29

Fecha de presentación: diciembre, 2021
Fecha de aceptación: enero, 2022
Fecha de publicación: marzo, 2022

HABEAS DATA

Y PROTECCIÓN DE DATOS PERSONALES EN LA GESTIÓN DE LAS BASES DE DATOS

HABEAS DATA AND PERSONAL DATA PROTECTION IN DATABASE MANAGEMENT

Silvio Amable Machuca Vivar[1]
E-mail: us.silviomachuca@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-4681-3045
Nelly Valeria Vinueza Ochoa[1]
E-mail: ub.nellyvinueza@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-4017-9557
Carlos Roberto Sampedro Guamán[1]
E-mail: us.carlossampedro@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-2784-1913
Alberto Leonel Santillán Molina[1]
E-mail: us.albertosantillan@uniandes.edu.ec
ORCID: https://orcid.org/0000-0001-8517-8980
[1] Universidad Regional Autónoma de Los Andes. Ecuador.

Cita sugerida (APA, séptima edición)

Machuca Vivar, S. A., Vinueza Ochoa, N. V., Sampedro Guamán, C. R., & Santillán Molina, A. L. (2022). Habeas data y protección de datos personales en la gestión de las bases de datos. *Revista Universidad y Sociedad*, 14(2), 244-251.

RESUMEN

Las Tecnologías de la Información y la Comunicación permiten el desarrollo e interacción de nuevas formas, medios y tiempos de relación social, nuevas formas de relaciones de las empresas y sus clientes, nuevas formas de aprehensión personal y social. Cada vez que realizamos alguna actividad a través de plataformas digitales se genera una gran cantidad de datos tales como: ubicación, género, preferencias de consumo, nombres, relaciones personales, problemas de salud, entre otros datos, todas las empresas e instituciones requieren de los datos para sus actividades, lo que se traduce en la necesidad de contar con buenos sistemas informáticos y las bases de datos, estos datos se constituyen en el nuevo oro, su aumento exponencial, su migración a sitios distantes y variados, con una difusión no controlada; han generado también que los datos personales y los datos confidenciales de las empresas estén más expuestos que nunca, haciendo necesaria la seguridad de la información, soluciones centradas en los datos y una normativa sobre la protección de datos a nivel nacional e internacional. La información personal se ha convertido en un producto de compraventa, es por esto que se aborda la problemática de protección de los datos personales desde la perspectiva de la gestión de las bases de datos y la normativa jurídica del Habeas Data, con el objetivo de motivar a los profesionales de desarrollo de software para considerar estos factores al diseñar y desarrollar los sistemas, más aún por tratarse de temas poco considerados de acuerdo con la encuesta realizada.

Palabras clave: Hábeas Data, protección de datos personales, derecho a la privacidad, gestión de base de datos.

ABSTRACT

Information and Communication Technologies allow the development and interaction of new forms, means and scenarios of social relationships, new forms of relationships between companies and their customers, new forms of personal and social apprehension. Every time we perform any activity through the digital platforms a large amount of data is generated, such as location, gender, consumption preferences, names, personal relationships, health problems, among other data. The companies and institutions require data for their activities, which translates into the need for good computer systems and databases, these data are constituted in the new gold. The exponential increase of this data, its migration to distant and varied sites, with uncontrolled dissemination, has also generated that personal and confidential company data are more exposed than ever, making it necessary to secure the information through data-centric solutions and data protection regulations at national and international levels. Personal information has become a commodity to be bought and sold, which is why the issue of personal data protection is approached from the perspective of database management and the legal regulation of Habeas Data, with the aim of motivating software development professionals to consider these factors when designing and developing systems, especially since these issues are hardly considered according to the survey conducted.

Keywords: Habeas Data, personal data protection, right to privacy, database management.

INTRODUCCIÓN

El tratamiento automatizado de los datos e información ha dificultado la protección de los datos personales y expuesto a que los datos sensibles de las personas se encuentren a la venta en sitios de la Deep web o que sean divulgados libremente en la web, esto se evidencia en noticias como las de la filtración de los datos personales de millones de usuarios de Facebook (530 millones y 1 500 millones en abril y octubre del 2021 respectivamente). En octubre del 2019 se difundió la noticia de la filtración más grande de datos personales (número de cédula, datos financieros, datos civiles, números telefónicos, datos de familiares, de vehículos, entre otros) de 17 millones de ecuatorianos, según publicación de la BBC NEWS (2019), y otros medios nacionales, las autoridades de telecomunicaciones anunciaron investigaciones, de las cuales aún no se han publicado resultados.

La información de la filtración de datos de los ecuatorianos, entre ellos 6,7 millones de niños, fue difundida en el sitio web ZDNet y descubierta por la firma especializada vpnMentor, quienes concluyeron que los datos salieron de un servidor de la empresa Novaestrat (firma consultora de análisis de datos, marketing y desarrollo de software), lo que motivó que se busque formas de eliminar esos datos de todos los sitios web en los que se publicaron sin verificación, incluso Eliminalia, una empresa especializada en la defensa del derecho al olvido en internet, puso a disposición un formulario de ayuda gratuita para borrar los dato, apoyados en herramientas de informática forense y de extracción de información.

En julio del 2021, la Corporación Nacional de Telecomunicaciones (CNT EP) presentó ante la Fiscalía General del Estado una denuncia por el delito de Ataque a los sistemas Informáticos, de acuerdo a publicaciones de los medios de comunicación y de empresas como Hackem Cybersecurity Research Group, se produjo un ataque informático por ransomware (secuestro informático) y que los atacantes revelaron parte de la información y amenazaron con divulgar toda la información si no les hacían el pago del rescate, el comunicado oficial de la entidad aceptó el haber sufrido el ataque informático y descartó la filtración de datos, expertos pidieron no acceder a las supuestas bases de datos que revelan la información, ya que pueda tratarse de datos falsos (fake) que buscan ser distribuidos como virus.

Paralelamente, al ataque informático a los servidores de la CNT surgieron en las redes sociales y medios de comunicación se hicieron eco de problemas de ataques informáticos y filtración de datos personales de usuarios del Instituto Ecuatoriano de Seguridad Social (IESS) y su banco (BIESS), al Servicio de Rentas Internas (SRI) a Petroecuador y al Banco del Pichincha, los representantes de estas instituciones emitieron comunicados manifestando en unos casos que no hay evidencia de vulneraciones o hackeos a sus sistemas, otros aceptaron que sufrieron ataques informáticos, pero que los protocolos de seguridad informática evitaron cualquier filtración de información, atribuyeron los problemas en sus sistemas informáticos a problemas de actualización y que la información que circula en la Deep web no corresponde al contenido de sus bases de datos.

Estos y otros hechos han puesto a trabajar arduamente a los expertos en seguridad informática en medidas de prevención, planes de contingencia, Hardening y otras estrategias para proteger sus servidores; no todos los casos de divulgación de datos personales se han generado por vulneración de las seguridades informáticas, como en el último caso de la red social Facebook en la cual se han recopilado datos que los mismos usuarios han expuestos en sus perfiles públicos, datos como: nombres, correo electrónico, localización, género, número telefónico, ID de usuarios, preferencias personales, estado civil, entre otros; según el portal especializado en temas de privacidad y seguridad informática Privacy Affairs.

La recopilación de datos es un proceso primordial para que una empresa o institución pueda desarrollar sus actividades y relaciones con sus clientes y proveedores, a partir de esa ingente cantidad de datos en constante crecimiento, las empresas que son capaces de extraer información relevante toman sus decisiones, por lo cual requieren de una base de datos (BD) que contengan datos fundamentales de las personas con las respectivas seguridades, al referir a seguridad de base de datos se debe considerar los niveles de seguridad: seguridad física (control de acceso físico), seguridad de Sistemas Operativos (Hardening), seguridad a nivel de red (Software de red), seguridad a nivel humano (métodos de acceso) y seguridad a nivel de gestión de base de datos (privilegios de usuarios base de datos).

Con el antecedente de la filtración masiva de datos de los ecuatorianos, la Asociación Ecuatoriana de Protección de Datos (2019), mediante un comunicado a la comunidad en general solicitó el inició de la discusión y aprobación de una ley sobre protección de datos de carácter personal, (Ecuador. Asamblea Nacional, 2021) se publicó la Ley Orgánica de Protección de Datos Personales, con el objetivo de garantizar el derecho a la protección de datos personales con la inclusión del acceso y decisión sobre la información y datos de este carácter, así como de su correspondiente protección.

Los hechos citados nos hacen reflexionar sobre ¿cuántos datos personales compartimos en la surface web de forma voluntaria u obligatoria?, ¿qué tipo de seguridad de los datos e información están considerados en estos registros de las bases de datos?, ¿Qué normativa jurídica existe en Ecuador para la protección de datos personales? Ante estas y otras preguntas de investigación se plantea como objetivo un estudio en derecho comparado sobre garantía jurisdiccional del Habeas Data y motivar a los profesionales de desarrollo de software a considerar esas acciones y derechos en el modelado y seguridad de las bases de datos de los sistemas informáticos, así como también concienciar a las personas en el cuidado que debemos tener al momento de entregar nuestros datos, un dicho popular dice que cuando un producto o servicio es aparentemente gratuito, el pago son nuestros datos.

Si bien la Constitución del 1998 de Ecuador establecía en su artículo 94 el derecho de toda persona al acceso a los documentos, bancos de datos e informes que sobre sí misma o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se hace de ellos, no se la debe confundir con el derecho de acceso a la información, la acción de hábeas data se dirige a proteger los datos personales, derecho a la intimidad, a la honra y buena reputación (Ortiz, 2008; Noguera & Criado, 2021).

Los cambios en la constitución del 2008 son: *"La acción de acceso a la información pública tendrá por objeto garantizar el acceso a ella cuando ha sido denegada expresa o tácitamente, o cuando la que se ha proporcionado no sea completa o fidedigna. Podrá ser interpuesta incluso si la negativa se sustenta en el carácter secreto, reservado, confidencial o cualquiera otra clasificación de la información. El carácter reservado de la información deberá ser declarado con anterioridad a la petición, por autoridad competente y de acuerdo con la ley".* (Ecuador. Asamblea Nacional Constituyente, 2008)

También, *"toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de 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".* (Ecuador. Asamblea Nacional Constituyente, 2008)

MATERIALES Y MÉTODOS

La investigación es de tipo cualitativa no experimental, se recopiló las opiniones de 51 profesionales en al área de sistemas mediante un cuestionario de 08 ítems con temas referentes al conocimiento sobre la normativa jurídica del hábeas data y criterios considerados en el diseño y gestión de un base de datos para proteger la confidencialidad de los datos personales.

El tipo de investigación es descriptiva, transversal y bibliográfica, analizando las fuentes bibliográficas de temas relacionados con la protección de datos personales en Ecuador, un estudio comparado de la normativa de habeas data de Ecuador, Perú y Colombia, además de un estudio de caso de dos sentencias sobre Habeas Data en Ecuador en enero del 2021.

La población está considerada corresponde a los graduados de la carrera de sistemas de la Universidad Regional Autónoma de los Andes Uniandes, sede Santo Domingo, con un registro de 267 graduados entre el 2015 y 2020, de acuerdo con información proporcionada por la coordinación de seguimiento a gradados. De este total se consideró como criterio de exclusión solo a los profesionales que están trabajando en el área de sistemas o desarrollando sistemas por cuenta propia, reduciéndose al 30% del tamaño, para recopilar su opinión referente a sus conocimiento y aplicación de medidas de protección de los datos personales. Con la técnica de muestreo aleatorio simple, se envió mediante correo el enlace de encuesta desarrollado en Microsoft Forms, obteniendo 51 respuestas.

Mediante el método analítico – sintético se realizó el análisis de los aspectos jurídicos referentes a la protección de datos personales y hábeas data de 2 casos en Ecuador, para sintetizarlos en las conclusiones del presente documento.

Con el método inductivo - deductivo se analiza los casos particulares tratados tanto de las respuestas de los encuestados como de las sentencias para llegar a las conclusiones generales sobre los principios a considerar en el tratamiento de datos personales.

RESULTADOS Y DISCUSIÓN

De los profesionales encuestados solo un 27,5% conoce lo que es el hábeas data, un 25% lo conoce parcialmente y un 47,5% desconoce del tema. En lo referente al acceso y solicitud de acciones con los datos por parte de las personas involucradas, las respuestas se muestran la Figura 1 y hacen referencia al derecho que tienen los involucrado

de actualizar, conocer, rectificar y suprimir sus datos, mayoritariamente coinciden en actualizar los datos.

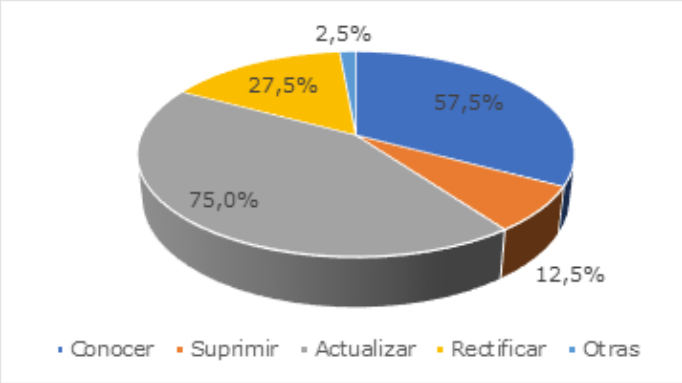

Figura 1. Opciones de tratamiento de datos personales por las personas involucradas.

Constantemente y de forma prácticamente obligatoria los sistemas informáticos nos obligan a compartir datos personales que al principio no nos parecen muy significativos o privados, como se muestra la Figura 2, son varios datos personales que están en poder de las empresas e instituciones públicas y privadas. No somos conscientes de las afectaciones que podemos tener al no controlar la divulgación de nuestros datos personales en los medios digitales, los encuestados si están al tanto de la problemática y el daño que puede ocasionar este problema a las personas.

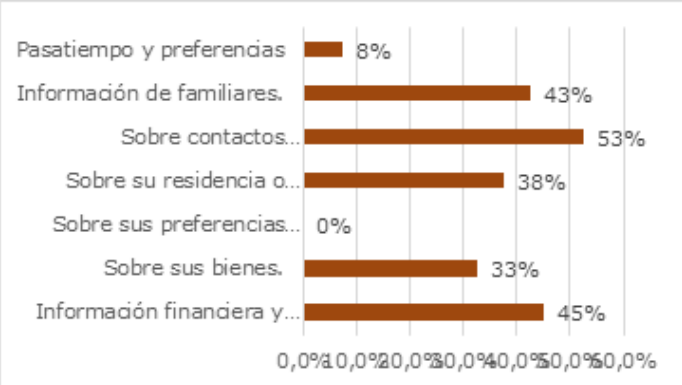

Figura 2. Datos personales obligados a las personas a registrar.

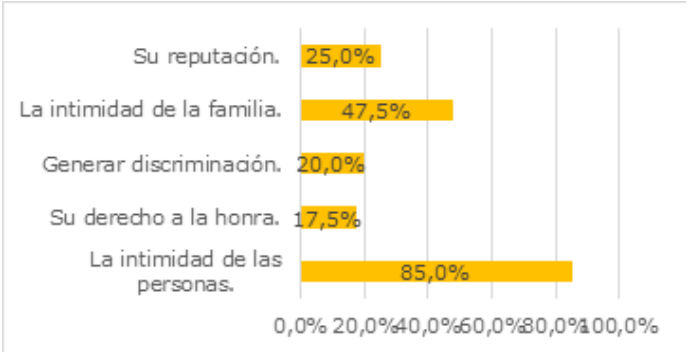

Figura 3. Afectación a las personas por la divulgación de sus datos personales.

Para el cuestionamiento de sí en el diseño de los sistemas informáticos considera la posibilidad de que las personas puedan especificar el nivel de visibilidad de sus datos personales (Figura 3) (privados, restringidos, públicos), el 86% de los encuestados señala que los sistemas informáticos deben dar esta opción a las personas, el 11% señala que lo debe hacer parcialmente y un 3% que no lo debería hacer.

En lo referente al cuestionamiento de sí los reportes de datos personales generados por un sistema informático filtran información en función de los privilegios del usuario que lo solicita, el 75% afirma que, si lo hace, un 20% lo hace de forma parcial y un 5% no filtra la información.

Las medidas de protección de los datos personales de mayor frecuencia son las de confidencialidad (72,5%), seguidas por las de protección de acceso (40%), de divulgación (27,5%), protección parcial (30%) y ninguna (2,5%). La pregunta abierta formulada sobre este mismo tema dio como resultados: Encriptación de datos, privilegios de usuario, control de acceso, preguntas de seguridad y robustez de las contraseñas.

El **CASO No. 2064-14-EP** trata de una sentencia (Ecuador. Corte Constitucional, 2021a), en la cual se analiza si existe vulneración del derecho constitucional al debido proceso en la garantía a recurrir el fallo y a la motivación, al principio de *non reformatium in pejus*, al derecho a la defensa; y, a la tutela judicial efectiva en la sentencia de segundo nivel, misma que se resolvió revocar la decisión de primer nivel y declaró sin lugar la acción de hábeas data planteada en contra de una persona natural que poseía fotografías íntimas y personales de la actora, La corte decide entrar al mérito del caso y encuentra que hubo violación al derecho a la protección de datos personales y autodeterminación informativa, a la imagen, a la honra y buen nombre e intimidad.

En este caso en particular se trata de fotos íntimas compartidas entre dos personas mediante mensajes de WhatsApp, al ser una conversación mantenida por un sistema que cuenta con un cifrado extremo a extremo, garantizando que solo los 2 participantes tengan acceso a dicha información, por el contenido de datos personales en los archivos, se concluye que la divulgación a terceros se trata de una violación al derecho a la intimidad y dispone la eliminación de esos archivos y suspender su divulgación, el habeas data no tiene como finalidad principal la indemnización del perjudicado, pero contempla las reparaciones materiales e inmateriales que el juez disponga.

En el caso No 89-19-JD del 07 de julio de 2021 (Ecuador. Corte Constitucional, 2021b), una ex servidora pública de la Presidencia de la República solicita mediante acción de hábeas data que dicha entidad le entregue los datos generados por dicha ex servidora a través de sistemas informáticos de dicha entidad, con el objetivo de ejercer su derecho a la defensa en un examen especial de auditoría iniciado en su contra. La sentencia establece que: a) los datos generados por servidores o exservidores públicos a través de sus correos electrónicos institucionales, así como en plataformas digitales de instituciones y entidades públicas no constituyen, prima facie y salvo situaciones que dependerán de cada caso concreto, datos personales para aquellos. Por lo tanto, su acceso y conocimiento no debe genéricamente ser tutelado mediante la garantía jurisdiccional de hábeas data; b) Las instituciones y entidades públicas deben brindar las facilidades necesarias a servidores y exservidores públicos cuando estos soliciten expresamente acceder a datos generados por aquellos durante su gestión. En caso de que no se brinde dichas facilidades y esto se derive en vulneraciones a derechos constitucionales, concretamente el debido proceso en la garantía de defensa está habilitado para dichos servidores o exservidores la acción de protección.

Los datos personales son los registros o información que por sí sola o vinculada con otros datos, puede revelar la identidad de una persona viva. Datos sensibles como: el origen racial o étnico, opiniones políticas, creencias religiosas, grupos sindicales a los que pertenece, su salud o estado físico y mental, su visa sexual, la comisión de delitos, entre otros. La protección de datos se refiere al derecho de las personas a saber que datos se han recopilado, se mantienen y se procesan, para poder corregir alguna inexactitud, considerando en el caso de las personas las obligaciones legales y éticas con respecto a compartir los datos (Millán, et al., 2013; -Benavent, 2021).

De acuerdo con la Organización para la Cooperación y el Desarrollo Económicos (2016), los principios básicos que, complementados con el desarrollo de una estrategia nacional de privacidad, implementación de principios de responsabilidad, libre flujo y restricciones legítimas, cooperación internacional e interoperabilidad y otras medidas que facilitan la protección de la privacidad y las libertades individuales son:

a) Principio de limitación en la recolección de datos, establecer límites para la recolección de datos personales, cualquiera de estos datos deberá obtenerse con medios legales y justos, siempre que sea apropiado, con el consentimiento y conocimiento de la persona implicada.

b) Principio de la calidad de los datos, estos datos deben ser relevantes para el propósito de su uso, exactos, completos y actuales.

c) Principio de especificación del propósito, en el momento en que se recopilan los datos personales se deberá especificar el propósito de estos, su uso se verá limitado al cumplimiento de esos objetivos u otros que no sean incompatibles con el propósito inicial, notificar en caso de cambio del objetivo.

d) Principio de limitación de uso, no divulgar, no poner a disposición o usar los datos personales para propósitos que no cumplan con lo establecido en el propósito, con excepciones de: Contar con el consentimiento de la persona implicada, por imposición legal de las autoridades.

e) Principio de salvaguardia de la seguridad, proteger los datos personales contra riesgos como: pérdida, acceso no autorizado, uso, modificación o divulgación de estos. Seguridad y privacidad son diferentes, las limitaciones de uso y divulgación se complementan con las medidas de seguridad físicas, organizacionales, cifrado, seguimiento y respuesta a los ataques informáticos.

f) Principio de transparencia, contar con una política de transparencia en cuanto a la evolución, prácticas y políticas relativas a datos personales. Se deberá contar con medios ágiles para determinar la existencia y la naturaleza de los datos personales, el propósito principal para su uso y la identidad y lugar de residencia habitual de quien controla esos datos.

g) Principio de participación individual, Las personas tienen derecho a:

1. Que el controlador de datos (persona o institución) u otra fuente le confirme que tiene datos sobre su persona.
2. Que se le comunique los datos relativos a su persona en un tiempo razonable, sin costo o que no sea excesivo, de forma razonable y de manera inteligible.

3. Que se le explique la razón o razones por las cuales una petición a los puntos 1 y 2 fue denegada e incluso cuestionar tal denegación.
4. Expresar dudas sobre los datos relativos a su persona y contactarse en caso de requerir que los datos se eliminen, rectifiquen, completen o corrijan.

a) Principio de responsabilidad, sobre el controlador de los datos debe recaer la responsabilidad del cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

La protección de datos personales, corresponde a una parte de la legislación que protege el derecho fundamental de la libertad, en particular del derecho individual a la intimidad respecto del procesamiento manual o automático de los datos, también se puede considerar como el conjunto de bienes e intereses que pueden ser afectados por la elaboración de informaciones referentes a las personas inidentificadas o identificables (García, 2007).

Las empresas e instituciones que solicitan estos datos personales están obligadas a: Contar con el consentimiento del titula tanto para la recepción y para su transferencia, realizar el análisis de riesgo, amenaza y vulnerabilidades, determinar las medidas de seguridad, evaluar el impacto del tratamiento de los datos personales, notificar la vulneración de seguridad de los datos personales, a más tardar 5 días después del incidente, la transferencia internacional se debe sustentar en un instrumento jurídico que contemple los estándares jurídicos determinados, el encargado del tratamiento debe notificar al responsable cualquier vulneración de la seguridad a más tardar dentro del término de 2 días (Salazar, 2021).

El habeas data es una garantía jurisdiccional que constituye un mecanismo procesal que permite la protección constitucional de ciertos derechos frente al impacto que ha tenido las nuevas tecnologías de la información y comunicación. El artículo 49 de la Ley Orgánica De Garantías Jurisdiccionales Y Control Constitucional (Ecuador. Asamblea Nacional, 2009), recoge al objeto de la acción de esta garantía, así mismo la Constitución (Ecuador. Asamblea Nacional Constituyente, 2008), se establece como uno de los derechos de libertad: "*Se reconoce y garantizará a las personas… El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley".*

Ahora bien, mediante sentencia No. 1868-13-EP/20, la Corte Constitucional manifestó que *"la información objeto de hábeas data es aquella relacionada con "datos personales" y/o "informes sobre una persona" o sobre "sus bienes", que reposen en instituciones públicas o privadas, en soporte material o electrónico*". (Ecuador. Corte Constitucional, 2021b)

En el caso que nos ocupa se puede colegir que toda esta información o "datos personales" al reposar en soporte digital o electrónico, las personas quienes se encargan de desarrollar bases de sistemas informáticos deberían considerar todos los aspectos legales y doctrinarios a fin de que los mismos presten las garantías necesarias para que esta sea protegida ante injerencia de terceros, al respecto existe un precedente jurisprudencial donde la Corte Constitucional de Colombia Sentencia T-547/17 (Colombia. Corte Constitucional, 2021a), en este se trata sobre la aplicación de mensajería instantánea WhatsApp indica que funciona a través de teléfonos inteligentes, que permite enviar y recibir mensajes a través de internet, aquí los usuarios pueden crear listas de distribución y grupos, lo que facilita el intercambio de videos, imágenes, grabaciones, mensajes escritos, notas de voz y contactos.

"Estas conversaciones cuentan con un sistema de cifrado de extremo a extremo, lo que garantiza que solo las personas participantes pueden tener acceso a dicha información, que ni terceros, ni WhatsApp mismo los pueden leer o escuchar con lo cual, queda demostrado que una conversación que mantienen dos personas concretas, así como los archivos que contengan datos personales y que se envíen por medio de esta aplicación, en principio cuentan con una expectativa razonable de privacidad, en razón de que esta aplicación digital de WhatsApp, está cerrada exclusivamente a esas dos personas concretas, sin que nadie más pueda ni deba acceder a ese espacio virtual". (Colombia. Corte Constitucional, 2021)

El derecho a la protección de datos personales o autodeterminación informativa, está recogido también en el artículo 92 de la Constitución (Ecuador. Asamblea Nacional Constituyente, 2008), es la antesala al derecho de protección de datos, así nació este concepto en los países en donde no se reconocía expresamente el derecho a la protección de datos personales, hoy en día, ambos derechos han sido prácticamente asimilados por lo mismo, se los utiliza para referirse a un mismo concepto de tal manera que la Corte Constitucional del Ecuador, al ser el máximo órgano de control, interpretación y administración de justicia constitucional, dentro su jurisprudencia vinculante esto es la Sentencia No. 001-14-PJO-CC de 23 de abril de 2014 ha señalado: En el caso de la autodeterminación informativa, como parte del derecho a la protección de datos personales, implica la necesidad de garantizar la

protección de la esfera íntima de las personas, así como la posibilidad de ejercer control sobre los datos personales del sujeto, aunque no se encuentren en su poder". (Ecuador. Corte Constitucional. 2014).

De tal forma que en el Ecuador se ha considerado la relevancia de la protección a los datos personales, a punto tal, que se ha concebido una garantía jurisdiccional específica y única para resguardarlos como es el habeas data; así mismo esta Corte le ha otorgado al hábeas data del siguiente contenido mínimo: a) Hábeas data informativo (derecho de acceso). Es la dimensión procesal que asume el hábeas data para recabar información acerca del qué, quién, cómo y para qué se obtuvo la información considerada personal. b) Hábeas data aditivo (derecho de modificación). Busca agregar más datos sobre aquellos que figuren en el registro respectivo, buscando actualizarlo o modificarlo según sea el caso. c) Hábeas data correctivo (derecho de corrección). Resuelve rectificar la información falsa, inexacta o imprecisa de un banco de datos. d) Hábeas data de reserva (derecho de confidencialidad). Persigue asegurar que la información recabada sea entregada única y exclusivamente a quien tenga autorización para ello. e) Hábeas data cancelatorio (derecho a la exclusión de información sensible). Busca que la información considerada sensible sea eliminada, por no ser susceptible de compilación. (Ecuador. Corte Constitucional, 2021b) Esta jurisprudencia es escasa en nuestro país, sin embargo, en legislaciones como la colombiana se ha asimilado el derecho a la autodeterminación informativa con el hábeas data.

Con base en este articulo 92 de la Constitución, se puede determinar que en efecto el hábeas data reconoce el derecho del titular a conocer sobre su información y cuestiones relativas a la obtención de ésta; de modificarla para actualizar, incluir o ratificar datos inexactos, imprecisos o incompletos; y, que abarca el derecho a que se excluya el dato, esto es, que se lo elimine o anule, con las excepciones previstas en la Ley. Finalmente se debe añadir que la sola verificación del tratamiento no autorizado de los datos personales vulnera el derecho a la protección de datos de carácter personal, sin que sea necesario que se verifique una vulneración adicional al derecho referido, para que proceda la acción de habeas data.

Por lo tanto, el derecho a la protección de datos personales y la autodeterminación informativa es un derecho constitucional autónomo al derecho a la intimidad, imagen, honra, buen nombre y al libre desarrollo de la personalidad. En suma, este derecho supone que el individuo, como titular de su información, en un mundo globalizado, goce de protección y resguardo suficiente para poder decidir qué información compartir sobre su vida privada y bajo qué lineamientos.

CONCLUSIONES

Los datos personales pueden ser entendidos básicamente como la información sobre una persona, tal como se encuentran recogidos en nuestra Constitución; mismos que al ser interpretados conforme al principio pro homine, deben ser entendidos en su forma más amplia como toda información que haga referencia de forma directa o indirecta a cualquier aspecto relativo a una persona o sus bienes, en sus distintas esferas o dimensiones susceptible de ser exigidos a través de la garantía de hábeas data.

La garantía jurisdiccional de Hábeas Data, es una garantía que protege dos derechos fundamentales como el derecho a la información y la autodeterminación informativa o protección de datos personales; los dos son parte del ámbito de los derechos humanos mismos que están reconocidos y protegidos por los Tratados Internacionales y las Cartas Constitucionales de los diferentes países en los que opera un estado de derecho.

Los administradores de bases de datos y sistemas informáticos deberán considerar los aspectos legales y jurisprudenciales a fin de desarrollar sistemas que generen una expectativa de seguridad de datos personales ya tutelados en nuestra constitución mismos que pueden ser exigidos a través de la garantía de Habeas Data.

Ecuador era uno de los pocos países de América Latina que no contaba con una Ley de Protección de Datos Personales, en comparación con otros países que lo hacía desde hace 20 años, al ser una ley nueva es necesario que los encargados del tratamiento de los datos estén al tanto de la normativa vigente para evitar incurrir en las infracciones contempladas y proteger de la mejor manera los datos personales.

REFERENCIAS BIBLIOGRÁFICAS

Asociación Ecuatoriana de Protección de Datos. (2019). Comunicado de la Asociación Ecuatoriana de Protección de Datos sobre la filtración de datos. AEPD http://aepd.org.ec/index.php/noticias/90-comunicado-de-la-asociacion-ecuatoriana-de-proteccion-de-datos-aepd-sobre-la-filtracion-de-datos

BBC NEWS. (2019). Filtración de datos en Ecuador: la "grave falla informática" que expuso la información personal de casi toda la población del país sudamericano. (Sitio web). BBC. https://www.bbc.com/mundo/noticias-america-latina-49721456

Benavent, R. A, Sapena, A. F., & Peset, F. (2021). Compartir los recursos útiles para la investigación: datos abiertos (open data). ***Educación Médica***, ***22***, 208-215.

Colombia. Corte Constitucional (2021). Sentencia T-547/17. Corte Constitucional del Colombia https://www.corteconstitucional.gov.co/relatoria/2017/t-547-17.htm

Ecuador. Asamblea Nacional Constituyente. (2008). Constitución de la República. Registro Oficial N. 449. https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Ecuador. Asamblea Nacional. (2009). Ley Orgánica de Garantías Jurisdiccional y Control Constitucional. Registro Oficial Suplemento 52. https://www.defensa.gob.ec/wp-content/uploads/downloads/2020/03/Ley-Organica-de-Garantias-Jurisdiccionales-y-Control-Constitucional_act_marzo_2020.pdf

Ecuador. Asamblea Nacional. (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento No. 459. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Ecuador. Corte Constitucional. (2014). Sentencia No. 001-14-PJO-CC. Caso N. 0067-11-JD. Corte Constitucional del Ecuador. http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J2FsZnJlc2NvJywgdXVpZDonYmU3ZGE3NjMtZjQ1OC00ZmVmLWFhYzYtOWZhODg2NjUxYjU2LnBkZid9

Ecuador. Corte Constitucional. (2021a). Tramitación de la acción de hábeas data. Caso No. 2064-14-EP/21. Corte Constitucional del Ecuador. https://portal.corteconstitucional.gob.ec/FichaRelatoria.aspx?numdocumento=2064-14-EP/21

Ecuador. Corte Constitucional. (2021b). Hábeas data y acceso a datos generados por servidores y servidoras públicos en ejercicio de sus funciones. Caso No. 89-19-JD. Corte Constitucional del Ecuador. http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOic2MWI1ZDhiMy1iYmE1LTRhN2UtOWZjNS02NzM1ZWFiMzVlNTYucGRmJ30

García González, A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. ***Boletín mexicano de derecho comparado***, ***40***(120), 743-778

Millán González, L., Saorín, T., Ferrer Sapena, A., Alexandre Benavent, R., & Peset Mancebo, M. F. (2013). Gestión de datos de investigación: infraestructuras para su difusión. ***El profesional de la información***, ***22***(4), 415-423.

Noguera-Fernández, A., & Criado de Diego, M. (2011). La Constitución colombiana de 1991 como punto de inicio del nuevo constitucionalismo en América Latina. ***Estudios Socio-Jurídicos***, ***13***(1), 15-49.

Organización para la Cooperación y el Desarrollo Económicos. (2016). Políticas de banda ancha para América Latina y el Caribe. Capítulo 15. Protección de la privacidad. OCDE. https://www.oecd-ilibrary.org/docserver/9789264259027-18-es.pdf?expires=1636259410&id=id&accname=guest&checksum=1CAEC11E76B714E4126F43AA5D8B8F8C

Ortiz Crespo, S. (2008). Participación ciudadana: la Constitución de 1998 y el nuevo proyecto constitucional. Íconos-Revista de Ciencias Sociales, (32), 13-17.

Salazar, J. (2021). EY Building a Better working world. Legal Alert. https://www.ey.com/es_ec/tax/tax-alerts-ecuador/ley-de-proteccion-de-datos-personales