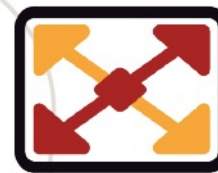


**A propósito del día internacional
de la protección del datos,
28 de enero de 2022...**



**Extensión
Universitaria**
y Educación Continua

Universidad Autónoma Latinoamericana



Extensión Cultural

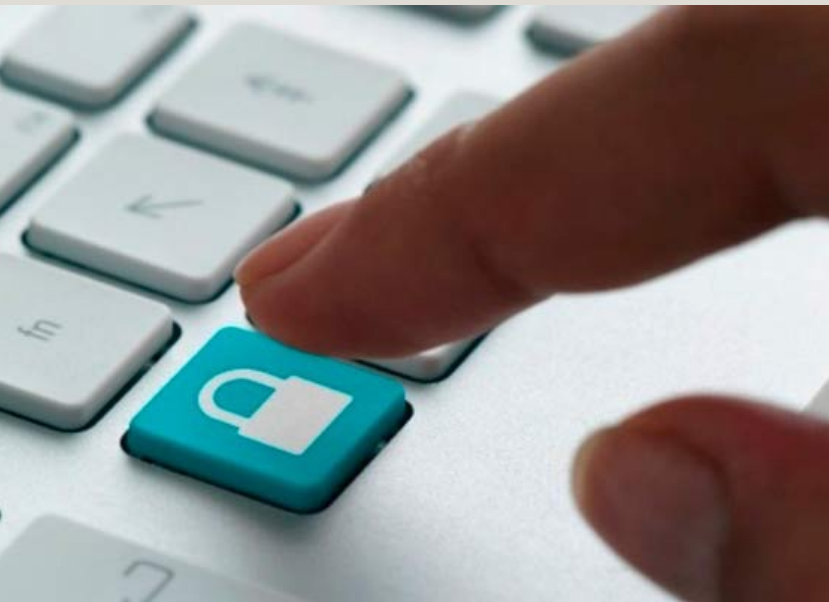
Mucho se ha dicho de los datos personales durante el trasegar de la historia del mundo, no en vano la época Nazi se permeó en su estrategia política para segmentar la raza aria caracterizando las personas con el objetivo de identificar y delimitar el pueblo merecedor de protección por la política Nazi. Algunos doctrinantes atribuyen a esa época el origen del *dato personal como hoy se concibe*.

Hoy por hoy, el dato personal e impersonal son insumos necesarios para operar cualquier aspecto de la vida de las personas naturales y jurídicas como es la seguridad, tecnología, comercio, empleo, industria, salud, educación, gobierno, en fin, serían innumerables los entornos dónde estos se convierten en el núcleo de la operación, derivado de ello *la protección del dato personal* se considera un derecho humano asociado a los principios de internet como se dispuso en la Carta de Derechos Humanos y Principios de Internet.



Ana María Mesa Elneser. PhD

Abogada, Doctora y Magister en Derecho Procesal Contemporáneo, Especialista en Investigación y Docencia. Investigadora y Docente de la facultad de Derecho de la Universidad Autónoma Latinoamericana. CEO de Law Tic Grupo Jurídico. Presidente de la corporación EDI Colombia. Miembro de COLADCA. Datos de contacto ana.mesael@lawtic.com.co.

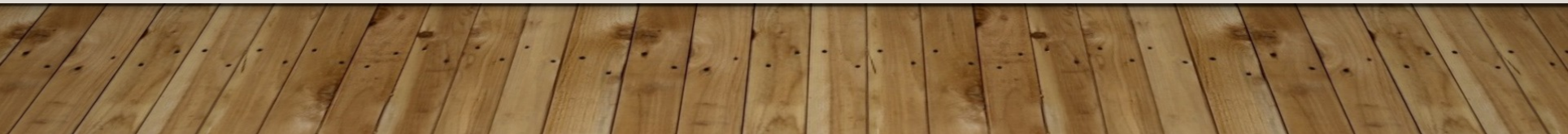


CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS: Toda persona tiene derecho a la privacidad online. Esto incluye el no ser vigilado, el derecho a utilizar cifrado y el derecho al anonimato. Todo el mundo tiene derecho a la protección de datos, incluyendo el control sobre la recolección, retención, transformación, eliminación y divulgación de sus datos personales. (Naciones Unidas, 2015)

Así mismo en la carta política de Colombia, constitución de 1991, en el artículo 15 consagra:

ARTÍCULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. (Congreso de la república de Colombia, 1991)

Ello permite colegir que las personas tienen derechos fundamentales como asociados a su identidad como la protección del dato personal, pudiendo ejercer la defensa propia respecto de cualquier uso indebido o fraudulento, en igual sentido empoderándose de sus datos respecto de quien los recolecta, usa, circula y almacena.





Cabe preguntarse ¿porqué el dato personal es una herramienta tan importante para la operación del mundo actual?, ¿porqué los desarrollos tecnológicos y las estrategias en favor de las personas se alimentan del dato personal?, estos cuestionamientos no tendrían un núcleo diferente a *la persona en sí misma* por ser a quien se dirige la educación, seguridad, salud, empleo, herramientas tecnológicas y todo cuanto existe, la persona es el núcleo de la vida humana, en corresponsabilidad es la academia, el Estado, la industria y el comercio, los encargados de diseñar, desarrollar y poner en marcha estrategias para satisfacer las necesidades que la misma sociedad va demandando para su quehacer diario, lo que hoy se vislumbra como desarrollo.

En la época contemporánea, lo que más demanda el mundo, e incluso se acentuó con la pandemia del CoVid-19, son las herramientas tecnológicas como celulares, Tablet, laptop, desktop, pendrive, smartwatch, smart glasses, Blockchain, inteligencia artificial, la investigación, desarrollo e innovación, eso si cada día con un grado alto de innovación, que permita a la persona vivir una vida más ágil, dinámica, con información a la mano y en tiempo real que le permita tomar decisiones más fáciles.

- 
-
- Cabe preguntarse ¿porqué el dato personal es una herramienta tan importante para la operación del mundo actual?, ¿porqué los desarrollos tecnológicos y las estrategias en favor de las personas se alimentan del dato personal?, estos cuestionamientos no tendrían un núcleo diferente a *la persona en sí misma* por ser a quien se dirige la educación, seguridad, salud, empleo, herramientas tecnológicas y todo cuanto existe, la persona es el núcleo de la vida humana, en corresponsabilidad es la academia, el Estado, la industria y el comercio, los encargados de diseñar, desarrollar y poner en marcha estrategias para satisfacer las necesidades que la misma sociedad va demandando para su quehacer diario, lo que hoy se vislumbra como desarrollo.
 - En la época contemporánea, lo que más demanda el mundo, e incluso se acentuó con la pandemia del CoVid-19, son las herramientas tecnológicas como celulares, Tablet, laptop, desktop, pendrive, smartwatch, smart glasses, Blockchain, inteligencia artificial, la investigación, desarrollo e innovación, eso si cada día con un grado alto de innovación, que permita a la persona vivir una vida más ágil, dinámica, con información a la mano y en tiempo real que le permita tomar decisiones más fáciles.
 - Sin desmeritar lo planteado hasta el momento, debemos señalar un par de situaciones emergentes que se nutren la necesidad desmedida del uso de datos personales, la industria tecnológica lo sabe, la sociedad lo permite, no más por el consumo de tecnología, y más grave aún los delincuentes encuentran su alimento para los diferentes ataques informáticos, poniendo en jaque la seguridad informática y de la información. Una situación es la sed de monetizar datos y otra es el dominio de las personas a costa del riesgo de seguridad del titular.



- Respecto del primer escenario, debemos partir de entender qué es monetizar los datos, es *hacer moneda* (RAE - Real Academia de la Lengua Española), producir dinero, a costa del uso y circulación de los datos de las personas almacenados en bases de datos estructuradas, que permite caracterizarlas de forma clara respecto de su identidad, ubicación, gustos, costumbres, patrimonio y más, o desestructuradas como es el *Big Data* (RAE: Real Academia de la Lengua Española) los cuales se procesan por medio de herramientas informáticas y bajo algoritmos configurados pudiendo extraer información y caracterizar las personas con fines comerciales, investigativos, científicos, culturales, políticos, o cualquier otro interés que sea afín al apoyo y beneficio de las necesidades sociales, ese uso se considera más que necesario y justificable, contrario a ello, cuando los fines de explotación económica son para enriquecer a un sector, es ahí donde el uso puede ser cuestionado, hecho suficiente para legitimarlo mediante la exigibilidad de que se obtenga una autorización de tratamiento de datos por parte del titular, o ilegítimo, cuando no se cuenta con autorización ni la ley establece la obligatoriedad a dicho uso, y aun así quien posee la información explota los datos, los monetiza.
- Para finalizar esta reflexión nos encontramos con el segundo escenario, el cual constituye la identificación de los riesgos asociados al uso de los datos personales de titulares, a su vez exige que la persona responsable de tratarlos lo haga de forma segura, como se manifiesta en la Guía de Incidentes adoptada por la SIC al indicar que:

El principio y el deber de seguridad tienen un criterio eminentemente preventivo, lo cual obliga a los Responsables o Encargados del Tratamiento a adoptar las medidas necesarias para evitar posibles afectaciones a la seguridad de los datos. Pero si las medidas de seguridad fallan, las organizaciones deben estar preparadas para mitigar los riesgos y daños que se pueden causar a los derechos y libertades fundamentales de los Titulares y a las organizaciones. (SIC, 2020).



Siendo necesario advertir que el tratamiento de los datos sin dar cumplimiento al principio de seguridad consagrado en el artículo 4, de la Ley 1581 de 2012, constituye en sí mismo un quehacer violatorio del derecho fundamental a la protección del dato personal, en consecuencia, un uso indebido y/o fraudulento del dato, salvo que el responsable logre demostrar la debida diligencia y el uso seguro de los mismos, con transparencia y legitimidad respecto del titular.

Toda ésta reflexión conlleva un fin último y es tocar la conciencia de todas las personas a que se reconozcan a sí mismos como titulares de sus datos, se empoderen de éstos, reflexionen antes de compartirlos, validen qué compran, qué consumen, que usan y qué les piden para brindarles servicios, sobre todo tecnológicos, limiten su información, conozcan el derecho a la privacidad y lo defiendan y que sean conscientes de entregar sus datos comprendiendo los beneficios y los riesgos asociados que estos traen.



REFERENCIAS

- Congreso de la república de Colombia. (20 de julio de 1991). Constitución Política de 1991. Bogotá D.C., Colombi. Obtenido de http://www.secretariassenado.gov.co/senado/basedoc/constitucion_politica_1991.html
- Naciones Unidas. (Enero de 2015). *Carta De Derechos Humanos Y Principios De Internet*. Obtenido de https://derechoseninternet.com/docs/IRPC_Carta_Derechos_Humanos_Internet.pdf
- RAE - Real Academia de la Lengua Española. (s.f.). Definición de monetizar. Obtenido de <https://dle.rae.es/monetizar>
- RAE: Real Academia de la Lengua Española. (s.f.). big data. Obtenido de <https://dpej.rae.es/lema/big-data>
- SIC. (diciembre de 2020). GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALES. Colombia. Obtenido de https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guía_gestion_incidentes_dic21_2020.pdf