PROTECCION DE DATOS COMO DERECHO FUNDAMENTAL EN LA SOCIEDAD GLOBAL: UNA MIRADA DESDE LOS DESAFÍOS CONTEMPORÁNEOS DE LA POSPANDEMIA

DATA PROTECTION AS A FUNDAMENTAL RIGHT IN THE GLOBAL SOCIETY: A LOOK FROM THE CONTEMPORARY CHALLENGES OF THE POST- PANDEMIC

Lissa María Pineda Castaño

Magister en Derecho Internacional, Universidad de los Andes. Docente Tiempo Completo, Institución Universitaria de Envigado. Correo electrónico: lmpineda@correo.iue.edu.co. Correo electrónico: lmpineda@correo.iue.edu.co. Orcid: 0000-0003-0113-1195.

Sergio Luis Mondragón Duarte

Magíster en Derecho Público, Universidad Santo Tomás. Coordinador de la Especialización en Derecho Disciplinario, Institución Universitaria de Envigado. Correo electrónico: slmondragon@correo.iue.edu.co. Orcid: 0000-0002-5189-6770.

Víctor Julián Moreno Mosquera

Doctor en Derecho, Universidad de Medellín. Docente Tiempo Completo, Institución Universitaria de Envigado. Correo electrónico: vjmoreno@correo.iue.edu.co Orcid: 0000-0002-4645-3553.

Proyecto de investigación: La presente investigación deriva del proyecto "JobSecuritySoft-JSS, un software para la gestión estratégica de la Seguridad y la Salud en el Trabajo, en las MIPYMES" aprobado por la Institución Universitaria de Envigado en el año 2021.

Objetivo de la Investigación: Mostrar el derecho a la protección de datos personales, en un marco jurídico independiente, como derecho fundamental dentro de los Estados Democráticos, a partir de los desafíos que demanda e impone la pospandemia por la Covid-19.

Introducción

Las organizaciones públicas y privadas en la actualidad reconocen la importancia del adecuado tratamiento de datos de las personas, empresas y Estados. En ese sentido, la información está reconocida como un bien intangible amparado constitucionalmente, donde la confidencialidad de los datos de las instituciones, como los secretos industriales, empresariales y la información reservada de los organismos públicos, es de especial relevancia para garantizar derechos fundamentales entre los que se destacan la seguridad nacional, la libertad de expresión, la libre competencia, entre otros. Por lo que debe haber máximos estándares jurídicos nacionales e internacionales para proteger la información confidencial de personas tanto naturales como jurídicas.

La independencia en el estudio de la protección de datos personales, considerándolo un derecho autónomo de otros derechos, implica entender este derecho mas allá del derecho a la libertad de expresión, según el articulo 13 de la Convención Americana de Derechos Humanos, pues "la separación entre el derecho a la privacidad y la protección de datos personales es un reconocimiento a un hecho social innegable como lo es la necesidad y practica frecuente de recolectar, cruzar, almacenar y poner a circular diariamente datos personales" (Cifuentes, 2013,p.280).

El derecho nacional e internacional al considerar la protección al tratamiento de datos personales, como un derecho autónomo, comprende por una parte la evolución del derecho por medio del análisis jurídico del derecho fundamental de toda persona jurídica y natural al debido tratamiento de los datos personales de clientes, empleados, proveedores y terceros; y por otro lado, el auge del tratamiento de información a través del derecho publico, reconociendo la relevancia del debido tratamiento de datos de las entidades estatales para garantizar y proteger la estabilidad de los Estados y la paz mundial. El estudio de ambos pilares se realizará en la presente investigación, conforme a la normativa de organismos externos e internos que han considerado los desafíos actuales en la normatividad del tratamiento de datos personales impuestos por la pandemia de la Covid 19.

Fundamentación teórica

En el derecho nacional colombiano, el contenido jurídico del derecho al tratamiento de datos personales se desarrolló a partir del correcto tratamiento de datos personales en el derecho privado. Sin embargo, deja de ser un asunto estrictamente privado, pues se requiere del derecho publico, de acuerdo a las tensiones que surgen por las nuevas tecnologías de la información. El contenido jurídico avanza, pero los desafíos cada vez son mas fuertes por la colisión con otros derechos fundamentales. De esta forma, el debate continúa presente en las cortes internacionales y nacionales por la jerarquía de derechos, cuando se quiera limitar el derecho fundamental a la protección de datos personales por excepciones claramente establecidas en la ley.

Los limites en la confidencialidad del tratamiento de datos personales a partir de las excepciones para su divulgación se analizará de acuerdo "al tratamiento (recolección, almacenamiento, circulación, etc.) de información personal que pueda vulnerar derechos fundamentales de las personas. El articulo 15 de la Constitución Política de 1991 (Const., 1991) consagró derechos en cabeza de ellas e impuso obligaciones a los administradores de datos personales, como los son los empresarios respecto de los datos de sus clientes, sus trabajadores, sus proveedores y terceros" (Cifuentes, 2013, p.273). Además, los Estados como autoridades competentes para recolectar, almacenar y publicar información, deberán garantizar la responsabilidad en su tratamiento, a partir de la jurisprudencia internacional para su adecuada aplicación.

Metodología

La presente investigación aborda un contenido de carácter descriptivo-explicativo con enfoque cualitativo que a partir de un método inductivo permitió arribar a conclusiones generales. En ese sentido, el ejercicio de rastreo bibliográfico, que demandó la revisión documental del tema en estricto sentido, obedeció

a una búsqueda de fuentes directas relacionadas con la protección de datos personales en el marco de las tensiones, retos y desafíos que ha impuesto la pandemia por la Covid-19, en el desarrollo de alternativas, estrategias y formas de envío, recepción o transmisión de los datos que circulan mediante distintos canales de comunicación, como redes de conexión o plataformas tecnológicas. Para el análisis de los datos obtenidos se procedió a contrastar la información extraída con los aportes teóricos consultados para referir las reflexiones profundas de los hallazgos obtenidos (Barbera et al., 2019).

Hallazgos

Conceptualización del derecho a la protección a los datos personales y sus limitaciones en el derecho de acceso a la información pública.

Los datos personales corresponden a aquellos datos que sirven para identificar directa o indirectamente a un individuo con vida (Comisión Europea, 2022), en la medida que, a través de su nombre, foto, números de contacto, dirección física o electrónica, entre otros datos, se puede dar con el paradero de una persona (AtInternet, 2022). De manera que, su recolección, tratamiento, almacenamiento y cobertura debe ser documentada con una trazabilidad plena, incluido el consentimiento válido, para evitar equivocaciones e injerencias en la vida privada de alguien (Chen Mok, 2010).

Estos datos pueden contar con ciertas excepciones para su tratamiento, acorde a los estándares pertinentes en la materia del derecho fundamental bajo estudio, pues algunos de ellos son de carácter sensible, como ocurre con los datos que revelan información acerca del origen racial o étnico de un individuo, su orientación política o convicción religiosa o filosófica, su vínculo con agremiaciones o asociaciones especiales, grupos minoritarios, movimientos políticos activos o colectivos sociales (Superintendencia de Industria y Comercio, 2014).

En ese sentido, el artículo 18 de la ley 1437 de 2011 (ley 1437, 2011) contiene las excepciones para limitar la publicación de datos personales, entre las cuales se destacan las siguientes: a) El derecho a la intimidad, con las limitaciones y reservas que demanda a los servidores públicos, en el marco de lo expuesto por el artículo 24 de la Ley 1437 de 2011; b) El derecho a la vida, la salud o la seguridad; c) Los secretos comerciales, industriales y profesionales.

Los datos personales deben ser: a) recogidos con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines; b) adecuados, pertinentes y no excesivos en cuanto a los fines para los que se recaben y para los que se traten posteriormente; exactos y actualizados; d) conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que traten ulteriormente (Cifuentes, 2013).

Los datos personales, en el marco de dos leyes estatutarias (Ley 1266, 2008; Ley 1581, 2012), no son información abierta al público, sino cuentan con un carácter restringido, que merece ser protegido por estar bajo el control o la custodia de un sujeto obligado, por lo que en esencia no pueden ser revelados, sin el consentimiento previo, expreso, libre y voluntario de su titular. Continuando con el análisis de estas normas,

se aprecia que, por su categoría de datos personales, se configura una excepción al derecho de acceso a la información pública, siempre que los mismos no pierdan su naturaleza, ni tampoco formen parte de la información pública clasificada.

La normatividad nacional contiene derechos para proteger los datos personales y las tensiones que surgen frente a la divulgación de los mismos. De acuerdo a lo anterior se debe desarrollar el estudio de los límites en el tratamiento de datos personales, según el test de proporcionalidad. En consecuencia, es menester que quien deba dar respuesta a una solicitud sobre acceso de datos personales, atienda al cumplimiento de un objetivo legítimo, respaldado en el artículo 15 de la Constitución Política de 1991, en la Ley 1266 de 2008 y en la Ley 1581 de 2012.

En un mundo globalizado cada vez más "los datos personales se han convertido en un bien permanente comercializado a escala nacional e internacional y en un insumo diario de los sistemas de información privados y del gobierno" (Cifuentes, 2013, pp. 273-274), son bienes intangibles o incorporales de las empresas e instituciones susceptibles de ser protegidas por instancias nacionales e internacionales, al considerarse elementos de la empresa indispensable para el adecuada organización interna de las corporaciones. En las empresas, los datos sobre las personas naturales y jurídicas son verdaderos activos determinantes para el good will de las compañías. Según "el artículo 516 del código de comercio colombiano" (Decreto 410, 1971), la fama comercial de la empresa como un elemento del establecimiento de comercio, permitirá incrementar la buena reputación de la empresa.

Los datos de las personas representan un elemento fundamental de la empresa para desarrollar su actividad económica partiendo de la garantía y protección del derecho a la propiedad intelectual, que podrá ser "vendido, alquilado o cedido" (Cifuentes, 2013) según el caso. Es decir, es un bien incorporal o intangible muy valioso de la empresa, incluso más valioso que los mismos activos corporales de las compañías, a través de los datos personales y la información reservada las empresas crecen en el mundo empresarial. La información y datos de las empresas son fuentes de derechos para todas las personas involucradas en el mundo comercial, su protección requiere de nuevas medidas implementadas para asegurar la protección, de acuerdo a los ataques externos para desorganizar y afectar las actividades económicas de las empresas.

De conformidad con lo afirmado por Cifuentes "algunos estudios realizados en otros países han concluido que los clientes prefieren hacer negocios con empresas que les garantizan un nivel adecuado de protección de datos personales" (Cifuentes, 2013,p.277). En este sentido, el tratamiento de datos personales es un elemento indispensable para la credibilidad y prestigio de las instituciones privadas. Si las empresas no cuentan con la estructura adecuada para proteger y garantiza el tratamiento de datos personales, incurrirán en sanciones legales de carácter comercial, civil o penal según el caso. Además, su buena reputación y su buena imagen comercial (good will) se afectará. En esta medida, para ser licito el tratamiento datos personales por las entidades privadas, deberá basarse en el consentimiento informado del interesado.

Los Estados y las compañías a través del monopolio de la información y las innovaciones tecnológicas empleadas en el uso de datos pueden desestabilizar organizaciones privadas y públicas de Estados según los intereses en juego en el escenario político. Las acciones pueden ser realizadas por parte de agentes estatales o

terceros donde emprenden acciones correspondientes a la desorganización y ruptura de canales de información internas tanto en las instituciones estatales como las privadas. Lo anterior acarrea consecuencias políticas y económicas considerando la importancia de los datos personales de acuerdo a la información de carácter sensible y fuertemente protegida.

El derecho nacional, el derecho económico y el derecho internacional público plantean nuevos paradigmas de acuerdo a los sucesos que implican una transformación en la forma de entender y aplicar el derecho fundamental a la protección en el tratamiento de datos personales. En ese orden de ideas, el debido tratamiento de datos personales, empresas y entidades públicas prevén la importancia de la protección y garantía del adecuado uso de la información para proteger los derechos humanos civiles y políticos de la población.

El tratamiento de datos personales en el derecho económico.

La organización mundial del comercio "asocia el internet como la nueva "ruta de la seda" para conectar empresas de todas las dimensiones a los mercados globales. No obstante, las nuevas formas de interacción social a través del ciberespacio han traído consigo cambios menos positivos y no deseados: la polarización de la sociedad, el refuerzo de la censura por parte de algunos gobiernos, la transición en el comportamiento del ciberusuario de la recepción a la reacción, las limitaciones a la manera tradicional de interactuar y comunicarse entre las personas, y los ataques que constantemente amenazan con interrumpir las actividades del mundo cibernético" (Relatores tematicos, 2016).

Como también puede desestabilizar economías y desorganizar instituciones transgrediendo la estructura interna de las organizaciones estatales y privadas. En materia de las compañías, la Organización Mundial del Comercio (OMC) en conjunto con la Oficina de Programación Multianual de Inversiones (OMPI) establece las regulaciones pertinentes para proteger los derechos de propiedad intelectual de las empresas nacionales e inversionistas de los Estados miembros, específicamente el tratamiento de datos personales de las compañías privadas para garantizar su correcto funcionamiento sin interferencia estatal, igualmente particulares que pretendan atacar las empresas a través de los ciberataques, con propósitos de desorganización económica, empresarial, y estatal.

De acuerdo a lo establecido por la OMC, "el tratamiento de datos como un derecho de propiedad intelectual de las empresas, deberá ser desarrollado de acuerdo a las circunstancias actuales (Organizacion Mundial del Comercio, s.f.)", donde los tratados bilaterales y multilaterales de inversión de los Estados exigen una mayor protección en materia de garantizar a las empresas nacionales y extranjeras normas claras, con el objetivo de fortalecer la seguridad jurídica de los derechos de propiedad intelectual y de esta manera cumplir por parte de los Estados los compromisos adquiridos en los tratados bilaterales y multilaterales de inversión de los Estados en materia de los derechos de propiedad intelectual.

Un ejemplo donde los Estados pueden exigir el debido tratamiento de datos a las compañías y los estados se presentó por parte de los jueces de la Unión Europea analizando un caso sobre el derecho fundamental a la protección del tratamiento de datos personales. "La adopción del llamado derecho al olvido como una

proyección del derecho a la protección de datos personales es una realidad insoslayable en el ámbito de la Unión Europea. La paradigmática resolución del Tribunal de Justicia de la Unión Europea (en adelante, TJUE) en el caso Google Spain y Google Inc. vs. la Agencia Española de Protección de Datos" (Ramírez, 2018,p. 80), en 2014 puso en el centro de debate la posibilidad de que las personas físicas pudieran obtener, previa solicitud, la remoción de los resultados en los motores de búsqueda asociados a su nombre (Ramírez, 2018,p. 80).

El tratamiento de datos personales de los Estados y la importancia para la seguridad de los Estados en el marco de la Covid- 19.

El uso de la fuerza según la Carta de Naciones Unidas se transforma de acuerdo a las nuevas tecnologías, la carta de naciones unidades se queda corta ante las tensiones actuales por los ciberataques por parte de países que encuentran ventajas o beneficios a través de la posición dominante para el acceso de datos o información de estados enemigos. De esta manera, la carta de naciones unidas y las normas internacionales deben considerar las nuevas tecnologías para la protección y mantenimiento de la paz mundial.

En este sentido la regla general que estableció la Carta es que los Estados deben abstenerse de recurrir a la fuerza, o a la amenaza del uso de la misma, pues según su artículo 2, los miembros adscritos a la organización de las naciones unidas, no podrán amenazar o hacer uso de la fuerza coercitiva en contra de la población asentada en territorio de cualquier Estado (Urueña, 2015), salvo que por autorización del Consejo de Seguridad se deba emplear esta última para hacer efectivas sus decisiones.

De manera que, es posible interrumpir total o parcialmente de las relaciones económicas y de las comunicaciones ferroviarias, marítimas, aéreas, postales, telegráficas, radioeléctricas, y otros medios de comunicación, así como la ruptura de relaciones diplomáticas; o también podrá hacerse uso de fuerzas aéreas, navales o terrestres, por medio de demostraciones, bloqueos u operaciones militares, para mantener o restablecer la paz y la seguridad internacional.

En la actualidad una vía que refleja claramente el uso de la fuerza, incluso desmedida o desproporcionada entre naciones, es el ciberataque. El ataque directo por medio de elementos armamentistas tradicionales evoluciona para atacar a los Estados por medios diferentes. De esta manera, la infiltración a los datos sensibles de las instituciones del gobierno y las compañías claves para el desarrollo económico de los Estados, han tenido un gran auge y mucho apogeo, en el marco de la implementación de nuevas técnicas y estrategias para generar un gran golpe a los enemigos, como ocurrió con el ataque cibernético al sistema electrónico del metro de Washington, que dejó como consecuencia, el deceso de 9 personas y 80 personas heridas ('Anomalies', 2009).

De esta forma, la regulación del uso de la fuerza para la salvaguarda de datos personales es uno de los desafíos que impone la pospandemia, a nivel nacional e internacional, para garantizar la protección efectiva de la información propia, pues a raíz de la pandemia por la Covid 19 (Comisión Interamericana de Derechos Humanos, 2020), se amplió la esfera de contacto y acceso a datos personales por medio de plataformas electrónicas, redes sociales y espacios ciberinformáticos, dada la necesidad de comunicación globalizada,

que se vio restringida durante los aislamientos preventivos obligatorios y las cuarentenas estrictas que fueron impuestas por distintos Estados.

En ese sentido, el derecho internacional durante y después de la pandemia, ha debido enfocarse más hacia la utilización, tratamiento y cubrimiento de datos, amparado por normas de la Unión Internacional de Telecomunicaciones, como organismo especializado de la Organización de las Naciones Unidas, que se encarga de estandarizar y regularizar las practicas globales de los Estados y las empresas operadoras de la industria, para garantizar la prestación de los servicios de telecomunicación e interconectividad a escala mundial" (Relatores tematicos, 2016).

Lo anterior, toda vez que distintos ciberataques se han dado durante la pandemia, como en el caso de Colombia, donde en el año 2021 se encendieron las alarmas por más de mil millones de intentos de ciberataques (El Colombiano, 2021), donde como bien lo ha expuesto Pachón (2021), el robo de datos e información por parte de hackers a grandes empresas ha aumentado en un 93%, en relación con la cantidad acaecida durante el año 2020, por lo que riesgo de violación de datos personales, por medio de ataques cibernéticos, contó con una brecha de aumento del 30% del año 2020 al 2021, según lo reportado por la Fiscalía General de la Nación a comienzos de este año.

Conclusiones

El estudio del derecho fundamental a la protección de datos personales genera unos desafíos en el que se aplican las herramientas jurídicas que proporciona la normativa nacional e internacional, pues la regulación internacional contiene una amplia gama de instrumentos jurídicos donde los Estados pueden desarrollar los marcos jurídicos en el tratamiento de la información. Además, las cortes nacionales atendiendo los litigios en el sector público y privado entienden cada vez más que el estudio al adecuado tratamiento de datos es primordial en las sociedades democráticas, considerando la gran responsabilidad en el manejo de los datos personales para el cumplimiento de los Derechos Humanos en la sociedad global.

Los desafíos del uso de la fuerza demandan una mayor acción por parte de agentes estatales que ejerzan un control social superior sobre la sociedad. En ese sentido, actuares como el ciberpatrullaje donde las fuerzas públicas de los Estados vigilan y controlan el terrorismo digital, son herramientas para recuperar, mantener y preservar el orden público. Por lo que algunos autores, como Tamara Peñalver (Colombiainforma, 2021), justifican los trabajos de inteligencia y perfilamiento a manos de agentes encubiertos o fuerza pública armada, donde se recolecte información pública para someterla a procesos de inteligencia.

No obstante, lo anterior puede contrariar de cierta manera la jurisprudencia de la Corte Interamericana de Derechos Humanos con respecto al tratamiento de datos personales de las personas, pues no es claro el cumplimiento del test de proporcionalidad para limitar la libertad de expresión a través del ciberpatrullaje contra el derecho a la dimensión individual y colectiva para expresar opiniones sobre determinada situación, pues el derecho a la libertad de expresión como un máximo derecho al interior de las sociedades democráticas, se puede ver restringido o cercenado por constantes perfilamientos, monitoreos y seguimientos a las comunicaciones de personas o grupos sociales, que violan la intimidad o privacidad tanto individual como

colectiva.

Fuentes Bibliográficas

'Anomalies', M. C. (Mayo 7, 2009). Washingtonpost. washingtonpost: https://www.washingtonpost.com/wp-dyn/content/article/2009/06/24/AR2009062400815.html

AtInternet.(2022). Datos personales. https://www.atinternet.com/es/glosario/datos-personales/

Barbera, N, Chirinos, Y y Posada, M. (2019). La planificacion del desarrollo sostenible desde los sistemas complejos adaptativos en Colombia. En Chirinos, Ramirez, Barbera y Rojas. *Tendencias de la Investigacion Universitaria. Una vision desde Latinoamerica.* Volumen XII. fondo editorial Servando Garces. DOI: www.doi.org/10.47212/tendencias_v_2019_3

Chen Mok, S. (2010). Privacidad y protección de datos: un análisis de legislación comparada. *Diálogos Revista Electrónica de Historia*, 11(1), 111-152. [fecha de Consulta 28 de febrero de 2022]. https://www.redalyc.org/articulo.oa?id=43915696004

Cifuentes, M. C. (2013). Responsabilidad por el tratamiento de los datos personales de clientes, empleados,proveedores y terceros. En N. Remolina Angarita, F*undamentos de derecho de los negocios para no abogados. Editorial Temis.*

Colombiainforma.info (2021). *El ciberpatrullaje como nueva restricción a las libertades individuales*. https://www.colombiainforma.info/el-ciberpatrullaje-como-nueva-restriccion-a-las-libertades-individuales/

Comisión Europea. (2022). *Datos personales.* https://www.atinternet.com/es/glosario/datos-personales/

Comisión Interamericana de Derechos Humanos. (2020). *Resolución 1. Pandemia y Derechos Humanos en las Américas. Organización de Estados Americanos.*

CPC. (1991). *Constitución Política de Colombia 2da.* Ed. Legis.

Congreso de la República. (18 de enero de 2011). Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Ley 1437 de 2011.

Presidencia de la República. (16 de Junio de 1971). Código de Comercio. Decreto 410 de 1971.

Congreso de la República. (Diciembre 31 de 2008). Disposiciones generales de Habeas Data y manejo de la información. Ley 1266 de 2008.

El colombiano. (junio 21, 2021). *Colombia ha recibido más de mil millones de intentos de ciberataques en 2021.* https://www.elcolombiano.com/colombia/colombia-continua-recibiendo-intentos-de-ciberataque-en-

2021-MD15169115

Pachón, C. (2021). *Los Ciberataques más famosos del 2021 en Colombia y el mundo.* https://www.nsit.com.co/los-ciberataques-mas-famosos-del-2021-en-colombia-y-el-mundo/

Ramírez, M. S. (2 de Diciembre de 2018). El derecho al olvido digital desde la perspectiva de la Unión Europea y la viabilidad de su extrapolación al caso de México. *Revista Latinoamericana de Derecho, 79- 97*

Relatores tematicos. (Mayo 7, 2016). *Globalización, poder y derecho.* https://relatorestematicos.uniades.edu.co/index.php/es/globalizacion-poder-y-derecho/articulos-e-investigaciones.html

Superintendencia de Industria y Comercio. (2014). *Régimen General de Protección de Datos Personales.*

https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Compendio%202%20FINAL%20V%2012%20Dic20.pdf

Organizacion Mundial del Comercio. (s.f.). *WTO.* Recuperado el Junio de 2022, de https://www.wto.org/spanish/tratop_s/trips_s/trips_s.htm

Urueña, R. (2015). *Derecho internacional poder y limites del derecho en la sociedad global.* Editorial Uniandes.