

LA PROTECCIÓN DE DATOS EN EL GOBIERNO ELECTRÓNICO ECUATORIANO COMO UN DERECHO HUMANO

Pablo Ricardo Mendoza Escalante

Universidad de Otavalo, Ecuador

pmendoza@uotavalo.edu.ec

<https://orcid.org/0000-0002-6029-8705>

Fecha de recepción: 01 de febrero de 2023

Fecha de aceptación: 05 de abril de 2023

Fecha de publicación: 30 de junio de 2023

Resumen

El constante avance de las nuevas tecnologías y el reconocimiento de los derechos digitales como una categoría de derechos humanos, aunado a las distintas formas de posible vulneración de estos, supone la protección de datos personales en las administraciones públicas del Ecuador; para ello, se hizo necesario abordar la nueva concepción de los derechos digitales desde lo internacional a lo interno tomando en consideración los principios de protección a la intimidad y de transparencia previstos en el Código Orgánico Administrativo de 2017 vigente desde el año 2018 en Ecuador específicamente en el gobierno electrónico. El objetivo de la investigación fue analizar la protección de los datos sensibles de los particulares por parte de las administraciones públicas electrónicas ecuatorianas para evitar la posible vulneración de sus derechos digitales. Metodológicamente se utilizó la investigación del tipo descriptivo, con un diseño no experimental y un enfoque cualitativo; se realizó un análisis hermenéutico jurídico, así como las tendencias actuales que involucran a las nuevas tecnologías como mecanismo indispensable para el acceso, ejercicio y protección de los derechos digitales. Se concluyó que las administraciones públicas como gobierno electrónico, cuando manejen datos sensibles, deben observar el derecho a la intimidad personal, familiar y respetar la vida privada de las personas; es medular reconocer que los datos personales deben limitarse a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento y, en caso de vulneración, el titular podrá presentar el correspondiente reclamo administrativo ante la autoridad de protección de datos personales.

Palabras clave: Derecho digital, protección de datos, derecho humano, gobierno electrónico, intimidad.

DATA PROTECTION IN ECUADORIAN E-GOVERNMENT AS A HUMAN RIGHT

Abstract:

The constant advance of new technologies and the recognition of digital rights as a category of human rights, together with the different forms of possible violation of these rights, implies the existence of personal data protection in the public administrations of Ecuador; to this end, it became necessary to address the new conception of digital rights from the international to the domestic level, taking into consideration the principles of privacy protection and transparency provided for in the 2017 Organic Administrative Code in force since 2018 in Ecuador, specifically for e-governance. This research aims to analyze the protection of individuals' sensitive data by Ecuadorian electronic public administrations to prevent the possible infringement of their digital rights. The research method used was descriptive, with a non-experimental design, and a qualitative approach; a legal hermeneutic analysis of the current trends involving new technologies, which constitute the indispensable mechanism for the access, exercise and protection of digital rights, was carried out. It is concluded that public administrations as e-governance, when handling sensitive data, must monitor the right to personal and family privacy, and respect the private life of individuals; it is essential to recognize that personal data must be limited to what is strictly necessary for the fulfillment of the purpose of their processing; in case of violation, the holder may file the corresponding administrative claim before the competent authority.

Keywords: Digital Law, data protection, human rights, e-governance, privacy

INTRODUCCIÓN

Adentrarse en la temática de la protección de datos personales implica remontarse históricamente a la Carta Iberoamericana de Gobierno Electrónico del año 2007, cuyo objetivo se centró en la regulación de las relaciones electrónicas entre las distintas administraciones públicas de los Estados y los particulares con énfasis en la garantía de seguridad. Posteriormente, la denominada Red Iberoamericana de Protección de Datos (2017) estableció un eje estratégico en esta materia, que se sustenta sobre la base de «impulsar y contribuir al fortalecimiento y adecuación de los procesos regulatorios en la región, mediante la elaboración de directrices que sirvan de parámetros para futuras regulaciones o para la revisión de las existentes en materia de protección de datos personales» (p. 3).

La problematización de la temática abordada radica específicamente en la precautela técnica y jurídica de los derechos digitales entendida como una obligación del Estado ecuatoriano ante el derecho que tienen todas las personas de que se garanticen sus derechos a la intimidad y protección de los datos sensibles, diferenciándolos de los denominados datos públicos, que sí son necesarios para cumplir con los fines de las administraciones públicas. Resulta pertinente recalcar que cualquier avance de protección jurídica en esta materia tiene una temporalidad condicionada por la velocidad vertiginosa en que avanzan las nuevas tecnologías y el reconocimiento de nuevos derechos digitales que ameritan regulación.

En vista de lo anterior y como respuesta a la necesaria adecuación normativa sobre la materia, la Constitución de la República del Ecuador en 2008 reconoce y garantiza a todos sus habitantes el derecho a la protección de datos de carácter personal; como consecuencia de ello, la recolección, procesamiento, archivo y difusión de estos amerita la obligatoria autorización del titular. De esta forma, la única manera excepcional de poder acceder a estos datos sensibles es a través de una orden emanada de autoridad judicial o de un mandato expreso de la ley.

En este sentido, los denominados datos sensibles serán objeto de medidas de seguridad que resguarden su contenido físico o electrónico en todas las administraciones públicas de la República del Ecuador; en todo caso, se dispone, dentro de la Ley Orgánica de Protección de Datos Personales del año 2021, a quien se le vulnere su derecho humano soportado en los derechos digitales, podrá incoar una demanda en contra del órgano o entidad que hubiere expuesto sus datos sensibles sin su autorización, incluso por daños y perjuicios ante la autoridad competente judicial.

Las anteriores consideraciones surgen de catalogar a los derechos digitales como un derecho humano a nivel internacional en diversos ordenamientos jurídicos. Los aportes de las nuevas tecnologías permiten el ejercicio ampliado pero a su vez dificulta la protección de estos; en el caso específico cuando las personas interesadas, a través del derecho fundamental de petición, sean parte de un procedimiento administrativo ante cualquier administración pública electrónica en Ecuador; ello supone que el ordenamiento jurídico se ajuste al principio

de protección de la intimidad, previsto en el artículo 24 del Código Orgánico Administrativo de 2017 vigente en Ecuador.

METODOLOGÍA

En esta investigación, se acudió al tipo de investigación descriptiva con paradigma cualitativo. Ello permitió que se revisaran en orden, en primer lugar, los convenios internacionales que ha suscrito el Estado ecuatoriano en materia de derechos digitales y, cómo, desde esa fuente internacional y al constitucionalismo, se han plasmado derechos relacionados con el gobierno electrónico. Del mismo modo, este abordaje documental cualitativo permitió proyectar un análisis integral o sistémico de los preceptos constitucionales relacionados con el gobierno electrónico, la protección de datos y el acceso a las plataformas digitales de las administraciones públicas en el Ecuador.

Esta investigación se fortaleció con la discusión de grupo focal realizada entre los docentes de la carrera de derecho de la Universidad de Otavalo, para analizar jurídicamente los efectos constitucionales que supone el reconocimiento de los derechos digitales en el ordenamiento jurídico del Ecuador al punto de proponer un proyecto de investigación para los años 2023 y 2024 intitulado «Los derechos digitales en los servicios de los consultorios jurídicos y centros de mediación: caso Universidad de Otavalo». Fueron varias las distintas posturas que aparecieron en el debate y la generación de ideas en los grupos focales y la opinión consultada de ciertos actores de la función, para llegar a los resultados que dieran respuestas al objetivo planteado.

1. Paradigmas de los derechos humanos

La protección de los derechos humanos es una temática propia de las ciencias jurídicas, en especial en Estados con ordenamientos jurídicos garantistas, como es el caso de la Constitución de 2008 de la República del Ecuador. De acuerdo con esta consideración y siguiendo a García (2019) «los derechos humanos sobrepasan el ámbito del derecho positivo, al considerarse anteriores a éste y con valor intrínseco que hace obligatorio su respeto y reconocimiento por los sistemas jurídicos particulares» (p. 1) En concordancia con esta afirmación, se pueden situar a los derechos humanos como una forma de protección que institucionaliza a los derechos de las personas en contra de los posibles abusos y excesos de las administraciones públicas de un Estado determinado, específicamente con la actual modalidad de gobierno electrónico.

Recorrer la evolución de los derechos humanos supone revisar algunos antecedentes históricos que dieron lugar a su origen; se hace referencia en este trabajo investigativo a: la Carta Magna Inglesa, de 1215; la Declaración de los Derechos del Hombre y del Ciudadano, de 1789, en el contexto de la Revolución francesa; el constitucionalismo moderno y el nuevo constitucionalismo latinoamericano, donde incluso la naturaleza es sujeto de derechos como en el caso ecuatoriano desde 2008. No obstante, a los derechos humanos se les ha caracterizado como universales,

transnacionales, irreversibles, progresivos y consensuales; se destaca, entre sus funciones, el contribuir al desarrollo integral de la personalidad, establecer límites a la actuación de los servidores públicos en materia de contratación pública y prestación de servicios públicos a través de las diversas plataformas tecnológicas que se colocan al servicio de los particulares para prevenir los posibles abusos de poder, entre otros.

En este orden de ideas, para la dogmática jurídica actual, múltiples opiniones y criterios anuncian y ratifican la aparición de un nuevo catálogo de derechos relacionados con la sociedad de la información, que son parte de la denominada «cuarta generación de derechos humanos». No resulta tarea fácil reconocerlos e identificarlos debido a que, de alguna manera u otra, pueden ser ubicados implícitamente en derechos anteriormente previstos en tratados del ámbito internacional; como ejemplo de ello, se puede indicar al derecho a la identidad digital, que pudiera ser relacionado directamente con el derecho de la persona natural a tener su propia identidad, su propia imagen, su propia voz.

Afirmar la existencia de una cuarta generación de derechos humanos relacionada con los derechos digitales estaría sujeta a la observancia de criterios objetivos y subjetivos, ya que resulta probable que las características muy propias de las nuevas tecnologías potencien y amplíen el catálogo de derechos ya existentes y reconocidos, brindándole una nueva concepción jurídica tecnológica que obviamente los recategorice desde su finalidad. Del mismo modo, es claro que los cibernautas no disponen de mecanismos y medios técnico-jurídicos eficientes para proteger sus derechos digitales concebidos como derechos humanos.

2. Los derechos digitales como derecho humano

A partir de los avances tecnológicos y su aplicación en el ámbito jurídico se da la apertura a distintos medios para ejercer los derechos humanos; sin embargo, también genera la oportunidad de la vulneración de los derechos digitales de sus titulares. La protección de los datos, la intimidad, la identidad digital, el acoso en línea son escenarios que ameritan su regulación y el establecimiento de sus correspondientes garantías. Según el Instituto Nacional de Estadísticas y Censos (INEC, 2020):

Poco más de la mitad de los hogares en Ecuador tuvo una conexión a internet: 61,7 % en el área urbana y 34,7 % en el área rural. Aunque es un gran salto adelante, esto no es suficiente, ya que el uso de la tecnología viene aparejado de importantes cambios sociales, culturales, económicos y profesionales. En este sentido, las personas sin un acceso asequible y sencillo de utilizar no pueden disfrutar plenamente de ciertos derechos, como la libertad de opinión, por lo que es esencial abatir la brecha digital (p. 2).

Al respecto, el secretario general de la ONU publicó en septiembre de 2021 su informe denominado “Nuestra Agenda Común” en la que se propone un pacto digital mundial que involucra a los gobiernos, el sistema de las Naciones Unidas,

la empresa privada, la sociedad civil, y a la academia, entre otros. Uno de los objetivos del Pacto Digital Mundial es el «esboce de principios compartidos para un futuro digital abierto, libre y seguro para todos» (p. 8). El informe de la agenda común presenta temáticas como la conectividad digital, evitar la fragmentación de internet, la promoción de una conexión confiable mediante la introducción de criterios de responsabilidad por discriminación y contenido engañoso.

Otro derecho que debe estudiarse es el relativo a la no discriminación en el entorno digital; para ello, un gran número de empresas consideran el enfoque de género y de diversidad que aseguren el trato igualitario, la reducción de las desigualdades y la brecha digital en lo urbano y lo rural, promoviendo una digitalización que incluya a los grupos de atención prioritaria, en respuesta al mandato constitucional en un Estado pluricultural y pluriétnico. En el área laboral, el teletrabajo está vinculado directamente con la salud mental de los trabajadores donde se requiere el descanso necesario y los espacios adecuados que eviten el impacto de los equipos tecnológicos.

En efecto, materializar un derecho a un entorno digital sostenible parte de que este y las nuevas tecnologías generan un impacto negativo en el derecho fundamental a un ambiente sano y ecológicamente equilibrado, lo que supone prácticas de gestión ambiental que mitiguen los efectos propios de las diferentes TIC. La cuarta ola de derechos humanos postulada actualmente está conformada por el derecho a existir digitalmente, el derecho a la reputación digital, la estima digital, la libertad y responsabilidad digital, la privacidad virtual, el derecho al olvido, el derecho al anonimato, el derecho a la paz cibernética y a la seguridad informática.

3. El principio de la protección a la intimidad

El Código Orgánico Administrativo (2017) consagra que «las administraciones públicas, cuando manejen datos personales, deben observar y garantizar el derecho a la intimidad personal, familiar y respetar la vida privada de las personas» (p. 5). En este contexto y para comprender el alcance de este principio, es necesario acoger los criterios esgrimidos por la Corte Constitucional de la República de Colombia, en la Sentencia C-640/10, agosto 18 de 2010, la cual dispone que «son cinco los principios que sustentan la protección del derecho a la intimidad, y sin los cuales, se perdería la correspondiente intangibilidad del contenido garantista de la inmunidad del individuo frente a la innecesaria injerencia de los demás» (p. 5). Del mismo modo, la Corte colombiana (2010) establece:

El principio de libertad, según el cual, los datos personales de un individuo sólo pueden ser registrados o divulgados con el consentimiento libre, previo, expreso o tácito del titular, a menos que el ordenamiento jurídico le imponga la obligación de relevar dicha información, en aras de cumplir un objetivo constitucionalmente legítimo (p. 6).

Al respecto, este principio de libertad supone una obligación estatal de que los datos personales solo pueden ser dispuestos bajo el criterio de voluntariedad de su titular; sin embargo, se establece excepcionalmente que las administraciones públicas podrán disponer de dicha información solo cuando exista un objetivo constitucional que, ante la ponderación motivada, el derecho individual del titular del dato sea sobrepasado por el cumplimiento de fines sociales o colectivos. En esta misma sentencia de la Corte Constitucional de Colombia (2010) se establece:

El principio de finalidad, el cual se expresa en la exigencia de someter la recopilación y divulgación de datos, a la realización de una finalidad constitucionalmente legítima, lo que impide obligar a los ciudadanos a relevar datos íntimos su vida personal, sin un soporte en el texto constitucional que, por ejemplo, legitime la cesión de parte de su interioridad en beneficio de la comunidad. El principio de necesidad, la información personal que deba ser objeto de divulgación se limita estrechamente a aquella que guarda relación de conexidad con la finalidad pretendida mediante su revelación. Así, queda prohibido el registro y la divulgación de datos que excedan el fin constitucionalmente legítimo (p. 6).

Estos dos principios de finalidad y necesidad, se soportan en un marco de constitucionalidad y de supremacía constitucional que, al igual que en Colombia, en Ecuador se sigue desde el denominado «bloque de constitucionalidad» junto a los tratados internacionales que versan sobre derechos humanos y las jurisprudencias vinculantes de la Corte Constitucional del Ecuador referidas al desarrollo de los derechos digitales de los ciudadanos en su relación con las administraciones públicas del Estado bajo la concepción general del principio de una buena administración pública, tal como lo dispone el Código Orgánico Administrativo de 2017. Finalmente, la sentencia de la Corte colombiana de 2010 dispone sobre el principio de integridad y de veracidad que:

El principio de veracidad exige que los datos personales que se puedan divulgar correspondan a situaciones reales y, por lo mismo, se encuentra prohibida la divulgación de datos falsos o erróneos. Por último, el principio de integridad, según el cual, la información que sea objeto de divulgación debe suministrarse de manera completa, impidiendo que se registre y divulgue datos parciales, incompletos o fraccionados (p. 6).

Medular importancia reviste este principio de veracidad en lo que concierne a la protección de los datos desde el principio de protección de la intimidad del titular del derecho digital y su familia, cuando prohíbe a las administraciones públicas y sobremanera al gobierno electrónico a no divulgar datos falsos o irreales que pudieran exponer la reputación de los particulares, aunado a la integridad de la información. La divulgación de datos fraccionados está prohibida pues pudiera generar confusión en estos.

En esta materia, la Corte Constitucional emite la sentencia No. 89-19-JD/21 (Hábeas data y acceso a datos generados por servidores y servidoras

públicos en ejercicio de sus funciones) Juez ponente: Agustín Grijalva Jiménez, donde se afirma que:

En lo atinente a los datos generados desde el correo electrónico, la jueza resolvió que tiene derecho al acceso al correo electrónico @presidenciagob.ec, que son datos personales que contienen información personal, se dispone que la entidad accionada Secretaría General de la Presidencia de la República entregue toda la información relacionada con dicho correo electrónico institucional a la accionante (p. 4).

De acuerdo con lo anterior, *sí* procede la acción de *habeas data*, para acceder a datos generados a través de sistemas informáticos de instituciones u organismos del Estado cuando quien solicita tal acceso es el servidor o exservidor público que los produjo o generó. Del mismo modo, la Constitución de la República regula:

Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de [sic] la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos (Art. 92).

La Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (LOGJCC) establece los casos en los que se puede interponer la acción de *habeas data*:

1. Cuando se niega el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que consten en entidades públicas o estén en poder de personas naturales o jurídicas privadas.
2. Cuando se niega la solicitud de actualización, rectificación, eliminación o anulación de datos que fueren erróneos o afecten sus derechos.
3. Cuando se da un uso de la información personal que viole un derecho constitucional, sin autorización expresa, salvo cuando exista orden de jueza o juez competente (Art. 50).

La Corte determinó que «los datos personales incluyen datos sensibles relativos a la vida privada y familiar de la persona, pero también información sobre cualquier tipo de actividad desarrollada por ella, como la referida a sus relaciones laborales, económicas o sociales, con independencia de su posición o capacidad» (p. 6). La Corte Constitucional ratifica que es obligación de instituciones y entidades públicas, organizar y mantener documentos electrónicos y físicos, así como garantizar a dichos exservidores públicos el acceso a los datos cuando así los soliciten expresamente, siempre y cuando tales datos no se encuentren calificados, por el ordenamiento jurídico, como

reservados. Los datos generados a través de correos electrónicos institucionales no pueden ser tratados como datos personales siempre que se produzcan como consecuencia del ejercicio de una actividad o gestión pública.

4. La protección de datos como derecho digital

La vulneración de la seguridad de los datos personales, como aspecto a tratar en esta investigación, debe entenderse de acuerdo con la Ley Orgánica de Protección de Datos Personales (2021) como: «aquel incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales» (p. 7). Dentro de los principios que la ley citada establece expresamente como aplicables en esta materia, se identifican los de juridicidad, lealtad, transparencia, finalidad, pertinencia y, sobre todo, el de minimización de datos, que implica que «Los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento» (p. 9). De igual modo, se suman los principios de proporcionalidad del tratamiento, confidencialidad, calidad, exactitud, conservación, responsabilidad proactiva, independencia de control; todos estos principios sobre el *indubio pro titular* de los datos sensibles, sobre lo cual Corripio (2001) sostiene que:

La salvaguarda de la propia vida privada se encuentra en el comportamiento y control que efectúa el usuario y, en Internet, pasa necesariamente por el derecho a realizar opciones informadas, de forma que cuando se recaban datos por el sector privado, el interesado pueda escoger libremente cuáles de sus datos quiere comunicar y para qué finalidades. Ligado a este derecho se encuentran el derecho al anonimato y a utilizar herramientas de seguridad (p. 2922)

En este mismo contexto, se reconocen, en el ordenamiento jurídico ecuatoriano, los derechos a la información, al acceso, a la eliminación de datos, a la rectificación, portabilidad y actualización de sus datos; especialmente, se reconoce el derecho a la oposición al tratamiento de sus datos personales, que se enumeran en el artículo 16 de la ley *in comento* específicamente cuando no se afecten derechos y libertades fundamentales de terceros; cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa y cuando no sea necesario su consentimiento para el tratamiento como consecuencia de la concurrencia de un interés legítimo. Del mismo modo, Porcelli (2019) afirma que «El poder de los datos masivos combinados, con inteligencia artificial, ha demostrado la increíble capacidad de predicción del comportamiento humano y modificarlo» (p. 3). El citado Porcelli (2019) sostiene que:

El derecho a la protección de datos personales se ha conceptualizado en algunos países iberoamericanos, legislativamente o jurisprudencialmente, como un derecho autónomo y de naturaleza distinta a los derechos a la vida privada y familiar, a la intimidad, al honor, al buen nombre y que tiene por objeto salvaguardar el poder de disposición y control que tiene todo individuo con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones (p. 6).

En caso de vulneración en el tratamiento de los datos personales, el titular podrá, de acuerdo con la Ley Orgánica de Protección de Datos Personales (2017) del Ecuador: «presentar el correspondiente reclamo administrativo ante la autoridad de protección de datos personales, acudiendo al procedimiento establecido en el COA, a la presente ley y demás normativa emitida por la Autoridad de Protección de Datos Personales» (Art. 64). Para este fin, debe entenderse por «autoridad de protección de datos personales», según la Ley Orgánica de Protección de Datos Personales en su artículo 76a:

El órgano de control y vigilancia encargado de garantizar a todos los ciudadanos la protección de sus datos personales, y de realizar todas las acciones necesarias para que se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley y en su reglamento de aplicación, para lo cual le corresponde las siguientes funciones, atribuciones y facultades [...] (p. 35).

Es oportuna la creación de un órgano de control que garantice la protección de datos a los usuarios del gobierno electrónico; de allí que la autoridad única de protección de datos personales tiene una responsabilidad en lo referido a los derechos digitales, así como de facilitar su ejercicio y su consecuente cautela. Para identificar el bien jurídico tutelado en materia de protección de datos, Herrán (2003) sostiene que:

Una aproximación al bien jurídico tutelado a través del derecho a la protección de datos permite concluir que el fundamento último de este derecho no consiste exclusivamente en preservar oculta información relativa a la vida privada, sino en garantizar el pleno desarrollo de la personalidad individual y el libre ejercicio de sus derechos; se trata en definitiva de impedir la instrumentalización del ser humano, que debe manifestarse en la sociedad con plena libertad (p. 16).

Por ello, el derecho a la protección de datos ante las administraciones públicas integradas por diferentes administraciones públicas conlleva, a su vez, el derecho de libertad y desarrollo de la personalidad de su titular, más aún en un Estado constitucional de derechos y de Justicia.

5. Administraciones públicas desde la visión del gobierno electrónico

El gobierno electrónico responsable deberá atender a la seguridad de datos personales que, de acuerdo con la Ley Orgánica de Protección de Datos Personales (2021) del Ecuador, en su artículo 37, regula:

El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos (p. 21).

Para definir al gobierno electrónico, Naser y Concha (2011) entienden «la transformación de todo el gobierno como un cambio de paradigma en la gestión gubernamental, que fusiona la utilización intensiva de las TIC, con modalidades de gestión planificación y administración como una nueva forma de gobierno» (p. 5). De acuerdo con ellos, el gobierno electrónico persigue suministrar servicios autónomos e independientes en cuanto a distancia y tiempo en favor de los particulares y el Estado mismo. Junto con la definición de *gobierno electrónico*, surge paralelamente la *governabilidad electrónica*, que desarrolla áreas importantes, como la administración y el servicio electrónico. En este sentido, Naser y Concha (2011) afirman que:

El correcto diseño de estrategias tecnológicas estandarizadas que viabilicen la implementación de un gobierno en línea con requerimientos de interoperabilidad, legales y de seguridad sobre servicios transaccionales de GE es la etapa más importante para lograr el éxito de un proyecto TIC. Lograr la interoperabilidad de los sistemas de información existentes en diferentes jurisdicciones para intercambiar información relevante es vital para evitar duplicaciones de datos que favorecen la inconsistencia de los procesos de gestión dentro del Estado (p. 21).

En cuanto a la responsabilidad de la administración pública en el tratamiento de datos personales, resulta pertinente recapitular el concepto de *responsable de la información* a través del Convenio No. 108 del Consejo de Europa, de 1981, del Consejo de Europa cuando refiere que es «una figura autónoma propia del derecho a la protección de datos personales, que solo o conjuntamente con otros determine los fines y los medios de tratamiento de los datos personales» (p. 4). A partir de ello, Correa y otros (2022) sostienen que:

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 (p. 80).

El Plan Nacional de Gobierno Electrónico en la República del Ecuador apunta a un modelo regido por el principio de inclusión, eficacia y eficiencia, alineado con la participación e interacción entre los ciudadanos y el Estado. Es importante vincular la normativa que regula esta materia en el Ecuador, donde se encuentra la Constitución de la República de 2008, la Ley de Transparencia de 2004, la Ley del Sistema de Registro Público de 2010, Ley de Comercio Electrónico Firma Electrónica y Mensajes de Datos de 2002, Ley Orgánica de Participación Ciudadana de 2010, Ley Orgánica de Telecomunicaciones de 2015, Código Orgánico Administrativo de 2017, el Decreto Ejecutivo 149 de 2013 para la implementación del gobierno electrónico en la administración pública.

RESULTADOS Y DISCUSIÓN

Un primer resultado se enmarca en sostener que lo digital es un escenario expuesto en múltiples grados al público y todos sus elementos son el producto de la actividad humana; lo que supone intrínsecamente una latente vulneración de derechos digitales bajo la concepción de derecho humano; las permanentes interconexiones entre el gobierno electrónico ecuatoriano y los particulares se expone a las miradas de terceros que pudieran directa o indirectamente conocer la intimidad del titular de los derechos digitales o su familia, lo que supone disponer de estrategias que minimicen los riesgos en la prestación de servicios públicos, contratación pública y en los procedimientos en línea para realizar reclamos, solicitudes e impugnaciones.

Las comunicaciones electrónicas o digitales donde se transfieren datos sensibles suelen realizarse en un contexto comunicativo de privacidad. Por un lado, en los contextos comunicativos de exposición, la reproducción de los contenidos es más libre, requiere menos autorizaciones, y está sujeta a menos controles que en los contextos de privacidad. Una gran exposición de la información conlleva mayores responsabilidades, como en el delito de injurias, donde las dimensiones del público que escucha la vejación determinan la magnitud de la ofensa.

Es pertinente mencionar que, con el surgimiento y vigencia de los derechos digitales en el mundo virtual, se adquiere una amplia gama de particularidades nunca vistos, cuya protección resulta muy deficiente en la actualidad, puesto que el uso indebido de la gran cantidad de datos personales recolectados gracias a ellas pueda exponer y vulnerar la privacidad, la reputación e incluso la dignidad del ser titular y su familia. Los particulares ante el gobierno electrónico han experimentado una pérdida del control de sus datos sensibles, lo que requiere que el derecho se constituya como un límite al posible abuso de las tecnologías de la información en dominio del Estado como sujeto regulador de las actividades administrativas en Ecuador.

CONCLUSIONES

La especial atención a la protección de los datos sensibles de las personas usuarias del gobierno electrónico en Ecuador es dinámica y permanente debido a los constantes avances tecnológicos que se ofrecen en las distintas plataformas gubernamentales, especialmente por la vulnerabilidad y el impacto que la transformación digital tiene en el desarrollo de su personalidad en cuanto a derecho humano se refiere.

Toda persona que haga uso de las tecnologías ante el gobierno electrónico ecuatoriano tiene derecho a la supresión de sus datos personales en los buscadores de internet y que se le garantice el derecho a impedir la difusión cuando su publicación no reúna los requisitos legales de actualidad y pertinencia.

Toda persona tiene derecho a que se respeten sus derechos fundamentales en el ciberespacio, atendiendo de forma especial al derecho a la intimidad, a la propia imagen y al honor, así como a tener las mismas oportunidades en el intercambio de bienes y servicios digitales, garantizando la libre competencia en materia de servicios públicos y en materia de contratación pública.

Toda persona tiene derecho a la protección de las producciones literarias, artísticas, científicas o técnicas de las que sea autora en la red y especialmente tiene derecho a una alfabetización digital que le permita encontrar y evaluar la información en la red, así como a crear su propio contenido, comunicarse y navegar de forma segura en internet o resolver los problemas técnicos que pueda encontrar.

Finalmente, las administraciones públicas, como gobierno electrónico, cuando manejen datos sensibles, deben observar el derecho a la intimidad personal, familiar y respetar la vida privada de las personas; es medular que los datos personales se limiten a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento y, en caso de vulneración, el titular podrá presentar el correspondiente reclamo administrativo ante la autoridad de protección de datos personales; aunado a ello se evidencia que la falta de observancia del principio de seguridad jurídica en la protección de datos personales reduce la confianza del ciudadano en el empleo de sistemas seguros por internet, lo que representa una limitante para la participación electrónica, así como para la liberación de datos por parte de las instituciones.

REFERENCIAS BIBLIOGRÁFICAS

Asamblea Constituyente (2008). Constitución de la República Ecuador.

Asamblea Nacional (2021). Ley Orgánica de Protección de Datos Personales.

Centro Latinoamericano de Administración para el Desarrollo (2007). Carta Iberoamericana de Gobierno Electrónico. CLAD.

Convenio No. 108. para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. 1 de octubre de 1985

Corripio, M. (2001). La Protección de Datos Personales en Internet. Boletín del Ministerio de Justicia.

Correa, A., Correa L. y Ordoñez L. (2022). Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria. Revista Estado & Comunes, 22, 15.

Derecho a la intimidad, derecho al buen nombre y derecho al habeas data, Sentencia C-640/10, 18 de agosto de 2010 (Corte Constitucional de Colombia.)

García, F. (2019). Positivismo y derechos humanos en la obra de Norberto Bobbio. Revista Hechos y Derechos, 49.

Hábeas data y acceso a datos generados por servidores y servidoras públicos en ejercicio de sus funciones, Sentencia No. 89-19-JD/21, 07 de julio de 2021 (Corte Constitucional del Ecuador)

Naser, A. y Concha, G. (2011). El gobierno electrónico en la gestión pública. CEPAL.

Porcelli, A. (2019). La protección de los datos personales en el entorno digital. Los estándares de protección de datos en los países iberoamericanos. *Quaestio Iuris*, 12, 2.

Red Iberoamericana de datos personales. (2017). Estándares de Protección de Datos Personales para los Estados Iberoamericanos. <https://bit.ly/3kVfdWr>

UNIR. (2022). ¿Qué y cuáles son los derechos digitales en Ecuador? <https://bit.ly/3kZJzaj>