Crítica y Derecho
Revista Jurídica
e-ISSN 2737-6281 / p-ISSN 2737-629X
https://revistadigital.uce.edu.ec/index.php/criticayderecho/issue/view/297

Derechos humanos y migración en América Latina

Los datos personales en el Ecuador como un derecho humano, una necesidad de mejoramiento en su regulación

Personal data in Ecuador as a human right a need for improvement in its regulation

Janetsy Gutiérrez Proenza
Máster en Derecho Empresarial.
Docente en la Facultad de Jurisprudencia, Ciencias Políticas y Sociales. Universidad Central del Ecuador. Ecuador.
jgutierrezp@uce.edu.ec
ORCID: https://orcid.org/0000-0002-9151-0801

DOI: https://doi.org/10.29166/cyd.v3i5.3950
Recibido: 2022-05-10 / Revisado: 2022-06-01 / Aceptado: 2022-06-12 / Publicado: 2022-07-01

RESUMEN

En el presente ensayo se aborda el tema de los datos personales y su creciente necesidad de regulación en el derecho ecuatoriano, aspectos como su origen, transferencia y su vinculación al ejercicio de otros derechos humanos pero independiente de estos, como un derecho "único" serán analizados sobre el estudio teórico de la opinión de importantes especialistas contemporáneos. Se analizará dogmáticamente la normativa vigente a partir de la reciente Ley Orgánica de Protección de Datos Personales en el Ecuador expedida en el 2021 para determinar aquellas contradicciones y vacíos legales relacionados al significado de los datos personales, su regulación respecto a la personas jurídicas como sujetos de derechos, sus formas de obtención, la comercialización y transferencia, y el sistema de protección fragmentario establecido dentro de la norma que hacen necesario adoptar medidas urgentes que permitan garantizar la protección de datos personales como un derecho humano.

Palabras clave: datos personales, derechos humanos, personas jurídicas, transferencia de datos, administración de datos, regulación.

ABSTRACT

This essay addresses the issue of personal data and its growing need for regulation in Ecuadorian law, aspects such as its origin, transfer and its link to the exercise of other human rights but independent of these, as a "unique" right will be analyzed on the theoretical study of the opinion of important contemporary specialists. The current regulations will be dogmatically analyzed from the recent Organic Law on the Protection of Personal Data in Ecuador issued in 2021 to determine those contradictions and legal gaps related to the meaning of personal data, its regulation regarding legal persons as subjects of rights, their forms of obtaining, marketing and transfer, and the fragmentary protection system established within the norm that make it necessary to adopt urgent measures to guarantee the protection of personal data as a human right.

Keywords: personal data, human rights, legal entities, data transfer, data management, regulation.

INTRODUCCIÓN

La utilización de redes telemáticas ha traído consigo la globalización de múltiples factores de forma interactiva. Dentro de esta globalización el Internet ha jugado un papel preponderante y de máxima expansión. Este fenómeno a escala mundial incide no sólo en aspectos financieros, sino también íntimos y personales en los seres humanos y ha reconfigurado los tradicionales esquemas de los Derechos íntimos y humanos.

Siendo así, las sociedades de la información, comunicación y conocimiento han creado un paradigma de ofertas en servicios y bienes en donde la información constituye un recurso clave. En este modelo existe un elemento fundamental pues las personas incididas e influenciadas por las tecnologías van a lo largo de su vida creando un sendero conformado por datos, en algunos casos aislados y en otros muy interrelacionados, que brindan interpretaciones distintas y significados relevantes constituyéndose en un perfil de su personalidad, en donde el Derecho ha entrado a salvaguardar aquellos elementos que de forma desapercibida, pero ineludible,

ejercen un control social que interfiere en la vida humana. Por ello, las libertades, derechos y garantías que ofrecen las normas pueden llegar a colisionar con el juzgamiento que se crea de la convivencia social. Como menciona (Frosini, 1982) es un contexto en el que nuestras vidas se encuentran sometidas a un "juicio universal permanente" ya que cada individuo que se encuentre en una base de datos se haya expuesto a una vigilancia inadvertida de forma continua. En otras palabras, mientras más desarrollo de las tecnologías de la información y comunicación, de menos privacidad disfruta el hombre.

El derecho de buscar, recolectar y difundir libremente información consagrado en la Declaración de los Derechos Humanos de 1948, ante los adelantos tecnológicos arrasa con el respeto y el ejercicio de algunos de los derechos más elementales relacionados a los datos personales, lo que ha provocado el intento de establecer límites para evitar el perjuicio de estos, ya sea desde la tutela a la seguridad nacional de los pueblos, o la permanencia del orden público o moral. No se puede negar que el uso de las tecnologías y su rápido esparcimiento vinculado a la información que se genera en la actualidad dota a quien la posee o accede a ella de un poder incalculable, ya que conocer el perfil de la vida de las personas y sus datos le permite regular, controlar, vigilar y hasta decidir sobre su comportamiento, lo que consiente proyectar a futuro estrategias que impactan en las esferas económicas, políticas, culturales y sociales.

Los datos personales son todos "aquellos datos, con la suficiente fuerza individualizante, como para poder revelar aspectos de una determinada persona" (García, 2011). Se consideran como datos personales: el nombre y el apellido, la fecha y el lugar de nacimiento, edad, domicilio, teléfono, estado civil, nombres y apellidos de sus progenitores, entre otros. Debido a la importancia de estos, se han convertido en indispensables para la realización de trámites y actos; sin embargo, no tenemos conocimiento sobre su tratamiento. El tratamiento de los datos personales consiste en el "procedimiento técnico, sea o no automatizado, que permite la recogida, conservación, modificación, consulta, o cancelación de estos datos." (Jiménez, 2001) Por esta razón, el Derecho ha considerado pertinente proteger los datos de carácter personal.

En palabras simples: los datos personales es toda la información que nos identifica de manera individual, nos permite que nos identifiquen y, a su vez, nos distingue a unos de otros. El numeral 19 del artículo 66 de la Constitución de la República del Ecuador establece el derecho a la protección de datos de carácter personal, que "incluye el acceso y la decisión sobre la 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" (CRE, 2008). En relación con ello, en Ecuador se publicó en el Registro Oficial Suplemento No. 459 de 26 de mayo de 2021 la Ley Orgánica de Protección de Datos Personales (LOPDP). La que en su artículo 4 define que son datos personales aquellos que identifican o hace identificable a una persona natural directa o indirectamente. Si bien la Ley establece una serie de "tipos de datos" a mi entender comienza a gestarse una cadena de elementos subjetivos en la propia denominación, pues ¿qué se entiende por identificar "indirectamente" a una persona?

Asimismo, se requiere de una necesaria distinción entre Datos Públicos y Datos Privados, los que debieron ser analizados en el cuerpo del texto y que incipientemente se puede interpretar una referencia cuando denomina "Datos sensibles" o "Base de datos de acceso público". Por ello, cuando se habla de protección jurídica de las

personas, en lo que respecta al tratamiento de sus datos personales, se tiene que entender que el objeto de la protección no puede circunscribirse exclusivamente a los datos íntimos, sino a cualquier dato personal, lo que incluye a aquellos de carácter público, pues para amparar a las personas de la posible utilización de sus datos por terceros hay que entender que estos identifican a la persona con ellos y que pueden afectar su entorno social, personal, familiar o profesional dentro de los límites legales del derecho a la intimidad.

Por lo antes expuesto el ejercicio o facultad que tiene toda persona para ejercer el control sobre la información personal que le concierne debe ser ejercido con independencia de que estos datos estén contenidos tanto en registros públicos como privados, a ello se le denomina “protección de datos personales o autodeterminación informativa”

Desde lo expuesto y con la finalidad de desarrollar un trabajo debidamente sustentado, se recurrió a una metodología teórica, basada en un amplio análisis de fuentes de elevado impacto. Así, los procesos metodológicos empleados, tienen base en el enfoque racionalista – deductivista que en su esencia conlleva a la construcción de conocimientos válidos y plausibles. (Castillo, 2021) Es decir, conocimientos creíbles, por sus aportes en la comprensión de la realidad estudiada, como base para la solución de problemas reales.

DESARROLLO

Origen, importancia y protección de los datos personales

Para conocer cuál es la necesidad de gozar de un derecho de protección de los datos personales, por qué es necesario reflexionar sobre su utilización o difusión, y por qué el Derecho se ha visto en la urgente necesidad de regular su tratamiento, debemos comprender sucesos de vital importancia que influyeron por su impacto y presionaron a las gestiones internas de cada estado para acelerarse en crear una regulación que proteja los datos personales de sus ciudadanos.

Históricamente los datos personales se han protegido desde 1890 en Estados Unidos pero su materialización se dio en el año de 1974 con la ley federal “Privacy Act” “Ley de Privacidad” que se encargaba se regular el manejo de datos personales por parte de las entidades públicas. Sin embargo, fue Europa la que demostró un notable avance legislativo a partir de 1960 respecto a la regulación que debía mantenerse en el flujo de información entre los estados parte. Es así como en 1976 se aprobó en Alemania la Ley Federal de Protección de Datos, y en 1983 con el pronunciamiento del Tribunal Constitucional Federal Alemán se creó el derecho a la protección de datos el cuál en virtud del libre desarrollo de la personalidad y dignidad humana denominó “Derecho a la autodeterminación sobre la información personal”. Durante 1977 y 1979 le siguieron estados como Dinamarca, Austria y Luxemburgo los que adoptaron leyes nacionales de protección de datos de carácter personal, en su mayoría teniendo como referencia la legislación sueca de 1973 e instituyendo autoridades independientes para la regulación y control de los datos de carácter personal. (Escobar, 2003)

La aprobación de dos textos esenciales para la compresión del contenido del derecho fundamental a la protección de datos de carácter personal, como son la Recomendación de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre circulación de internacional de datos personales para la protección de la intimidad en septiembre de 1980 (constituye el primer documento de ámbito

supranacional que analiza en profundidad el derecho a la protección de datos de carácter personal) y el Convenio 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de sus datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, dieron lugar a la iniciación de un nuevo y prolongado período en el que un gran número de países adaptaron su legislación a los principios consagrados en ambos instrumentos. Por otra parte, el 14 de enero de 1990 se aprobó la Resolución 45/95 de la Asamblea General de Naciones Unidas, relativa a los principios rectores para la reglamentación de los ficheros computarizados de datos personales. Al propio tiempo, en el ámbito de la Unión Europea, durante este periodo se gestó la adopción del texto de mayor relevancia en el marco de la protección de datos, se trata de la Directiva 95/46/CE, la que ha incidido normativa y exponencialmente rebasando los límites de la Unión Europea como referente internacional. (Gamarra, 2010)

Otro hecho importante que marca una manifestación por parte de la Comisión Europea en el 2003 sobre elementos vinculados al intercambio y transferencia internacional de los datos personales entre los estados, son los sucesos acontecidos en los Estados Unidos de América el 11 de septiembre de 2001, pues a partir de estos últimos la administración norteamericana exigió la transferencia de datos personales llamados “Passanger Name Record” (PNR) a las compañías aéreas, bajo regímenes de fuertes sanciones económicas impuestas por la legislación norteamericana de no cumplirse.

En épocas contemporáneas también se debe considerar como un hecho relevante que marca la preocupación de proteger los datos personales, la sanción que la Comisión Federal de Comercio de Estados Unidos impuso a Facebook en 2018 por violentar la privacidad de 50 millones de usuarios en el caso de Cambridge Analytica imponiéndole una multa de 5.000 millones por las malas prácticas en el manejo de la seguridad de los datos de los usuarios. En este caso se acusaba a la red de Facebook de haber violado las reglas de privacidad de sus usuarios, al compartir de forma inapropiada los datos de estos, los que serían analizados para observar las tendencias de votos en la campaña presidencial de Donald Trump, creando perfiles e incidiendo en sus comportamientos. Este hecho fue muy mediatizado y sentó un precedente sobre el peligro que conlleva la incorrecta utilización de los datos personales, exigiéndose mayores regulaciones en las redes sociales.

Es así que el uso de los datos personales, su análisis y almacenamiento se han convertido en una herramienta trascendental y útil en el mundo de los negocios, vinculado esto a procesos como el -Data Warehouse y el Data Mining- herramientas informáticas para el manejo de datos especialmente en el ámbito corporativo en los que se almacena y se analiza la información recopilada-, que permiten a las empresas satisfacer sus requerimientos de información para mejorar su gestión y ser más competitivos, por medio de la focalización del marketing utilizando los datos recabados. (Chen, 2010)

La información proveniente de los datos personales desde el Derecho se ha posesionado como un bien jurídico de trascendental importancia que para muchos supera otros bienes tradicionalmente ambicionados, consecuentemente la obtención de las bases que lo almacenan se ha convertido en una actividad cotizada y altamente lucrativa, pues su utilización rebasa los límites de aspectos políticos, económicos o sociales. Implica la manipulación en la toma de decisiones y el manejo de grupos con un alcance global que se materializa a través de entornos informáticos.

Los casos y usos descritos anteriormente no fueron suficientes para que, dentro de la legislación ecuatoriana, se pensara en proteger los datos personales de sus ciudadanos. El suceso que demostró la necesidad de su normalización dentro del derecho ecuatoriano fue la fuga de información de 20 millones de ecuatorianos incluidas personas fallecidas y 6.7 millones de menores de edad (Silva, 2019). Esta información se dio a conocer por una publicación en la red social Twitter, por parte de dos expertos que colaboraron con la compañía de seguridad informática israelí vpnMentor el 24 de septiembre de 2019. Este hecho obligó al poder legislativo a crear una normativa que protegiera los datos personales de los ecuatorianos, y es así cómo -después de dos años- se aprobó el 11 de mayo de 2021 la Ley Orgánica de Protección de Datos Personales (LOPDP), para poder regular el flujo de datos digitalizados.

Los datos personales como un nuevo derecho humano. Los derechos de privacidad, intimidad, imagen y dignidad humana como derechos independientes pero relacionados

Es evidente que todo lo que se crea está sujeto al Derecho. Por ello, es necesario gozar del derecho de protección de nuestros datos personales sin tener en cuenta el formato en que se encuentren, sean escritos o mediante su archivo en la red (digitalizados). Los datos personales han alcanzado tal relevancia que se han postulado como un bien jurídico que goza de protección jurisdiccional e institucional mediante garantías de acceso y control a las informaciones procesadas en los diferentes sistemas o bases de datos, creándose una nueva figura jurídica de relevancia de estos derechos fundamentales como es el Habeas Data. Cuando se habla de datos personales se hace referencia tanto a los derechos de privacidad, intimidad, imagen, honor; como al conjunto de valores implicados en los mismos. Sin embargo, es necesario establecer la autonomía que a mi criterio existe de estos derechos.

Los primeros antecedentes regulatorios si de privacidad se trata datan de 1890 en los Estados Unidos cuando se destapa el escándalo del caso Watergate y cuando con posterioridad los famosos abogados Samuel D. Warren y Louis D. Brandéis escriben un artículo titulado “The right to Privacy” (el derecho a la privacidad) relacionado a las múltiples injerencias de la prensa de aquel entonces en la vida privada. Este clásico de la literatura jurídica denominado así por grandes teóricos será el documento que sienta las bases de la privacidad dentro del campo de los derechos fundamentales, relacionándola a aquella facultad del individuo de proteger cualquier intrusión en su vida privada. Es así como la Real Academia Española la define en los siguientes términos “Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión” (RAE,2021). Si para aquellos tiempos con el desarrollo de nuevos pero incipientes medios tecnológicos comparado con los actuales ya se deslumbraba una injerencia de los medios en la vida privada de las personas que hacía surgir este nuevo derecho de privacidad, en la actualidad para muchos el mismo ha perdido su esencia, pues nadie escapa de aparecer en la ¨red¨ -internet- como parte del sistema.

La intimidad por su parte es mucho más reducida y se refiere a una esfera más singular y reservada de la vida de las personas. De tal forma que la privacidad engloba a la intimidad, pero la diferencia de aquella, considerándola como aquella “zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia.” (RAE, 202)

Dentro del lenguaje jurídico ha sido muy difícil diferenciar estos términos y en muchas legislaciones se utilizan los mismos indistintamente, alcanzando iguales significados. Sin embargo, una gran parte del mundo doctrinario ha determinado las diferencias entre uno y otro; para Emilio del Peso Navarro se diferencian estos conceptos en que: Si quisiéramos representar la intimidad y la privacidad respecto al individuo las representaríamos como círculos concéntricos de lo que el más próximo al individuo comprendería la intimidad, con los datos más próximo mejor guardado por la persona y el círculo exteriores comprendería la privacidad compuesta por aquellos datos que perteneciendo a una persona ésta no puede evitar que otro los conozca, por ejemplo, titulación académica, cuenta corriente, teléfono, etc. (Navarro, 2000)

Por tanto, la privacidad dentro de los datos personales se refiere precisamente a la reserva que tienen toda persona sobre la utilización y tratamiento de sus datos, que le permita hacer un control de aquellos por su persona, obligatoriamente para protegerse de injerencias en su vida privada. Esto marca una diferencia desde el sistema de protección en el derecho, pues las herramientas jurídicas a utilizarse en uno y otro caso son diferentes; a la privacidad de sus datos se responde con medidas de carácter precautorio para evitar la lesión de este ante su mal utilización, se intenta evitar que aspectos individuales se den a conocer para perfilar al individuo invadiendo su espacio personal “to be let alone” “para ser dejado en paz”, lo que no restringe el hecho que ante una violación exista medidas sancionatorias. Por su parte la intimidad se caracteriza principalmente por un sistema indemnizatorio y con elementos mucho más rígidos de represión.

En otras palabras, los datos personales y su tratamiento pueden, pero no necesariamente afectan los derechos a la intimidad pues estos no obligatoriamente entran en el campo de informaciones íntimas o secretas. Además, hay que considerar un aspecto interesante que introduce Lucas Murillo de la Cueva cuando menciona que el bien jurídico que tutelan los sistemas de protección de datos no es la intimidad “física” entendida en sentido estricto, sino la privacidad informativa. Según este autor no caben dudas razonables que impidan hablar de la existencia de este nuevo derecho el cual se diferencia del derecho a la intimidad.

Vislumbramos mayor claridad en un fallo trascendental para la materia que estamos tratando; la sentencia 292/2000 de 30 de noviembre del Tribunal Constitucional Español en el que realiza una clara y marcada diferenciación entre los conceptos de intimidad y protección de datos personales argumentando que:

> La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran…la función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. (STC 929, 2000)

Respecto a la imagen este derecho se refiere a que el individuo al igual que en otros derechos humanos, goza de las garantías a decidir libremente respecto de su imagen, de tal forma que pueda contar con medidas para decidir la divulgación o no de su imagen. El derecho a la propia imagen debe identificarse con los derechos de

libertad, de manera que al individuo le sea garantizado el derecho a decidir libremente respecto a su retrato, aun cuando estas no afecten ningún otro derecho. Algo realmente preocupante, en este caso, es que existe una serie de bases de datos que cuentan con imágenes de sujetos en lo que no se ha emitido su consentimiento, sumamente alarmante cuando su imagen es utilizada de forma inadecuada.

En este sentido la LOPDP, se restringe a aquellos soportes sean materiales o no que se encuentran administrados, ejecutados y operandos en el territorio nacional o a partir de formas contractuales a las que se sometan a la competencia nacional. Es así como, a pesar de existir una serie de documentos de carácter internacional, estos constituyen principios y estándares que no ofrecen acuerdos vinculantes para ser sometidos a la fiscalización de organismos internacionales como estados parte suscriptores de estos, lo que en ocasiones trae consigo la vulneración sin garantías de protección a la imagen de la persona. Corredores de búsquedas en Internet, por ejemplo, en los que el sujeto no puede eliminar determinados datos o imágenes, en otras palabras, lo que se conoce como “derecho al olvido digital” y que sería interesante tratar en otra ocasión. Siguiendo con este análisis la imagen de cada persona representa la reproducción de su aspecto físico, pero también podríamos de hablar de otros tipos de imágenes vinculadas a posiciones ideológicas, políticas o sociales, en las que se exponen al exterior las cualidades propias del individuo y los aspectos integrantes de su personalidad. Por ello, la imagen también guarda una relación directa con los datos personales y debe ser tutelada mediante medios legales.

Muy relacionado a la imagen se encuentra al honor, como se había mencionado anteriormente las imágenes en ocasiones son utilizadas de forma violenta o grotesca y por tanto afecta al honor, visto este último como un valor íntimo del ser humano, que forma parte de su personalidad y en el que influye el criterio que tenga la sociedad o terceros frente a la persona, que le ofrece un “buen” nombre en el desarrollo de su dignidad.

Desde el punto de vista jurídico, el derecho al honor constituye el derecho que cada ser humano tiene al reconocimiento de respeto, ante él mismo y ante las demás personas, de su dignidad humana y de los méritos y cualidades que ha ido adquiriendo como fruto de su desarrollo personal (Marecos, 2010). No obstante, aunque puede verse afectado el honor ante una incorrecta utilización de datos personales, es importante acortar que la diferencia no sólo radica en la esencia propia del honor que representa la dignidad humana desde una dimensión social, sino que en el Derecho lo que se protege en este caso son las divulgaciones inexactas, calumniosas o injuriosas de información relativa a su persona o núcleo familiar, mientras que la protección de datos se protege la identificación de cualquier dato personal ya sea porque afecte su honor o no. Sin embargo, no se puede dejar de mencionar que ambos derechos son elementos de uno de los bienes inmateriales que más aprecia el ser humano: el respeto a su dignidad personal. Por ello, la protección de sus datos personales es también una herramienta con la que se puede defender el honor de las personas.

En conclusión, en el derecho a la protección de datos personales es posible afirmar que se identifica con otros derechos de humanos y que se encuentra muy afín con el derecho a la intimidad, privacidad, imagen y honor, pero en la actualidad ha adquirido autonomía y es considerado un derecho fundamental e independiente por la mayoría de los tratadistas y en las interpretaciones de las legislaciones a nivel internacional de avanzada en estos temas.

El ostentar con una regulación interna, que se cerciore de que los datos personales de cada individuo no se encuentren a disposición de terceros sin el consentimiento de sus titulares, es lo que lleva a analizar cuál es la problemática que existe en torno a la transmisión de datos personales y cuál es la solución que el Estado Ecuatoriano ofrece en caso de que esta se destine a fines distintos a los convenidos por el titular.

Las personas jurídicas excluidas de la protección de datos

Un aspecto interesante en la LOPDP es que su ámbito de aplicación se reduce a las personas naturales, lógicamente ello puede responder a la necesaria vinculación de los derechos antes mencionados y que sería difícil establecer la privacidad, la intimidad o la personalidad a la figura de las personas jurídicas, por tanto, cuando la ley se refiere a la protección de libertades y derechos fundamentales de las personas físicas, su protección no ampara a las personas jurídicas. Respecto a ello existen debates muy interesantes sobre el reconocimiento de los derechos de protección de datos en las personas jurídicas.

Según Davara, no se puede admitir la tesis de la persona jurídica por cuanto estas pertenecen al ámbito de las sociedades, vinculadas más hacia el derecho de Propiedad Intelectual e Industrial y el Derecho de Competencias, por lo que no se pueden asociar derechos de intimidad a las personas jurídicas. En su tesis refiere que los bienes que se protegen y los intereses que se encuentran en juego responden a el mundo empresarial y de negociaciones, de tal forma que ante una vulneración existen vías legales en los que se pueden ejercer los mismos, como por ejemplo ante datos vinculados a secretos empresariales, la norma correcta sería el derecho de propiedad industrial o en su caso esgrimir la existencia de una competencia desleal.

Sin embargo, existen otros autores como Lucas Murillo de la Cueva que sostienen que al permitirse el reconocimiento de las personas jurídicas como sujetos de un derecho de protección de datos personales se puede ejercer una mayor defensa del propio objeto social de los datos que dentro de un sistema informático se realizan sobre ellos. Ello no sólo protege a la propia persona jurídica y los elementos que le rodean, sino también a los sujetos o socios que lo conforman a través de sus órganos, dotándolos de una mayor eficacia en el ejercicio de sus derechos. Se debe considerar además que en este caso existe un peligro real de aquellos elementos expuestos en la norma como conductas prohibitivas que pueden llegar a afectar a las personas jurídicas y al no establecerse una tutela a los mismos, ni estar amparadas en la norma, se hace tortuoso la defensa de estos.

A mi entender debiera establecerse a las personas jurídicas como sujetos de estos derechos considerando su reconocimiento en la propia existencia de los derechos que ellas ejercen de forma autónoma. Si se analizan por ejemplo derechos que si pudiesen verse vulnerados en este caso podríamos recurrir al honor o a la imagen de estas en las que no necesariamente estemos ante un derecho industrial o de competencias desleales. Lo cierto es que si se hace una interpretación de lo establecidos en el artículo 66.19 de la Constitución de la República “Se reconoce y garantizará a las personas” se podría afirmar que cualquier persona puede exigir la tutela de tales derechos, sin la existencia de límites a las personas jurídicas. Por tanto, las personas físicas como jurídicas pueden tener interés en ejercitar el derecho de acceso, de rectificación o de cancelación de datos inexactos, falsos o desfasados, y si las personas de existencia ideal por ejemplo tienen la potestad de ejercer sus derechos ante daños civiles por la no rectificación o réplica ante un tipo de información u opinión que se produzca, reciba, difunda e intercambie a través de los medios de

comunicación social que vaya en detrimento de su reputación negocial, también deberían tener la facultad para reclamar el acceso, rectificación o cancelación de sus datos de carácter personal. (Véase Art. 21 de la Ley Orgánica de Comunicación, Registro Oficial Suplemento 22 de 25-jun.-2013, última reforma en 2019)

La autora Hernando Collazo manifiesta que las personas jurídicas pueden tener un interés real en la rectificación de sus datos que figuren en soportes electrónicos y establece un caso bien interesante de aquellas compañías que desean poder ejercer un derecho o acceso a un crédito, sin embargo, le son rechazados por encontrarse datos inexactos en el sistema crediticio financiero, lo que les impide acceder a estos por los bancos, en especial si se trata de pequeñas y medianas empresas.

También es atrayente los debates que surgen respecto a la exclusión de las personas fallecidas en el ejercicio de este derecho de acuerdo con la LOPDP. En este sentido, habría que analizar los derechos que se protegen en los datos personales, pues si bien estos están íntimamente ligados a los derechos de intimidad, privacidad, imagen y honor, ello representa que el fallecimiento de una persona, no significa que no puedan verse afectados estos derechos que subsisten con posterioridad a su muerte, lo que no impediría que puedan ejecutarse acciones correspondientes por los familiares, designados del difunto o cualquier otra que ostente legítimo interés en defensa de estos derechos. Ahora bien, en el caso de nuestra norma el artículo 27, dispone el ejercicio de acceso, rectificación, actualización o eliminación de datos de personas fallecidas, sólo ante el caso de aquellos sujetos que sean titulares de derechos sucesorios del causante, lo que reduce el ámbito de personas que puedan tener un interés legítimo, pero que, sin embargo, no presenten derechos derivados del causante.

Formas de obtención de datos personales. La comercialización y transferencia de datos personales según la LOPDP en el Ecuador

Son variadas las formas mediante las cuales se puede obtener datos personales de terceras personas, existiendo para tal efecto mecanismos lícitos y otros al margen de la norma, es así que, en una sociedad globalizada donde las relaciones comerciales, personales, laborales, educativas, financieras e incluso gubernamentales se han volcado a lo electrónico, cada vez que interactuamos con personas o instituciones privadas o públicas, es posible que estemos trasladando nuestros datos personales, al utilizar sitios web con aplicaciones de registro y cookies, cuando llenamos un formulario para acceder a un servicio, o cuando damos permiso para que una red social comparta algunos de nuestros datos al registrarnos. Básicamente, cada vez que pulsamos en un “acepto las condiciones” estamos dando permiso para que se cedan o usen nuestros datos sin que seamos muy conscientes de ello. (Comisión Europea, 2019)

Otro método de obtención de datos personales, que se encuentra regulado por la recientemente emitida Ley Orgánica de Protección de Datos Personales, es la originada desde los contratos de adhesión, cuando una persona acepta las cláusulas de este, las cuales establecen la forma en cómo se manejarán sus datos, cómo estos serán transferidos a terceros y los fines de tal transacción. Sin embargo, ya se mencionó en líneas anteriores, existen también mecanismos ilegales para la obtención de datos personales, entre los que se encuentran principalmente la vulneración de los sistemas de seguridad de las bases de datos de instituciones públicas o privadas, así como la estafa en redes sociales de mensajería instantánea, mediante llamadas fraudulentas o enlaces de dudosa procedencia, para que a partir

de la ingeniería social los delincuentes accedan a esta información valiosa. (Sandoval, 2017)

Por lo rentable que resulta esta actividad, en efecto, existen compañías dedicadas a la recopilación de datos de la vida real y virtual de las personas, para ser vendidas posteriormente. Las datas broker recopilan datos y a través del Big Data (o ciencia de datos) analizan las tendencias de los usuarios en áreas que van desde los intereses políticos, la economía, a qué se dedica en tiempo de ocio, hasta tendencias religiosas o sexuales, por poner algunos ejemplos. Estas empresas utilizan algoritmos cada vez más eficaces para generar un conocimiento en torno a los usuarios que cada vez tiene más valor. (Meneses, 2018)

En este punto, cabe cuestionarnos si la venta de datos personales es ilegal o no. La ley que regula esta actividad en el Ecuador, establece en efecto la posibilidad que una empresa o institución transfiera los datos personales de una persona a un tercero, siempre que este tercero realice actividades o ayude a cumplir propósitos de la relación entre el titular y la responsable de los datos en base a un presupuesto: El consentimiento informado del titular, el cual se entiende, de acuerdo al último inciso del artículo 33 ibídem como la entrega de la información suficiente al titular que le permita conocer la finalidad en la que sus datos se van a utilizar, empero no establece de manera clara la exigencia de un consentimiento expreso, a diferencia de la legislación española que si solicita tal condición.

Este particular de no pedir el consentimiento se agrava y puede ser interpretado incorrectamente en la norma, un ejemplo es cuando los bancos, sin el consentimiento de sus clientes transfieren las bases de datos a las llamadas empresas cobradoras o gestoras de cobros, las que hacen uso de todos los datos e información proporcionada por este último, sin que medie consentimiento de su titular. No es de extrañar que se ha dado los casos en que llamen a teléfonos proporcionados como ¨referencias iniciales del negocio¨ (compañeros de trabajo, jefes o superiores, por citar un patrón), con el propósito de localizar al cliente, no sólo causando un malestar al usuario que desconoce de la deuda o cobro hacia la persona inicial sin que sea garante de la misma o que se encuentre ajeno a estos hechos, sino que en su gestión dejan escapar información que sólo corresponde al deudor o cliente bancario ocasionando un desmérito frente a personas que pueden pero no necesariamente tener un grado de confianza. Por su parte resulta más alarmante cuando los datos provienen de una fuente pública, como por ejemplo redes sociales, donde la transferencia de datos a terceros puede realizarse sin autorización previa. (LOPDP, 2021)

Otro aspecto para resaltar es que la Ley Orgánica de Datos Personales, no utiliza el término “venta” o “comercialización” de datos personales, sino que utiliza el término “transferencia” la cual puede realizarse en los términos descritos en el párrafo anterior. En ese sentido se entendería que la venta de datos no es ilegal, sino que la ilegalidad recaería en la forma en la que se obtienen los mismos para su posterior puesta en el mercado, y si estas se hacen sin el consentimiento informado del titular en los casos que así se requiera.

Ahora bien, con lo antes mencionado, se recalca la interpretación arbitraria a la manera en cómo puede comprobarse que la información personal, que es transferida desde el responsable de datos a un encargado de datos se hace en razón de los fines que yo acepté previamente, en tal cuestión es positivo el reconocimiento del derecho de oposición establecido en el artículo 16, sin embargo, el control se ve ampliamente limitado cuando los datos, obtenidos principalmente de manera ilegal, o en sitios públicos, donde la autorización del titular no es necesaria, y por ende el derecho de

información no tendría eficacia, llegan a parar a sitios donde serán utilizados para actividades ilícitas. Mediante el manejo de datos personales, puede no sólo realizarse actuaciones de mercadotecnia directa, sino que se convierte en la materia prima para ataques de ingeniería social, como el pishing, baiting o vishing afectando seriamente el patrimonio de quienes son víctimas de estos delitos.

Es así como la protección de los datos personales resulta fundamental, por el uso inadecuado que pueda suscitarse evitando con ello se afecten otros derechos y libertades. En este sentido, la protección de los datos personales tiene varias aristas: En primer lugar, el normativo, el cual debe crear normas específicas para controlar la privacidad de personas naturales y jurídicas; como siguiente aspecto es la responsabilidad que deben tener en cuanto a la seguridad de los datos, quienes fungen de responsables o encargados de los mismos, aspecto que se encuentra regulado en el capítulo sexto de la ley rectora de la materia, sin embargo es importante determinar para cada caso la reparación pertinente más allá de las sanciones administrativas establecidas en la ley.

Sistema estatal de Protección de datos personales en el Ecuador

En la línea de lo que se ha mencionado hasta el momento, hay varias infracciones en materia penal que se pudieran cometer, sin embargo, recordemos que en derecho las ciencias penales son consideradas de ultima ratio, esto quiere decir que se deben agotar todas las vías jurídicas previas a la lesión, daño o puesta en peligro de un bien jurídico protegido como son los datos personales. Para ello es necesario que exista un sistema estatal encargado del control, supervisión y prevención de este tema en específico. En ese sentido y en concordancia con la LOPDP, misma que ha sido tratada a lo largo del presente trabajo, es obligatorio analizar ciertos organismos estatales que son los encargados del cuidado y protección de datos personales.

La ley en cuestión, en su artículo 77 plantea la creación de una Autoridad de Protección de Datos, la autoridad se personifica en la Superintendencia de Protección de Datos, no obstante, se plantea su creación para dentro de dos años posteriores a la ley, por tanto, se vuelve casi que obsoleta en los mecanismos de protección y en los procedimientos o infracciones establecidos para su control y seguimiento. Asimismo, obliga en su artículo 48 la creación de la figura del “Delegado de protección de datos personales” al que asigna una serie de funciones, vinculadas precisamente a la protección en su artículo 49 y 50, empero, no especifica cuál es la responsabilidad jurídica más allá de las sanciones administrativas ante la vulneración de los derechos consagrados, ya sea por culpa leve o grave, o por dolo, lo que hace suponer que ante la vulneración de los derechos la única vía indemnizatoria correspondería al derecho civil, volviendo extremadamente tortuoso los caminos legales para definir los perjuicios causados.

Por su parte el artículo 54 establece determinadas responsabilidades a las “Entidades de Certificación”, sin embargo, no consta en la ley a razón de la Autoridad de Protección, quiénes y qué requisitos y responsabilidades, así como alcance que las mismas tienen. En otras palabras, ello constituye a mi entender un vacío legal de incalculables consecuencias, pues ¿hasta dónde llega la responsabilidad de quien solicita los servicios de una entidad de certificación y de esta respecto a una eventualidad o daño ocurrido? Hagamos en este caso una analogía a lo que establece la Ley de Comercio electrónico y firmas electrónica, cuando instituye las también denominadas “Entidades de Certificación”, en este caso se le atribuye una alta consecuencia al uso de la firma electrónica como manifestación de voluntad, y por

tanto se delimita las responsabilidades e incluso de daños acontecidos por el incumplimiento de sus responsabilidades a las mismas, que obliga que ellas sean aprobadas en su creación por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) bajo estrictos requisitos establecidos en la ley, debiendo de contar con capitales económicos mínimos que aseguren las respuestas ante eventos dañosos o incluso en el uso de tecnología eficientes y de avanzada que garanticen y eviten las vulneraciones a sus funciones con el uso de la firma electrónica. En el supuesto de la LOPDP ello queda en total vacío pues, aunque se menciona en el artículo 52 lo que pueden hacer, los aspectos antes mencionados no se encuentran regulados, por tanto, se podría pensar que queda al arbitrio de intereses que quedarán plasmados en un posible Reglamento a la Ley.

En el ámbito administrativo, la ley en sus artículos 71 y 72, ha propuesto diversas sanciones para las entidades que, siendo responsables de la protección de datos, hagan caso omiso a aquello. Lo cuestionable, es que si bien existe sanciones en caso de que existan infracciones leves o graves, las mismas son muy escuetas y se refieren a multas de carácter económico, pudiendo aplicar otras penalidades como intervención a la entidad responsable, cierre o suspensión de esta, acciones que de alguna forma ayudarían a presionar a la entidad entorno a su compromiso moral y legal de protección de información personal.

CONCLUSIÓN

Los datos personales son toda aquella información respeto de un individuo, de la cual este es el titular y único facultado para poder consentir su utilización y transmisión, en función de los fines para los cuales este ha dado consentimiento, por ello la Ley Orgánica de Protección de Datos personales expedida en el año 2021 en el Ecuador debe garantizar la tutela efectiva de estos derechos mediante mecanismos coherentes y eficaces. Consecuentemente la protección de datos e información personal es un derecho fundamental de las personas que aunque se encuentra estrechamente ligado a los derechos a la intimidad, privacidad, imagen y honor entre otros, se independiza de ellos no sólo por el bien jurídico que protege, sino por las herramientas jurídicas que garantizan su efectiva aplicabilidad de acuerdo a lo dispuesto en el artículo 66 numeral 19 de la Constitución de la República y que debe ser garantizado por el Estado, siendo necesario comenzar por una revisión pormenorizada de la norma para que su aplicación no resulte en una incapacidad práctica.

REFERENCIAS BIBLIOGRÁFICAS

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

BBC News Mundo. (2019, septiembre 6) Filtración de datos en Ecuador: la “grave falla informática” que expuso la información personal de casi toda la población del país sudamericano. https://n9.cl/2bpcl

Comisión Europea (2019). Los datos personales, manejados por tercera. Página institucional. Apartado Derechos de los ciudadanos. https://n9.cl/ap7f5

Chen Mok, Susan. (2010). Privacidad y protección de datos: un análisis de legislación comparada. [Diálogos Revista Electrónica de Historia], 14(2), 111-152.

Castillo-Bustos, M. R. (2021). Técnicas e instrumentos para recoger datos del hecho social educativo. Retos de la Ciencia. 5(10), pp. 50-61. https://doi.org/10.53877/rc.5.10.20210101.05

Del Peso Navarro, Emilio (2000) “La protección de Datos y la Privacidad en Internet”, Informáticos Europeos Expertos.

Frosini, V (1982) Cibernética, derecho y sociedad. Madrid. Editorial Tecnos.

Puente Escobar, A (2006). Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal.” Tirant lo Blanch. Valencia, p. 40

Herrán, A. (2003) El derecho a la protección de datos personales en la sociedad de la información. [Universidad de Deusto]. Bilbao.14(2) https://n9.cl/0qpw1

Hernando, C. (1986) La Comunidad Económica Europea y la informática. Jornadas Internacionales sobre Informática y Administración Pública. Instituto Vasco de Administración Pública. Volumen 3. VVAA. Bilbao p.90

Ley Orgánica de Protección de Datos Personales Registro Oficial Suplemento No. 459 de 26 de mayo de 2021.

Davara Rodríguez, M.A. (1998) La protección de datos en Europa. Principios, derechos y procedimiento, ASNEF-EQUIFAX, Madrid. p. 94-95.

De La Cueva, L. M, (1990) El derecho a la autodeterminación informativa. Madrid. Tecnos. p 123, 182

Marecos Gamarra, Adriana R (2010). La protección de datos personales como núcleo del derecho fundamental a la autodeterminación informativa. Una mirada desde el derecho español y europeo. Paraguay.

Meneses Rocha, María E. (2018). Big data, grandes desafíos para las ciencias sociales. [Revista mexicana de sociología] 14(2), 415-444.

Orlando José y Cirio Claudio, El ABC de los datos personales, (México: Conferencia Mexicana para el acceso a la Información Pública). https://n9.cl/81n31

Ortiz E. (2021, junio 21). ¿Cuáles son las deudas de Ecuador en ciberseguridad? Revista Vistazo. Portal web,

Puente Escobar, (2006) Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal. 2ª Edición Protección de datos de carácter personal en Iberoamérica. Tirant lo Blanch. Valencia. p. 40.

Toussaint, Florence, (1975) Crítica de la información en masa, Ed. Trillas, México, p. 43.

Silvia, María. (2019, septiembre 24) “Los datos personales de millones de ecuatorianos están en manos de terceros y a la venta, dicen investigadores internacionales”, El Comercio, sección Negocios. https://n9.cl/130dr

Sandoval E. (2017). Ingeniería Social, corrompiendo la mente humana. Universidad Nacional Autónoma de México, web institucional. Revista Seguridad. 1 251 478, 1 251 477

Meneses Rocha, M.E. (2018). Big data, grandes desafíos para las ciencias sociales. [Revista mexicana de sociología], 14(2), 415-444.

S. Warren y L. Brandeis (1995), The Right to Privacy. Civitas. p. 22

Tribunal Constitucional de España, STC 292/2000, de 30 de noviembre, fundamento jurídico 5, Recurso de inconstitucionalidad Nº 1463-2000. https://n9.cl/xh30i