaría lejos de ser universal" (UNESCO 2013, 7). De ahí que cualquier norma que busque regular internet debe enmarcarse en la promoción y respeto a los derechos humanos. En efecto, cualquier restricción deberá cumplir con los preceptos básicos vinculados a la posible limitación de derechos fundamentales: la legalidad, la proporcionalidad y la necesidad (Center for International Media Assistance 2017)[1].

En el mismo sentido, la universalidad implica la accesibilidad de todas las personas a internet. Este acceso es absolutamente contrario a cualquier tipo de discriminación digital, carencia de acceso a las tecnologías a causa de desigualdad socioeconómica o espacial respecto de los espacios urbanos y rurales; es decir, para considerarse como tal, el acceso implica el cumplimiento de estándares mínimos para ser efectivo. En efecto, no es posible hablar de acceso si es que la población no cuenta con un nivel mínimo de infraestructura tecnológica, o si desconoce el funcionamiento de la tecnología (lo contrario sería la alfabetización tecnológica[2]), y las evidentes condiciones de conectividad favorables. También se debe evitar que ciertos espacios geográficos no tengan cubierto este servicio, como suele suceder con los medios rurales en los países emergentes como Ecuador. Es decir, "la participación es esencial a efectos del valor que Internet tiene para la paz, el desarrollo sostenible y la erradicación de la pobreza" (UNESCO 2013, 9). El acceso efectivo es, entonces, el mecanismo por el que la población obtendrá ventajas reales del internet; y, para lograr dicho acceso, esta herramienta debe ser regulada. La creación y aplicación de normas para el uso del internet

1 En este sentido, la jurisprudencia de la Corte IDH ha desarrollado este test tripartito en caso de limitación de derechos. A través del test se exige que las restricciones aplicadas a un derecho se encuentren previamente establecidas en una ley clara y precisa; que dicha restricción se produzca con el objetivo de alcanzar un fin determinado por la Convención Americana sobre Derechos Humanos; y, que sea una limitación necesaria dentro de un Estado democrático (Corte IDH 1985).

2 La UNESCO conceptualiza a la Alfabetización Mediática e Informacional como "la capacitación de los usuarios de Internet para participar de forma crítica, competente y ética" (UNESCO 2013, 8).

indudablemente pasa por el análisis del derecho a la libertad de expresión. Este ha sido reconocido ampliamente por la legislación internacional de los derechos humanos y, en consecuencia, ha sido recogido por diversos instrumentos internacionales que buscan garantizar su respeto y ejercicio.

En el Sistema Universal de Protección de los Derechos Humanos, la libertad de expresión consta en el artículo 19 de la Declaración Universal de Derechos Humanos[3], dentro de los artículos 19 y 20 del Pacto Internacional de Derechos Civiles y Políticos[4]; así como también lo incluye la UNESCO en el artículo 1 de su Constitución.[5] Asimismo, el Comité de Derechos Humanos de la ONU, organismo responsable de la verificación del cumplimiento, por parte de los Estados, del Pacto Internacional de Derechos Civiles y Políticos, ha emitido observaciones generales relativas a la libertad de expresión, como la Observación General N°. 34, donde desarrolla, de manera amplia, la naturaleza de este derecho a la luz del sistema universal de derechos humanos. De igual forma lo ha hecho la Relatoría Especial sobre el Derecho a la Libertad de Expresión. Es decir, el Sistema Universal protege ampliamente el ejercicio de este derecho a través de diversos mecanismos, tales como las normas, y el control que ejerce mediante sus organismos e instituciones creadas para tal efecto.

Dentro del marco del Sistema Interamericano, el derecho a la libertad de expresión está garantizado por el artículo 13 de la Convención Americana sobre Derechos Humanos (CADH)[6], en el artículo IV de la Declaración Americana de los Derechos y Deberes del Hombre[7], y el artículo 4 de la Carta Democrática Interamericana.[8] Asimismo, la Corte Interamericana de Derechos Humanos (Corte IDH) ha desarrollado ampliamente el contenido del derecho a la libertad de expresión a través de su jurisprudencia y, respecto

3 Declaración Universal de Derechos Humanos. Artículo 19. "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión".

4 Pacto Internacional de Derechos Civiles y Políticos. Art. 19.-
"1. Nadie podrá ser molestado a causa de sus opiniones.
2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:
a) Asegurar el respeto a los derechos o a la reputación de los demás;
b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas."
Artículo 20.-
"1. Toda propaganda en favor de la guerra estará prohibida por la ley.
2. Toda apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia estará prohibida por la ley."

5 UNESCO Constitución. Art. 1. "Este organismo fomentará el conocimiento y la comprensión mutuos de las naciones prestando su concurso a los órganos de información para las masas; a este fin, recomendará los acuerdos internacionales que estime convenientes para facilitar la libre circulación de las ideas por medio de la palabra y la imagen".

6 Convención Americana sobre Derechos Humanos, Art. 13: "Libertad de Pensamiento y de Expresión
1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:
a) el respeto a los derechos o a la reputación de los demás, o b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.
3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.
4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.
5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional."

7 Declaración Americana de los Derechos y Deberes del Hombre, artículo IV: "Toda persona tiene derecho a la libertad de investigación, de opinión y de expresión y difusión del pensamiento por cualquier medio".

8 Carta Democrática Interamericana, Artículo 4: "Son componentes fundamentales del ejercicio de la democracia la transparencia de las actividades gubernamentales, la probidad, la responsabilidad de los gobiernos en la gestión pública, el respeto por los derechos sociales y la libertad de expresión y de prensa.
La subordinación constitucional de todas las instituciones del Estado a la autoridad civil legalmente constituida y el respeto al estado de derecho de todas las entidades y sectores de la sociedad son igualmente fundamentales para la democracia."

al alcance del artículo 13 de la CADH, ha manifestado que "constituye una indicación de la importancia asignada por quienes redactaron la Convención a la necesidad de expresar y recibir cualquier tipo de información, pensamientos, opiniones e ideas" (Corte IDH 1985).

Para abordar el estudio del derecho a la libertad de expresión dentro del marco del uso de internet, es importante comprender que aquel implica no solo un derecho individual, sino también que su ejercicio coadyuva para el ejercicio de otros derechos y, además, constituye la base sobre la cual se funda un Estado democrático. La jurisprudencia interamericana ha señalado que la libertad de expresión tiene dos dimensiones, una individual y otra colectiva. La primera se refiere al derecho de cada persona para expresarse, y la segunda, también llamada dimensión social, se refiere al derecho del colectivo a recibir información y las opiniones de diferentes individuos. De esta forma, la dimensión colectiva tiene una íntima relación con el derecho al acceso a la información proveniente de una diversidad de fuentes (Corte IDH 2008)[9].

En lo concerniente a la dimensión individual, la libertad de expresión procura la independencia de la persona en la difusión de sus ideas y pensamientos a través de incontables medios. Este derecho se convierte, entonces, en un "canal", pues "tiene una función instrumental" respecto del ejercicio de otros derechos (Botero 2017, 11).

Al respecto, la jurisprudencia de la Corte IDH ha reconocido a la libertad de expresión como un derecho que garantiza a su vez la protección de otros asociados[10] y que constan en los instrumentos internacionales de derechos humanos. En este sentido, la Comisión Interamericana de Derechos Humanos ha manifestado que "se trata de un mecanismo esencial para el ejercicio del derecho a la participación, a la libertad religiosa, a la educación, a la identidad étnica o cultural y, por supuesto, a la igualdad no solo entendida como el derecho a la no discriminación, sino como el derecho al goce de ciertos derechos sociales básicos" (CIDH–Relatoría Especial para la Libertad de Expresión 2012, 4).

Por otro lado, respecto a su dimensión colectiva, una de las características principales del derecho a la libertad de expresión es que mantiene una relación ineludible con el funcionamiento de los Estados democráticos. Este hecho ha sido calificado como un rasgo estructural del sistema democrático (Corte IDH 1985). Por las razones previamente expresadas, el Sistema Interamericano de Derechos Humanos ha otorgado un rol fundamental a la libertad de expresión, a través de la creación y aplicación de un sistema único para restringir este derecho[11].

La libertad de expresión y el acceso a la información son elementos fundamentales para la democracia. En efecto, a través de ellos es posible ejercer control ciudadano sobre la gestión del Estado. De hecho, la

9 Este contenido es desarrollado también en: Corte I.D.H., Caso Claude Reyes y otros. Sentencia de 19-IX-2006. Serie C N.° 151, párr. 75; Corte I.D.H., Caso López Álvarez Vs. Honduras. Sentencia de 1-II-2006. Serie C, N.° 141, párr. 163.

10 La Comisión Interamericana ha expresado que "la carencia de libertad de expresión es una causa que 'contribuye al irrespeto de los otros derechos humanos'" (CIDH 16-X-1997, párr. 72)

11 Al respecto la Convención Americana sobre Derechos Humanos ha establecido, de manera clara y precisa, los casos dentro de los cuales el derecho a la libertad de expresión puede ser sujeto a restricciones.
"Art. 13.- Libertad de Pensamiento y de Expresión.
1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:
a) el respeto a los derechos o a la reputación de los demás, o
b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.
3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones. (subrayado de la autora)
4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.
5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional" (OEA 1969).

ciudadanía se informa a partir de fuentes diversas y, en consecuencia, cada quien puede ejercer de manera coherente sus derechos políticos. Además, resultan ser derechos indispensables para levantar la voz ante cualquier condición de desigualdad que sea ignorada por las autoridades públicas, ya sea que provenga de grupos vulnerables, o de otros que buscan equidad respecto de espacios geográficos o grupos humanos alejados de las políticas de desarrollo promovidas por el Estado. Resulta evidente, entonces, que el ejercicio a la libertad de expresión tiene un rol fundamental dentro de un Estado verdaderamente democrático.

Sin embargo, dentro del examen de las dimensiones social y colectiva del derecho a la libertad de expresión, pueden presentarse claras falacias que podrían ser utilizadas para intereses ajenos a los de la libertad de la población. A este respecto, la Corte IDH en la Opinión Consultiva OC-5/85 expresó que:

> "No sería lícito invocar el derecho de la sociedad a estar informada verazmente para fundamentar un régimen de censura previa supuestamente destinado a eliminar las informaciones que serían falsas a criterio del censor. Como tampoco sería admisible que, sobre la base del derecho a difundir informaciones e ideas, se constituyeran monopolios públicos o privados sobre los medios de comunicación para intentar moldear la opinión pública según un solo punto de vista". (Corte IDH 1985, párr. 33)

El análisis llevado a cabo por la Corte IDH podría ser representado de manera gráfica, como se presenta a continuación. "No sería lícito invocar el derecho de la sociedad a estar informada verazmente para fundamentar un régimen de censura previa supuestamente destinado a eliminar las informaciones que serían falsas a criterio del censor. (…)" (Corte IDH 1985, párr. 33). Esta aseveración se representa de la forma siguiente:

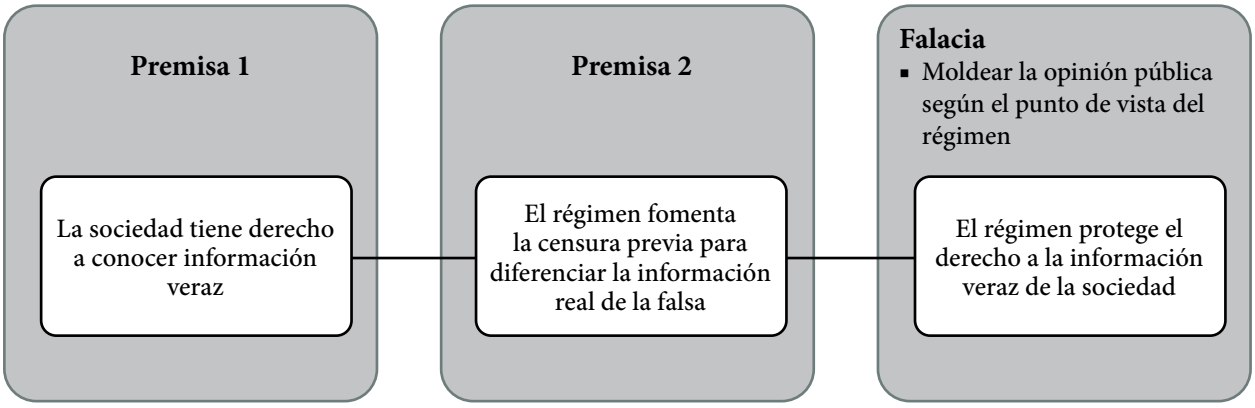


Ilustración N°. 1, elaborada por la autora de este artículo.

En efecto, es cierto que la sociedad tiene derecho a acceder a información real tal como lo garantiza el derecho a la libertad de expresión en su dimensión colectiva; sin embargo, la censura previa no podría ser un acto a favor de este derecho, ya que contraría su esencia, a pesar de aparentar ser un camino para su ejercicio efectivo. La censura previa puede constituir una herramienta para moldear la opinión pública.

Por otro lado, la Corte IDH complementa así su argumento: "(…) Como tampoco sería admisible que, sobre la base del derecho a difundir informaciones e ideas, se constituyeran monopolios públicos o privados sobre los medios de comunicación para intentar moldear la opinión pública según un solo punto de vista" (Corte IDH 1985, párr. 33). Estos elementos teóricos son representados en la ilustración Nº 2 de la página siguiente.

Difundir ideas e información se configura como la dimensión individual del derecho a la libertad de expresión. No obstante, si un solo individuo o un grupo

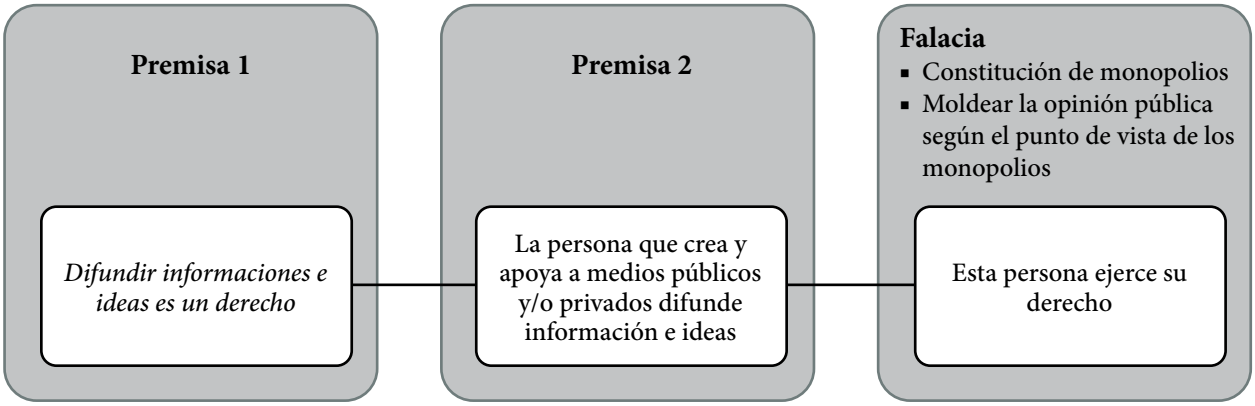


Ilustración N°. 2, elaborada por la autora de este artículo.

reducido crea y patrocina medios de comunicación públicos y/o privados, no significaría automáticamente que esta persona ejerce su derecho de libre expresión. Cuando un pequeño grupo de individuos ejerce control sobre los medios, sería totalmente reduccionista limitar este hecho a su ejercicio individual de libre expresión; ya que esta circunstancia podría constituir la creación de monopolios que uniformizan la opinión pública.

Justamente de esta doble dimensión se derivan tanto el derecho individual de compartir información y conocimiento como el derecho de la colectividad para recibir tal información. Sobre la base de esta naturaleza "no se puede restringir uno de los dos derechos en nombre de la protección del otro, pues son esencialmente inescindibles" (Botero 2017, 14).

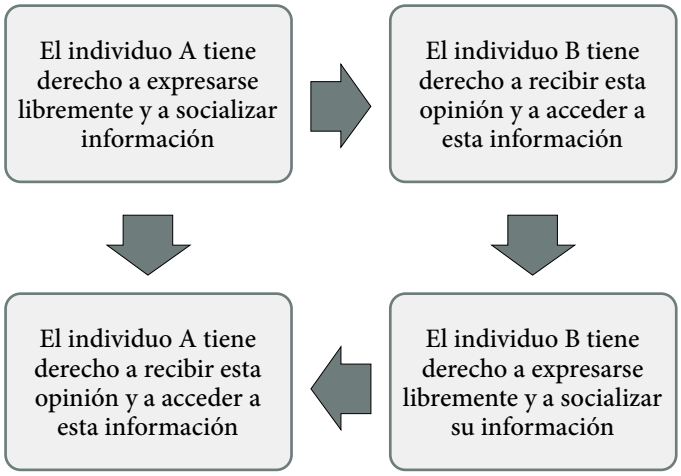


Ilustración N°. 3, elaborada por la autora de este artículo.

A través de este gráfico se busca comprender la relación complementaria entre la dimensión individual y colectiva del derecho a la libertad de expresión. Es derecho de los individuos expresar sus criterios e información a los demás, y es también derecho de los demás recibir esta información y, a partir de ella, formar sus propias opiniones y criterios. Las fuentes diversas de opiniones y de información son la base esencial del derecho a la libertad de expresión. En lo concerniente a las restricciones, es necesario indicar que, según las disposiciones del derecho internacional de los derechos humanos, la libertad de expresión no es un

derecho absoluto. Efectivamente, frente a determinadas circunstancias, es un derecho restringible. De esta forma, cualquier limitación al derecho a la libertad de expresión debe justificarse a partir de los artículos 13 numeral 2 y artículo 30 de la CADH, además de la normativa relativa al Sistema Universal de Protección a los Derechos Humanos. A fin de restringir efectivamente este derecho, se debe aplicar el test tripartito a dicha limitación, es decir: 1) la legalidad o que tal restricción se encuentre respaldada por una norma; 2) que tenga un fin legítimo, y 3), que sea necesaria, o sea, que existan razones lógicas para llevar a cabo la limitación (Corte IDH 1985). Este es un ejercicio analítico que correspondería a los servidores judiciales dentro de cada Estado, con el objetivo de limitar el poder y proteger este derecho.

En este sentido, la íntima relación entre el derecho a la libertad de expresión y el uso de internet implica que cualquier regulación o control que se ejerza sobre esta herramienta debe considerar su esencia y su influencia social.

> "(…) los enfoques de reglamentación desarrollados para otros medios de comunicación —como telefonía o radio y televisión— no pueden transferirse sin más a Internet, sino que deben ser diseñados específicamente para este medio, atendiendo a sus particularidades (…)".[12] (2011, Punto 1 (c))

Por este motivo, para la regulación de una herramienta de comunicación global como internet, la comunidad internacional requiere desarrollar y adecuarse a los principios que orientan la creación de normas y políticas públicas al interior de los Estados, de manera que conjuguen el acceso libre al internet con el ejercicio efectivo a la libertad de expresión. Sin duda son los Estados los sujetos llamados a aplicar estas regulaciones, siempre a la luz de las normas consensuadas a nivel global, debido a la naturaleza universal de internet.

Estos principios tienen su base en el acceso en igualdad de condiciones, la no discriminación y el derecho a la intimidad o privacidad de la información personal. Los principios esenciales encaminados a la creación de un marco regulatorio de la libertad de expresión a través del uso de internet serían el acceso universal, el pluralismo, la no discriminación, la neutralidad de internet, y el respeto a la privacidad individual (Relatoría Especial para la Libertad de Expresión de la CIDH/OEA 2013).

En primer lugar, en lo concerniente al principio relativo al acceso a internet, este debe ser universal; es decir, que la ciudadanía cuente con una igualdad de oportunidades que permita conseguirlo, sin discriminación de ningún tipo, ya sea de opinión política, opción sexual, origen nacional, entre otras. Dentro de este marco, el acceso universal no se restringe únicamente a la infraestructura tecnológica necesaria, sino también a la eliminación de barreras dentro del acceso a la información digital, tal como el analfabetismo tecnológico.

En segundo lugar, el principio de pluralismo evoca propender al máximo el número de opiniones provenientes de diversas fuentes, con el objetivo de discutir amplios temas desde diferentes frentes. Esta diversidad de información debe ser protegida por los Estados, de forma que se evite la restricción arbitraria de datos de interés público, y la promoción del acceso a infraestructuras que lleguen a los espacios históricamente marginados. Este principio tiene estrecha relación con el desarrollo de un Estado democrático.

En tercer lugar, el principio de no discriminación busca que los Estados revean sus marcos normativos internos, y apliquen medidas positivas que contrarresten cualquier margen discriminatorio (Relatoría Especial para la Libertad de Expresión de la CIDH/OEA 2013). Los Estados deberán propender al goce del derecho a la libertad de expresión mediante la creación de normas, políticas públicas, etc., para eliminar cualquier indicio de discriminación en el acceso a internet. Es importante resaltar que, si bien las opiniones o información compartida por individuos o colectivos resulta incómoda para el poder, es deber del Estado precautelar que esta información sea de dominio público, caso contrario resultaría a todas luces discriminatorio.

12 Relator Especial de las Naciones Unidas sobre la Promoción y Protección del derecho a la Libertad de Opinión y de Expresión, Organización para la Seguridad y la Cooperación en Europa OSCE, OEA y CADHP. 2011. *Declaración conjunta sobre libertad de expresión e Internet*.

Respecto a la neutralidad de internet, se trata de un principio que establece que la información que circula en la red no puede ser objeto de censura previa, mucho menos en función del autor, o de su contenido (Asamblea General de la ONU 2011).

En cuanto a la privacidad, la CADH, en su artículo 11 dispone que "nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación" (Organización de los Estados Americanos 1969). Dentro de este marco, los Estados tienen la obligación de respetar el derecho a la privacidad, al abstenerse de ejecutar actos que intervengan de manera arbitraria en la vida privada de un individuo y, además, garantizar que otros no ejerzan este tipo de conductas. Y los discursos especialmente protegidos, que son aquellos que contienen datos de interés público y son fundamentales para ejercer los derechos políticos, no podrían ser objeto de censura gracias a su carga importante de información para la ciudadanía.

Por otro lado, en caso de producirse un daño a la honra o reputación, siempre hay que analizarlo, no desde la generalidad, sino desde los hechos concretos, y aplicar la primera herramienta menos perjudicial, como es la retractación de información falsa. Así se evita recurrir a una de las armas más poderosas con las que cuenta un Estado, como es el derecho penal, y se mantiene el respeto a la proporcionalidad de las limitaciones al derecho de libertad de expresión (Botero 2017). Como último recurso, los estándares internacionales de derechos humanos recomiendan la aplicación de sanciones civiles, a fin de evitar el detrimento de la libertad de expresión.

Finalmente, las medidas restrictivas al ejercicio de la libertad de expresión en internet deben ser sometidas a rigurosos controles especializados. Existen ciertas condiciones para dichas limitaciones. En un primer momento es indispensable la existencia de la posibilidad de dicha restricción mediante normas claras y precisas. En un segundo momento, es fundamental que esa limitación esté orientada a un objetivo trascendental y autorizado por el marco normativo interno y externo respecto de un Estado. La CADH establece que se podrá alegar la seguridad nacional, el orden público, o la moral pública. Sin embargo, este análisis no debe ser escueto ni desprovisto de argumentos sólidos, al respecto el siguiente análisis resulta fundamental:

> "(…) la protección de la seguridad nacional puede ser invocada para imponer restricciones al derecho a la libertad de expresión. No obstante, una restricción a la libertad de expresión que pretenda justificarse en la defensa de la seguridad nacional no debe fundarse en una idea de seguridad nacional incompatible con una sociedad democrática. No tendría entonces una finalidad legítima un programa de vigilancia que, pese a invocar la defensa de la seguridad nacional, intercepte, capture o utilice información privada de disidentes, periodistas o defensores de derechos humanos con finalidades políticas o para evitar o comprometer sus investigaciones o denuncias". (CIDH–Relatoría Especial para la Libertad de Expresión 2012, 29)

En un tercer momento, cualquier restricción a la libertad de expresión debe ser analizada a la luz de la persecución de los objetivos dentro de un Estado democrático. Así pues, para el solo planteamiento de la restricción de este derecho es fundamental comprobar la real existencia de una amenaza o hecho cierto que pueda perturbar las instituciones democráticas.

Dentro de este análisis sobre la restricción del derecho a la libertad de expresión, resulta inevitable pensar que dicha limitación podría afectar el funcionamiento particular de internet, ya que la proscripción de cierta información causaría daño a su carácter universal y afectaría no solo a un individuo o grupo sino a la sociedad entera. Cuando se prohíbe que determinada información circule en internet, este hecho afecta a todo aquel que pudo acceder a ella mediante la red; no se trata solo de una sanción para la persona o grupo que se busca censurar, sino que, por la naturaleza de internet, esta sanción abarca a todo aquel que no tuvo acceso a esos datos. Estas son justamente las particularidades que se deben tomar en cuenta al momento de regular la información en internet.

CONCLUSIONES Y RECOMENDACIONES

Internet es una herramienta que propicia el intercambio de ideas e información de manera global, con amplio espectro de diversidad. Por este motivo, desde su creación, internet ha modificado la forma de relación entre individuos, pues presenta un escenario social relativamente nuevo para el derecho actual, que trae amplias ventajas como acceso libre a la información y al conocimiento, y libertad para expresar ideas. Pero también, al no encontrarse normado, puede traer conflictos en las relaciones sociales, tal como ocurre en cualquier relación entre dos o más individuos. Entonces, el ejercicio del derecho a la libertad de expresión dentro de internet debe ser regulado por los Estados. Estos son los sujetos legítimos llamados a garantizar el efectivo ejercicio de derechos y a aplicar restricciones únicamente bajo el análisis de la necesidad, legalidad y proporcionalidad de dichas limitaciones. Asimismo, debido a la naturaleza universal de internet, los Estados deben regular su uso a la luz de las normas del derecho internacional de los derechos humanos; y de los principios que rigen a un Estado democrático.

Cabe agregar que aún queda mucho por hacer en materia de derechos y el mundo digital a través del uso de internet. Con todo, esta herramienta es un elemento moderno con enorme potencial para promover la libertad de expresión, el acceso a la información y al conocimiento, y, la libertad de pensamiento; de manera que, dadas las condiciones favorables, es un instrumento positivo y provechoso para las diversas sociedades actuales.

Podemos recomendar:

- El análisis de las posibles restricciones al derecho a la libertad de expresión en internet debe realizarse ineludiblemente a la luz del derecho internacional de los derechos humanos, con el objetivo de evitar limitaciones o una censura ilegítima a este derecho.

- El estudio del uso de internet se encuentra íntimamente relacionado con el examen de su acceso tanto tecnológico como en conocimiento respecto de su manejo. Por esta razón, no resultaría eficiente restringir el análisis únicamente dentro del marco del derecho, sino que sería necesario obtener elementos desde otras perspectivas interrelacionadas. Así pues, se recomienda revisar otras perspectivas presentes en diferentes ámbitos de estudio, tales como el acceso a internet y su conexión con el desarrollo de los países emergentes; el análisis espacial desde una perspectiva de desigualdades: espacios rurales y urbanos con diferente nivel de acceso a esta herramienta; y modificación de las relaciones sociales a partir de la creación de internet, entre otras.

- La comprensión del rol de los Estados es fundamental para discurrir sobre las posibles regulaciones del derecho a la libertad de expresión en internet. Son los Estados los sujetos llamados a regular las limitaciones, y por tal causa deben restringir sus actuaciones dentro del marco de los principios democráticos y de amplia participación de la población. De ahí que resulta de suma importancia profundizar en el estudio de los Estados como sujetos globales para la regulación del uso de internet. No obstante, dentro del mundo globalizado, habría que analizar también el rol protagónico que han adquirido los proveedores de internet, los motores de búsqueda, y las empresas asociadas al servicio de internet. Estos nuevos actores en el panorama internacional no pueden ser excluidos de este estudio, ni de las posibles regulaciones aplicadas a través de instrumentos internacionales.

BIBLIOGRAFÍA

Asamblea General de la Organización de las Naciones Unidas. 2011. *Informe del Relator Especial sobre la promoción y la protección del derecho a la libertad de opinión y de expresión*. A/66/290.

Botero, Catalina. 2017. *Guía político-pedagógica sobre la incorporación de la temática de libertad de expresión y de acceso a la información pública en la formación de operadores judiciales en América Latina*. UNESCO.

Center for International Media Assistance (CIMA). 2017. *Estándares internacionales de libertad de expresión: Guía básica para operadores de justicia en América Latina*.

CIDH–Relatoría Especial para la Libertad de Expresión. 2012. «El derecho de acceso a la información en el marco jurídico interamericano».

CIDH–Relatoría Especial para la Libertad de Expresión. 2013. «Libertad de Expresión e Internet».

Relator Especial de las Naciones Unidas sobre la Promoción y Protección del derecho a la Libertad de Opinión y de Expresión. 2011. «Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression » A/HRC/17/27.

UNESCO. 1945. *Constitución de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura*.

UNESCO. 2013. *Universalidad de Internet: un medio para crear sociedades del conocimiento y la agenda de desarrollo sostenible después de 2015*.

Legislación y jurisprudencia

Asamblea General de Naciones Unidas (ONU). 1948. *Declaración Universal de Derechos Humanos. Resolución 217. A (III)*.

Asamblea General de la Organización de las Naciones Unidas. 1976. *Pacto Internacional de Derechos Civiles y Políticos. Resolución. 2200 A (XXI)*.

Corte IDH. 2006 . Caso *Claude Reyes y otros Vs. Chile. Fondo, Reparaciones y Costas. Sentencia de 19-IX-2006. Serie C N.° 151*.

Corte IDH. 2008.*Caso Kimel Vs. Argentina. Fondo, Reparaciones y Costas. Sentencia de 2 de mayo de 2008 Serie C N.° 177*.

Corte IDH. 2006. *Caso López Álvarez Vs. Honduras. Fondo, Reparaciones y Costas. Sentencia de 10-II-2006. Serie C N.° 141*.

Corte IDH. 1985. *La Colegiación Obligatoria de Periodistas (Arts. 13 y 29 Convención Americana sobre Derechos Humanos). Opinión Consultiva OC-5/85*.

Organización de los Estados Americanos. 2001. *Carta Democrática Interamericana*.

Organización de los Estados Americanos. 1969. *Convención Americana sobre Derechos Humanos*.

Organización de los Estados Americanos. 1948. *Declaración Americana de los Derechos y Deberes del Hombre*.

Relator Especial de las Naciones Unidas sobre la Promoción y Protección del derecho a la Libertad de Opinión y de Expresión, Organización para la Seguridad y la Cooperación en Europa OSCE, OEA y CADHP. 2011. *Declaración conjunta sobre libertad de expresión e Internet*.

ENTREVISTA

CASO WIKILEAKS
Entrevista con Carlos Poveda*

WIKILEAKS CASE
Interview with Carlos Poveda

CASO WIKILEAKS
Entrevista com Carlos Poveda

*María Carbonell***

Entrevista realizada en Quito, de forma virtual, el 4 de junio de 2020, transcrita y editada

* Carlos Poveda es abogado por la Universidad Central del Ecuador (Quito), Especialista y Máster en Derecho Procesal por la Universidad Andina Simón Bolívar (Quito). Fue Juez de lo Penal en Cotopaxi. Es abogado en libre ejercicio y abogado integrante de ILOCAD, bufete jurídico presidido por Baltasar Garzón Real (Madrid). Fue asesor en temas relacionados con interculturalidad para la ONU. Fue asesor en la Comisión de la Verdad del Ecuador en temas de reparación integral. Ha escrito varios artículos y participado en conferencias nacionales e internacionales en temas de justicia Indígena, derechos humanos, verdad y reparación, independencia judicial, y libertad de expresión.

** María Helena Carbonell Yánez es abogada y máster en International *Humanitarian Law and Human Rights*. Actualmente se encuentra realizando su PhD en Derecho, en la Universidad Andina Simón Bolívar. Es docente de varias universidades del Ecuador, a nivel de pregrado y de posgrado. Ha escrito varios artículos relacionados al Derecho Internacional de los Derechos Humanos que han sido publicados en el Ecuador, México e Indonesia. Ha sido consultora para instituciones del Estado, así como para organizaciones de la sociedad civil. Sus principales líneas de investigación son: derechos humanos, Derecho Internacional Público, sistemas internacionales de protección de derechos, Derecho Internacional Humanitario, refugio y movilidad.

MARÍA HELENA CARBONELL (MHC): Julian Assange es una figura que genera sentimientos, hay quienes le admiran muchísimo, pero, por otro lado, hay quienes realmente no solo tienen un rechazo, sino que lo odian. Ahora, el impacto de sus actuaciones es innegable. Entonces, nos gustaría que nos cuente la cronología del caso, de los hechos, y cómo llegó a participar en el caso.

CARLOS POVEDA (CP): Cuando fui juez, de 1998 hasta el 2007, pude tener una beca de la Agencia Española de Cooperación y pude estudiar en la Escuela Judicial Europea, básicamente en España. Ahí me vinculé con Jueces para la Democracia, que son colectivos de jueces progresistas a nivel mundial. Uno de los impulsores o referentes en ese momento, después del caso Pinochet, era Baltazar Garzón. A través de amigos en común, tuvimos varios encuentros básicamente para promover la independencia judicial y el asocianismo. Luego, retorné al Ecuador y formamos aquí la primera Asociación de Jueces para la Democracia. Yo sigo considerando, más allá de eso, es un mecanismo de defensa e independencia judicial, hablando ahora en tiempos actuales. Pudimos invitar a Baltazar Garzón, y ahí configuramos y estrechamos una relación más fuerte.

Posteriormente, en la reforma judicial de 2012, él estuvo como coordinador internacional de la reforma judicial y quería tener una contraparte ecuatoriana que pudiera apoyarle en esa coordinación. Esto también se ha invisibilizado, a pesar de que el aporte fue enorme en esa época. Y ahí también pude, no solamente trabajar sobre temas de independencia judicial, sino también sobre otros temas puntuales en el Ecuador.

Es ahí precisamente que surgió el tema Assange. En ese momento ya se conocían los antecedentes de Julian Assange y ya se había otorgado el asilo por parte del gobierno ecuatoriano. En este contexto, una vez que finalizó la colaboración nacional, entramos a formar un consorcio internacional, con contrapartes también del Ecuador: cerca de treinta abogados de diferentes países. Entonces me pidieron colaborar con su defensa jurídica. Baltazar Garzón ya había salido de la magistratura; de forma injusta se le había sancionado y, por lo tanto, él ya estaba en el libre ejercicio profesional.

Como bien se mencionó, Julian no es una persona que solamente genere aceptación y adhesiones, sino también rechazo. Y la concesión del asilo generó un sinnúmero de reacciones, nacionales e internacionales. Lo que es importante mencionar es que, a veces, los medios, por ciertos rechazos de ciertos poderes fácticos, no develan o no visibilizan toda la información referente al caso. Solamente se veía lo malo. Evidentemente, las motivaciones que dan el asilo son independientes de cualquier línea ideológica. Esto lo digo porque se le dio un matiz ideológico. Lo que se decía entonces es que como el asilo fue otorgado por el gobierno de Rafael Correa, entonces Assange es una persona *non grata* para el Ecuador.

Ahora, es importante conocer la estructura de WikiLeaks, que a veces es asimilado con Julian Assange: no es lo mismo WikiLeaks que Assange. WikiLeaks es una fundación, una organización periodística muy seria que puede ser considerada como un ícono de información y comunicación. Las informaciones que llegan a WikiLeaks son informaciones que cubren fuentes y que son totalmente verificadas, ya que tienen determinados filtros para la publicación. Son periodistas y no *hackers*. Esto se ha tenido que explicar muchísimo porque Assange es un periodista y es un periodista laureado, candidato al premio Nobel de la Paz. Y WikiLeaks, con Assange y Kristinn Hrafnsson, que es también uno de los fundadores, lo que generan es una antipatía de los poderes.

Cuando yo hablo de estos poderes, no es solamente de los formales sino también de los fácticos. ¿Y cuáles son estos poderes fácticos? Cuando se empieza a señalar la difusión de información sensible en la situación de las guerras de Irak y los abusos de las cárceles de Abu Ghraib, yo creo que una de las cosas que más impacta es la muerte y el asesinato de los periodistas, en plena guerra. Este tipo de información, este tipo de situación, nos pone en una encrucijada. ¿Debía ser difundida o no debía ser difundida? Y ellos decidieron que sí porque son graves violaciones de derechos humanos.

También interpela la situación de las grandes empresas tecnológicas y la utilización de los medios telemáticos y electrónicos para afectar derechos de

privacidad. Entre más información se tenía, más libertad de expresión se tenía, y también mayor riesgo de afectación a los derechos de privacidad. Por ejemplo, plataformas informáticas como YouTube, WhatsApp, Facebook, podrían ser miradas de forma ingenua. Así lo hacemos diariamente todos. ¿Pero que hay atrás? Información tuya, de todos tus contactos, de todas tus actividades. Y eso en definitiva no solamente servía para esta plataforma y otras entidades no gubernamentales, privadas; sino que servía también para centrales de inteligencia, que es algo que también se denunció, de la CIA, de Estados Unidos, para empezar a vigilar en todos los sentidos.

Esto es fácil de ver. Por ejemplo, si alguien va a pedir una visa, ve que tienen toda su información. ¿Cómo tienen toda la información? Yo creo que es un aporte enorme que se ha invisibilizado. Lo que hicieron nos permitió reaccionar, nos permitió espabilarnos y decir: ¿qué es lo que está ocurriendo? Y de esto todavía no están conscientes todas las personas. Es importante el nivel de concienciación que podemos tener frente a este tipo de mecanismos que pueden ser a simple vista inocuos, pero que en definitiva son tremendamente dañinos, porque entran en las casas, están en los hogares, están presentes.

Inclusive Mark Zuckerberg, dueño de Facebook, había afirmado eso, que recolectaba los datos y los pasaba a centrales de inteligencia. Es una situación abusiva, y ahí se ve el enlace de los poderes económicos privados, con el poder estatal público, y la vigilancia a toda la población. Ese me parece que es el valor primigenio de la fundación de WikiLeaks: ser un verdadero contrapoder de todos estos abusos. Recientemente, por ejemplo, Anonymous publicó información de espionaje. Lo mismo que hacía Correa. Pero no se puede justificar diciendo: "es que antes también se hacía". No, hoy también se hace; nos tienen vigilados. Por ejemplo, cuando alguien va a portales digitales y ve unas fotos del seguimiento de tal o cual personaje. Por ejemplo, Ola Bini: uno ve que Ola Bini se vio con tal personaje en el restaurante El Cafetal, en Quito. ¿Cómo pasa esto? Eso viene del seguimiento que le hacen. Y eso, claro, son abusos.

Entonces, al conocer el tema, veo que Assange, más allá de ser un ícono publicitario, un ícono mediático, es un ser humano que necesitaba protección de forma urgente.

Un segundo elemento importante son las acusaciones de violación. Con esto surgió un dilema: ¿a quién voy a defender? Me mandaron mucha información, conversamos con la gente de Assange y del consorcio español, y ahí pude darme cuenta de que eran situaciones creadas para buscar la judicialización, la persecución y la prisión de Assange. Y eso, al final, se verificó. Lo que se hizo fue contrarrestar, a través de la cobertura que los medios de comunicación dieron a estas denuncias, la adhesión que había en una época a favor de Assange. Esta estrategia de persecución buscaba acallarle. No le iban a callar secuestrándole, torturándole, porque ese tipo de mecanismos ya no se hacen, sino con algún tipo de acción para perjudicar su imagen y tener un escarnio de carácter público internacional. Fue muy duro porque se posicionó en todo el mundo que estábamos defendiendo a un violador.

Ahora, ya con una información correcta, que muchas veces no sale en los medios de comunicación, era un deber ineludible participar en el caso, sobre todo cuando se trabaja en esta temática. Pero también hay un riesgo, porque se me ha dicho de todo y se han entrometido en todos los aspectos de mi vida privada. En una ocasión, incluso, me dijeron que se me tenía que retirar la nacionalidad ecuatoriana por ser traidor a la patria. Pero esos son los riesgos y esos son los antecedentes de la defensa.

Hay un tercer elemento, que es muy interesante, porque el tema Assange es un tema para debatir ampliamente; es decir, el debate es multidisciplinario y no solamente jurídico, es comunicacional, es sociológico, es un tema de Derecho Internacional, de Derecho Internacional de Derechos Humanos, y hasta de lesa humanidad, porque es una persona protegida. Entonces es un campo multidisciplinario con diversas aristas, y es así como nosotros entramos a este análisis. Y para la defensa de Assange era indispensable tener un abogado ecuatoriano, porque estaba en una embajada ecuatoriana que es territorio ecuatoriano según el Convenio de Viena; y para cualquier actuación judicial de impacto en Londres o en Ecuador, necesitaban

un abogado en Ecuador. Además, también necesitaban profesionales de altísima confianza.

Estos son los puntos básicos y estos son los motivos por los que yo acepté la defensa. Y sigo siendo su defensor. Ahora estamos trabajando, para el mes de septiembre, porque ahí se va a dar la recepción de pruebas para la decisión de extradición. Para la extradición desde Inglaterra se formularon o se van a formular nuevos cargos basados en la supuesta recepción de evidencias en la embajada de Londres.

MHC: Ahora, el caso Assange se puede analizar desde diferentes aristas y una que es particularmente interesante son los derechos humanos. Tenemos todas estas nuevas tecnologías con aspectos buenos y malos. Muchas veces, los Estados buscan limitar estas tecnologías y, a la larga, lo que hacen, directa o indirectamente, es una limitación del ejercicio de los derechos.
En el caso de WikiLeaks, de Julian Assange, es interesante ver cómo el Derecho Penal, es decir una de las formas que utiliza el Estado para limitar el alcance de estas nuevas tecnologías, choca con los derechos humanos. ¿Qué argumentos se utilizaron en la defensa del caso para poder contrarrestar esto? Es decir, el Estado está por un lado limitando ciertos derechos, obviamente teniendo en cuenta argumentos del fin legítimo dentro de una sociedad democrática. Entonces, ¿cómo ustedes pueden defender el choque de los derechos?

CP: ¿Cómo afecto la existencia de Julian Assange, siendo sutil, delicado y aparentando que vivimos un Estado democrático? Creando una ficción jurídica-penal, utilizando el Derecho Penal, con escarnio público: diciendo que Assange es un violador. Éstas son las acusaciones fuertes. El Estado no usa la censura directamente, sino que usa técnicas más sutiles.

Frente a esto, la protección de Assange era necesaria. En este caso, se verificó que había argumentos suficientes para otorgar el asilo frente a una persecución de Estados Unidos. No hay prueba más fehaciente, oportuna, contundente, que ver que, cuando termina el asilo, aparecieron todos los cargos, toda la investigación. Entonces, lo que se decía en el 2012, cuando se le otorgó el asilo, eran expectativas reales, eran expectativas fundadas, y ahora mucho más.

Ahí también tenemos el Derecho Internacional de Derechos Humanos, porque es una persona que requiere protección internacional y, a esto hay que añadir que es ecuatoriano y el Ecuador no puede lavarse las manos. Sobre este último punto la pregunta que debemos hacernos es: ¿por qué la nacionalización? Ha estado siete años asilado y, de conformidad con varios convenios internacionales en materia del asilo, existe la posibilidad de conceder la nacionalidad del país que otorga el asilo. No había ningún inconveniente, no era ningún caso extremo ni una coartada para salir del país como diplomático ecuatoriano.

Cuando compareció en la Asamblea, porque era necesario que los asambleístas conozcan el caso, lo que se vio es un nivel muy limitado. Se usaron expresiones burlonas como: "ah, sí, que el suquito, no, el gringuito se fue a sacar la cédula en una parroquia de Quito"; y un reglamentarismo que no es propio de un Estado constitucional de derechos y justicia.

MHC: Lo que faltó fue una interpretación pro-ser humano de las normas vigentes.

CP: Así es.

MHC: Una pregunta sobre el asilo. Teniendo en cuenta que la figura del asilo en Latinoamérica es diferente a aquella que existe en el resto del mundo, ¿qué requisitos cumplía Assange para que le otorguen el asilo?

CP: Había una persecución de carácter político que se evidencia a través de la información que ya teníamos. Ésta fue obtenida de manera casi fortuita, porque Estados Unidos argumentaba que no tenían ninguna investigación en contra de Assange. Básicamente, uno de los abogados que tenemos en los Estados Unidos ingresó a un sistema como el Satje[1], y se percató de que había información de investigación colateral que

1 Nota de la editora: El Satje es el Sistema Automático de Trámite Judicial Ecuatoriano, que permite realizar consultas sobre procesos judiciales en línea.

se estaba solicitando ya en esa época. Y, ¿cuál fue la reacción? Los mismos pronunciamientos de las autoridades públicas de los Estados Unidos que ya decían que era el enemigo número 1, que era un espía, que era un hacker, que era, inclusive, un objetivo a nivel mundial. Eso, evidentemente, generó una situación de relevancia y de persecución. ¿Cuál fue la conclusión? Esos niveles de persecución política generaron los elementos para la solicitud de asilo y para la concesión del asilo.

Y sí, la postura latinoamericana referente al derecho al asilo es muy diferente al acercamiento europeo. En Latinoamérica se han dado persecuciones políticas muy importantes. Europa ha sido mucho más respetuosa, digamos, de los procesos de cambio y de transición, y no ha tenido mucho estos tipos de persecución. Debido a que Latinoamérica tiene sus circunstancias muy propias, el desarrollo del asilo se ha dado de distinta manera que en Europa. Esto acarreó un choque, porque los ingleses jamás aceptarán un tipo de asilo de esa naturaleza.

Yo asevero que no fue una situación circunstancial, no; fue orquestado. Es decir que hay una confabulación de estos Estados y de los intereses de los Estados para terminar el asilo y luego aprehenderlo. Entonces, el tema del asilo se volvió muy importante.

Ahora, yo siempre recomiendo la opinión consultiva de la Corte Interamericana que se generó a raíz del proceso Assange. Ahí se evidencia el tema del asilo, del refugio y de la aplicación de convenios internacionales en este tipo de situaciones. Una de las cosas más importantes que debo recatar de la opinión consultiva es la no devolución a un país donde corre riesgo la vida o la integridad de la persona. Lamentablemente, en este caso no se cumplió con esto.

Y un segundo tema importante, reconocido igualmente en ese documento y en jurisprudencia internacional, es que la persona tiene derecho a un proceso previo a la terminación del asilo. Esto lo incumplió abiertamente el Estado ecuatoriano. Si yo estoy asilado, lo mínimo que debo conocer es la terminación del asilo, y se me debe dar la posibilidad de defenderme. Por ese motivo presentamos nosotros una acción de protección. Recibimos hasta burlas desde diversos sectores, incluida la Cancillería. Su fundamento era el incumplimiento del Protocolo de Convivencia; se mencionaron incidentes como que había excrementos en las paredes y que andaba en patineta.

Debo advertir que el Ecuador ya está demandando en la Comisión Interamericana de Derechos Humanos, desde octubre del año anterior, por la serie de violaciones que se dieron. Y ahora, inclusive, hemos puesto una carta en Inglaterra indicando que Assange sigue siendo ecuatoriano y que, lamentablemente, no ha habido asistencia consular por parte de Ecuador. La naturalización sigue vigente, Assange sigue siendo ecuatoriano. Ésta es otra de las situaciones de omisión del Estado ecuatoriano, que en algún momento tendrá que rendir cuentas.

MHC: Sobre la opinión consultiva de la Corte Interamericana y el desarrollo del principio de no devolución, ¿qué pasa con las necesidades de personas en necesidad de protección internacional? El asilo puede ser territorial o diplomático; en este caso entiendo que fue concedido el asilo diplomático, pero, en Latinoamérica existe la posibilidad de pedir un salvoconducto y la obligación de que sea concedido. ¿Cómo funciona esto con Inglaterra? ¿Cómo se puede funcionar con el principio de no devolución y la concesión del salvoconducto?

CP: Cuando se otorgó el asilo diplomático a Assange, nuestro equipo formó escenarios. Mi opinión (yo recién estaba empezando en estos temas y, era algo nuevo para todos), entonces, fue que por lo menos tendría que aguantarse cuatro años. Sabíamos que no iba a ser inmediato, que Inglaterra, en el momento en que Correa le daba el asilo, no iba a decir: "tome el salvoconducto y salga de aquí". Eso era imposible. ¿Por qué? Porque esta actitud concertada de Estados Unidos, Inglaterra, Ecuador y Suecia tenía que ir de la mano con la no concesión del salvoconducto, porque el salvoconducto era para sacarlo.

Pero, personalmente, yo creo que Assange estaba más seguro en la embajada que afuera. Yo creo que le convenía a Estados Unidos y a todos estos tipos de poderes, tenerle encerrado, vigilado. Era mucho más factible

que tenerlo afuera, porque en la embajada espiaban todo, ponían micrófonos, ponían cámaras hasta en el baño. Había agentes ecuatorianos que trabajaban con los agentes americanos y con los ingleses; y sabían todo lo que hacía, hasta en la noche. Hasta vendieron esa información a agencias noticiosas privadas. Así que me parece que era mucho más cómodo solo coger el celular y ver lo que está haciendo a la una de la mañana, que no sabiendo dónde está (¿está en Australia, o está en Estados Unidos, o está en Venezuela o está en Bolivia? ¿O está en Rusia? ¿Dónde está?).

MHC: La nacionalidad es un derecho humano, pero también tiene una contraparte que es el Estado que tiene la capacidad de otorgar la nacionalidad. Y uno de los procesos de otorgamiento de la nacionalidad es a través de la naturalización. ¿Cómo afecta esto a la situación de Assange, el ser otorgado la nacionalidad ecuatoriana? ¿Cómo afecta a su condición de asilado?

CP: Bueno, creo que, en términos normales, en un Estado respetuoso de los derechos, esto hubiera afectado de manera positiva, pero aquí lo afectó de manera negativa, para tener otro escarnio público, sobre todo por la concesión. Dijeron que fue muy rápida, se preguntaron qué labor relevante había hecho. ¿Y qué hace un futbolista? En definitiva, ya llevaba siete años en la embajada, entonces él se identifica mucho con Ecuador.

Pero, pongamos que yo soy jefe de Estado: si alguien me resulta una piedra en el zapato, así, de manera muy frontal, yo voy a ver las maneras legales, y hasta diplomáticas, de que el señor salga. En esa posición de jefe de Estado, yo no quisiera tener problemas, menos fuera del país. Pero en la audiencia de la acción de protección, el argumento fue que "la expedición del protocolo de convivencia es el mecanismo para sacarle legalmente". Ahora, el Ecuador, en algún momento, va a tener que ser responsable.

MHC: La idea sería: naturalizarle, otorgarle el cargo diplomático, que con la Convención de Viena genera inmunidades, ¿y así podía salir tranquilamente?

CP: Exactamente. Yo creo que, si preguntaban opciones a cualquier profesional del Derecho, esa era una. ¿Dónde está lo ilegítimo? "¡Ah, es que es un extranjero!" Mira, nosotros podemos viajar a otros países si nos encontramos en los consulados, y no necesariamente ecuatorianos; hay consulados *ad honoren*, que son precisamente de otros países. ¿Cuál es ahí la dificultad? ¿Qué nos extraña? Lo que se podía hacer era generar una solución legal, internacional.

MHC: Y finalmente, de acuerdo con la segunda Convención de Viena de relaciones Consulares, los locales diplomáticos y consulares tienen inmunidades. ¿Cómo hace la policía inglesa para ingresar? La policía ecuatoriana no puede ir aquí a la embajada estadounidense y entrar.

CP: Ahí hubo otro asesoramiento inadecuado, que resultó en lo que sucedió: yo, siendo ministro de relaciones exteriores, suspendo la naturalización (eso es lo que hizo el ministro Valencia). ¿Cuál era el objeto? Como suspendo la naturalización, ya no tengo un ecuatoriano dentro de la embajada con protección, por tanto, es un extranjero cualquiera. Entonces, como funcionario diplomático, abro la puerta de la embajada, ingresa la policía y lo saca. Y, como no es ecuatoriano, entonces, no pasó nada. Pero no se percataron que no hay suspensión de naturalización. Pero esa es la asesoría que tuvieron.

Yo estuve de madrugada con la gente de Assange. El embajador nunca, nunca exhibió la orden de terminación del asilo. Yo les gritaba: "¡diles que muestren la orden de terminación de asilo!". Y me respondió que no le querían dar. En ese momento lo sacó la policía, arrastrándolo. Pedimos las filmaciones de esa noche y hasta ahora no nos quieren dar, porque saben lo que hicieron.

En cuanto lo sacaron, activaron las órdenes de arresto de Estados Unidos. Todo fue así, de un momento al otro; lo que muestra que hubo un complot y una conspiración de los Estados. Ecuador da por terminada la naturalización; Estados Unidos se pronuncia por los cargos; Gran Bretaña le sanciona por el tema del desacato. Todo fue concatenado. Y claro, como no había suspensión de naturalización, ¿qué es lo que hicieron? Entraron a una delegación ecuatoriana a arrestar a un ecuatoriano, y eso, obviamente, viola todo tipo de inmunidades y de protección consular.

MHC: Una vez que se le otorgó la nacionalidad ecuatoriana, ¿no hay ningún documento que demuestre cuándo terminó el asilo? ¿Tácitamente se termina el asilo una vez que le otorgó la nacionalidad ecuatoriana? En ese caso, aunque se suspenda la nacionalización, sigue siendo un asilado. Entonces, se está dejando entrar a la policía a la embajada ecuatoriana a sacar a un asilado. De igual manera, por ejemplo, en el artículo 25 de la Convención Interamericana, y también en la Constitución, se dice que cuando están en juego derechos siempre se tiene derecho al debido proceso.

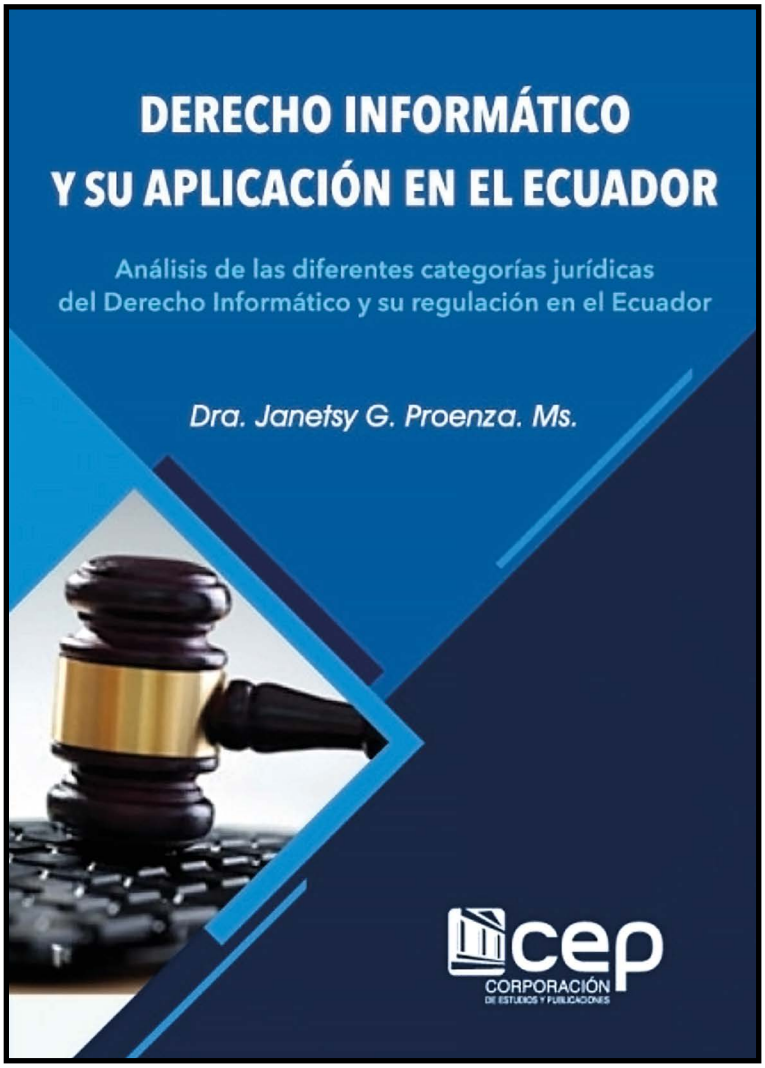
CP: La terminación del asilo era porque había violado el protocolo de convivencia. Ya sabíamos cuál era la hoja de ruta. Pero regresemos a la opinión consultiva. Si se iba a terminar el asilo, ¿tenía derecho o no tenía derecho a un proceso? El protocolo de convivencia no tiene procedimiento de terminación de asilo. Y ese fue el espíritu de la acción de protección. Porque también decían que él se oponía a que hubiese reglas de convivencia. Eso es una mentira. Es más, antes del protocolo ya había reglas verbales que se acordaron en la época de la diplomática Arboleda y su sucesor.

No hubo procedimiento para que él conozca las razones por las que se quería dar por terminado el asilo, ni para que pueda defenderse. Ese fue el espíritu de la acción de protección y, debo decir que, lamentablemente, la justicia ecuatoriana quedó corta. La jueza a la cual le correspondió esta acción dijo que no había derechos violentados. Una de las integrantes de la sala de la Corte Provincial de Justicia de Pichincha, profesora de Derecho Internacional de Derechos Humanos de una universidad, falló en contra de este caso. En una vergüenza. Yo quería tener por lo menos una explicación. Además, ni siquiera le dieron la oportunidad de hablar: le dieron un tiempo mínimo y le interrumpían a cada rato. A esos niveles se llegó. Y los medios de comunicación festejaban que le habían negado la acción de protección.

RESEÑA

DERECHO INFORMÁTICO Y SU APLICACIÓN EN EL ECUADOR
Análisis de las diferentes categorías jurídicas del Derecho Informático y su regulación en el Ecuador*

Dra. Janetsy G. Proenza. Ms.



Sonia Chávez**

* Proenza, Janetsky 2019. *Derecho Informático y su aplicación en el Ecuador*. Ecuador: Corporación de Estudios y Publicaciones.

** Sonia Fernanda Chávez es abogada por la Universidad de las Américas, Ecuador, y lingüista con mención en Traducción por la Pontificia Universidad Católica del Ecuador. Actualmente se desempeña como perito traductor, acreditada ante el Consejo de la Judicatura del Ecuador, y como abogada en libre ejercicio.

La doctora Janetsy Proenza hace una amplia explicación de los conceptos fundamentales de la informática y su interacción con el Derecho; explica cómo, con el pasar de los años y por el expedito desarrollo de esta disciplina, el Derecho se ha modificado y evolucionado para poder mantenerse actualizado frente a los avances de la informática. En el libro se hace uso del concepto de sociedad de la información; empieza con una explicación de este y lo valida dentro de la reflexión que hace la autora sobre el Derechos Informático, como un marco conceptual útil y pertinente.

En el primer capítulo, Proenza explica la noción de sociedad de la información, a partir de los años 70 del siglo XX. Desde entonces, la conceptualización de esta noción ha sido discutida por diversos expertos, quienes, dentro de su campo de trabajo, explican la transformación del método de almacenamiento y procesamiento de la información, gracias a nuevos instrumentos tecnológicos. Por ejemplo, Proenza menciona a Daniel Bell (1976), sociólogo, quien explicó el cambio operado en la sociedad, recolectó cantidad de información, la estructuró y, tras procesarla, la utilizó como una fuente para tomar decisiones informadas sobre diversos ámbitos de la sociedad, por ejemplo, el económico.

Proenza sigue con la presentación de los conceptos de cibernética, robótica e inteligencia artificial, y sus antecedentes e influencia dentro de la sociedad actual. Al final de este primer capítulo precisa la conexión entre la cibernética y el Derecho, y explica la cibernética en su relación con la creación de instrumentos tales como bases de datos de jurisprudencia, sentencias y normativa. Dichas compilaciones han facilitado el trabajo de abogados y jueces, al proporcionarles información actualizada y precisa en cuestión de segundos. En síntesis, el primer capítulo presenta, de forma clara y concisa, estos términos tecnológicos y cómo ellos se relacionan con el Derecho, de tal forma que el lector obtiene información indispensable para el estudio del Derecho Informático.

En el segundo capítulo, Proenza reitera que existe mucho debate entre los expertos sobre este tema, por cuanto algunos consideran al Derecho Informático como una rama diferenciada dentro del Derecho, mientras que otros consideran que es parte del Derecho de la comunicación. Luego continúa con el análisis del desarrollo del Derecho Informático en Ecuador y con una breve mención de aquellas áreas de éste cuyo desarrollo ha sido más relevante en nuestro país: comercio electrónico, contratación electrónica, firma electrónica y delitos informáticos. A decir de la autora, el salto más importante para el Ecuador se presentó a partir del año 2001, con la creación de la Comisión Nacional de Conectividad, cuyo eje central consiste en garantizar el acceso y uso de las tecnologías de la información y comunicación, para todos los ecuatorianos. Desde entonces, se han realizado políticas públicas para masificar el acceso al internet. Entre ellas, la autora destaca cuatro que tuvieron mayor relevancia:

1. Establecimiento de una tarifa plana, cuyo propósito era ampliar el acceso de internet a un menor costo.
2. Plan de Servicio Universal sobre el desarrollo de la infraestructura necesaria para el acceso nacional a Internet. Su objetivo era llegar a las zonas marginales para proveer un servicio básico de Internet.
3. Plan Nacional de Conectividad, cuyo eje central era el acceso igualitario de servicios de comunicación para toda la ciudadanía.
4. Estrategia Ecuador Digital, que cuenta con cuatro ejes:
    a) La masificación de las TIC y de Internet a toda la sociedad ecuatoriana.
    b) Educación digital para los grupos prioritarios y la sociedad en general.
    c) Mejorar el ámbito investigativo con ayuda de las TIC.
    d) La innovación con ayuda de las TIC.

Según la autora, pese a la toma de dichas acciones, aún existe un gran porcentaje de la población ecuatoriana sin acceso al Internet, de modo que la brecha digital es aún muy marcada en este país. Durante este año 2020, cuando se presentó la Pandemia del Virus COVID-19, se evidenció, más que nunca antes, la gran brecha tecnológica existente en Ecuador. Varios problemas en la educación primaria, secundaria y superior, así como en el cambio repentino del

trabajo presencial al teletrabajo, son tan solo ejemplos del trabajo que aún falta por realizar en Ecuador para tener una auténtica sociedad tecnológica.

En el tercer capítulo, Proenza centra su investigación sobre el comercio electrónico, contratación y firmas electrónicas. Sobre las últimas, la autora enfoca su explicación en la importancia de este instrumento en el ordenamiento jurídico ecuatoriano. Dichas firmas sirven como respaldo de la voluntad y autenticidad del documento emitido, de manera que la expedición de documentos públicos es mucho más efectiva. El valor probatorio de las firmas electrónicas reside en la normativa establecida en el ordenamiento jurídico ecuatoriano sobre estas y sobre sus métodos de verificación. Sin embargo, pese al avance jurídico que se ha dado con tal instrumento, la autora aclara que aún se presentan ciertas fallas en torno a su efectividad en el ámbito procesal, en razón de que no todas las instituciones públicas comprenden a cabalidad la autenticidad y funcionamiento de la firma electrónica, motivo por el cual suelen darse retrasos procesales. En el ámbito legal ecuatoriano, durante el tiempo de confinamiento, los abogados se adaptaron rápidamente al ingreso de la tecnología dentro de los procesos judiciales, mediante la presentación de escritos por medio de ventanillas virtuales y con la respectiva firma electrónica. Sin embargo, en el ámbito jurisdiccional, se presentan demoras en relación a la digitalización de las audiencias, por cuanto aún no se logra que todas las audiencias tengan lugar con comparecencia virtual. La causa de tal situación es la falta de compra de licencias del *software* para videollamadas, un tema que debe solucionarse con rapidez para precautelar la salud no sólo de las partes procesales, sino también de los funcionarios públicos.

El último capítulo versa sobre los delitos informáticos y su introducción en la normativa penal ecuatoriana. Comienza con una concisa enunciación de las características y elementos esenciales de los delitos informáticos, y continúa con la explicación de los bienes jurídicos tutelados dentro de la esfera de los delitos informáticos. En este capítulo se expone el principio de territorialidad de la ley, que, en la perspectiva de Proenza, pierde su relevancia, por cuanto el uso indebido o ilegal dentro de Internet no se limita a un territorio específico; de forma que la cooperación internacional cobra importancia. La obra concluye con la explicación de los delitos informáticos y su regulación normativa dentro del Código Orgánico Integral Penal.

En suma, el presente libro está dirigido a quienes están interesados en conocer la interrelación entre la cibernética y el Derecho. El texto contiene explicaciones claras sobre conceptos complejos de la cibernética y, así, brinda al lector un apoyo al momento de comprender esta nueva rama del Derecho. El texto contiene la explicación no solo de términos de la rama de la cibernética, sino también de aquellas propias del Derecho Informático. El aporte de este texto en el ámbito académico es fundamental, pues es útil para que estudiantes de Derecho y abogados se informen sobre el Derecho Informático, y entiendan los fundamentos de la informática y su relación con el Derecho.

Referencia

Bell, Daniel. 1976. *El advenimiento de la sociedad post-industrial*. Madrid: Alianza.

POLÍTICA EDITORIAL

Cálamo, Revista de Estudios Jurídicos es la revista de la Facultad de Derecho de la Universidad de las Américas. Cálamo es una revista especializada en Estudios Jurídicos pensada para la comunidad científica y en general interesada por los estudios del Derecho y su relación con las demás ciencias. La revista recibe durante todo el año ensayos y artículos de investigación que aporten para el conocimiento y análisis del Derecho, así como estudios interdisciplinares que muestren las conexiones de esta disciplina con el todo social, desde la Filosofía, la Sociología y la Teoría Política y Constitucional, fundamentalmente.

Política por secciones

Todas las contribuciones recibidas, una vez validadas por el Comité editorial de Cálamo, serán evaluadas bajo la modalidad de revisión por pares.

Dossier: Es la sección principal de la revista. Los artículos que se publican bajo este rubro giran en torno a la temática principal que es el hilo conductor del número en cuestión. Es una sección que recibe trabajos de académicos internos y externos a la institución. Los artículos deben ser originales, inéditos y no estar simultáneamente postulados para publicación en otras revistas u órganos editoriales.

Ensayos: En esta sección se publican ensayos de diversas temáticas, independientes al tema central del Dossier. Es una sección que recibe trabajos de académicos internos y externos a la institución. Los ensayos deben ser originales, inéditos y no estar simultáneamente postulados para publicación en otras revistas u órganos editoriales.

Entrevista: Esta sección recoge entrevistas a académicos, profesionales del Derecho o figuras públicas vinculadas al escenario jurídico y político del país. Se reciben entrevistas realizadas por académicos internos y externos a la institución. Las mismas deben ser originales, inéditas y no estar postuladas para publicación simultáneamente en otras revistas u órganos editoriales. Se privilegian aquellas entrevistas relacionadas con el tema central del Dossier.

Reseña: Es una breve evaluación crítica o análisis reflexivo de un libro que haya sido publicado en los últimos dos años. En esta sección, se reciben trabajos de académicos internos y externos a la institución. Las reseñas deben ser originales, inéditas y no estar postuladas para publicación simultáneamente en otras revistas u órganos editoriales.

Normas de publicación

Requisitos para las secciones de Dossier y Ensayos

- El artículo debe estar precedido de un resumen no mayor a 800 caracteres con espacios, en español y en inglés.

- Los autores deben proporcionar de cinco (5) a ocho (8) palabras clave que reflejen el contenido del artículo y que no se repitan en el título del mismo; en español y en inglés.

- El título del artículo no podrá contener más de diez (10) palabras. El autor podrá ampliar la extensión del mismo utilizando un subtítulo. Sin embargo, si el editor sugiere cambios, serán aplicados en mutuo acuerdo.

- El artículo deberá contar con conclusiones y recomendaciones.

- La extensión de los artículos será de 30.000 a 45.000 cce (caracteres con espacios, incluyendo notas al pie y recuadros).

- El artículo en su totalidad deberá ajustarse a las normas de citación CHICAGO.

- El Centro de Publicaciones, en la etapa de edición, podrá realizar la corrección de estilo que considere necesaria.

- Los artículos que se ajusten a las normas señaladas se considerarán como recibidos y se procederá a notificar al autor. Los que no, serán devueltos a sus escritores.

Requisitos para la sección de reseñas

Además de cumplir con las mismas normas que los artículos del Dossier, en el caso de las Reseñas:

- No deben contar con resumen.

- Deben presentar los siguientes datos técnicos: apellidos y nombres del autor, año, título de la obra, edición, editorial, lugar, páginas de que consta. Luego puede señalarse la formación del autor, su competencia, experiencia, su fin al escribir la obra. También debe presentar la portada escaneada de la publicación.

- Tendrán que indicar cómo está organizado el texto (capítulos, partes, relatos, etc.), su ordenación o composición precisa, es decir, la manera en que sus diversas partes se relacionan y articulan entre sí construyendo una estructura.

- Por último, deben contar con conclusiones o juicios críticos, donde se hablará sobre las aportaciones y repercusiones teóricas, sociales, políticas, educativas, futuras, etc., y se hará un balance de las observaciones personales, reducidas a líneas generales.

- Tendrán una extensión de entre 3.000 y 5.000 *cce* (caracteres con espacios, incluyendo notas al pie y recuadros).

Orientaciones para los autores

Los artículos deben ser originales e inéditos, lo cual implica que, al momento de la recepción del artículo por el Centro de Publicaciones de la Facultad de Derecho, no habrán sido entregados a otra revista para su evaluación y publicación.

El autor deberá remitir junto al artículo un FORMULARIO DE AUTOR que será facilitado por la coordinación editorial de la revista, donde especifique su grado académico/ institución a la que se encuentra vinculado, el título del artículo, la fecha de envío y dirección (postal o electrónica). Además, debe indicar si desea que se publique su correo electrónico en el artículo.

ÍNDICE