DOI: https://doi.org/10.56712/latam.v4i2.912

Protección de datos personales en el uso de la aplicación ASÍ Ecuador

Personal data protection in the use of ASÍ Ecuador application

Jenny Patricia Lazo Barrera
jenny.lazo@est.ucacue.edu.ec
https://orcid.org/0000-0001-7755-6654
Universidad Católica de Cuenca
Cuenca – Ecuador

Artículo recibido: 17 de julio de 2023. Aceptado para publicación: 02 de agosto de 2023.
Conflictos de Interés: Ninguno que declarar.

Resumen

Debido a la pandemia de la Covid-19, Ecuador incorporó el uso de la aplicación ASÍ Ecuador que consistía en notificar en el celular, si una persona estuvo en contacto con un caso positivo. Resulta de importancia determinar si este intercambio de información que se realiza por bluetooth ofrece una adecuada protección sobre los datos personales de cada usuario. Por ello, la presente investigación tiene como objetivo determinar si existe o no vulneración al derecho a la protección de datos personales, en el uso de la aplicación ASÍ Ecuador. Es una investigación, con un aporte cualitativo respecto al análisis del derecho a la protección de datos personales en la legislación ecuatoriana mediante un método sistemático. Concluyendo que la aplicación fue elaborada bajo el protocolo de rastreo descentralizado en el que se solicita la ubicación geográfica que, si bien es un dato personal, existe un anonimato en el intercambio de los datos.

Palabras clave: aplicación ASÍ ecuador, covid-19, intimidad, protección de datos personales

Abstract

Because of covid-19 pandemic, ASÍ Ecuador application was incorporated in Ecuador which aim was to notify in the cellphone, if a person was in contact with a positive covid-19 case. Therefore, it is important to determinate if this information exchange that is doing by bluetooth offers enough personal data protection of every single user. The objective of this investigation is to determinate whether or not there is a violation of the right of personal data protection, in the use of ASÍ Ecuador application. This is an investigation, with a qualitative contribution regarding the analysis of the protection of personal data right in Ecuadorian legislation through a systematic method. Having as a result of this investigation that the application was developed under the decentralized tracking protocol, where requests the geographic location which is a personal data. However, it indicates there is anonymity in data exchange.

Keywords: ASI Ecuador application, covid-19, privacy, personal data protection

Todo el contenido de LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, publicados en este sitio está disponibles bajo Licencia Creative Commons . 

Como citar: Lazo Barrera, J. P. (2023). Protección de datos personales en el uso de la aplicación ASÍ Ecuador. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades 4(2), 4449–4462. https://doi.org/10.56712/latam.v4i2.912*

INTRODUCCIÓN

En el siglo XIX tomó relevancia el derecho a la vida privada, por ende, a finales de los años 70, países europeos como Alemania y Francia hicieron énfasis en la protección de datos personales como "un mecanismo jurídico para amparar el derecho a la vida privada de las personas y sobre todo toma relevancia en las décadas siguientes debido al avance tecnológico en el campo de la informática y tecnologías de la comunicación" (Enríquez Álvarez, 2017). El rápido desarrollo de las nuevas tecnologías como es la Internet y las aplicaciones móviles, han generado que una cantidad innumerable de datos estén disponible en la web, incluso información de carácter personal. Esta conexión y tráfico de datos, a la vez genera problemas en la difusión de esta información a terceras personas que pueden conocer nuestros datos, y, que podría resultar en la vulneración de derechos fundamentales como la protección de datos o la intimidad.

La pandemia de la Covid 19 ha ocasionado que, el intercambio de la información se la realice por medios digitales, por ejemplo en muchos países se declararon confinamientos que buscaron contrarrestar el avance del virus, provocando que temas como el trabajo, salud, educación y otros se vean volcados al uso de plataformas y programas digitales, que permitan tener una adecuada comunicación, exacerbando el derecho de las personas a decidir y consentir de manera informada sobre el uso y tratamiento automatizado de los mismos.

Ecuador, no fue ajeno a esta realidad, ya que durante la pandemia por parte del ejecutivo se formularon Decretos Ejecutivos para declarar estados de excepción. También se desplegó el uso de tecnologías de vigilancia, como es el caso de la aplicación digital "ASÍ Ecuador", la que tuvo como finalidad mitigar la propagación de la Covid-19. Por ello, es de suma importancia analizar si la utilización de esta aplicación, vulnera o no el derecho a la protección de datos personales, lo cual es un derecho de rango constitucional. Pues, como se ha manifestado anteriormente, la disrupción tecnológica, la aceleración en el uso de aplicaciones, recursos de hardware y software, durante la pandemia, son el principal factor de que la data, de índole personal, se encuentre disponible en la red, lo cual genera un dilema complejo en función de confidencialidad e integridad, por el acceso a nuestra información y la cantidad de personas que pueden conocer nuestros datos.

Además, en su lanzamiento, se indicó que "la información de los ciudadanos está protegida, pues la herramienta es bastante robusta en materia de privacidad" (Gobierno, 2020). Sin embargo, es importante analizar bajo qué parámetros y sistemas de comunicación funciona y que tipo de permisos se otorgan, pues, debería cumplir con los tres pilares fundamentales de seguridad: confidencialidad, integridad y disponibilidad; y si se encuentra disponible para descargas en teléfonos inteligentes, hasta qué punto es confiable y si el eslabón más débil en muchos de los casos es la persona natural que descarga aplicaciones, está protegida en sus derechos humanos fundamentales.

En este sentido, la Organización de las Naciones Unidas (ONU) reconoce que tan solo 121 países de 194 han incorporado legislación respecto a la protección de datos personales, lo que equivale al 62%, "existiendo un grupo grande que no cuenta con un estándar alto de protección de datos personales o con leyes específicas que lo regulen" (Roldán Carrillo, 2021). En el caso ecuatoriano, salió del grupo de países que no contaba con una ley específica para proteger los datos personales, ya que el 10 de mayo de 2021 se aprobó la Ley Orgánica de Protección de Datos Personales. Esto a pesar de que, en su norma constitucional de 2008 ya se reconocía el derecho a la protección de datos personales. El artículo 66 numeral 19, establece que "el derecho a la protección de datos de índole personal engloba el acceso y la decisión sobre la información y para su difusión se requiere el consentimiento del titular" (Constitución de La República Del Ecuador, 2008).

Sin embargo, cuando no se contaba con esta ley, fue la jurisprudencia quien vino a dotar de contenido este derecho. La Corte Constitucional, a través de diferentes sentencias, entre las cuales se puede destacar la sentencia N° 2064-14-EP/21 señaló que los datos personales consisten en "la información de una persona identificada o identificable, como es el nombre, número único de identificación, datos de localización, identidad física, genética, económica, etc"(Sentencia No. 2064-14-EP/21, 2021).

El trabajo se estructura de la siguiente manera: primero se aborda el marco jurídico interno que posee Ecuador para efectivizar el derecho a la protección de datos personales, segundo se aborda el uso de aplicaciones de proximidad de personas contagiadas de Covid -19 en varios países, tercero se aborda la vulnerabilidad en el tratamiento de los datos personales en el uso de las tecnologías y por último se analiza el funcionamiento y uso de la aplicación ASÍ Ecuador.

METODOLOGÍA

Es una investigación con un enfoque cualitativo respecto al análisis del derecho a la protección de datos personales en la legislación ecuatoriana mediante los siguientes métodos: método sistemático, partiendo de un análisis constitucional e infraconstitucional respecto al análisis del derecho a la protección de datos personales. A esto se ha sumado una importante búsqueda jurisprudencial que en su momento aportó de forma significativa para cubrir el vacío normativo, hasta mayo de 2021 fecha en la cual se aprueba la Ley Orgánica de Protección de Datos Personales. En una segunda fase se aplicó el método de investigación científico, a fin de analizar el funcionamiento y uso de la aplicación del control de proximidad ASÍ Ecuador, con el fin de identificar si existen vulnerabilidades que supongan una vulneración al derecho de protección de datos personales.

RESULTADOS Y DISCUSIÓN

La protección de datos personales en el Ecuador

Siendo conscientes de la evolución y transformación de la tecnología de la información en los últimos años, se ha llegado a la necesidad de dar una adecuada valorización a los datos personales, fundamentada en la correcta e incorrecta utilización de los mismos, frente a riesgos de vulneración de derechos humanos. En este marco, la Constitución de la República en su artículo 66 numeral 19, incluyó el derecho a la protección de datos de carácter personal. Siendo necesario contar con un marco normativo infraconstitucional que regula varios aspectos que devienen de este derecho.

En el año 2019 en la Asamblea Nacional se presentó el Proyecto de Ley Orgánica de Protección de Datos Personales, con el objetivo-finalidad de ser un instrumento de regulación del "ejercicio del derecho a la protección de datos personales, la autodeterminación informativa y demás derechos digitales en el tratamiento y flujo de datos personas, a través del desarrollo de principios, derechos, obligaciones y mecanismos de tutela"(Proyecto de Ley Orgánica de Protección de Datos Personales, 2019, p. 10). La misma fue aprobada el 10 de mayo de 2021. Su importancia radica en la definición de ciertos conceptos tales como: dato personal, dato sensible, titular, responsable del tratamiento de los datos, entre otros. Así como en establecer una autoridad responsable en el tratamiento de los datos personales, denominándose Autoridad de Protección de Datos Personales.

En lo correspondiente al consentimiento para el tratamiento de datos personales se indica que el mismo debe ser libre, específico, informado e inequívoco. Además, al abordar el tratamiento de datos relativos a la salud, se estableció que por razones de interés público se puede omitir el consentimiento del titular cuando se tenga como finalidad la "prevención, diagnóstico o

tratamiento" (Ley Orgánica de Protección de Datos Personales, 2021). Sin embargo, los datos deben ser anonimizados o seudonimizados, para evitar identificar a los titulares, en la misma línea es necesario tener en cuenta que los datos de salud corresponden a una categoría especial de datos personales tal como lo establece el artículo 25.

También, se determinó que es posible una excepcionalidad, que en este caso es el recabar datos con la finalidad de investigación científica. Situación que se encuentra en relación al tema abordado, ya que se reconoce la necesidad de crear bases estadísticas para el estudio epidemiológico que representa el Covid-19.

Otro aspecto destacable de la ley, es el reconocimiento del derecho a la limitación del tratamiento de la información, que consiste principalmente en que se use el mínimo de datos personales en el tratamiento efectuado por responsables o encargados del tratamiento de datos, de igual forma se incluye el derecho a que los datos personales no se encuentren disponibles en internet u otros medios de comunicación masiva salvo que exista capacidad de control técnico de los mismos. Este aspecto evita o controla de alguna forma el intercambio de información sin consentimiento que existe por parte de empresas nacionales y extranjeras con respecto a datos de carácter personal, sin embargo, se hace complejo cuando la información repose en bases de datos extranjeras.

Aplicaciones de control de proximidad de personas para efectos de Covid-19

La pandemia originada por la aparición de la variante SARS-CoV-2, ha ocasionado grandes afecciones en la salud de la población a nivel mundial, generando elevadas tasas de mortalidad, cuantiosos problemas económicos y el aumento del desbalance social en todo el mundo. Es por ello, que los gobiernos dentro de sus estrategias para contener la expansión de la enfermedad, han optado por utilizar la tecnología móvil celular para monitorear los casos en relación con el Covid-19. En este punto, el apoyo brindado por los organismos multilaterales ha sido fundamental, puesto que dieron paso al desarrollo de sistemas que regulan la comunicación entre plataformas o los denominados "protocolos", que permiten el rastreo de contagiados utilizando el hardware y software de los dispositivos celulares.

La Unión Europea a finales de marzo del año 2020, encontró un consenso para crear tecnología móvil de rastreo de proximidad con la finalidad de aplanar la curva de contagios del Covid-19, para ello los laboratorios como "Fraunhofer, en Alemania y la Escuela Politécnica Federal de Lausana, en Suiza", diseñaron el primer protocolo para el Rastreo de Proximidad Paneuropeo para Preservar la Privacidad (PEPP-PT)" (Berchi, 2020). Este es un protocolo diseñado para facilitar el rastreo de contactos digitales de los participantes infectados de una manera centralizada.

El modelo centralizado se basa en el registro y permiso del sistema operativo, seguimiento de proximidad, verificación, carga del estado de infección y la advertencia de proximidad. Además, su forma de operación consiste en el envío, recepción y almacenamiento de datos en los dispositivos celulares, utilizando la tecnología Bluetooth Low Energy (BLE), puesto que es una tecnología de comunicación inalámbrica que requiere un bajo consumo de energía. La tecnología BLE, en el modelo centralizado puede enlazar dos dispositivos móviles, estableciendo una comunicación directa y a corta distancia, sin necesidad de utilizar la red celular, permitiendo el intercambio de identificadores anónimos de largo plazo, es decir los identificadores anónimos permanecen constantes por un largo tiempo, por lo que, este comportamiento dinámico desencadena la presunción de presencia de riesgos y vulnerabilidades, provocados por la ausencia de técnicas de seguridad de la información, aplicadas a la infraestructura de datos de las organizaciones. Como una salvedad, las aplicaciones basadas en PEPP-PT no almacenan

datos de ubicación y los datos generados son eliminados cuando el usuario desinstala la aplicación.

A partir de este primer ensayo, se planteó la posibilidad de que la información generada por las aplicaciones del Covid-19 debería ser almacenada en servidores centrales, administrados por los gobiernos, con la premisa de que las autoridades sanitarias puedan adoptar estrategias y tomar decisiones más acertadas en la lucha contra la pandemia; es así que se desarrolló la propuesta de un Protocolo de Rastreo de Proximidad Robusto y que Conserva la Privacidad (ROBERT), por sus siglas en inglés, cuya función se basó en utilizar un servidor federado para la base de datos Backend, el cual consiste "en aquel entorno en el cual se ejecutan los programas informáticos los cuales almacenan, aseguran, procesan y analizan los datos de manera continua para posteriormente producir información la cual será presentada de manera visual"(GALICIA-GARCÍA et al., 2015). En las consideraciones para su arquitectura, se puntualiza que:

Se comparte la información entre la aplicación y el servidor Backend, así mismo, la recopilación de datos de contactos de proximidad se realiza y almacena localmente en cada aplicación. Estos datos no son revelados al servidor excepto cuando el usuario es diagnosticado con Covid-19 positivo y en este caso específico, se establece un acuerdo entre el paciente y la autoridad sanitaria para compartir de manera anónima los datos de proximidad recogidos durante el ciclo de contagio, permitiendo al Backend utilizar estos datos para calcular la puntuación de riesgo de exposición de cada una de las personas (identificadores anónimos) que han estado en contacto con el usuario infectado.(Castelluccia et al., 2020, p. 3)

El servidor Backend utiliza la información de cada usuario en contacto con un paciente infectado, y luego realiza un cotejo periódico del servidor para determinar la puntuación de riesgo, finalmente, para los usuarios será visible únicamente la información del servidor: "con riesgo" o "sin riesgo", permitiendo además que la información de otros usuarios permanezca anónima, pero a la vez, manteniendo el servidor Backend con un listado de usuarios expuestos e identificados con seudónimos anónimos, que no relacionan información personal de los usuarios del sistema presentando una mejora con respecto a PEEP-T, pero con deficiencias semejantes en términos de tratamiento de la información personal y la protección de datos de los individuos.

Luego, en búsqueda de resguardar aún más la confidencialidad de los datos, un equipo liderado por la científica Carmela Troncoso de la Escuela Politécnica Federal de Lausana (EPFL) y otras instituciones científicas y académicas, desarrollaron el protocolo de Rastreo de Proximidad Descentralizado Preservando la Privacidad (DP-3T), que ofrecía una solución desconcentrada para el rastreo de contactos de proximidad, conservando los datos en los terminales móviles, mejorando el anonimato de la información y garantizando la privacidad. Es decir, el usuario será quien envíe de manera voluntaria la información en caso de dar positivo de Covid-19 e informe a las autoridades.

El principio de funcionamiento del protocolo DP-3T se cimienta en la transmisión de los identificadores anónimos (EBID) a través de la característica BLE del equipo móvil celular del usuario, permitiendo recibir y almacenar en éste, los EBID de usuarios más cercanos. Cuando un usuario resulta positivo de Covid-19, envía sus EBID al Backend y a los usuarios del sistema, en donde proceden a comparar con los EBID almacenados, y en caso de coincidir con alguno de los identificadores, la aplicación informa al usuario que ha estado en contacto con un paciente positivo de Covid-19. Los EBID tienen un cambio continuo para evitar el rastreo de la persona que está en uso de la aplicación, brindando de esta manera seguridad en el intercambio de información, para ello se priorizan dos aspectos relevantes, por un lado, el intercambio de los EBID entre los dispositivos móviles y, por otro lado, la distancia de proximidad entre dispositivos móviles.

Así en varios países se crearon algunas aplicaciones similares como: Swiss COVID, "utilizada en Suiza con la finalidad de generar un rastreo de los contactos de Covid-19, con un enfoque descentralizado haciendo uso de la tecnología BLE"(FOPH, 2021). Se basa en estabilizar los acercamientos de proximidad con el fin de controlar los contagios. Esta aplicación ha sido muy criticada por su carencia de efectividad en la protección de datos hacia los ataques cibernéticos.

En el caso español fue creador el Radar COVID con "la finalidad de llevar un registro de cercanía de contactos a través de los dispositivos celulares con la finalidad de determinar la exposición con un contacto de Covid-19 positivo que la aplicación almacena" (Gobierno de España, 2021). Según estadísticas del Gobierno de España existieron 8,600,858 descargas en Market Places, desde agosto de 2020" (España, 2021). Además, cuentan con datos de cada comunidad autónoma que se generaron durante la pandemia. "Esta aplicación finalizó su actividad el nueve de octubre de 2022" (RadarCOVID, 2022).

Por otra parte, NHS COVID 19 tuvo acogida en Inglaterra y Gales en septiembre de 2020, a través del uso de la plataforma de notificación de exposición Bluetooth. La misma genera una alerta indicando que los usuarios han tenido contacto con un individuo positivo de Covid-19, además "ayuda a establecer la rapidez con la cual se está propagando el virus de manera que ayuda a rastrear el virus mas no a los individuos" (NHS, 2020). Esto incluyó una gama de servicios como: informes de resultados positivos de pruebas, información del área local, registró en el lugar, verificación de síntomas, acceso a pagos de aislamiento (Kendall et al., 2023). Asimismo, se estimó que durante los tres primeros meses de la aplicación se redujo el número total de casos en un 13% (rango central del 95% de los análisis de sensibilidad 5-19%) o 24% (95% intervalo de confianza 14-33%) según la técnica de atribución. Concluyendo que "las aplicaciones de rastreo de contactos digitales tienen un gran potencial para reducir la transmisión del SARS-COV-Z cuando se combinan con una fuerte participación de los usuarios" (Kendall et al., 2023).

Vulnerabilidad al tratamiento de los datos personales en las tecnologías

Antes de la aprobación y entrada en vigencia de la Ley Orgánica de Protección de Datos Personales, no existía en el país una regulación específica que permitiera garantizar el desarrollo del derecho fundamental a la protección de datos personales como "un derecho autónomo que contribuya a la efectivización de otros derechos fundamentales como la privacidad, no discriminación, libertad de conciencia, expresión, acceso a la información, entre otros" (Betancourt, 2020).

La transmisión, uso y difusión de los datos, se realizaba sin ninguna restricción, ni medidas legales ni regulatorias que protegieran la vida personal y los datos de las personas, restándoles control sobre su propia información, siendo incluso en algunos casos utilizada tanto con fines políticos y comerciables y sin consentimiento del titular. Lamentablemente, el país fue noticia a nivel mundial ya que "se expuso información personal de casi la totalidad de la población en 2019, por no contar con protocolos de protección de datos, dejando expuestos nombres, información financiera y datos civiles" (BBC News, 2019).

A nivel internacional, el reconocimiento jurídico del derecho a la protección de datos personales no ha sido nada fácil, existieron diversos dilemas que han venido enfrentando los Estados, sobre todo en cuanto se refiere al vínculo de la protección de los datos personales con el derecho a la autodeterminación de sus ciudadanos en el contexto de las nuevas tecnologías. Desde la constitucionalización de ciertos derechos fundamentales "la protección de datos personales se define como un derecho autónomo, esto es un derecho nuevo vinculado a la necesidad de proteger la dignidad personal frente a las nuevas tecnologías" (Ordóñez Pineda, 2017).

Fue el Tribunal Constitucional Federal Alemán quien desarrolló en el año de 1983 el derecho a la protección considerando su derecho a la libertad esto es, " (…) de decidir la difusión y utilización de los datos personales, de igual manera alerta del peligro en caso de una intrusión"(Herrán Ortiz, 2003). Buscando proteger derechos como la intimidad, dignidad, honor entre otros, que eventualmente pueden verse vulnerados al inferir en la esfera misma de la persona.

El derecho a la protección de datos se ubica dentro de los derechos de tercera generación y dentro de ello, lo relativo a la autodeterminación informativa. Esta última, está supeditada a la existencia de información que atañe a un determinado sujeto o a la necesidad de que este tenga una esfera mínima de actuación libre respecto a dicha información, sobre la cual no debería existir una interferencia ilegítima por parte de terceros.

La Corte Constitucional del Ecuador ha manifestado al respecto en la sentencia N° 001-14-PJO-CC de 2014, señalando:

La autodeterminación informativa está supeditada, entonces, a la existencia de información que atañe a determinado sujeto y a la necesidad de que este tenga una esfera mínima de actuación libre respecto de dicha información, sobre la cual no debería existir una interferencia ilegítima por parte de terceros; asimismo, implica 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 (...) 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.(SENTENCIA N° 001-14-PJO-CC, CASO N° 0067-11-JD, 2014)

De esta manera "su protección en el ámbito jurídico es esencial y su desarrollo debe converger con el ejercicio pleno de sus derechos" (Ordóñez Pineda, 2017). Considerando que constituye un derecho fundamental, personalísimo e inherente a las personas y que debe ser garantizado por el ordenamiento jurídico vigente, tal como lo ha establecido la Corte Interamericana de Derechos Humanos, así como su desarrollo legislativo a nivel nacional e internacional.

Todo esto nos lleva a considerar la necesidad de regular y proteger el tratamiento de la información, tomando en cuenta los avances de la tecnología de manera articulada a la vida privada de las personas. Las nuevas tecnologías han irrumpido de manera abrupta en el ámbito del derecho produciendo un profundo cambio en los entornos comunicativos que inciden directamente en los derechos de las personas. Las nuevas tecnologías se pueden definir como "las bases fundamentales de la comunicación, mediante lo cual se puede tener acceso a información actualizada y en tiempo real" (Moya Martínez, 2009). Cuyo acceso y difusión es ilimitado, pudiendo constituirse en un eventual peligro por la magnitud de posibilidades a las que las personas pueden tener acceso.

"Las nuevas tecnologías, permiten, por una parte, la comunicación a un colectivo amplio de personas independientemente de su situación geográfica y por otra, poner a disposición de todas ellas, la información sin limitaciones de lugar de residencia" (Cabero Almenara, 2004). Es decir, son aparatos que sirven para la información, por ejemplo, la Internet, también es necesario tener en cuenta que son los datos personales, básicamente son "el conocimiento, alusivo al hombre y su dignidad, en cuanto pensamientos, creencias que conforman el dominio íntimo del ser humano" (Nájera Montiel, 2008). Respecto al uso y difusión de esta información se suscita la mayor problemática, toda vez que no existe una verdadera garantía de acceso y control a la misma.

Los datos a su vez pueden ser: datos sensibles, estos hacen alusión a datos de origen étnico, identidad de género, salud, creencias religiosas, afiliación política; entre otros, que afectan la esfera más íntima del ser humano, y su mal uso pueda ser causa de discriminación. Los datos personales como el nombre, número de cédula y la firma; y los datos públicos que son aquellos a los cuales se puede acceder sin necesidad del consentimiento del titular. En cada uno de ellos, pueden existir datos que por su propia naturaleza no deben ser conocidos por terceras personas, es así que la protección de datos personales aparece como un instrumento jurídico para salvaguardar el derecho a la vida privada de los individuos frente a las nuevas tecnologías. Su protección según el autor Hondius, "debe garantizar el derecho constitucional de la libertad, derecho a la intimidad e individualidad, en base al procesamiento manual o automático de datos personales" (García González, 2007).

Actualmente, a nivel internacional, el derecho a la vida privada ha sido consagrado como un derecho humano, tanto en el Sistema Universal de Derechos Humanos como en los sistemas regionales (específicamente en los sistemas europeo e interamericano). Por lo que hace al Sistema Universal, esto es, con un alcance global, la Declaración Universal de los Derechos Humanos de 1948 (artículo 12), el Pacto Internacional de Derechos Civiles y Políticos de 1966 (artículo 17), la Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares, de 1990 (artículo 14), y la Convención sobre los Derechos del Niño de 1989 (artículo 16), lo contemplan prácticamente en los mismos términos.

De cierta manera vemos un gran desarrollo normativo internacional respecto al derecho a la protección de datos personales, sin embargo, es indispensable una normativa interna que determine la operatividad de la protección a través del Estado, a fin de tutelar de mejor manera el derecho a la protección de datos y evitar la afectación de la esfera íntima del ser humano tan importante para su desarrollo y existencia.

Ya en el caso ecuatoriano, la Constitución del 2008 reconoce y garantiza en el artículo 66 numeral 19 a sus ciudadanos; "el derecho a la protección de datos personales, incluye el acceso, decisión y protección de la información. La recolección, archivo, procesamiento, y difusión de estos datos requerirán la autorización del titular o el mandato de ley" (Constitución de La República Del Ecuador, 2008).

En este sentido, Ecuador cuenta con normativa infraconstitucional para amparar el derecho a la protección de datos personales, como es el caso de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, que en su artículo 9 ha dispuesto "para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá la autorización expresa del titular de éstos, quien seleccionará la información a compartirse con terceros"(LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS, 2002). Es decir, para la difusión de la información personal se requiere el consentimiento del titular de los mismos.

Y con la aprobación de la Ley Orgánica de Protección de Datos Personales en mayo de 2021, se sigue la línea establecida en la Constitución al desarrollar de manera más amplia el derecho a la protección de datos personales, y sobre todo regula de manera eficiente la protección de los datos personales, en cuanto establece la definición de datos personales dejando de la lado interpretaciones, se da la creación de la Autoridad de Protección de Datos Personales, es decir de un organismo público independiente que supervise el cumplimiento del ordenamiento jurídico respecto a la protección de datos personales. Debiendo considerar lo ya antes señalado que, se puede omitir el consentimiento del titular en la comunicación de los datos personales relativos a la salud respecto a la realización de estudios epidemiológicos (artículo 35).

Análisis del funcionamiento y uso de la aplicación ASÍ Ecuador

El gobierno ecuatoriano, en colaboración con el Banco Interamericano de Desarrollo (BID) y el Grupo Link implementaron el uso de la aplicación ASÍ Ecuador, la misma es una herramienta gratuita que sirve para el rastreo de proximidad de contactos de Covid-19, tiene como finalidad disminuir la propagación del Covid-19. En los primeros meses del 2021, la Organización Mundial de Salud y los gobiernos implementaron un plan de vacunación a nivel mundial, en coordinación con diferentes casas farmacéuticas, mismas que utilizan diversas tecnologías biológicas para combatir los efectos adversos de las nuevas variantes y cepas del Covid-19. Sin embargo, el virus aún continúa presente debido a la falta de vacunación y otros factores que justifican la necesidad de utilizar herramientas de control de proximidad de contactos. Esta aplicación fue desarrollada utilizando el protocolo de rastreo descentralizado de contactos DP-3T, lo que exige que los contactos rastreados se mantengan en el anonimato.

En términos de privacidad, la aplicación ASÍ Ecuador fue elaborada en base a rigurosos protocolos principalmente usados en la Unión Europea con lo cual se busca garantizar "la confidencialidad de la información, integridad de los datos obtenidos y la disponibilidad de la información (CID)" (Carmona & Lara Alcántara, 2012). Es decir, se busca asegurar el cumplimiento de la triada CID, seguridad y protección de datos personales.

Para su funcionamiento, la aplicación solicita la ubicación geográfica permanente del usuario que se encuentra utilizando el servicio, y de igual manera el Bluetooth siempre deberá estar en modo activo. Estos requisitos se encuentran en la fase de configuración y puesta en operación del sistema, siendo un acto de total voluntad, sin ningún tipo de imposición hacia quien desee hacer uso de la aplicación. De igual manera será un acto voluntario, el hecho de que el usuario diagnosticado positivo notifique su código al personal sanitario para efectos de prevención y notificación.

El Backend es exclusivo de los desarrolladores o administradores de la solución, y al momento del presente estudio, no registra indicios de vulneración de datos de usuarios finales; esto se cumple, porque registra únicamente los códigos generados y actualizados por los servidores de la aplicación; visto de otra manera, la información que se maneja en el Backend es un registro de códigos generados por la aplicación, el cual, es actualizado en línea y comparado con los códigos de usuarios positivos que se tiene en las bases de datos de la aplicación.

La aplicación ASÍ Ecuador respecto al anonimato de la información considera que al hablar de intimidad se hace alusión al derecho al anonimato que poseen los individuos de conservar su información de manera privada, lo que se justifica en los artículos que hemos mencionado con anticipación.

Sin embargo, todas las aplicaciones tienen sus riesgos y son inseguras, porque al momento de instalarlas acceden a nuestros contactos, imágenes, entre otras opciones, debido a que los usuarios dan permiso sin darse cuenta, en la aplicación ASÍ Ecuador, fundamentalmente se permite conocer la ubicación de las personas, hecho que podría resultar vulnerable si lo pensamos desde el punto de vista del derecho de los ciudadanos frente al Gobierno, es por ello que, José Miguel Vivanco, director de las Américas de Human Rights Watch manifestó que, llevar a cabo medidas de vigilancia para evitar la propagación de la Covid-19 sin una ley clara que proteja datos personales ni un organismo independiente que supervise su cumplimiento pone en riesgo el derecho a la privacidad de los ecuatorianos.

De lo manifestado se puede deducir que en Ecuador no se vulnera el derecho a la protección de datos personales, en cuanto a partir del 10 de mayo de 2021 se aprobó la Ley Orgánica de Protección de Datos Personales, dando paso a que Ecuador posea una ley especial para regular

la protección de datos personales, en la cual se hace alusión a la limitación del tratamiento de la información es decir, que se use el mínimo de datos personales, frente a esto se puede manifestar que la aplicación ASÍ Ecuador actualmente está respaldada por la Ley Orgánica de Protección de Datos Personales, a más de que dicha aplicación ha sido desarrollada en base al protocolo de rastreo descentralizado el cual va a la par con el anonimato en cuanto usa identificadores anónimos que cambian de manera continúa con lo cual se evita el rastreo del usuario, brindando de esta manera seguridad y confidencialidad. Además, se determinó la creación de un organismo público independiente que supervise el cumplimiento de la efectivización del derecho a la protección de datos personales, claro está que dicha aplicación tiene como objetivo frenar la propagación del Covid- 19, por ello conforme el artículo 30 de la Ley Orgánica de Protección de Datos no es necesario el consentimiento del titular para dar tratamiento a los datos referentes a la salud frente a un interés público pero eso no significa que se revelara datos personales como es el nombre, Número Único de Identidad, datos de localización, puesto que dichos datos van a la par con el anonimato o seudónimos con lo cual se evita identificar a los titulares de la información.

CONCLUSIÓN

Los datos personales consisten en la información referente al dominio íntimo de cada ser humano. Es decir, es aquel dato que identifica o hace identificable a una persona natural. En el caso ecuatoriano vemos como a través de conceptos jurisprudenciales se dotó de contenido a qué se debe entender por dato personal, así como los elementos que lo caracterizan. Por lo tanto, su protección se ha vuelto necesaria en los ordenamientos jurídicos, ya que su tratamiento debe garantizar su debida tutela.

Es importante destacar que los datos relativos a la salud según la ley ecuatoriana de protección de datos personales son datos sensibles y por lo tanto goza de una categoría especial de dato personal. Sin perjuicio de ello, su tratamiento está permitido para fines de investigación científica, o fines estadísticos. Más aún en tiempos de pandemia en donde la generación de información fue indispensable para evitar un mayor número de contagios y muertes; y, contar con ella por el contrario permitía una mejor toma de decisiones.

En esta misma línea, los estados volcados a proteger a su población, aplicaron diferentes acciones como restricciones al libre tránsito, cierres de fronteras, planes de vacunación, etc para mitigar la propagación del Covid-19. En el caso ecuatoriano, se analizó la aplicación “Así Ecuador” vigente desde 2020 que tuvo la finalidad de reducir el número de contagios, pero no se logró identificar información respecto a su impacto durante su vigencia, el número de descargas, o cómo esta herramienta evitó o disminuyó el número de contagios. Situación diferente la observamos en España o Inglaterra en donde esta iniciativa mantuvo un monitoreo.

En lo relacionado a la herramienta y la protección de datos personales, queda claro entonces que el sistema PEPP-PT no almacena datos de ubicación. Si bien los datos de localización son datos personales, la aplicación “Así Ecuador” garantiza el anonimato en el intercambio de información. Tutelando el derecho a la protección de datos personales y el derecho a la intimidad. Sin embargo, esto no quiere decir que el estado no se encontraba facultado para utilizar esta información para levantar información útil para enfrentar la pandemia y quizás mantener un monitoreo. A esto se suma que en google play, se indica que existieron más de 500 mil descargas, lo cual parece ser una aplicación que no llegó a ser conocida por la gran mayoría de la población y por tanto no generó el impacto deseado.

Agradecimientos

El presente artículo científico responde a un proyecto de Investigación Formativa de la Universidad Católica de Cuenca denominado "La vulneración a los derechos de protección de datos personales, a consecuencia de la proliferación del uso de las tecnologías de la información y comunicación por efectos del COVID-19", donde agradezco a las docentes de la Universidad Católica de Cuenca: Dra. Adriana Mora. Mgs, Dra. Marcela Sánchez. Mgs. y Mgs. Juan Ortega por su amplio apoyo y conocimientos para la realización del presente artículo científico.

REFERENCIAS

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. BBC News Mundo. https://www.bbc.com/mundo/noticias-america-latina-49721456#:~:text=BBC Extra-,Filtración de datos en Ecuador%3A la %22grave falla informática%22,la población del país sudamericano&text=Pie de foto%2C,de 17 millones de personas.

Berchi, M. (2020). La privacidad es necesaria para tener libertad. Ámbito. https://www.ambito.com/negocios/google/la-privacidad-es-necesaria-tener-libertad-n5118227

Betancourt, V. (2020). Protección de datos personales : un tema aún pendiente en Ecuador. Universidad Andina Simón Bolívar, 1–4.

Cabero Almenara, J. (2004). La transformación de los escenarios educativos como consecuencia de la aplicación de las TICs: estrategias educativas. Formación de La Ciudadanía : Las TICs y Los Nuevos Problemas / XV Simposio Internacional de Didáctica de Las Ciencias Sociales. Pag: 15-, 1–28.

Carmona, R. C., & Lara Alcántara, J. G. (2012). Seguridad de la información - Como una ventaja Competitiva. In TECNOLÓGICO DE MONTERREY. Instituto Tecnológico y de Estudios Superiores de Monterrey.

Castelluccia, C., Bielova, N., Boutet, A., Cunche, M., Lauradoux, C., Métayer, D. Le, & Roca, V. (2020). ROBERT: ROBust and privacy-presERving proximity Tracing. HAL Archives-Ouvertes, 1, 1–14. https://hal.inria.fr/hal-02611265

Constitución de la República del Ecuador, Pub. L. No. Registro Oficial 449 de 20-octubre de 2008, 1 (2008).

Enríquez Álvarez, L. (2017). Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de la Ley Orgánica de Protección a los Derechos a la Intimidad y la Privacidad sobre los Datos Personales. FORO: Revista de Derecho, (27), 43–61.

España, G. de. (2021). Estadísticas. Radar COVID. https://radarcovid.gob.es/estadisticas/descargas-radar

FOPH, F. O. of P. H. (2022). SwissCovid app and contact tracing. Bag Admin Ch. https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing.html#-1601404801

GALICIA-GARCÍA, C., ORTEGA-GINÉS, H. B., & CURIOCA-VARELA, Y. (2015). Desarrollo de un Back-End adaptativo para portales web Development of a Back-End adaptive to web portals. Revista de Sistemas Computacionales y TIC ' s, 1(1), 52–60. https://www.ecorfan.org/spain/researchjournals/Sistemas_Computacionales_y_TICs/vol1num1/Sistemas Computacionales y TIC-52-60.pdf

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. https://www.scielo.org.mx/pdf/bmdc/v40n120/v40n120a3.pdf

Gobierno de España. (2021). Home | Radar covid19. Radar COVID. https://radarcovid.gob.es/home

Gobierno, M. de. (2020). APP "ASÍ" PARA COMBATIR LA PANDEMIA. https://www.ministeriodegobierno.gob.ec/app-asi-para-combatir-la-pandemia/

Herrán Ortiz, A. I. (2003). El derecho a la protección de datos personales en la sociedad de la información. In Universodad de Deusto (Universida, Vol. 26). Universidad de Deusto. http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf

Kendall, M., Tsallis, D., Wymant, C., Francia, A. Di, Balagun, Y., Didelot, J., Ferretti, L., & Fraser, C. (2023). Impactos epidemiológicos de la aplicación NHS COVID-19 en Inglaterra y Gales durante su primer año. Nature Communications. https://doi.org/10.1038/s41467-023-36495-z

LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS, Pub. L. No. Registro Oficial Suplemento 557 de 17-abr-2002, 1 (2002).

Ley Orgánica de Protección de Datos Personales, Pub. L. No. Quinto Suplemento del Registro Oficial No.459, 26 de Mayo 2021 Normativa:, 1 (2021).

Moya Martínez, A. M. (2009). Las nuevas tecnologías en la educación. Bordón. Revista de Pedagogía, 1–9.

Nájera Montiel, J. (2008). El thelos de la protección de los datos personales ante el derecho al acceso a la información. Ius Humani. Revista de Derecho., 1, 177–199.

NHS. (2020). Introducing the NHS COVID-19 app. Profi Olrhain Diogelu, 1, 1–13. https://covid19.nhs.uk/pdf/features-pack.pdf

Ordóñez Pineda, 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), 83–114. http://repositorio.uasb.edu.ec/handle/10644/5947

Proyecto de Ley Orgánica de Protección de Datos Personales, 1 (2019).

RadarCOVID. (2022). RadarCOVID. RadarCOVID. https://twitter.com/AppRadarCovid/status/1579165618578026496?t=eZP-WphK0QYhBCQNuIP_aA&s=08

Roldán Carrillo, F. N. (2021). Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador. USFQ Law Review, 8(1), 175–202. https://doi.org/10.18272/ulr.v8i1.2184

SENTENCIA N° 001-14-PJO-CC, CASO N° 0067-11-JD, (2014).

Sentencia No. 2064-14-EP/21, (2021).

Todo el contenido de **LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades**, publicados en este sitio está disponibles bajo Licencia Creative Commons (cc) BY.