Tema central

Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria

Government policies and data protection in Ecuador: ideas around health emergency

Luis Ordóñez Pineda

Docente de la Facultad de Ciencias Sociales, Educación y Humanidades de la Universidad Técnica Particular de Loja, Ecuador

Correo electrónico: loordonez@utpl.edu.ec

Orcid: https://orcid.org/0000-0002-0262-2212

Liliana Correa Quezada

Docente de la Facultad de Ciencias Sociales, Educación y Humanidades de la Universidad Técnica Particular de Loja, Ecuador

Correo electrónico: ldcorrea@utpl.edu.ec

Orcid: https://orcid.org/0000-0002-5834-3159

Andrea Correa Conde

Docente de la Facultad de Ciencias Sociales, Educación y Humanidades de la Universidad Técnica Particular de Loja, Ecuador

Correo electrónico: arcorrea@utpl.edu.ec

Orcid: https://orcid.org/0000-0002-9982-221X

Recibido: 13-diciembre-2021. Aceptado: 11-marzo-2022. Publicado: 15-julio-2022.

Resumen

Esta investigación tiene por objeto evidenciar la necesidad de fortalecer la tutela del derecho fundamental de protección de datos personales, mediante la formulación y ejecución de políticas públicas en Ecuador. Para dicho fin, en el contexto nacional, se analizó la política pública "Por una internet segura para niños, niñas y adolescentes" y se estudiaron tres sentencias de la Corte Constitucional al respecto. El estudio considera importante fortalecer instancias de garantía de protección de datos y que se subraye que existe información sensible, cuyo tratamiento

Estado & comunes, revista de políticas y problemas públicos. N.° 15, vol. 2, julio-diciembre 2022, pp. 77-97.
Instituto de Altos Estudios Nacionales (IAEN). Quito-Ecuador.
ISSN impreso: 1390-8081 - ISSN electrónico: 2477-9245
https://doi.org/10.37228/estado_comunes.v2.n15.2022.270

incide en el ejercicio de los derechos de las personas afectadas por la emergencia sanitaria. Frente a las intromisiones ilegítimas en la intimidad de las personas, se concluye que las políticas públicas fortalecen y coadyuvan a generar programas de prevención y concienciación para el respeto del derecho a la protección de datos personales en Ecuador, como lo que acontece en otros países de la región.

Palabras clave: políticas públicas, protección de datos, intimidad de las personas, garantías constitucionales, emergencia sanitaria.

Abstract

This research aims to demonstrate the need to enhance the fundamental right to data protection through public policy formulation and implementation in Ecuador. For this purpose, this study examined the public policy "For a safe internet for children and adolescents" as well as three rulings of the Constitutional Court. To this end, it is relevant to support instances that guarantee data protection and to underline that handling sensitive data can affect the exercise of the rights of persons affected by the health emergency. In the face of illegitimate intrusions into the privacy of individuals, public policies help to strengthen and generate prevention and awareness programs regarding the protection of personal data, both regionally and in Ecuador.

Keywords: public policies, data protection, privacy of people, constitutional guarantees, health emergency.

1. Introducción

En los sistemas jurídicos latinoamericanos, el desarrollo del derecho a la protección de datos personales refleja una gran influencia regulatoria originada a partir de otros contextos o realidades jurídicas, en su mayoría, apegados al modelo europeo, el cual se caracteriza por establecer un esquema de protección preventivo o proactivo, a partir del uso responsable de la información y que, en todo caso, promueve la garantía de "los principios de privacidad desde el diseño y por defecto, la aproximación a la protección de datos basada en el análisis de riesgos, la figura del Delegado de protección de datos, el fortalecimiento de los códigos de conducta, la exigencia de llevar un registro de las actividades del tratamiento" (Piñar, 2016, p. 14). En 2003 y 2012 Argentina y Uruguay, de forma respectiva, recibieron sendos reconocimientos de la Unión Europea por haber consagrado dentro de su marco de regulación nacional principios y derechos relativos a la protección de los datos de carácter personal (Ordoñez, 2017). Este modelo referencial, afianzado en el respeto de los derechos y libertades que se desprenden del tratamiento de la información personal –derivado de la protección de la intimidad y privacidad– ha llegado a significar el horizonte y, a la vez, el principal paradigma en el marco de implementación de mecanismos de protección para la tutela de este derecho fundamental.

En la actualidad, estimando los avances tecnológicos y procesos de integración comercial, se entiende que "el derecho fundamental a la protección de datos personales no trata de impedir el recurso a las nuevas tecnologías sino de conciliarlo con el respeto a la dignidad de la persona" (Troncoso, 2010, p. 595). En todo caso, asumiendo que la emergencia sanitaria ha planteado verdaderos desafíos para el respeto de los derechos y libertades fundamentales, hay que ser conscientes de que "la inusitada expansión de la vigilancia y control estatal por medio de tecnologías digitales para monitorear la posible transmisión del virus implica una importante regresión en materia de derechos humanos" (Bizberge y Segura, 2020, p. 71).

En el caso de Ecuador, la protección de datos personales se ha desarrollado en tres etapas: primero, la protección constitucional por medio del *habeas data*; segundo, la regulación de la información personal y de la intimidad con una perspectiva garantista mediante leyes sectoriales; tercero, el reconocimiento de un derecho fundamental a la protección de datos personales en la Constitución de 2008. Sin embargo, a partir de la promulgación de la Ley Orgánica de Protección de Datos (LOPD) de 2021, se da una cuarta etapa. Ahora bien, desde el paradigma constitucional ecuatoriano, la tutela de los bienes jurídicos que se desprenden de la protección de datos en la era digital tiene especial importancia, a partir de la diversidad de los medios que existen para la difusión de los datos personales y las intromisiones ilegítimas en las que puede derivarse en el momento en que no se cuenta con el consentimiento del titular de los datos. En este orden, el derecho a la protección de datos personales advierte una adecuada protección. Tipologías como la discriminación, actos de odio, humillaciones, acoso, entre otras, que se desprenden del mal uso de la información personal, requieren de un marco jurídico integral que promueva el efectivo ejercicio de los derechos y libertades informáticas. De esta manera, "las empresas de telecomunicaciones, los Gobiernos y las organizaciones de activistas digitales son los principales actores que no solo están condicionados por la infraestructura y las políticas públicas, sino que son quienes las producen y modifican" (Bizberge y Segura, 2020, p. 75).

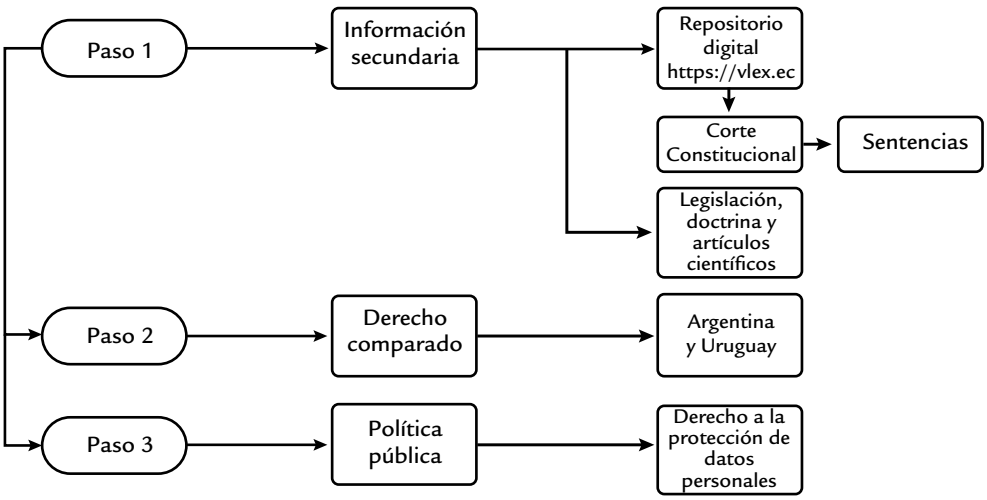
Conforme a estas circunstancias, por una parte, el derecho a la protección de datos requiere de un necesario equilibrio social, materializado por medio de un marco que desarrolle los principios, garantías y políticas relativas a la protección de los datos. Autores como Antonio Troncoso y Pérez Luño coinciden en la necesidad de "buscar equilibrio", desde el ámbito de relación entre la administración y los ciudadanos, en lo que respecta al tratamiento de la información. Este planteamiento sugiere un "pacto social", que garantice la proporcionalidad de las libertades que se desprenden del derecho a la protección de datos personales. Para este fin, Pérez Luño (2010) señala que es necesario "un adecuado ordenamiento jurídico de la informática, capaz de armonizar las exigencias de información propias de un Estado avanzado con las garantías de los ciudadanos" (p. 363). En especial, en la era de la información es imprescindible contar con políticas públicas, por cuanto, "del activismo social y las decisiones estatales depende que

esta situación adversa constituya una ventana de oportunidad para garantizar y ejercer más y mejores derechos" (Bizberge y Segura, 2020, p. 80).

La implementación de políticas y programas, idóneos para la difusión de las libertades informáticas, constituye un elemento cardinal para el ejercicio del derecho a la protección de datos. Así, la idea de políticas públicas supone que se "asuman total o parcialmente las tareas de alcanzar objetivos estimados como deseables o necesarios, por medio de un proceso destinado a cambiar un estado de las cosas percibido como problemático" (Roth, 2002, p. 27). Si bien, frente a la emergencia sanitaria, "los derechos digitales implican la protección y realización de derechos existentes, como el derecho a la privacidad, al acceso a la información, o a la libertad de expresión en el contexto de las nuevas tecnologías digitales y de conectividad" (Bizberge y Segura, 2020, p. 63) –conforme lo establece la Constitución de la República– debe entenderse que las políticas públicas están orientadas a hacer efectivos el ejercicio de todos los derechos, de manera particular, de las libertades relacionadas con la protección de datos personales. Por tanto, a partir de los efectos de la emergencia sanitaria en la privacidad de los titulares de los datos personales, esta investigación tiene por objeto describir la importancia de las políticas públicas en el marco de protección de los datos personales.

De esta manera el estudio se desarrolló en tres pasos metodológicos (gráfico 1). En el paso 1 se trabajó con información secundaria obtenida desde el repositorio digital https://vlex.ec/, en el que se obtuvo jurisprudencia vinculante mediante las sentencias de la Corte Constitucional: Resolución Nro. 19-9-SEP-CC, Resolución No. 1-14-PJP-CC y Resolución 182-15-SEP-CC, que son las que mejor han desarrollado el derecho a la protección de los datos personales. Además, se revisó la legislación, doctrina y artículos científicos relacionados con el tema de protección de datos personales. Mediante el paso 2 se realizó un estudio de derecho comparado con los países de Argentina y Uruguay, se los escogió por ser los dos países de la Comunidad Andina que han recibido por parte de la Unión Europea reconocimiento internacional con respecto a un manejo adecuado de la protección de datos personales. Por último, en el paso 3, con base en el análisis de los pasos anteriores se analizó en Ecuador el derecho a la protección de datos personales, tomando en cuenta la política pública "Por una internet segura para niños, niñas y adolescentes" (arcotel.gob.ec), definida como la primera política de la región que previene y mitiga riesgos en las redes sociales usadas por niños, niñas y adolescentes, considerados por el Estado ecuatoriano como personas y grupos de atención prioritaria.

Gráfico 1
Diagrama metodológico del estudio



Fuente: elaboración propia de los autores (2022).

Desde esta perspectiva, el presente artículo se subdivide en tres apartados específicos desarrollados de la siguiente manera. El primero describe la esencia y el contenido del derecho fundamental a la protección de datos personales en el marco de la emergencia sanitaria; el segundo aborda la garantía de la protección de datos desde el paradigma del neoconstitucionalismo contemporáneo o Estado constitucional de derechos y justicia en Ecuador; en tanto que el tercero conceptualiza a las políticas públicas como mecanismos de prevención y garantía del derecho a la autodeterminación informativa.

2. Discusión teórica y conceptual

2.1. Derecho de la protección de datos personales frente a la emergencia sanitaria

La información personal abarca una diversidad de aspectos relacionados con los derechos de personalidad. Entre ellos, los que se derivan de rasgos ideológicos, de salud, sexualidad, identidad, financieros, económicos, bancarios, comerciales y hasta de hábitos. Esta información se encuentra disponible en diferentes medios de información y comunicación, como las redes sociales, los blogs o, incluso, por medio de dispositivos que indican la ubicación en la que una persona se encuentra. Así, conviene considerar que las tecnologías "plantean retos para la protección de datos, dado que puede implicar la pérdida del control por parte de los individuos de su información potencialmente sensible cuando almacenan sus datos utilizando programas alojados en servidores ajenos" (Rallo, 2012, p. 18).

En el caso de Ecuador, el derecho a la protección de datos es un derecho fundamental por dos razones. La primera, por ser una libertad fundamental que se deriva de la teoría del constitucionalismo contemporáneo o neoconstitucionalismo, en el que "la concepción del Estado garantista es la del Estado constitucional de derechos, es decir, aquel que se construye sobre los derechos fundamentales de la persona y en el rechazo al ejercicio del poder arbitrario" (Resolución 344, 2016). Y, la segunda, porque su proximidad con la dignidad humana[1] advierte una dimensión ética, con una alta pretensión moral que debe ser atendida para hacer posible una vida digna (Peces-Barba *et al*., 2004, pp. 20 y 28). Esta libertad fundamental busca que el tratamiento de datos cumpla y respete una serie de principios, los cuales, en todo caso, aseguran a las personas un conjunto de garantías para que no se violenten derechos relacionados con la intimidad, dignidad, igualdad y no discriminación. En este orden de ideas, se transforma en un instituto de garantía de otros derechos, "fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento" (Rallo, 2017, p. 650).

Como se observa más adelante, en el marco del Estado constitucional de derechos, la protección de datos no puede estar alejada del principio de estricta legalidad, lo cual exige preservar ciertos aspectos que se relacionan con la moral pública, la seguridad nacional, la protección de grupos de atención prioritaria, el orden público y la salud en general; bienes jurídicos, relacionados con la dignidad, la intimidad, el honor, la imagen, el secreto fiscal o financiero. Así, puede ser evidente que "las autoridades públicas también utilizan cada vez más datos personales con distintos fines: para buscar personas cuando se declara una enfermedad transmisible, para prevenir y luchar más eficazmente contra el terrorismo y la delincuencia" (Rallo, 2012, p. 18). Desde este planteamiento, la protección de datos requiere de garantías que posibiliten ejercer el dominio de la información personal. En consecuencia, la protección de este derecho no solo corresponde a los individuos sino a toda la sociedad. Es decir, pasó de ser un derecho individual y privado a convertirse en un derecho público y colectivo (Pérez, 2010, pp. 228-230).

La dimensión del derecho a la intimidad, a la dignidad y al honor demuestra que el derecho a la protección de datos personales ha mutado, por diferentes circunstancias. La primera es el factor del ser, en el que el "ser social" prevalece sobre el "ser individual"; la razón parte de que el ser humano pertenece a un conglomerado social y no puede estar y mucho menos crecer en aislamiento. La segunda razón es que el desarrollo de las tecnologías ha ocasionado el surgimiento de nuevas formas en que el derecho a la protección de datos personales se ve afectado. Por ello, hoy en día debe considerarse que algunos modelos internacionales –el europeo, por

1 La Constitución de 2008 es la construcción de una sociedad que respeta, en todas sus dimensiones, la dignidad de las personas, de allí que el reconocimiento de este derecho fundamental coincida con el respeto de la dignidad de los individuos y tome en cuenta la diversidad de bienes jurídicos que pueden verse afectados por el mal uso, fin o tratamiento de datos personales.

ejemplo– exigen "adoptar decisiones propias en función de los tratamientos de datos que se lleven cabo y de la naturaleza de estos" (Piñar, 2016, p. 15). Este progreso plantea que los medios, recursos y preceptos para garantizar los derechos fundamentales también se actualicen y desarrollen, acorde con la época actual.

> Existe la percepción de que los tratamientos abusivos de datos personales menoscaban una parte importante de nuestra vida, por lo que es necesario, como señala Joseph Ratzinger, que la razón ética del hombre crezca al ritmo de la modernidad. Estamos, por tanto, ante la necesidad de proteger al hombre frente a las tecnologías de la información y las comunicaciones; ante la obligación de hacer presentes los derechos y tutelarnos en la era de Internet (Troncoso, 2010, p. 33).

Sobre este respecto, desde lo en estricto sentido individual, el derecho a la protección de datos personales ha pasado a tener un enfoque global. En todo caso, respecto al flujo transfronterizo de datos, la falta de armonía en los ordenamientos jurídicos "ha sido especialmente denunciada por los representantes de los sectores económicos (que en un mundo empresarial y económico globalizado dicen ver multiplicados los costes y los requisitos burocrático-administrativos nacionales) y se ha traducido en un cierto grado de inseguridad jurídica" (Rallo, 2012, p. 23). Todo ello conlleva a proyectar la búsqueda de un adecuado equilibrio del ordenamiento jurídico, el cual se direccione, sobre todo, a garantizar la seguridad jurídica, a partir de una legislación clara y de políticas públicas que canalicen en la sociedad la protección integral de este derecho.

> De ahí que tenga gran relevancia el contar con un ordenamiento legal coherente, principista y que incentive la realización de la transformación digital con un enfoque sistémico y proyección holística. Tener al ciudadano como centro en modo alguno constituye una mera declaración de voluntad; es en esencia un principio rector que tiene que instrumentalizarse en todo el proceso de participación y toma de decisiones (Amoroso, Bárzaga y Fabelo, 2020, p. 1009).

En este marco, la CRE reconoce y garantiza en el artículo 66, literal 19, —como un derecho de libertad— el derecho fundamental a la protección de datos personales. Asimismo, el artículo 362 garantiza la confidencialidad de información de los pacientes, en tanto que el artículo 66, literal 11 ofrece garantía para el tratamiento de los datos sensibles. A partir de las condiciones que plantea la seguridad jurídica, el marco de protección y regulación de este derecho debe orientarse a concretar normas claras y legítimas que, asegurando la confianza ciudadana, respeten de manera integral la Constitución y los principios establecidos en instrumentos internacionales.[2] Por tanto, el tratamiento de la información debe singularizarse, dentro de un marco jurídico integral y equilibrado, que atribuya al titular de los datos la capacidad de ejercer –con certeza y coherencia– el

2 La Sentencia 182-15-SEP de la Corte Constitucional de Ecuador advierte que, además, la seguridad jurídica "tiene como consecuencia el conocimiento y la confianza que tienen los ciudadanos respecto de que los diferentes aspectos y situaciones de la vida social se encuentran regulados y resueltos por normas y previstas en el ordenamiento jurídico". Véase la Resolución de la Corte Constitucional Nro. 182, Sentencia Nro. 182-15-SEP-CC –CASO Nro. 1493-10-EP–.

control sobre el uso y la finalidad de dichos datos. La promulgación de la LOPD en mayo de 2021 está llamada a desarrollar estos presupuestos, por cuanto en su exposición de motivos se invoca la imperiosa necesidad de generar confianza y garantizar las oportunidades que brindan los adelantos tecnológicos.[3] Como señalan dichas motivaciones, por una parte, todo esto "obliga a los países a realizar marcos jurídicos compatibles en distintos niveles: nacional, regional y mundial que faciliten el intercambio y al mismo tiempo respeten y protejan los derechos humanos" (LOPD, 2021); y, por otra, se espera que su normativa "salvaguarde los derechos, promueva la actividad económica, comercial, de innovación tecnológica, social, cultural, entre otras y delimite los parámetros para un tratamiento adecuado en el ámbito público y privado" (LOPD, 2021).

A propósito de la emergencia sanitaria de la covid-19, la protección de los derechos humanos acentúa la importancia del respeto de las obligaciones que tienen los Estados, tanto en el ámbito nacional como supranacional. La emergencia sanitaria –covid-19–, a más de afectar la vida de las personas en todos los ámbitos, también ha hecho reflexionar acerca de la importancia del derecho a la protección de datos personales. En el momento en que se conocieron los primeros casos de personas afectadas por la pandemia, en su mayoría, por intermedio de las redes sociales y medios de comunicación, se hizo pública información considerada sensible y de interés exclusivo de sus titulares, provocando reacciones, más negativas que positivas, que nos llaman a reflexionar.

En el caso de Ecuador, el Decreto Ejecutivo n.° 1017 del 16 de marzo de 2020, que declaró el Estado de excepción por calamidad pública, posibilitó, entre otras cosas, la utilización de plataformas satelitales y de telefonía móvil para monitorear la ubicación de personas en estado de cuarentena o aislamiento obligatorio y, por tanto, tratar datos personales de los ciudadanos para hacer el seguimiento y evitar el incumplimiento de las restricciones sobre movilidad. Así también, el Ministerio de Salud Pública (MSP), por medio de la Ley Orgánica de Salud, requirió a las instituciones privadas reportar sobre la existencia de casos de contagios sospechosos y confirmados. Algunas instituciones respondieron en el marco legal del decreto de excepción, cumpliendo las finalidades para las cuales el usuario haya consentido proporcionar sus datos. Por una parte, estas medidas se enmarcaron en los principios de seguridad y confidencialidad de los datos personales de sus empleados; así como en el tratamiento adecuado de información sensible. Por otra, recordando uno de los principios de aplicación de los derechos previsto en el artículo 11, literal 2, de la Constitución de Ecuador, se entiende que la protección de las personas afectadas por la pandemia debía enmarcarse en las garantías de igualdad y no discriminación, permitiendo la tutela de la información personal relativa a la salud, toda vez que el respeto del derecho a la protección de datos implica, además, una garantía que se ejerce, por medio de *habeas data*, descrita en el artículo 92, cuyo tercer inciso manifiesta que "en el caso de datos

3 La Ley Orgánica de Protección de Datos Personales fue publicada en el Registro Oficial, Quinto Suplemento, Nro. 459, el 26 de mayo de 2021. Fue aprobada por unanimidad con 118 votos afirmativos y una abstención –de un total de 119 asambleístas presentes–, durante la sesión 707 (en modalidad virtual) del pleno legislativo.

sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias".

No se trata de dejar de hacer uso de la tecnología y de limitar el tratamiento de datos –como es el caso del monitoreo de las personas contagiadas por la emergencia sanitaria–, por medio de las plataformas satelitales y de telefonía móvil, sino, que se respeten la garantía de protección de datos y, en suma, la vida privada de las personas. Además, entendiendo que la información relativa a la salud constituye una serie de datos muy sensibles, debe evitarse posibles discriminaciones e intromisiones ilegítimas que afecten a la intimidad y el derecho a la integridad personal de los pacientes. En este orden, es esencial estimar que "un marco ético debe sostener los cimientos de la construcción de un ecosistema digital como el señalado, partiendo del respeto y la salvaguarda de la dignidad, en tanto contrapeso fundamental a la vigilancia omnipresente y a la notoria asimetría de poder que ahora confronta a las personas" (Amoroso, Bárzaga y Fabelo, 2020, p. 1009).

Un claro ejemplo, en el ámbito internacional, de un adecuado respeto del derecho a la protección de datos frente a la pandemia es la aclaración que realizó la Agencia Española de Protección de Datos (AEPD), la cual señaló que la normativa de protección de datos personales no quedaba suspendida.[4] Por el contrario, las garantías del derecho fundamental permanecerían vigentes, en tanto estén dirigidas a salvaguardar un derecho fundamental, sobre todo, en la situación derivada de la emergencia sanitaria. Esta interpretación se sustentó en el Reglamento General de Protección de Datos de la Unión Europea (RGPD), el cual reconoce que: "en situaciones excepcionales, como una epidemia, la base jurídica de los tratamientos puede ser múltiple, basada tanto en el interés público, como en el interés vital del interesado u otra persona física" (Considerando 46 y las previsiones contempladas en los artículos 6 y 9 del RGPD, relativos a las bases de legitimación de las categorías especiales de datos personales).

En el inicio de la pandemia, Ecuador no contaba con una Ley de protección de datos que desarrolle este derecho fundamental, menos aún, normativa relacionada con los principios del tratamiento de la información, de manera específica, para el caso de los datos relativos a la salud. No obstante, a la luz del Estado constitucional de derechos y justicia, este derecho fundamental presentaba otras fuentes que debían observarse, atendiendo el paradigma del constitucionalismo contemporáneo y el respeto de la dignidad humana, toda vez que la protección de datos se ha manifestado como una libertad autónoma y una garantía instrumental reconocidas en el texto constitucional.

4 El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD), contiene las salvaguardas y reglas necesarias para permitir los tratamientos, de forma legítima, de datos personales en situaciones, como la presente, en que existe una emergencia sanitaria de alcance general. Estas prescripciones plantean que para el tratamiento de datos de salud no basta con que exista una base jurídica. Se requiere de una habilitación legal que levante la prohibición de tratamiento de dicha categoría especial de datos, de conformidad con los artículos 6 (licitud del tratamiento), 9.1 y 9.2 (circunstancias en las que queda prohibido el tratamiento de los datos personales) del RGPD.

Por tanto, como ha precisado la Corte Constitucional de Ecuador, se advierte que bajo este paradigma "el legalismo no es suficiente para considerar frenado o limitado al poder legislativo que, libérrimo en cuanto a dotar de cualquier contenido a las leyes, puede ejercerse, junto a su aplicación automática por parte de los operadores de la justicia, en forma autoritaria y despótica" (Resolución 344, 2016). Desde esta perspectiva, tanto el derecho a la protección de datos como la garantía de *habeas data* concretan la realización del buen vivir. En efecto, esto podría estar relacionado "con los casos en que se plantea la resignificación de la tecnología por vía de su inclusión en tanto paradigma central superador de la persona y en el centro de las relaciones que con ella se desenvuelven" (Amoroso, Bárzaga y Fabelo, 2020, p. 1010). Es decir, en la convivencia pacífica y respetuosa de los hombres en la sociedad, toda vez que el derecho a la protección de datos es una obligación directa del Estado y particulares, a partir del respeto del principio de estricta legalidad.

2.2. Derecho a la protección de datos en el Estado constitucional de derechos y justicia

La Corte Constitucional de Ecuador (CCE) precisa que la CRE establece una nueva forma de Estado, "cuyos rasgos básicos son: 1) el reconocimiento del carácter normativo superior de la Constitución, 2) la aplicación directa de la Constitución como norma jurídica, y, 3) el reconocimiento de la jurisprudencia constitucional como fuente primaria del derecho" (Resolución, s. n., 2008). Así, el derecho a la protección de datos personales se transforma en una norma o regla de decisión que está "por encima del resto de las normas jurídicas y vincula a todos los sujetos públicos y privados en todas sus actividades" (*Ibid.*). Por ello, la ausencia de disposiciones o medidas relativas a la protección de datos personales en la emergencia sanitaria, no impide –o no debería– a que, en el ámbito público o privado, se garantice su ejercicio y aplicación.

Al respecto, "son todas las funciones del Estado, todas las autoridades públicas y en ocasiones los particulares, y no solo los jueces, los obligados a respetar y hacer respetar los derechos fundamentales que establece la Constitución" (Grijalva, 2012, p. 252). En este sentido, la CRE advierte que los derechos "serán plenamente justiciables. No podrá alegarse falta de norma jurídica para justificar su violación o desconocimiento" (artículo 11, literal 3). Incardinado a este primer rasgo, en el Estado constitucional de derechos y justicia, la Constitución se manifiesta como una norma jurídica de aplicación directa –principio de eficacia directa– que "implica que los jueces y los demás operadores jurídicos, incluyendo los particulares, habrán de tomar a la Constitución como una regla de decisión" (Resolución s. n, 2008). Por tanto, uno de los efectos de este principio es que "no se requiere de intermediación de autoridad alguna para que se pueda invocar el cumplimiento de una norma. Los pretextos de falta de Ley o reglamento para excusarse de cumplir un derecho, tan comunes en un estado burocratizado, no tienen cabida" (Ávila, 2012, p. 77).

Frente a estos primeros supuestos, el Estado constitucional de derechos y justicia propone una nueva forma de Estado, en el que el respeto y la garantía de los derechos fundamentales están por encima de cualquier ordenamiento secundario, mandato, e incluso, falta o ausencia de normativa. Hay que insistir en que "en el neoconstitucionalismo toda norma constitucional es aplicable, aun cuando tenga la estructura de un principio [...] Por supuesto que esta afirmación implica que las personas están sometidas además de la Ley a la Constitución" (Ávila, 2012, p. 75). Bajo este principio –que se conoce como de estricta legalidad– el derecho a la protección de datos personales obliga a que, en el ámbito público y privado, el tratamiento de la información respete las condiciones, facultades y principios que la Constitución prescribe.

Además, la aplicación directa e inmediata de los derechos y garantías se concreta en el respeto y aplicación de instrumentos internacionales. La Guía Legislativa de la Organización de Estados Americanos (OEA) de 2015 –actualizada en 2021–, plasmada en los "Principios de privacidad y protección de datos personales"[5] y los "Estándares de protección de datos personales"[6] de 2017 para los Estados Iberoamericanos, se manifiestan como instrumentos que proponen en el ámbito de las Américas apuntar hacia un modelo regional uniforme y coherente. La Corte Interamericana de Derechos Humanos, en la Opinión Consultiva 24/17 de 2017 "sobre identidad de género, e igualdad y no discriminación a parejas del mismo sexo", ya ha destacado que la Guía Legislativa de la OEA significa un importante instrumento regional destinado a proteger a los titulares de los datos, frente a intromisiones ilegítimas.[7] Así también, a propósito de la emergencia sanitaria, la Resolución No. 1/2020, adoptada por la CIDH, contiene prescripciones respecto a la garantía y plena vigencia del derecho a la protección de datos durante la pandemia.[8]

5 La finalidad de estos principios plasmados en la Guía legislativa de la OEA es "establecer un marco para salvaguardar los derechos de la persona a la protección de los datos personales y a la autodeterminación en lo que respecta a la información". Cfr. Guía legislativa de la OEA. Veáse https://tinyurl.com/mpn4mz8s.

6 Los "Estándares de protección de datos personales para los Estados Iberoamericanos" fueron aprobados por unanimidad el 20 de junio de 2017 por la Red Iberoamericana de Protección de Datos (RIPD), de los que Ecuador forma parte en calidad de país observador. Cfr. Estándares de protección de datos personales para los Estados Iberoamericanos. Véase https://tinyurl.com/y8wvqzb2.

7 Cfr. Corte Interamericana de Derechos Humanos. Opinión Consultiva 24/17 de 2017 "sobre identidad de género, e igualdad y no discriminación a parejas del mismo sexo". Véase https://tinyurl.com/2p9duxcz. Esta Opinión Consultiva significa un importante precedente en materia de protección de datos, a partir de la interpretación que hace la CIDH sobre la Guía Legislativa de la OEA. Esta cuestión ya ha sido analizada en otro momento, considerando que "la Opinión Consultiva OC-24/17 significa un avance no solamente en derechos relativos a la identidad de género, sino que además representa un importante precedente jurídico internacional en materia de protección de datos personales" Cfr. Ordóñez (2019). El procedimiento de solicitud de adecuación de los datos de conformidad con la identidad de género. Reflexiones desde el derecho fundamental a la protección de datos. *Revista de Derecho Foro* (32), pp. 2631-2484. Véase https://tinyurl.com/mrxaz7zm.

8 Dicha resolución manifiesta la necesidad de "proteger el derecho a la privacidad y los datos personales de la población, especialmente de la información personal sensible de los pacientes y personas sometidas a exámenes durante la pandemia" (Resolución 1, 2020).

De esta forma, en nuestro paradigma constitucional, el derecho a la protección de datos impone la obligación de respetar y hacer respetar no solo el ordenamiento constitucional sino, además, los instrumentos internacionales que prescriban normas y políticas públicas relacionadas con la garantía de la información personal. Si bien, son pocos los instrumentos regionales que se han desarrollado en la materia, su observancia contribuye a la tutela de los derechos de las personas y al fortalecimiento del sistema internacional de protección de derechos humanos. Ahora bien, la CCE reconoce como un tercer pilar del Estado constitucional de derechos y justicia a la jurisprudencia constitucional. Así, frente a este paradigma, dicho pilar se destina a invalidar las normas que atenten al ejercicio de los derechos a partir de precedentes jurisprudenciales vinculantes, que aseguren la correcta aplicación y justiciabilidad de los derechos. Al respecto, se destaca que:

> La Corte Constitucional puede y debe, basada en la interpretación jurídica de la propia Constitución y al respeto a la libertad de configuración legislativa, marcar constantemente los parámetros normativos que el legislador debe observar para que sus Leyes no violen los derechos constitucionales, y por el contrario los concreten, desarrollen y regulen, conforme lo establecen el artículo 11, numeral 8,18 y 11, numeral 1 de la Constitución [...] El desarrollo jurisprudencial de los derechos tiene, justamente, como ventaja su nivel de concreción respecto a la dimensión comparativamente más abstracta y general en que opera el legislador. En términos hermenéuticos, como se sabe, incluso las dificultades y posibilidades de interpretación de las normas pueden mostrar nuevas facetas al confrontarse con los hechos y contextos de conflictos específicos (Grijalva, 2012, pp. 229 y 231).

Siendo la jurisprudencia constitucional un resultado de la actividad interpretativa de la CCE, el desarrollo del derecho a la protección de datos se ha concretado en varias resoluciones. En todo caso, considerando su inclusión en la actual CRE, la especificación del derecho a la protección de datos en la jurisprudencia constitucional es, de manera relativa, significativo. Son tres sentencias las que se destacan luego de este reconocimiento. Las Resoluciones 19-9-SEP-CC, 1-14-PJP-CC y 182-15-SEP-CC de la CCE constituyen importantes bases para la protección de este derecho en el Estado constitucional de derechos y justicia. Así, la Resolución n.° 19-9-SEP-CC advierte que el *habeas data* constituye:

> Una garantía constitucional con objetivos muy precisos, que busca que el accionante sepa: 1) Cuáles son los motivos legales por los que el poseedor de la información llegó a ser tenedor de la misma; 2) Desde cuándo tiene la información; 3) Qué uso se ha dado a esa información y qué se hará con ella en el futuro; 4) Conocer a qué personas naturales o jurídicas, el poseedor de la información hizo llegar la misma; por qué motivo, con qué propósito y la fecha en la que circuló la información; 5) Qué tecnología usa para almacenar la información; y, 6) Qué seguridades ofrece el tenedor de la información para precautelar que la misma no sea usada indebidamente (Resolución 19, 2009).

El uso de las tecnologías de la información y comunicación es una de las características del siglo XXI. En este marco, el uso ilícito de estas tecnologías representa serios riesgos en la protección de los datos personales. Tomando en cuenta que tanto el *habeas data* como el derecho a la protección de datos constituyen un derecho en sí mismo, en una sociedad digital, la garantía de los datos personales supone "conocer a qué personas públicas o privadas, naturales o jurídicas, el titular de los archivos o bases de datos, transmitió informaciones personales referentes al sujeto que ejercita la acción" (Pérez-Luño, 2017, p. 119). Frente a ese conocimiento, el *habeas data* permite ejercer la facultad de "comprobar si la información es actualizada y correcta y, de no serlo, solicitar y obtener su actualización o rectificación" (*ibid*., 2017, p. 119).

Por otra parte, la Resolución No. 1-14-PJP-CC de la CCE se dedica, de forma expresa, a fijar algunas reglas jurisprudenciales vinculantes.[9] Así, respecto al derecho a la protección de datos, precisa "la posibilidad de que dentro de los límites que franquean la Constitución y la Ley, se tenga capacidad para ejercer cierto control sobre el uso que se haga de tal información, aunque el poseedor de la misma sea otra persona" (Resolución 1, 2014). Dicha protección –junto con las disposiciones de la LOPD de Ecuador, la cual ha tomado como base el RGPD y los EPEI– supone un esquema de regulación compuesto por un nuevo modelo que "pasa de la gestión de los datos al uso responsable de la información [...] reforzando los derechos de los interesados y estableciendo nuevas obligaciones de los responsables y encargados, que han de acostumbrarse a asumir un papel mucho más proactivo y responsable" (Piñar, 2016, pp. 14 y 20).

Por último, la Resolución 182-15-SEP-CC determina que los derechos y garantías (arts. 66.19 y 92) reconocidos en la CRE tienen un "carácter autónomo, por cuanto, posee un perfil propio regulado tanto en la Constitución como en la Ley de la materia y tutela datos o información inherente a una persona, a fin de salvaguardar su derecho a la intimidad personal y familiar" (Resolución 182, 2015). Y que, además, el *habeas data* protege una órbita específica, "esto es, la información íntima de una persona, la cual puede estar contenida en diversas formas, tales como documentos, datos genéticos, bancos o archivos de datos personales" (Resolución 182, 2015).

A partir de factores políticos y sociales que originan una cultura de inconstitucionalidad, "es necesario ubicar qué aportes pueden generarse desde el mundo del derecho para superar esta situación. El desarrollo de una jurisprudencia constitucional que contribuya a la definición de los derechos es sin duda uno de estos aportes" (Grijalva, 2012, p. 229). Frente a las asimetrías que plantea la emergencia sanitaria, respecto a la justiciabilidad de los derechos, la jurisprudencia constitucional –como una fuente primaria del derecho– facilita la correcta

9 En esta Resolución, la CCE ha señalado que "el derecho a la protección de datos –y específicamente, su elemento denominado 'autodeterminación informativa'– tiene un carácter instrumental, supeditado a la protección de otros derechos constitucionales que se pueden ver afectados cuando se utilizan datos personales, como puede ser la intimidad, la honra, la integridad psicológica, etc." (Resolución 1, 2014).

interpretación jurídica y garantía del derecho a la protección de datos personales. No obstante, en la práctica, su garantía requiere mucho más. Como señala la CRE, los derechos no solo deben desarrollarse en la jurisprudencia o normativa secundaria, sino también por medio de políticas públicas. Así, entendemos que "los derechos humanos y en especial los derechos sociales pueden y deben ser criterios consistentes de diseño, ejecución y evaluación de las políticas públicas" (*ibid*., p. 61).

En todo caso –a partir de las medidas de seguridad contenidas en el capítulo Vl de la LOPD de Ecuador– debe considerarse que las políticas públicas pueden significar una magnífica oportunidad para potenciar, por ejemplo: las medidas de seguridad en el ámbito del sector público (artículo 38); la privacidad y la protección de los datos personales desde el diseño y por defecto (artículo 39); las evaluaciones de impacto del tratamiento de datos personales (artículo 42); y las notificaciones de vulneración de seguridad (artículo 43). Se trata, como se ha advertido, de constituir un modelo proactivo de manejo responsable de la información, en el que todas las medidas que se adopten "podrán consistir en la aplicación de las oportunas políticas de protección de datos. Es decir, la prevención y el cumplimiento normativo pasan a ocupar un papel principal en la protección de datos" (Piñar, 2016, pp. 18-19).

La misma CCE, a propósito de la emergencia sanitaria, ha recalcado la necesidad de "políticas públicas efectivas, con planificación y control permanente, por parte del Gobierno [...] políticas públicas de conformidad con lo dispuesto en la Constitución y con enfoque en los derechos reconocidos en ella" (Dictamen 2-21, 2021). "Los tiempos de covid-19 han alentado la guerra tecnológica desde diversos ángulos. En primer lugar, ha puesto en el centro de la discusión en temas acerca de tecnología digital y política comunicacional la interrogante de: ¿Quién controla nuestros datos?" (Amoroso, Bárzaga y Fabelo, 2020, p. 1003). Por ello, es indispensable concienciar a la Administración pública y particulares sobre un manejo responsable de la información personal. *A priori*, se advierte la necesidad de una cultura de prevención, frente a las intromisiones ilegítimas en la intimidad de los datos de carácter personal. En el Estado constitucional de derechos y justicia, las políticas públicas pueden considerarse como garantías preventivas que "tratan de evitar la violación de derechos" (Ávila, 2012, p. 188).

2.3. Políticas públicas y la necesidad de resignificar la prevención y la concienciación

En Ecuador, las políticas públicas no han logrado ajustarse a las necesidades que requiere el ejercicio del derecho fundamental a la protección de datos. El concepto de políticas públicas supone la idea de un cambio, a partir de la identificación de un problema que requiere atención y regulación desde la instancia gubernamental. Así, estas garantías preventivas emergen "de una construcción social y de una construcción de un objeto de investigación" (Roth, 2002, p. 28) orientadas a definir el quehacer del Estado, frente a un determinado problema.

Aquellos países que han recibido reconocimiento internacional por parte de la Unión Europea han afianzado el desarrollo de políticas de prevención mediante prácticas asociadas con las autoridades de protección de datos. En la región constituyen ejemplos el Programa Nacional "Con Vos en la Web" en Argentina, que se ejecuta por intermedio de la Agencia de Acceso a la Información Pública (AAIP). Dicho programa es una iniciativa del Ministerio de Justicia, dirigido a concienciar y desarrollar, en padres, docentes, alumnos y ciudadanía en general: "conductas seguras y responsables en el uso de dispositivos tecnológicos conectados a Internet y en el manejo de sus datos privados y personales". En el caso de Uruguay, la Unidad Reguladora y de Control de Datos Personales (URCDP) constituye un ente de regulación y control que ha implementado políticas sobre las implicaciones tecnológicas y culturales que se desprenden del tratamiento de la información personal, mediante el programa "Tus datos Valen. Cuídalos". Además, en el ámbito europeo destaca la actividad que desarrolla la Agencia Española de Protección de Datos (AEPD), mediante programas de protección de datos relacionados con la emergencia sanitaria; internet y redes sociales; violencia de género; junto con educación y menores "Tú decides en internet".

En Ecuador, aunque no como política pública, destaca la campaña "Mis datos soy yo", desarrollada, a partir de 2018, por la Dirección Nacional de Registros Públicos (Dinarp), que tiene por objetivo enseñar a los jóvenes la importancia de la protección de su información personal. Sin embargo, en septiembre de 2020, el Consejo Nacional para la Igualdad Intergeneracional (CNII) implementó la "Política pública por una internet segura para niños, niñas y adolescentes", la cual se orienta a "promover una cultura preventiva para el uso seguro de la internet y las tecnologías digitales, así como el adecuado seguimiento y sanción en caso de vulneraciones de derechos" (CNII, 2020, p. 6). Si bien son iniciativas dirigidas a menores de edad, el vacío existente frente a la emergencia sanitaria ha dejado al descubierto la carencia de políticas públicas en la materia.

En todo caso, la "política pública para una internet segura" desarrollada por el Consejo Nacional para la Igualdad Intergeneracional constituye un modelo referencial de un tipo de política de pública que precisa las bases para formular programas de prevención, frente al tratamiento de datos personales en la pandemia, por cuanto está construida o formulada desde un enfoque, tanto de protección como de fortalecimiento de los derechos digitales en la era de las tecnologías de la información y comunicación. Así, como advierte esta propuesta:

> Los derechos humanos son aplicables y exigibles en el mundo online con la misma intensidad que en el mundo real, los Estados tienen la responsabilidad de proteger y garantizar los Derechos Humanos, esta obligación incluye: i) La protección contra los abusos a través de internet y las nuevas tecnologías; ii) Igual derecho sin discriminación a acceder y utilizar internet de forma segura y libre; iii) Derecho a buscar, recibir y difundir información libremente en internet sin censura ni interferencias; iv) Derecho a asociarse libremente a través de internet, con fines sociales, políticos, culturales o de otro tipo; v) Derecho a la privacidad online, esto incluye el no ser vigilado, el derecho

> a utilizar cifrado y el derecho al anonimato; vi) Derecho a la protección de datos, el control sobre la recolección, retención, transformación, eliminación y divulgación de sus datos personales, entre otros (CNII, 2020, p. 25).

De esta forma, el Estado ecuatoriano tiene el más alto deber de respetar y hacer respetar los derechos y libertades fundamentales que son inherentes a los titulares de los datos personales, lo cual se traduce en la responsabilidad y la obligación interinstitucional de ejecutar programas que promuevan la garantía del derecho a la protección de datos personales en la emergencia sanitaria. En este orden, la normativa de protección de datos personales, en nuestro país, coincide en que será la autoridad de protección de datos la que promueva e incentive, tanto en el ámbito público como privado, el ejercicio de este derecho fundamental, "así como la concientización en las personas y la comprensión de los riesgos, normas, garantías y derechos, en relación con el tratamiento y uso de sus datos personales" (LOPD, 2021). No obstante, también dicha normativa exige que la administración –en suma, a los responsables del tratamiento– implemente "políticas de protección de datos personales afines al tratamiento de datos personales en cada caso particular" (LOPD, 2021). Así, como se ha señalado en otro momento, esto obliga a que se observe el principio de responsabilidad proactiva: "un deber de la administración de asegurar, no solamente, las facultades de control y disposición de la información personal sino, además, [de] establecer medidas proactivas y preventivas, frente a su tratamiento" (Ordóñez, 2021, p. 151).

Como advierte la política del CNII, "los avances de nuestras sociedades hacia las tecnologías digitales en los últimos años han sido acrecentados; sin embargo, la emergencia sanitaria causada por la covid-19 trajo consigo que la digitalización sea mucho más acelerada" (CNII, 2020, p. 5). Según la CIDH, este escenario supone que "el almacenamiento de datos de las personas con covid-19 debe estar limitado al fin legítimo y limitado de contener y revertir la pandemia, por el tiempo estrictamente necesario y estarán desvinculados de la identidad y otros aspectos personalísimos" (Resolución 4, 2020).

Por ello, la implementación de una política pública que garantice el derecho a la protección de datos personales frente a la emergencia sanitaria debería contener los siguientes ejes: a) cumplimiento del marco legal previsto en la Constitución, la LOPD e instrumentos internacionales ; b) medidas técnicas y organizativas apropiadas que promuevan el tratamiento lícito de datos en el marco de la pandemia y que aseguren la garantía de los derechos y libertades que se desprenden del derecho de autodeterminación informativa; c) seguimiento y control a las distintas estructuras organizacionales, mediante la actividad de evaluación y vigilancia que le corresponde a la autoridad de protección de datos; d) capacitación a las instituciones que conforman el Sistema Nacional de Salud, respecto a los deberes que corresponden a los responsables del tratamiento y a los derechos de los titulares de los datos; y, e) posibilitar canales de promoción y difusión que promuevan la comprensión de los riesgos que implica utilizar datos personales sensibles. Como ocurre en el ámbito internacional, los recursos para su ejecución serán dispuestos

por la autoridad de protección datos, como parte de las garantías formales de independencia o autonomía financiera.[10]

Bajo estas consideraciones, las políticas públicas como garantía de la protección de datos son imprescindibles, por cuanto, por una parte, "la implementación de nuevas tecnologías sustentadas en el tratamiento de datos personales, unido al uso de técnicas propias de la analítica de datos e inteligencia artificial, comportan importantes beneficios y representan una importante oportunidad para ganar la batalla al covid-19" (Domínguez, 2020, p. 610); y, por otra, "los responsables del tratamiento, en aras de garantizar su correcta actuación y salvaguardar de forma efectiva los intereses vitales de la ciudadanía, deberán actuar conforme a las instrucciones facilitadas por las autoridades sanitarias" (*ibid*., 2020, p. 615). En este orden, con la participación de la autoridad de protección de datos personales y las instituciones que conforman el Sistema Nacional de Salud, las políticas públicas como garantías de prevención implican el diseño de un conjunto de acciones interinstitucionales del Estado, que buscan contribuir y dar solución a un problema de la sociedad. Por ejemplo, garantizar el derecho a la protección de datos frente a la emergencia sanitaria. En todo caso, las alternativas que se propongan como políticas públicas no serán suficientes, permanentes y de acción sostenida si es que no se trabaja a la par en la concienciación y prevención del problema social. Bajo estas consideraciones, advertimos que:

> Varios estudios plantean la necesidad de abordar dos cuestiones centrales: cómo puede el ciudadano recuperar el control sobre la información que ha generado y cómo imaginar un modelo alternativo para una economía de datos que reduzca la actual asimetría entre la información que las grandes plataformas tienen de sus usuarios y la falta de transparencia sobre los algoritmos y modelos de negocio con que estos datos se procesan y explotan (Amoroso, Bárzaga y Fabelo, 2020, p. 999).

Asimismo, considerando que la protección de datos tiene una tutela constitucional, aquello implica que se deberá enmarcar en un desarrollo en "Leyes sectoriales y las políticas públicas y privadas que se implementen en la práctica a través de sus autoridades de control y supervisión" (Ordóñez, 2017, p. 99). En todo caso, entendiendo que "la salvaguardia de los intereses esenciales en el ámbito de la salud pública corresponde a las distintas autoridades sanitarias de las diferentes Administraciones públicas, quienes podrán adoptar las medidas necesarias para salvaguardar dichos intereses esenciales públicos en situaciones de emergencia sanitaria de salud pública" (Domínguez, 2020, p. 616); esto significa reconocer y respetar los principios que se desprenden del derecho a la protección

10 Por ejemplo, el Reglamento General de Protección de Datos de la Unión Europea (RGPD) determina como una garantía de independencia de la autoridad de control que esta "disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes". Si bien el principio el principio de independencia se encuentra recogido en el artículo 10, literal m, de la LOPD, es necesario subrayar la necesidad de que el reglamento a dicha ley deberá desarrollar las suficientes garantías formales de independencia, en las que se incluye la autonomía presupuestaria, financiera y la disponibilidad de recursos económicos para el cumplimiento de sus funciones.

de datos, "con el fin de asegurar que el tratamiento de la información responda a unos fines legítimos y, sobre todo, que este se enmarque en el instituto de garantía que comprende el derecho a la protección de datos" (Ordóñez, 2021, p. 152).

Por otra parte, no está por demás señalar que la CIDH, en la Resolución n.° 1/2020, precisa que "toda política pública con enfoque de derechos humanos para la prevención, atención y contención de la pandemia requiere un abordaje amplio y multidisciplinario a partir del fortalecimiento de mecanismos de cooperación internacional entre Estados"; de tal manera que se consoliden canales para el intercambio de buenas prácticas, políticas públicas e información oportuna para enfrentar la crisis global provocada por la covid-19. En este marco, en Uruguay la URCDP ha formulado varias recomendaciones, para las personas y las entidades públicas o privadas que realizan tratamiento de datos asociados a la covid-19; y enfatiza en la reserva y cuidado de la información. Entre ellas, "desaconseja el uso de formularios o sistemas en línea que no brinden las debidas garantías de seguridad o confidencialidad en el tratamiento de los datos personales".

Así también, en Argentina, la AAIP presentó algunas acciones respecto al uso de herramientas de geolocalización y sondeo continuo, empleadas tanto en el sector público como privado durante la emergencia sanitaria; considerando que "la recopilación de datos de ubicación podrá realizarse cuando: el titular de los datos haya prestado su consentimiento libre, expreso e informado; los datos se obtengan de fuentes de acceso público irrestricto; se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; y, se deriven de una relación contractual, científica o profesional del titular de los datos y resulten necesarios para su desarrollo o cumplimiento". Por ello, las políticas que quedan señaladas en el ámbito internacional son un elemento clave y sustancial para promover en el país la efectiva garantía de los derechos a la privacidad y protección de datos de las personas, siempre que se fomente, tanto en la ciudadanía como en la administración, una verdadera cultura sobre el cuidado y difusión de sus datos personales.

En el caso de Ecuador, a excepción de la "política pública para una internet segura" desarrollada por el Consejo Nacional para la Igualdad Intergeneracional, con motivo de la actual situación sanitaria, no se evidencian iniciativas sobre buenas prácticas en el manejo y uso de los datos de salud en las instituciones públicas y privadas. Tampoco se han formulado estrategias educativas específicas dirigidas a la sociedad que ayuden a prevenir, concienciar y proteger la información general y, en especial, la relacionada con la pandemia de la covid-19. La sociedad civil, en el ejercicio de sus derechos fundamentales, solicita del Estado la protección, transparencia y control en el uso y tratamiento de sus datos personales por medio de garantías preventivas constituidas en políticas públicas; así como su participación activa y responsable para fomentar una cultura de prevención y concienciación de los titulares de la información que mucha falta hace, en especial, en época de emergencia sanitaria. Por ello, se advierte la necesidad de que el Estado ecuatoriano proponga políticas públicas que garanticen y respeten la privacidad

de las personas, de manera tal que se genere una cultura de corresponsabilidad a la hora de compartir información personal.

3. Conclusiones

El derecho fundamental a la protección de datos responde a los avances tecnológicos, el uso de internet y la globalización. Las exigencias para la protección integral de la información personal son cada vez más considerables e imprescindibles y, por tanto, los presupuestos que lo constituyen deben ser fortalecidos con la formulación de garantías preventivas. El Estado constitucional de derechos y justicia proyecta un significativo paradigma para la protección de datos, el cual exige de todos los poderes del Estado y particulares la adopción de mecanismos de prevención y tutela para la efectiva vigencia de los derechos que se desprenden del derecho a la protección de datos, sin que pueda alegarse falta de normativa para justificar su violación o desconocimiento.

Las políticas públicas deben encaminarse a la efectiva prevención y concienciación sobre el correcto uso y tratamiento de datos, con el fin de reorientar y difundir una cultura de seguridad y respeto sobre el derecho a la protección de datos. En todo caso, frente a la emergencia sanitaria ocasionada por la covid-19, la garantía de este derecho advierte la necesidad de contar con políticas públicas que hagan efectivos los derechos de las personas sobre la base de la dignidad humana y, sobre todo, permitan desarrollar concienciación y educación sobre los riesgos que implica compartir información sensible, sin el consentimiento del titular. De manera evidente, para concretar el desarrollo de estos objetivos, un papel esencial cumplirá la autoridad de protección de datos, en calidad de órgano de supervisión y control de la normativa. En los últimos años se observa una marcada proactividad en el funcionamiento de estas autoridades de control, lo que se ha traducido en nuevas formas de intervención administrativa novedosas e innovadoras orientadas a la concienciación en materia digital del conjunto de la población.

La intromisión del Estado ecuatoriano en relación con el derecho a la protección de datos personales, de forma específica en la salud en el contexto de los primeros momentos de la covid-19, pudo considerársela como ilegal, sin embargo, debe analizarse que, en una crisis de salud global, el uso de los datos debe ser manejado por los órganos y autoridades estatales siempre pensando en el beneficio de la colectividad, cuidando la seguridad y supervivencia de la población. La protección de datos personales en Ecuador no posee una reglamentación concerniente a salud, sin embargo, cuenta con una ley orgánica y con jurisprudencia cuyos principios y normas jurídicas pueden ser utilizados a plenitud para una interpretación y aplicación ética en el momento en que las circunstancias lo ameriten. No obstante, aún falta concienciar a la Administración pública y a los particulares sobre la intimidad de los datos de carácter personal, sobre todo en el sector salud en el ámbito digital.

La política de "Por una internet segura para niños, niñas y adolescentes" tiene por finalidad empoderar a la ciudadanía, en especial, a los padres de familia y personas o instituciones en calidad de garantes de los derechos de los menores de edad para que se eduque en el uso de las herramientas y mecanismos tecnológicos; para que se acompañe en los aprendizajes primeros de las redes sociales y otros medios de interacción tecnológico de los menores; así como para que se ayude a prevenir los múltiples riesgos al que se expone esta población vulnerable de la sociedad, pues esta información sensible se constituye en un modo lucrativo y pernicioso que debe ser vigilado de forma permanente y denunciado a los correspondientes organismo de control.

4. Referencias bibliográficas

Agencia Española de Protección de Datos [AEPD] (2020). *Gobernanza y política de protección de datos*. Ministerio de Justicia. Recuperado de https://tinyurl.com/y3k8vo7b

Amoroso, Y., Bárzaga, M., y Fabelo, S. (2020). Guerra tecnológica y resignificación de la dignidad humana. *Revista Direitos Sociais e Políticas Públicas (Unifafibe)*. Recuperado de https://tinyurl.com/2p8ajfbc

Asamblea Nacional (2021). *Ley Orgánica de Protección de Datos Personales de Ecuador*. Registro Oficial n.° 459.

Asamblea Nacional Constituyente (2008). *Constitución de la República del Ecuador*. Registro Oficial n.° 449.

Ávila, R. (2012). *Los derechos y sus garantías: Ensayos críticos*. Corte Constitucional para el período de transición (Centro de Estudios y Difusión del Derecho Constitucional-Cedec).

Bizberge, A., y Segura, M. (2020). Los derechos digitales durante la pandemia COVID-19 en Argentina, Brasil y México. *Revista de Comunicación*. Recuperado de https://tinyurl.com/muh22edr

Comisión Interamericana de Derechos Humanos [CIDH] (10 de abril de 2020). *Resolución n.° 1/2020 Pandemia y Derechos Humanos en las Américas*. Organización de los Estados Americanos. Recuperado de https://tinyurl.com/y8uehpx2

_____ (27 de julio de 2020). *Resolución n.° 4/2020 Derechos Humanos de las personas con COVID-19*. Organización de los Estados Americanos. Recuperado de https://tinyurl.com/5hvhujvx

Consejo Nacional para la Igualdad Intergeneracional [CNII] (2020). *Política Pública para una internet segura para niños, niñas y adolescentes*. Recuperado de https://tinyurl.com/y2fcv9el

Corte Constitucional del Ecuador (20 de octubre de 2008). Resolución s.n. Registro Oficial n.° 451 Suplemento. Recuperado de https://tinyurl.com/yxkacab9

_____ (20 de agosto de 2009). Resolución 19-9 (Caso signado n.° 14-9-EP). Consultado en base de datos lexis.com.ec

_____ (25 de junio de 2014). Resolución 1-14 (Caso signado n.° 67-11-JD). Consultado en base de datos lexis.com.ec

_____ (5 de octubre de 2015). Resolución 182-15 (Caso signado n.° 1493-10-EP). Consultado en base de datos lexis.com.ec

_____ (10 de noviembre de 2016). Resolución 344-16 (Caso signado n.° 1180-10-EP). Consultado en base de datos lexis.com.ec

_____ (28 de abril de 2021). Dictamen 2-21-EE/21. Consultado en base de datos lexis.com.ec

Corte Interamericana de Derechos Humanos (24 de noviembre de 2017). Opinión consultiva OC-24/17. Recuperado de https://tinyurl.com/y4cuzhad

Domínguez, J. (2020). La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al COVID-19. *Revista de Comunicación y Salud*. Recuperado de https://tinyurl.com/3uhad3bn

Grijalva, A. (2012). *Constitucionalismo en Ecuador*. Corte Constitucional para el período de transición (Centro de Estudios y Difusión del Derecho Constitucional-Cedec).

Ordóñez, L. (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 Revista de Derecho*, (27) pp. 83-114. Recuperado de https://tinyurl.com/y4kt5oqs

_____ (2021). Gobierno electrónico, Administración pública y protección de datos personales: importancia del principio de responsabilidad proactiva. En C. Paladines e I. Jara (coords.), *Retos 2020: Gobierno abierto*, pp. 151-179. IAEN.

Peces-Barba, G., De Asís, R., y Barranco, M. (2004). *Lecciones de Derechos Fundamentales*. Editorial Dykinson.

Pérez Luño, A. (2010). *Derechos humanos, Estado de derecho y Constitución*. Editorial Tecnos.

Pérez-Luño, E. (2017). *El procedimiento de Habeas Data: El derecho procesal ante las nuevas tecnologías*. Editorial Dykinson.

Piñar, J. (2016). Introducción. Hacia un nuevo modelo europeo de protección de datos. En J. Piñar, M. Álvarez y M. Recio. *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, pp. 13-20. Editorial Reus.

Rallo, A. (2012). Hacia un nuevo sistema europeo de protección de datos: Las claves de la reforma. *UNED: Revista de Derecho Político*. Recuperado de https://tinyurl.com/y2n8yzu3.

_____ (2017). De la "libertad informática" a la constitucionalización de nuevos derechos digitales (1978-2018). *UNED: Revista de Derecho Político.* Recuperado de https://tinyurl.com/y3cnmdns.

Roth, A. (2002). *Políticas Públicas. Formulación, implementación y evaluación*. Ediciones Aurora.

Troncoso, A. (2010). *La protección de datos personales. En busca del equilibrio*. Tirant Lo Blanch.