Regulación del Internet de las cosas para la protección de los datos personales en Colombia

Trabajo de Grado

Carlos Yamid Paiba Díaz

Director:

Ing. Pedro Alejandro Mancera Lagos, MSc

Codirector:

Ing. Tatiana Zona codirector, PhD

UNIVERSIDAD SANTO TOMAS
FACULTAD DE INGENIERIA DE TELECOMUNICACIONES
MAESTRÍA EN TELECOMUNICACIONES Y REGULACION TIC
BOGOTÁ, 2024

Este proyecto está dedicado a Dios, quien ha sido mi guía a lo largo de mi vida, brindándome bendiciones y fortaleza para seguir adelante en mis logros y nunca rendirme. Agradezco a mi familia por su apoyo incondicional, amor y confianza, que me han permitido completar mi carrera.

Agradecimientos

En primer lugar, quiero expresar mi más profundo agradecimiento a mi asesor Anthony Castellanos, por su invaluable guía, paciencia y apoyo durante todo el proceso de investigación y redacción de esta tesis. Su experiencia y dedicación fueron fundamentales para la culminación de este trabajo.

A los profesores de la maestría en telecomunicaciones y regulación tic, quienes a lo largo de estos años me han impartido conocimientos, inspiración y han contribuido de manera significativa a mi formación académica y profesional.

Contenido

Índice de tablas

Índice de Figuras

Acrónimos

MIT	Massachusetts Institute of Technology.
EU	Unión Europea
LOPDGDD	Ley Orgánica de Protección de Datos Personales y Garantía de los derechos digitales
GDPR	Reglamento General de Protección de Datos
RNBD	Registro Nacional de Base de Datos
OEA	Organización de los Estados Americanos
CJI	Comité Jurídico Interamericano
RNBD	Registro Nacional de Base de Datos
OCDE	Organización para la Cooperación y el Desarrollo Económico
IoT	Internet de las Cosas
ANE	Agencia Nacional del Espectro

Resumen

La explotación de los datos personales en el entorno digital se ha convertido en la nueva monedad del siglo XXI, debido al rápido desarrollo de las tecnologías, caso contrario sucede con la falta de legislación de políticas para la adecuada regulación y protección de los datos personales como es el uso de los datos en el Internet de las cosas (IoT), es de vital importancia crear mecanismos jurídicos necesarios para la protección de la información personal, lo anterior se logra con políticas de privacidad adecuadas a las necesidades de los empresarios y medidas de seguridad robustas que garanticen la confidencialidad de la información, con el objetivo de salvaguardar los derechos fundamentales de las personas.

Palabras clave: Constitución Política de Colombia, Internet de las Cosas (IoT). - Derecho a la privacidad- Datos personales- Ley 1266 del 2008, ley 1581 del 2012, habeas data, Regulación europea al IoT, Derecho comparado, Explotación de datos, vulneración a la privacidad.

Abstract

The exploitation of personal data in the digital environment has become the new currency of the 21st century, due to the rapid development of technologies, the opposite is the case with the lack of policy legislation for the proper regulation and protection of personal data such as the use of data in the Internet of Things (IoT), it is of vital importance to create legal mechanisms necessary for the protection of personal information, this is achieved with privacy policies appropriate to the needs of entrepreneurs and robust security measures to ensure the confidentiality of information, with the aim of safeguarding the fundamental rights of individuals.

***Keywords**:* Political Constitution of Colombia, Internet of Things (IoT). - Right to privacy - Personal data - Law 1266 of 2008, Law 1581 of 2012, habeas data, European regulation of IoT, comparative law, data exploitation, privacy violations.

1 Introducción

El rápido avance de Internet de las cosas (IoT) a nivel global ha generado importantes desafíos regulatorios, particularmente en áreas como la seguridad de los datos y la gestión de recursos digitales. Desde finales de los años 90, el IoT ha evolucionado significativamente, transformando múltiples aspectos de la vida cotidiana y diversas industrias. Sin embargo, estos avances también traen consigo riesgos importantes relacionados con la privacidad y la seguridad de los datos.

El internet de las cosas es parte esencial de la vida de millones de personas y del desarrollo económico global. En Colombia, la inversión en IoT representa más del 3% del PIB en 2021, posicionando al país como el sexto mayor inversionista en esta tecnología en América Latina en 2022. Sin embargo, a nivel mundial, Colombia ocupa el puesto 132 en el ranking de ciudades inteligentes (Berrone & Ricart, 2022).

En la era digital, la información personal tiene un valor incalculable, el uso indebido puede generar graves riesgos de seguridad y vulnerar la privacidad de las personas. En Colombia, el marco regulatorio en materia de protección de datos personales avanza lentamente generando incertidumbre jurídica y exponiendo a los usuarios a potenciales riesgos.

Actualmente el país está viviendo la transición de IoT en los sistemas energéticos mejorando la eficiencia y sostenibilidad de tecnologías avanzadas, como los medidores inteligentes de energía. Conocidas como Infraestructura de Medición Avanzada (AMI), por sus siglas en inglés) y Medidores inteligentes de agua (MIA), está transformando la forma de gestionar y consumir estos recursos.

Los sistemas AMI integran tecnologías IoT para recopilar, procesar y transmitir datos de consumo eléctrico en tiempo real. Este enfoque permite a los proveedores de energía optimizar sus redes, detectar anomalías, mejorar la facturación y promover el uso eficiente de los recursos.

Por su parte, los Medidores Inteligentes de Agua (MIA), se centra en la automatización del monitoreo y la gestión de datos de consumo, ofreciendo beneficios similares, pero con una menor complejidad tecnológica.

En Colombia, la implementación de AMI y MIA ha cobrado relevancia debido a la necesidad de modernizar la infraestructura y mejorar la sostenibilidad energética. Estos sistemas permiten tomar decisiones más automatizados sobre el consumo, fomentando prácticas responsables y reduciendo

costos. Esta tecnología se alinea con los objetivos de sostenibilidad promovidos por el gobierno y las empresas del sector.

Sin embargo, el despliegue de estas tecnologías plantea desafíos muy grandes en términos de regulación, protección de datos y privacidad. La recopilación masiva de datos de consumo, subraya la necesidad de garantizar la privacidad y la seguridad en el manejo de estos datos.

La presente investigación busca analizar los desafíos asociados a la recolección y tratamiento de datos en los medidores inteligentes AMI y MIA en Colombia. Además, se explorarán las políticas regulatorias actuales y las mejores prácticas internacionales, con el objetivo de proponer recomendaciones que potencien el uso responsable y efectivo de estas tecnologías en el contexto nacional.

Estos riesgos son los que nos lleva a hacer un estudio sobre el panorama del IoT en nuestro país y los diversos problemas que implica, siendo el más importante la protección de los datos, durante los últimos años se ha incrementado los dispositivos conectados al IoT, recopilan datos sobre patrones de comportamiento de las personas, por ejemplo, el tiempo de uso, intereses y preferencias de las personas luego pueden ser utilizados para beneficiarse económicamente o cometer delitos.

Lo anterior, nos hace preguntarnos si en verdad se respeta la privacidad de las personas y su consentimiento y en muchos casos la recopilación de datos de manera maliciosa. Finalmente, el trabajo se enfoca en analizar la regulación que existe en nuestro país en materia de protección de datos y compararla con otras regulaciones como la unión europea, el Reino Unido y Estados Unidos, proponiendo algunas directrices para un modelo de mejor regulación en nuestro país.

2 Objetivos

2.1 Objetivo General.

- Determinar el estado actual de las políticas de regulación existentes implementadas a nivel internacional en el ámbito del Internet de las cosas (IoT), para la protección de los datos y compáralo en Colombia.

2.2 Objetivos Específicos.

- Analizar las diferencias y semejanzas entre los distintos sistemas del derecho comparativo de otros países a nivel normativo, a nivel de legislación del IoT que sirva como ejemplo en el contexto que se ha dado la norma, para hacer una comparación.

- Estudio sistemático de las normas regulatorias de otras regiones como una interpretación que nos ayude a mejorar la adopción de las tendencias tecnológicas del país.

- Evaluar los retos regulatorios para determinar el punto de partida tener una mejor adopción de las tecnologías.

- Analizar los desafíos de la protección de los datos personales en el entorno digital en Colombia.

2.3 Alcance

Este estudio explora el estado actual de las políticas regulatorias para proteger la información y privacidad de las personas ante el auge del IoT a nivel global.

La investigación se orienta en analizar los antecedentes, investigaciones científicas, artículos y en temas de protección y privacidad de los datos en la era digital.

Sugerir recomendaciones, sugerencias críticas a la regulación existente en el país como la ley 1581 del 2012, debatir los mecanismos que han implementado otros países adelantados en el tema de la regulación IoT.

Los desafíos en temas de seguridad en IoT son enormes especialmente en la protección y control de los datos más aún cuando las tecnologías evolucionan más rápidamente que la regulación.

Europa es uno de los países referentes en temas de regulación de políticas como GDRP para los datos del IoT, por medio de un estudio comparado que nos permita realizar una interpretación gramatical del panorama actual.

Las entidades encargas de la regulación en Colombia, encabezada por el Mintic y vigilado por la superintendencia de industria y comercio.

2.4 Propuesta Regulatoria

La protección de datos es esencial en el contexto del Internet de las Cosas (IoT), cada día hay más dispositivos recopilan y procesan datos en tiempo real. La Ley 1581 de 2012 establece el marco regulatorio para la protección de datos personales, ampliando las definiciones previas de la Ley 1266 de 2008 sobre datos financieros. Ante este panorama, es crucial definir directrices claras que aseguren la protección de los datos, adaptándose a los nuevos avances tecnológicos.

Para lo anteriormente indicado es clave desarrollar una Guía de Evaluación de Impacto de Protección de Datos Personales (EIPD) para identificar y mitigar los riesgos a los que pueden estar expuestos los datos personales, según el propósito de su recolección. Esta herramienta facilita el cumplimiento de las normativas y asegura la privacidad de los individuos desde el inicio.

Con la implementación de una guía de EIPD tenemos las siguientes ventajas

1. **Contexto**
   A. Documentar el ciclo de vida de los datos asociados al tratamiento y de las áreas involucradas en el proceso.
   B. Analizar las necesidades y finalidad del tratamiento

2. **Gestión de riesgos**
   A. Identificar riesgos y amenazas
   B. Evaluar los riesgos
   C. Tratar los riesgos

3. **Conclusiones**
   A. Plan de acción
   B. Informe y conclusiones

4. **Comunicación y consulta**
   A. para aquellos casos donde el estudio del EIPD el nivel de riesgo es alto.

La creación de herramientas como el Privacy Impact Assessment (PIA) es fundamental para cumplir con la normativa nacional y como base para realizar la Evaluación de Impacto de Protección de Datos (EIPD)**.** Este tipo de herramientas son ampliamente utilizadas en países europeos para asegurar el cumplimiento de las regulaciones de privacidad y protección de datos.

Es necesario definir el perfil del Oficial de Protección de Datos en Colombia (ODP) y establecer funciones claras, apoyados por la SIC. Esto permitiría mejorar la realización de Evaluaciones de

Impacto en la Protección de Datos (EIPD) y Privacy Impact Assessment (PIA), así como brindar asesoria a las empresas y trabajar de la mano con las autoridades para cumplir con la normativa vigente.

Teniendo en cuanta que Colombia solamente cuenta con una única base legal de protección de datos (El consentimiento).

En contraste, en otros países el rol de Delegado de Protección de Datos (DPD) es obligatorio y cuenta con funciones claramente definidas apoyados por la regulación de protección de datos de la Unión Europea.

Los casos de estudio que han sido un éxito en el despliegue de tecnología IoT apoyados de la regulación son.

Smart Cities: En ciudades como Ámsterdam y Barcelona, el IoT se ha implementado en el contexto de "smart cities". La estrategia de la UE ha impulsado estos proyectos mediante regulaciones que aseguran que los dispositivos IoT utilizados para gestionar el tráfico, la energía y los servicios públicos sean compatibles entre sí, y al mismo tiempo, respeten la privacidad de los ciudadanos (Telefónica, Smart Cities).

IoT en infraestructuras críticas: En el reino Unido las empresas como las energéticas o de telecomunicaciones, deben cumplir con la Directiva NIS para proteger sus sistemas IoT contra ciberataques. Un ejemplo es el uso de sensores IoT para gestionar redes eléctricas inteligentes, deben implementar medidas estrictas de seguridad para evitar interrupciones en el suministro o acceso no autorizado a la información (Ince, 2022).

Otro ejemplo es el impulso a la red 5G, que se considera un habilitador crucial para la expansión de dispositivos IoT en España. Para asegurar que los dispositivos conectados a la red 5G sean seguros, se están desarrollando estándares de seguridad específicos para IoT en colaboración con la Agencia Española de Protección de Datos (AEPD) y otras instituciones.

Europa ha sido líder en la creación de regulaciones que abordan tanto los aspectos técnicos como éticos del IoT. A través de legislaciones como el GDPR, la Directiva NIS y la Estrategia para el IoT, la UE no solo ha promovido la innovación, sino que también ha garantizado que las preocupaciones de seguridad y privacidad sean consideradas desde el inicio de la implementación de estas tecnologías.

3 Marco general del proyecto

3.1 Antecedentes

El desarrollo de las diferentes revoluciones industriales varió según el nivel de avance de cada país. Mientras Reino Unido lideró la primera y segunda revolución industrial, seguido por Europa y Estados Unidos. Colombia en ese periodo, centró su economía en la extracción de recursos. Tras su independencia (1810-1819), el país enfrentó conflictos internos que generaron inestabilidad política, jurídica y económica. Solo después de la Guerra Civil de 1885 y con la Constitución del 1886.

Tras el final de la Segunda Guerra Mundial, comenzó una pugna entre Estados Unidos y Rusia, conocida como la “Guerra Fría”, marcada por la ausencia de enfrentamientos directos pero caracterizada por una competencia tecnológica y armamentista. Este periodo impulsó el desarrollo de tecnologías inicialmente diseñadas para uso militar, como las computadoras, que más tarde se adaptaron al ámbito comercial. Un ejemplo de esta transición fue la UNIVAC, la primera computadora de uso comercial, empleada en 1950 para procesar datos del censo de Estados Unidos (Hernández, 2011).

Mientras, Colombia enfrentaba el desafío de compensar siglos de retraso industrial mediante la adopción de nuevos sistemas de transporte, energía y la creación de grandes industrias que permitieran competir en el mercado global (Echavarría, Villamizar, M., & González).

Sin embargo, antes de que el Estado colombiano se enfocara en regular el uso de la información personal, el sector privado comenzó a alinearse con tendencias internacionales, como la recolección, uso y circulación de datos personales. Un ejemplo destacado fue la creación en 1964 de la Central de Riesgos del Sector Financiero (CIFIN), destinada a gestionar y compartir información sobre el riesgo y endeudamiento de los usuarios financieros (Asociación Bancaria y de Entidades Financieras de Colombia, s.f.).

Aunque la adopción tecnológica fue lenta en Colombia, la globalización y el avance de las nuevas tecnologías permitieron que empresas de alta tecnología y entidades financieras expandieran su influencia a nivel mundial. No obstante, la falta de regulación jurídica en torno al uso de datos personales dejó a los individuos expuestos, al no existir organismos administrativos o judiciales competentes para sancionar el uso indebido, la divulgación no autorizada o la gestión incompleta

de la información personal. Esta situación fue mitigada con la entrada en vigencia de la Constitución Política de 1991, que incluyó disposiciones fundamentales para la protección de datos personales.

3.2 ¿Qué es un dato personal?

La definición de dato personal se define en el artículo 3 de la ley 1266 de 2008 señala que se trata:

***Dato personal**. Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados* (Ley 1266 de 2008, Art. 3, 2008).

Otra definición más completa y acorde con los avances tecnológicos, es la que da el Comité Jurídico Interamericano (CJI) de la Organización de los Estados Americanos (OEA) en el reciente informe sobre Principios Actualizados sobre la privacidad y la protección de datos personales, al considerar que este término abarca.

"La información que identifica o puede usarse de manera razonable para identificar a una persona física de forma directa o indirecta, especialmente por referencia a un número de identificación, datos de localización, un identificador en línea o a uno o más factores referidos específicamente a su identidad física, fisiológica, genética, mental, económica, cultural o social. Incluye información expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica, electrónica, visual o de cualquier otro tipo. La frase no abarca la información que no identifica a una persona en particular (o no puede usarse de manera razonable para identificarla)" (…) (Comité Jurídico Interamericano CJI de la Organización de los Estados Americanos, 2021),(Protección Datos Pers, 2021).

3.3 Datos personales

Cabe destacar que la información pública, que abarca aspectos relacionados con el estado civil de las personas y aquellos datos incluidos en registros públicos. Por su naturaleza, no se necesita la autorización del titular para su uso. Los Datos se define en el artículo 5 de la ley 1581 de 2012 y el artículo 3 del Decreto 1377 de 2013, comprenden:

como aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos (Ley Estatutaria 1581 de 2012, Art. 5, 2012).

La ley establece que el tratamiento de datos sensibles está prohibido salvo en excepciones. Estas excepciones incluyen situaciones en las que el titular ha dado su consentimiento explícito, es necesario para proteger la vida del titular cuando esté física o jurídicamente incapacitado, el tratamiento es realizado por ONGS o entidades sin ánimo de lucro con fines políticos, filosóficos o sindicales, siempre que se refieran a sus miembros, es necesario para el reconocimiento o ejercicio de un derecho en un proceso judicial o tiene una finalidad histórica, estadística o científica."

Por su naturaleza, los datos sensibles requieren protección especial de los responsables y encargados de su tratamiento. Es importante aclarar que estos responsables no son simplemente las personas designadas en la empresa para manejar los datos, sino que se refiere a la empresa y socios comerciales que puedan recibir dichos datos.

3.4 Políticas de protección de datos personales

Los responsables y encargados del tratamiento de información tienen la obligación de implementar políticas de protección de datos personales, según lo estipulado en la ley 1581 de 2012 y el decreto 1377 de 2013. Estas políticas, también conocidas como políticas de privacidad, deben incluir:

- Identificación del responsable
- Tratamiento y finalidad de los datos
- Derechos de los titulares
- Responsable de atención
- Procedimiento de ejercicio de derechos
- Vigencia

Cualquier cambio sustancial en estas políticas debe ser comunicado previamente a los titulares.

3.5 Registro nacional de base de datos

La ley de protección de datos personales establece la creación del Registro Nacional de Base de Datos (RNBD), administrado por la Superintendencia de Industria y Comercio (SIC). Este registro garantiza el derecho de los titulares a conocer quiénes son los responsables del tratamiento de su información (Registro Nacional de Bases de Datos, RNBD., 2015).

Es obligatorio para algunos responsables del tratamiento de información inscribir sus bases de datos en el RNBD.

Autoridad de Protección de Datos en Colombia

La ley 1581 de 2012 Articulo 19, establece que la autoridad de protección de datos en Colombia es la Superintendencia de Industria y Comercio, a través de la Delegatura de Protección de Datos Personales. Esta entidad se encarga de garantizar el respeto a los principios, derechos y garantías establecidos en la ley (Ley 1581 de 2012, Art. 19, 2012).

Según el artículo 21 de la ley 1581 de 2012, la Superintendencia de Industria y Comercio tiene funciones, como velar por el cumplimiento de la legislación de protección de datos, investigar, promover los derechos de las personas, impartir instrucciones, administrar el Registro Nacional Público de Bases de Datos, entre otras. (Ley 1581 de 2012, Art. 19, 2012)

3.6 Superintendencia de industria y comercio (SIC)

La Superintendencia de Industria y Comercio (SIC) es la entidad encargada de supervisar y controlar las relaciones comerciales en Colombia, con un énfasis particular en la protección de los derechos de los consumidores

La SIC tiene varias delegaturas encargadas de desarrollar diferentes funciones.

- Delegatura de propiedad intelectual.
- Delegatura Protección al Consumidor.
- Delegatura para el Control y Verificación de Reglamentos Técnicos y Metrología legal.
- Delegatura para la Protección de la Competencia.
- Delegatura para Asuntos Jurisdiccionales.
- Delegatura para la Protección de Datos Personales.

Cuenta con varias dependencias entre estas la Delegatura para la Protección de Datos Personales, establecida por la entrada en vigor de la Ley 1581 de 2012.

La Delegatura para la Protección de Datos Personales tiene la responsabilidad de vigilar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos establecidos en la ley. Además, es la encargada de supervisar y regular los procedimientos de la ley 1266 de 2008, especialmente en lo relacionado con datos personales.

Estas normas eran urgentes dada la globalización, la apertura de mercados, la inversión extranjera, el comercio electrónico y las nuevas tecnologías, por ende, un riesgo para los derechos de los titulares de la información.

La protección de los datos personales implica una serie de obligaciones que las empresas deben cumplir, el uso indebido de los datos puede vulnerar derechos fundamentales como la intimidad, la dignidad humana y el derecho a la honra, e incluso inducir al suicidio.

Es recomendable revisar regularmente las políticas de protección, diseñarlas en función de la empresa y los principios rectores de protección de datos, también es necesario capacitar a empleados y contratistas para notificar cualquier filtración de información o falla de seguridad a la Superintendencia y a los titulares.

Siguiendo estas recomendaciones, se puede reducir el riesgo de incumplimiento de la normativa de protección de datos y las sanciones correspondientes por parte de la Superintendencia de Industria y Comercio. Es importante tener en cuenta que, entre septiembre de 2020 y agosto de 2021, esta entidad impuso multas significativas, en su mayoría por quejas ciudadanas relacionadas con suplantación de identidad en reportes a centrales de riesgos de información financiera.

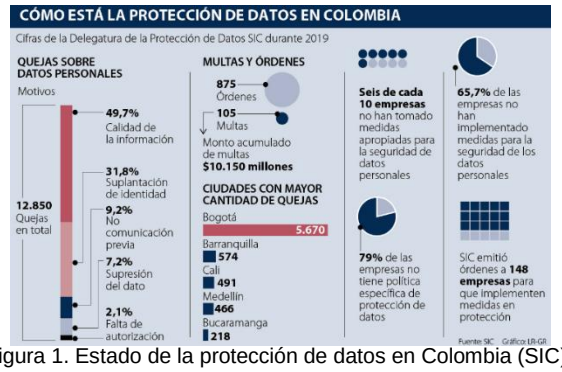


Figura 1. Estado de la protección de datos en Colombia (SIC)

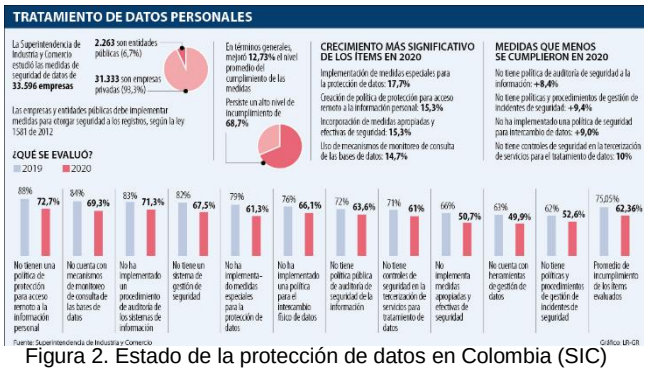


Figura 2. Estado de la protección de datos en Colombia (SIC)

En la figurar 1 se muestra las estadísticas de protección de datos de la SIC en el año 2019, y en la figura 2 se observa como estamos en materia de protección de datos.

Los motivos más frecuentes de los reclamos son: la calidad de la información (49,7%); la suplantación de la identidad (31,8%); la no comunicación previa (9,2%); la supresión del dato (7,2%); y la falta de autorización (2,1%).

Un estudio entregado por la SIC en diciembre del año pasado, se observó que 65,7% de las empresas y las entidades públicas no han implementado medidas apropiadas y efectivas para garantizar la seguridad de los datos personales.

Por ciudades, Bogotá y Barranquilla son las que registraron el mayor número de quejas, con 5.670 y 574 respectivamente. A estas, les sigue Cali, con 491; Medellín con 466; y Bucaramanga, con 218.

3.7 Derecho a la privacidad Internet de las cosas

El derecho a la privacidad ha sido un componente esencial de la condición humana desde tiempos antiguos. La necesidad de mantener ciertos aspectos de nuestra vida fuera del escrutinio público es crucial para el desarrollo de nuestra individualidad. Un ejemplo significativo es la conceptualización presentada por Warren y Brandeis en 1890. *El derecho a la privacidad, como parte del derecho más general, es el derecho a la propia personalidad.* (Warren & Brandeis, 1890)

En la segunda mitad del siglo pasado, la Corte Suprema de Estados Unidos introdujo otro concepto del derecho a la privacidad. "*la idea de que el derecho a la vida privada, en última instancia, implicaba la libertad de tomar decisiones personales sin interferencias externas*. Este enfoque se evidencia en casos como Griswold (1965), Eisenstadt (1972) y Roe (1973), donde se ratifica el derecho de las personas a tomar decisiones libres de influencias externas y a mantener la confidencialidad de sus asuntos personales (Corral Talciani, 2000).

3.8 Interpretación del derecho a la privacidad

Como señala Herrera, tanto la jurisprudencia como la doctrina enfrentan una tarea difícil al intentar determinar cuándo una situación vulnera la privacidad de un individuo y cuáles son los límites entre lo público. En consecuencia, es necesario establecer límites para evitar la colisión entre ambos espacios, el público y el privado. Un ejemplo de esto es una conversación telefónica en un espacio público, la cual puede ser igual de privada que una conversación realizada en la intimidad de nuestro hogar (Herrera Carpintero, 2016).

4 Desarrollo Jurisprudencial

Para llevar a cabo un análisis sobre los principios de protección y tratamiento de los datos personales en Colombia, es esencial referirse a lo estipulado en el artículo 230 de la Constitución Política de 1991, que establece lo siguiente:

Los Jueces, en sus providencias, sólo están sometidos al imperio de la ley. La equidad, la jurisprudencia, los principios generales del derecho y la doctrina son criterios auxiliares de la actividad judicial" (…) (Constitución Política 1 de 1991 Asamblea Nacional Constituyente, Art. 230, 1991). Después con la Sentencia (Sentencia No. T-414 de 1992, 1992) se observa la vinculación entre el derecho a la intimidad y el derecho al habeas data, en los siguientes términos:

Se protege la intimidad para asegurar la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas, como un derecho de la personalidad.

Durante 20 años este derecho consagrado en la Constitución de 1991 no tuvo desarrollo legislativo, fue exigible a través de los mecanismos constitucionales establecidos en el artículo 23, el Derecho de Petición, y el artículo 86, la Acción de Tutela.

En este contexto, el derecho al habeas data experimentó un amplio desarrollo jurisprudencial, con sentencias como la T-161 de 1993 y la C-913 de 2010, que fueron fundamentales para dar contenido a las leyes estatutarias 1266, relacionada con el habeas data financiero, y 1581, referente al habeas data en general.

El derecho al habeas data fue primero interpretado como una garantía del derecho a la intimidad, de allí que se hablara de la protección de los datos personales, la vida privada y familiar, se entiende como el espacio individual impenetrable en la que cada uno puede realizar su proyecto de vida donde ni el Estado ni otros particulares pueden interferir." (Sentencia C-748, 2011).

Así mismo, en la Sentencia T-414 de 1992 la Corte delimitó el objeto de protección del habeas data, así:

El dato es un componente material de ser convertido en información cuando se inserta en un modelo que lo relaciona con otros datos y hace posible que dicho dato adquiera sentido. El dato que constituye un elemento de la identidad de la persona, que en conjunto con otros datos sirve para identificarla a ella y solo a ella, y por lo tanto sería susceptible de usarse para coartarla, es de su

propiedad, en el sentido de que tendría ciertos derechos sobre su uso (Sentencia No. T-414 de 1992, 1992).

A partir de lo expuesto anteriormente, se puede afirmar que el principal legado de la Corte Constitucional en relación con la protección de datos personales permite determinar si la actividad de tratamiento de datos se está llevando a cabo de manera adecuada. En estas sentencias, se centró en gran medida en los datos de carácter financiero y crediticio, principios que fueron incorporados en las leyes estatutarias 1266 y 1581.

La Superintendencia de Industria y comercio, a través, de la Delegatura para la Protección de Datos Personales, ha emitido varias decisiones que buscan la protección del habeas data de los usuarios a quienes se les realiza tratamiento de datos personales, entre las más recientes se encuentra:

La Resolución 30412 de 2020, se analizó el caso de un fotógrafo contratado para una sesión de fotos en un hotel. Posteriormente, estas fotos se publicaron en la Revista Caras, basándose en una autorización de propiedad intelectual que firmó el fotógrafo. (Resolución 30412 Del 23 de Junio de 2020 (fotógrafo).)

(Resolución 12192 Del 1 de Abril de 2020, Facebook, 2020) La Ley Estatutaria 1581 de 2012 es adaptable a las políticas de Facebook Inc. Por la recolección de datos abusiva sin el permiso o consentimiento de los titulares de la información al recolectar datos personales en Colombia a través de software instalado en los navegadores de los equipos.

Confirmó la resolución 1321 de 2019, mediante la cual ordenó a la sociedad Facebook, adecuaciones a su política de protección de datos, para fortalecer el cumplimiento de la ley 1581/12 (Superintendencia de Industria y Comercio).

Además, señaló que la Sociedad Facebook debe poder demostrar la eficiencia en sus políticas de protección de datos. (Resolución 12192 Del 1 de Abril de 2020, Facebook, 2020) SIC, 2020).

5 El Internet de las Cosas

5.1 Definición de IoT

El término internet de las cosas (IoT) se da a finales del siglo pasado, exactamente en 1999, cuando Kevin Ashton, del grupo Procter & Gamble, crea un grupo de investigadores en el Tecnológico de Massachussets (MIT), que se dedicaban a investigar información sobre la identificación por radiofrecuencia en red (RFID) y tecnologías de sensores (Wikipedia, 2021).

Siendo este el origen, la definición del concepto internet de las cosas (IoT) lo podemos concretar que es una colección de objetos ilimitados permanentemente conectados en un escenario digital que aspiran a que todo funcione correctamente, mediante la utilización de la información recolectada.

El primer dispositivo conectado a lo que hoy conocemos como Internet fue una tostadora en 1990. Esta tostadora estaba conectada a la red a través del protocolo TCP/IP y su funcionamiento era gestionado mediante una base de información de SNMP MIB. El dispositivo disponía de un interruptor para encender y apagar, mientras que la intensidad de tostado se ajustaba según el tiempo que permaneciera activa (Cheta & Ashton, 2023).

La llegada del siglo XXI y el avance tecnológico ha permitido la interconexión de una amplia gama de dispositivos, que van desde electrodomésticos y sistemas de seguridad hasta vehículos y equipos médicos. En la actualidad, se estima que hay cientos de millones de estos dispositivos conectados a Internet, y se proyecta que esta cifra aumentará a billones en los próximos años (Fernandez, 2023).

Hoy en día nos referimos a escenarios en los que las capacidades de red y la capacidad informática se extienden a objetos físicos, "Objetos que normalmente no se considera que podían conectar al internet y realizar acciones según la información", lo que ahora estos dispositivos pueden crear, intercambiar y utilizar datos con una mínima intervención humana (Rose et al., 2015).

5.2 Historia y evolución del IoT

El primer objeto conectado a Internet fue realizado por John Romkey en 1990. Diseño una tostadora que se podía encender y apagar a través de Internet para la conferencia INTEROP de octubre de 1989 (Cheta & Ashton, 2023).

Como resultado de ese hecho y con la llegada del nuevo milenio comenzaron a aparecer cada vez más dispositivos conectados a Internet.

- **2000:** LG introdujo lo que ahora se considera uno de los dispositivos emblemáticos del Internet de las cosas: publica su primera nevera conectada a internet.

- **2003-2004**: El término "Internet de las cosas" comienza a tener mayor importancia cuando aparece en importantes publicaciones de la época como The Guardian, Scientific American y Boston Globe.

- **2005:** Internet de las cosas alcanza un nuevo nivel cuando la sección de las Naciones Unidas y la UIT publica su primer informe sobre el tema.

- **2005:** Surge arduino como plataforma para desarrollar aplicaciones basadas en Thing of Internet.

- **2006-2008**: Obtiene reconocimiento por parte de la comunidad europea, se realiza la primera conferencia IoT en Europa.

- **2008-2009**: surge finalmente IoT al superar el número de dispositivos conectados con el número de habitantes.

- **2010**: El gobierno chino reconoce el IoT como una tecnología clave y anuncia su inclusión en su plan de desarrollo a largo plazo.
- **2011**: La firma de investigación de mercado Gartner incluye al IoT en su "ciclo comparación y validación", un gráfico que mide la popularidad de una tecnología en comparación con su utilidad real a lo largo del tiempo.

- **2013**: Google Glass surge como un avance revolucionario en IoT de la tecnología portátil, aunque fue adelantado a su tiempo experimentó un fracaso significativo.

- **2014:** Amazon no pasa desapercibido desarrolla Echo, un altavoz de manos libres que se controla con la voz.

- **2016**: General Motors, Lyft, Tesla y Uber están realizando pruebas con vehículos autónomos. Sin embargo, también se confirma el primer ataque masivo de malware de IoT.

- **2017-2019**: El desarrollo de IoT se vuelve más económico, accesible y ampliamente aceptado, lo que genera pequeñas olas de innovación en toda la industria.

- **2023**, se invirtieron aproximadamente 805.000 millones de dólares estadounidenses en tecnología de Internet de las cosas (IoT) en todo el mundo. (Fernadez, 2023)

Se espera el crecimiento continúe acelerándose del 2023 a 2025, alcanzando 27.000 millones de dispositivos conectados a IoT en todo el mundo (Fernandez, 2023).

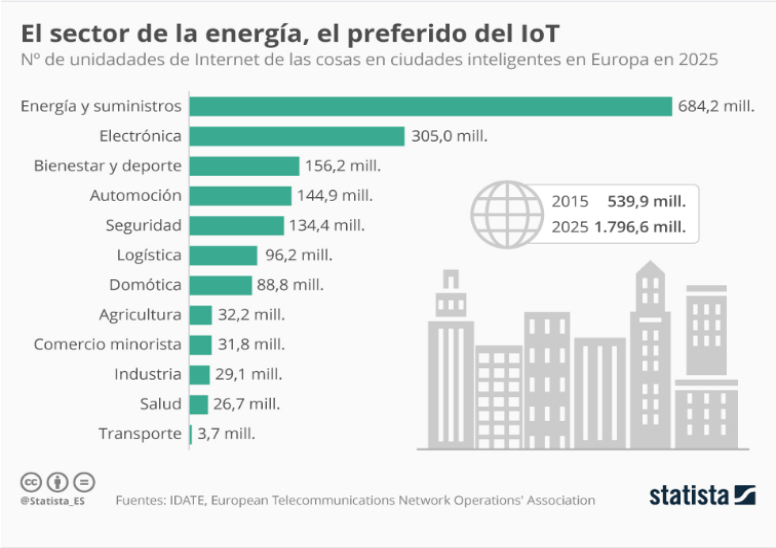


Figura 3. El sector energético lidera el crecimiento del IoT en Europa

El número total de dispositivos conectados a Internet de las Cosas (IoT) en Europa ha experimentado un crecimiento del 233% entre 2015 y 2025, pasando de 539,9 millones a 1.796,6 millones, según un informe de la Asociación Europea de Operadores de Redes de Telecomunicaciones (ETNO). Además, el sector de la energía y los suministros liderará este incremento, representando casi un tercio del total con 685 millones de dispositivos, impulsados principalmente por la adopción de contadores inteligentes para medir el consumo de electricidad y gas.

A nivel global el IoT tiene una gran aplicabilidad en diversas áreas mejorando la eficiencia, la seguridad, y la calidad de vida. En la siguiente tabla se muestras las áreas donde más se ha implementado IoT y los países correspondientes.

ÁREAS DE APLICACIÓN DEL IoT A NIVEL GLOBAL				
ÁREA	**JAPÓN**	**ESTADOS UNIDOS**	**REINO UNIDO**	**EU**
SALUD	Monitores de glucosa Dispositivos de presión arterial Monitoreo remoto de pacientes en hospitales y clínicas	Dispositivos de monitoreo continuo de glucosa que envían datos a aplicaciones móviles para el manejo de la diabetes	Dispositivos de monitoreo de glucosa que envían datos a plataformas en línea para ayudar a la gestión de la diabetes	Dispositivos de monitoreo remoto como los monitores de glucosa o presión arterial, que transmiten datos para su análisis.
ENERGÍA	Los medidores inteligentes y sistema de paneles solares, que registran y envían datos de consumo eléctrico para una gestión más eficiente de la energía	Medidores inteligentes que registran el consumo eléctrico y permiten una gestión más eficiente del uso de energía.	Medidores inteligentes que registran el consumo energético y permiten una gestión más eficiente de los recursos	Medidores inteligentes monitorizar y gestionar su consumo de electricidad en tiempo real.
SEGURIDAD Y VIGILANCIA	Cámaras de seguridad y alarmas conectadas, para conocer imágenes en tiempo real	Cámaras de seguridad conectadas que permiten a los usuarios acceder a imágenes en tiempo real a través de aplicaciones móviles.	Cámaras de vigilancia que permiten el acceso remoto a imágenes y datos grabados.	Cámaras de seguridad que transmiten imágenes y datos en tiempo real.
VEHÍCULOS	Sistemas de navegación y asistencia al conductor en vehículos que recopilan y procesan datos de tráfico en tiempo real	Sistemas avanzados de asistencia al conductor (ADAS) y vehículos autónomos que recopilan datos para mejorar la seguridad y la eficiencia del tráfico	Sistemas de asistencia al conductor que recopilan datos para mejorar la seguridad y la navegación	Sistemas de navegación y asistencia al conductor que recopilan y procesan datos para mejorar la seguridad vial
AGRICULTURA	Sensores IoT que monitorean condiciones del suelo y clima para optimizar el riego y el uso de fertilizantes en los cultivos	Sensores IoT que monitorizan las condiciones del suelo y las necesidades de riego para optimizar el uso de agua y fertilizantes	Sistema de monitoreo de las condiciones del suelo y el clima para optimizar el riego y la gestión de cultivos	Monitorear las condiciones del suelo y el uso de recursos en la agricultura.
GESTIÓN DE RESIDUOS	Contenedores de basura inteligentes que notifican a las autoridades cuando están llenos y cuando deben ser vaciados	Sensores inteligentes en contenedores de basura que notifican a las autoridades sobre el nivel de llenado y la necesidad de vaciado	La Agencia de Protección Ambiental (Environment Agency) regula los dispositivos utilizados en los contenedores de basura inteligentes	Contenedores de residuos inteligentes para validar el nivel de llenado y planificación de la recolección.

Tabla 1. Campos de aplicación IoT a nivel global

Al comparar el estado actual del Internet de las Cosas (IoT), observamos su adopción en una amplia variedad de campos, respaldada por marcos normativos cada vez más sólidos que fortalecen la protección de datos y la seguridad de los datos.

Al evaluar las distintas regulaciones sobre protección de datos, se observó que muchos países colaboran activamente para fortalecer sus políticas de protección de datos y así garantizar la seguridad y privacidad de la información a nivel global.

En la siguiente tabla se muestras las áreas donde más se ha implementado IoT y los países correspondientes de la región y Asia.

ÁREAS DE APLICACIÓN DEL IoT A NIVEL GLOBAL			
ÁREA	**CHINA**	**BRASIL**	**COLOMBIA**
SALUD	Dispositivos de monitoreo de glucosa en sangre que transmiten datos a plataformas en línea para el control y gestión de diabetes.	Dispositivos de monitoreo de glucosa o presión arterial que transmiten datos para la gestión de condiciones de salud crónicas	Dispositivos de monitoreo de glucosa y presión arterial.
ENERGÍA	Medidores inteligentes que registran el consumo de electricidad para una gestión más eficiente	Medidores inteligentes que registran y reportan el consumo eléctrico para una mejor gestión energética	Empresa **Celsia**, ha empezado a implementar medidores inteligentes. Implementación de sistemas IoT para controlar y gestionar el alumbrado público y semafórico
SEGURIDAD Y VIGILANCIA	Cámaras de seguridad que transmiten datos en tiempo real y almacenan imágenes para la vigilancia.	Cámaras de seguridad que procesan datos y grabaciones deben cumplen, la ley LGPD, protección de datos	cámaras inteligentes, Botones de pánico y Dispo. Rastreo, drones con cámaras, control de acceso inteligente
VEHÍCULOS	Sistemas de asistencia al conductor y recopilan datos para la navegación y seguridad.	Sistemas avanzados de asistencia al conductor y vehículos autónomos que recopilan datos para mejorar la seguridad vial	Sistema de pago de peajes inteligente
AGRICULTURA	Sensores de suelo y sistemas de riego inteligentes que optimizan el uso de agua y fertilizantes	Sensores IoT utilizados para monitorear condiciones del suelo y optimizar el uso de recursos en la agricultura	Sistemas de riego automatizados. monitoreo del suelo. permiten gestionar de manera más eficiente el riego y los insumos agrícolas. No hace referencia a ninguna Norma
GESTION DE RESIDUOS	Contenedores de basura inteligentes que monitorizan el nivel de llenado y optimizan la recolección de residuos	Contenedores de basura inteligentes que informan sobre el nivel de llenado y optimizan la recolección de residuos.	En algunas ciudades, se están utilizando contenedores de basura inteligentes. No hace referencia a ninguna norma

Tabla 2. Campos de aplicación IoT a nivel regional y Asia

Evaluar y fortalecer la implementación de estándares regulatorios para el Internet de las Cosas (IoT) en Colombia, tomando como referencia el marco normativo del Reglamento General de Protección

de Datos (GDPR) de la Unión Europea, con el fin de garantizar la protección de datos y la seguridad de la información en proyectos IoT en Colombia.

Al comparar la regulación existe en Colombia con otras regiones, se evidencia la necesidad de ampliar las definiciones para abordar de manera más efectiva los desafíos que plantea la evolución tecnológica.

BASES LEGALES PARA EL TRATAMIENTO DE DATOS PERSONALES	
Reglamento General de Protección de datos RGPD-GDPR	**Normativa Colombiana de Protección de Datos Ley 1581 del 2012**
1) Consentimiento para el tratamiento de datos	La ley 1581 del 2012, tiene una única base. 1) Consentimiento para el tratamiento de datos.
2) Ejecución de un contrato y/o aplicación de medidas precontractuales	
3) Cumplimiento de una obligación legal.	
4) Proteger intereses vitales.	
5) Interés legítimo.	
6) Interés público.	

Figura 4. Bases legales para el tratamiento de datos vs RGPD

En la tabla anterior se evidencia una diferencia significativa en las bases legales para el tratamiento de datos personales. Actualmente, la Ley 1581 de 2012 en Colombia establece únicamente el consentimiento como base legal. En contraste, regulaciones como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea contemplan cinco bases legales adicionales, lo que les otorga mayor flexibilidad y adaptabilidad para regular nuevas tecnologías.

Esta discrepancia representa una desventaja considerable para Colombia en la gestión y regulación de tecnologías emergentes.

Al evaluar el concepto de dato personal en Colombia, solo se limita a identificar una persona, basado en la constitución Política del 1991 como identificar el sexo, número de identificación, lugar de residencia entre otros. La regulación analizada aparte de los datos mencionados relaciona datos tecnológicos como: dirección IP, datos de navegación e incluso la fotografía de una persona es un dato personal. Esto ha permitido mejorar el despliegue de internet de las Cosas (IoT), respaldadas con un marco robusto de políticas y regulaciones que evolucionan de manera paralela.

Otra desventaja de la regulación colombiana en materia de protección de datos es el rol del Oficial de Protección de Datos.

Principales funciones que tiene el Oficinal de protección de datos en Colombia y comparado con el delegado de protección de datos de otras regulaciones.

Aspecto	Oficial de Protección de Datos en Colombia (OPD)	Delegado de Protección de Datos Unión Europea (DPD)
Base Legal	Regulado por la ley 1581 de 2012 no es obligatoria asignar un OPD	El DPD Está regulado por la ley GDPR de la UE es obligatorio en entidades públicas o privadas
Obligatoriedad	No es obligatorio en las organizaciones tener un OPD,	La asignación de un DPD es obligatoria, especialmente para entidades públicas o entidades que manejan volúmenes de datos
Funciones	Es responsabilidad del OPD que las entidades cumplir con la normativa ley 1581 de 2012. Trabaja de la mano con con la SIC	Tiene funciones más específicas: supervisar el cumplimiento del GDPR. Asesoría en la EIPD Intermediario entre la organización y las autoridades de PD de la UE
Relación con autoridades de control:	El OPD puede actuar con la SIC, autoridad encargada en la protección de datos	El DPT mantiene una comunicación con las autoridades de protección de datos como (Data Protección Authorities)
Requisitos de formación	No especifica requisitos específicos para el OPD	El DPD debe tener conocimientos especializados en derecho y prácticas de protección de datos
Autonomía	El OPD no tiene un nivel de independencia legal estrictamente establecida. Se espera que pueda actuar con autonomía	El DPD debe actuar con total independencia y no recibir instrucciones respecto a cómo llevar a cabo sus tareas
Sanciones por incumplimiento	La SIC Puede imponer sanciones a las empresas que no cumplan con la norma de PD.	El no asignar un DPD y el incumplimiento de la ley GDPR tiene multas hasta del 4% de la facturación anual o hasta 20 millones de euros

Tabla 3. Diferencias delegadas de protección de datos

La SIC en su manual de protección de datos 2023, menciona las posibilidades y características que puede contribuir la asignación de un Oficial de protección de datos, pero sin embargo este mismo manual indica que no es obligatorio tener un área específica para este cargo o contratar con terceros.

En países como España, las regulaciones en materia de protección de datos, lideradas por la Agencia Española de Protección de Datos (AEPD), exigen la asignación obligatoria del Delegado de Protección de Datos (DPD).

Para ayudar a garantizar el cumplimiento normativo. Estos roles tienen funciones claramente definidas y trabajan en estrecha en colaboración con las autoridades reguladoras para garantizar la correcta implementación de las normativas y proteger los derechos de los ciudadanos en materia de datos personales.

6 Internet de las cosas en Colombia

6.1 Estrategia Nacional Digital de Colombia 2023-2026

Actualmente los datos y las tecnologías están revolucionando la forma en que las personas, empresas y gobiernos interactúan, abriendo nuevas oportunidades para enfrentar desafíos tecnológicos como el Internet de las Cosas (IoT). En este contexto, Colombia se destaca como uno de los países de América Latina y el Caribe que más ha avanzado en su camino hacia la digitalización (Banco Mundial, 2023).

Sin embargo, el país aún enfrenta importantes desafíos para cerrar las brechas en el acceso, uso y apropiación de las tecnologías digitales entre hogares, entidades públicas, empresas y territorios. Abordar estas disparidades es fundamental para impulsar el desarrollo digital de Colombia.

Un ejemplo claro de esta situación es la conectividad digital, donde existen marcadas diferencias entre las regiones. Según datos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y el Departamento Administrativo Nacional de Estadística (DANE), en el cuarto trimestre de 2022 la penetración de Internet fijo en hogares varió significativamente: 6% en zonas rurales dispersas, 11,6% en áreas rurales, 25,8% en ciudades intermedias, y 68% en centros urbanos y aglomeraciones, con un promedio nacional del 50,7%.

Para facilitar el acceso, uso y apropiación de los datos y las tecnologías digitales se plantea como un asunto central a lo largo de todo el Plan Nacional de Desarrollo 2022-2026 “Colombia, Potencia Mundial de la Vida”, destacando que la conectividad y la transformación digital son elementos clave para promover otras transformaciones relevantes en el país como el internet de las cosas.

En Colombia, varios proyectos han sido implementados utilizando Internet de las Cosas. sectores como la agricultura, las ciudades inteligentes, la salud y la industria.

Smart Agro: El sector cafetero está viviendo una transformación significativa gracias a la implementación de tecnologías avanzadas como el Internet de las Cosas (IoT) en el marco del concepto de Smart Agro. Este enfoque combina herramientas como sensores IoT, análisis de datos y sistemas de monitoreo en tiempo real para supervisar variables críticas del cultivo, como la humedad y la temperatura del suelo. Estas innovaciones permiten optimizar el uso de recursos

clave, como agua y fertilizantes, promoviendo una agricultura más sostenible, eficiente y orientada a maximizar la calidad y cantidad de la producción.

6.2 Ciudades Inteligentes

Medellín: Ha sido un pionero en la implementación de soluciones IoT. Ha desarrollado proyectos que incluyen la sincronización de semáforos, sistemas de monitoreo de tráfico en tiempo real y sensores que gestionan el alumbrado público de manera eficiente. Además, el proyecto "Medellín Digital" promueve el uso de tecnologías IoT para mejorar la seguridad, la gestión de residuos y la calidad del aire.

Bogotá: Sistema Integrado de Transporte Público (SITP): ha implementado un sistema que utiliza IoT para monitorear el tráfico, optimizar las rutas y mejorar la experiencia del usuario. Los buses están equipados con sensores que envían datos en tiempo real sobre la ubicación, la velocidad y el estado del vehículo.

Salud y Energía

Telemedicina en Zonas Rurales: En varias regiones rurales, se han implementado sistemas de telemedicina utilizando IoT. Los dispositivos conectados permiten a los médicos monitorear a distancia los signos vitales de los pacientes y enviar alertas en caso de anomalías y proporcionar diagnósticos y consultas en tiempo real.

Monitoreo de Enfermedades Crónicas: Se han implementado dispositivos portátiles (wearables) que monitorean continuamente la salud de pacientes con enfermedades crónicas como la diabetes y la hipertensión.

Gestión de Recursos y Energía

Enel-Codensa: Ha implementado los medidores inteligentes como parte de su estrategia de modernización de redes eléctricas y mejora del servicio. Esto ayuda gestionar más eficiente el servicio eléctrico, tanto para los usuarios como para la empresa, al ofrecer ventajas significativas, como:

Lectura remota: Los medidores inteligentes eliminan la necesidad de visitas físicas para la lectura del consumo eléctrico, ya que transmiten datos en tiempo real.

Detección de fallas: Ayudan a identificar interrupciones o irregularidades en el suministro eléctrico de manera inmediata, facilitando una respuesta más ágil.
Consumo en tiempo real: Permiten a los usuarios monitorear su consumo eléctrico desde aplicaciones o plataformas digitales, promoviendo un uso más eficiente de la energía.
Facturación precisa: Al registrar el consumo exacto, evitan estimaciones y errores comunes en los sistemas tradicionales.
Conexión y desconexión remota: Ofrecen la posibilidad de realizar estos procesos sin la necesidad de intervención física, ahorrando tiempo y costos.

Acueducto de Bogotá: La Empresa de Acueducto y Alcantarillado de Bogotá ha inicado el despliegue sensores IoT en su red de distribución de agua para monitorear la presión y detectar fugas en tiempo real. Esto ha permitido una respuesta más rápida a las emergencias y una mejor gestión del recurso hídrico.
Lectura remota: Permiten recopilar datos de consumo en tiempo real a través de sistemas inalámbricos, eliminando la necesidad de visitas físicas para la lectura.
Monitoreo en tiempo real: Ofrecen información detallada del consumo de agua, lo que facilita el seguimiento por horas, días o meses.
Detección de fugas: Alertan sobre fugas o consumos anómalos, ayudando a prevenir el desperdicio de agua y reduciendo costos para los usuarios.
Facturación precisa: Garantizan lecturas exactas, evitando estimaciones y disputas por errores en las facturas.
Integración con plataformas digitales: Los datos de los medidores inteligentes pueden visualizarse a través de aplicaciones móviles o portales web, lo que proporciona mayor control a los usuarios.
En América del Norte, la penetración de IoT es alta gracias al despliegue avanzado de redes 5G y un ecosistema de innovación robusto. En Europa, los proyectos de IoT están fuertemente alineados con iniciativas de sostenibilidad y ciudades inteligentes. En América Latina, Brasil y México lideran la región en implementación de IoT, mientras que Colombia está en una posición intermedia en términos de avance

Según el informe **IESE Cities in Motion Index 2022**, Colombia ha mostrado esfuerzos por avanzar en el desarrollo de ciudades inteligentes. Sin embargo, la tendencia indica que los países líderes en este ámbito en la región son Brasil, México y Chile, que han implementado soluciones tecnológicas más integradas y sostenibles en sus entornos urbanos.

6.3 Servicios Públicos

El Internet de las Cosas (IoT) está avanzando rápidamente en Colombia, aunque aún existen retos por superar. En 2024, se proyecta que el número de dispositivos IoT en el país superará los 100 millones, con aplicaciones que abarcan sectores como la agricultura, la industria y las ciudades inteligentes. A nivel de consumo, ya es común encontrar dispositivos domésticos conectados, como asistentes de voz y sistemas de seguridad.

El uso de IoT en empresas colombianas está creciendo, particularmente en áreas como la logística, el monitoreo de flotas de vehículos y la gestión de energía, mejorando la eficiencia y reduciendo costos. En el sector agrícola, por ejemplo, se utilizan sensores para monitorear variables que afectan los cultivos. Sin embargo, aunque muchas empresas están adoptando IoT, aún hay un largo camino por recorrer. Solo el 60% de las empresas colombianas han integrado estrategias de transformación digital.

A pesar de los avances, se necesitan políticas más claras y un mayor enfoque en la formación especializada para que el IoT se convierta en una parte integral de la economía colombiana.

En el ámbito de los servicios públicos como el agua y electricidad, el IoT permite integrar medidores inteligentes que recolectan, procesan y transmiten datos en tiempo real, mejorando la eficiencia en la gestión del consumo de energía y agua. Estos dispositivos monitorean parámetros clave como el consumo, calidad, flujo, y envían la información a través de redes de comunicación hacia plataformas de análisis, donde se pueden realizar diagnósticos y optimizaciones automáticas.

Beneficios del IoT en los servicios públicos

Para las empresas:

1. Eficiencia operativa:
    - Reducción de pérdidas y optimización del uso de recursos.
    - Automatización de procesos, como la lectura remota de medidores y el diagnóstico de fallas.
2. Reducción de costos**:**
    - Optimización de rutas de mantenimiento y recolección.
    - Minimización de desperdicios en redes de distribución.
3. Toma de decisiones basada en datos:
    - Uso de analítica avanzada para prever demandas, detectar anomalías y planificar inversiones.

Para los usuarios:

1. Transparencia:
   - Acceso en tiempo real a información sobre consumo y costos.
2. Control:
   - Monitoreo personalizado del uso de recursos a través de aplicaciones móviles o portales web.
3. Ahorro:
   - Identificación de hábitos de consumo ineficientes y ajuste del uso de los servicios.

Para el medio ambiente:

1. Sostenibilidad:
   - Reducción del desperdicio de recursos como agua, energía y gas.
   - Menor huella de carbono gracias a redes optimizadas y recursos renovables.
2. Monitoreo ambiental:
   - Mejora en la gestión de residuos y control de la calidad del aire y el agua.

6.4 Medidores inteligentes energía AMI en Colombia

Sin duda los Smart Cities está transformando las ciudades del mundo con tecnologías que antes no era posible ahora con la actualización de dispositivos que ofrecen opciones avanzadas, mayor precisión de la medición del consumo, control energético, identificar patrones de consumo, se elimina la opción de lecturas manuales, etc.

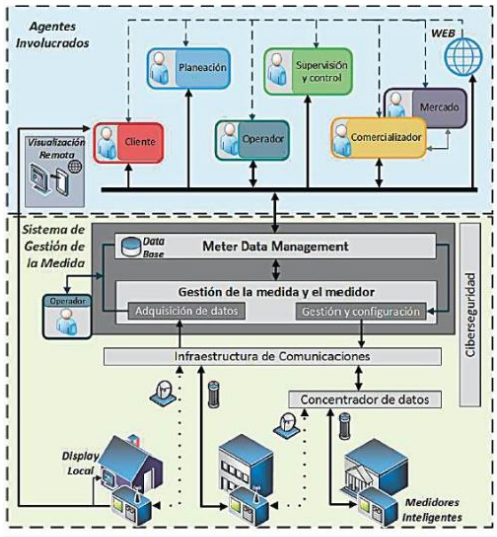


Figura 1
Esquema general sistema AMI.

Figura 5. Diagrama de funcionamiento sistema AMI

En la figura anterior se muestra el diagrama por bloques del funcionamiento de un medidor AMI, los cuales son implementados actualmente en el país.

Infraestructura de comunicación

La comunicación de datos entre el medidor y el sistema de gestión puede llevarse a cabo de varias maneras: primeramente, de manera directa desde el medidor hasta el centro de control o mediante un concentrador de datos que agrupa la información de varios medidores antes de enviarla al centro de gestión. La red de comunicaciones abarca no solo los medios físicos, sino también las herramientas, recursos y estrategias esenciales para salvaguardar la ciberseguridad de la información en el sistema.(Universidad del Norte, 2018).

Sistema de gestión de la medida

Se divide en dos componentes principales:

1. La gestión de la medida, representada por el medidor, que se ocupa de recibir y enviar datos entre el equipo y el sistema.

2. La administración de datos del medidor (MDM), que se encarga de almacenar y procesar toda la información recopilada. El vínculo interno del Sistema de Gestión de la medida encapsulada la información vinculada a la operación, fluyendo incesantemente a través de la red de comunicaciones.

Colombia ha iniciado un proceso gradual para la implementación de medidores inteligentes en todo el país. Este esfuerzo, realizado en conjunto con las empresas distribuidoras de energía Enel, busca modernizar el sistema de medición y fomentar una mayor eficiencia energética.

La Comisión de Regulación de Energía y Gas ha informado que el avance en la vinculación de medidores está progresando de manera satisfactoria. Además, se han elaborado y publicado resoluciones para su revisión y posterior implementación. Desde el año 2018 la (Resolución 40072 DE 2018, n.d.) se ha definido los requisitos y metas para el despliegue de estos medidores inteligentes en todo el país.

El gobierno nacional proyecta para el 2030 llegar a un 75% de la implementación de este sistema, en zonas urbanas un 95% (12 millones de usuarios) y en zonas rurales el 50% (2 millones de usuarios) (Luis, 2021). Aunque no se han reportado fugas de datos masivas específicas relacionadas con medidores inteligentes en Colombia, el contexto regulatorio actual sugiere que

este es un riesgo latente. La falta de un marco claro puede permitir la implementación de tecnologías vulnerables, y cualquier incidente podría tener consecuencias graves.

La fuga de datos podría tener impactos significativos tanto en la privacidad de los usuarios como en la credibilidad de los programas de modernización tecnológica en el sector energético y otros servicios públicos.

La ausencia de una regulación clara y específica para el Internet de las Cosas (IoT), que incluya a los medidores inteligentes, deja vacíos legales que pueden ser explotados. Las empresas proveedoras de servicios pueden implementar medidores sin las medidas de protección adecuadas.

Colombia cuenta con la Ley 1581 de 2012, que regula la protección de datos personales, esta ley no aborda específicamente las particularidades del manejo masivo de datos que se genera con los medidores inteligentes. Esto incluye la falta de directrices sobre cómo se debe obtener y gestionar el consentimiento de los usuarios.

6.5 Medidores inteligentes agua MIA

El Proyecto **MIA** (Medición Inteligente de Agua) se implementó en las instalaciones del hospital, Fundación Santa Fe de Bogotá donde se instalaron dos medidores ultrasónicos también en el Hotel Grand Hyatt y el Centro Empresarial 156 son los primeros usuarios pioneros en la instalación del sistema que se compone de un medidor ultrasónico con modem incorporado para telemetría, más el uso de plataformas digitales para la gestión de datos en conjunto con otras tecnologías como Inteligencia artificial desarrollado por el equipo de ingenieros de la Empresa de Acueducto de Bogotá.

Figura 6. Medidor inteligente de agua MIA Funcionamiento

En la figura anterior se observa la instalación del primero medidor MIA en Bogotá

Los medidores inteligentes MIA se comunican vía dispositivos móviles como celulares y Tablet, registran la lectura cada 30 minutos, es decir, se tienen 48 lecturas diarias del medidor. El usuario tiene la facilidad de monitorear e identificar adecuadamente las posibles anomalías o desviaciones, controlar su propio consumo, racionalizar los costos y ajustar sus hábitos de consumo de agua.

Este sistema está diseñado para ayudar a los consumidores a controlar y optimizar el uso del agua, proporcionando estadísticas en tiempo real, alertas para la gestión de procesos productivos y detección temprana de fugas internas. Con estos datos, cada cliente puede monitorear de cerca su consumo y avanzar en sus programas ambientales.

El usuario se beneficia de la gestión de datos: visualiza sus consumos en una plataforma con acceso controlado. Descarga sus datos seleccionando los años, meses, días u horarios de su interés. Visualiza sus curvas y tendencias de consumo de agua.

Figura 7. Medidor inteligente de agua, proceso instalación MIA

En la figura anterior se observa los primeros registros de un medidor en operación y posteriormente son enviados esos datos a un centro de procesamiento.

Según Cristina Arango, gerente de la Empresa de Acueducto y Alcantarillado de Bogotá (EAAB), la telemetría, o la lectura remota de medidores, es una parte esencial de la modernización sostenible que la empresa ha implementado. Esta tecnología impulsa la transformación digital del servicio de agua y fomenta un cambio cultural hacia ciudadanos más informados, responsables y comprometidos con el medio ambiente.

- Empresas Públicas de Medellín (EPM): EPM ha estado implementando medidores inteligentes de agua en algunos sectores de la ciudad.

- Emcali (Empresas Municipales de Cali): ha explorado la implementación de medidores inteligentes en algunos barrios de Cali.

Con la digitalización del consumo de agua, surge la necesidad de garantizar la seguridad y privacidad de los datos recolectados por estos dispositivos. La regulación en Colombia debe abordar una amplia gama de aspectos técnicos, legales y de protección al consumidor. Un marco regulatorio sólido debe garantizará que la implementación de estos dispositivos sea segura, eficiente y confiable.

7 Tarjetas inteligentes de transporte público

7.1 Tarjeta Tullave Transmilenio

Es el medio de pago utilizado para desplazarse en el sistema de transporte público, incluyendo Transmilenio, el SITP y otros servicios complementarios y especiales. Las tarjetas *Tú Llave*, cuando están personalizadas, ofrecen beneficios como descuentos en transbordos, viajes a crédito y recuperación del saldo en caso de pérdida.

7.2 ¿Cuáles son las clases de Tarjeta tú llave?

- **Tarjeta Básica o anónima**

  Esta tarjeta tiene un **costo de $8000 (COP), no requiere de** los datos personales del usuario para su uso y no tiene ningún tipo de beneficio.

- **Tarjeta Personalizada**

  Personalizada con los datos del usuario, tiene varios beneficios como descuento en transbordos, viajes con pasajes fiados o a crédito y recuperación del saldo en caso de pérdida.

- **Tarjeta Personalizada Especial**

  Este tipo de tarjetas son subsidiadas, dirigidas a población adulto mayor y personas en condición de discapacidad y estudiantes. Debe estar personalizada cuenta con beneficios como descuentos por transbordos, viaje a crédito, recuperación del saldo en caso de pérdida y descuentos adicionales dirigidos a esta población.

7.3 ¿Cuáles son los beneficios de Tú llave?

- Ahorra tiempo evitando, esperar devolución de dinero, reduce el riesgo de pérdida o robo de dinero.
- Disminuye costos asociados al manejo del dinero recaudado, como transporte y contabilidad.
- Facilita la entrada y salida de pasajeros, reduciendo los tiempos de espera.
- La tarjeta Tú llave, permite obtener descuentos por trasbordos.
- Hasta 2 viajes a crédito para que puedas movilizarse en el Sistema cuando la Tarjeta Tú llave no está recargada. Protección del saldo por pérdida o robo de la tarjeta
- Para los adultos mayores de 62 años y personas en condición de discapacidad, existen descuentos adicionales.

7.4 Formas de recarga las tarjetas Tú llave digitalmente

Para realizar la recarga digital a través de aplicaciones móviles o páginas web, es indispensable tener acceso a internet. Esto puede ser un inconveniente para personas que no cuentan con una conexión estable o con planes de datos limitados.

Las transacciones en línea pueden estar sujetas a problemas de seguridad, como fraudes, robo de datos personales o intentos de phishing. Los usuarios que no toman las precauciones adecuadas pueden estar expuestos a estos riesgos.

Las Recargas digitales son desde 9.000 hasta 200.000 pesos a través de aplicaciones autorizadas como app más y pagina web del Transmilenio entidades bancarias.

Para poder disfrutar de la recarga digital una vez efectuado el pago, es necesario activar la recarga 30 minutos más tarde en los puntos físicos o a través de los dispositivos identificados con el icono rosado.

Las recargas por medio de estas aplicaciones tienen un costo adicional de 300 pesos adicional.

Figura 7. Sistema de recarga Tu llave con aplicaciones

En la figura anterior muestra el proceso para recargar la tarjeta tu llave por medio de las diferentes aplicaciones, pero a la vez debe esperar 30 minutos para hacer efectiva la recarga y luego debe acercase a un validador de pasajes ubicado en las estaciones y tiene un costo adicional de 300 pesos.

7.5 Riesgos de datos en las tarjetas Tú llave de Transmilenio

Problemas de recarga

- La red para recarga es limitada en algunas zonas, especialmente en áreas periféricas, lo que dificulta a los usuarios reponer saldo de manera ágil.
- No todas las máquinas o puntos de recarga están en funcionamiento o disponibles en horarios extendidos.

Falta de integración total

- Aunque las tarjetas permiten acceso al SITP y TransMilenio, no están completamente integradas con otros sistemas de transporte, como bicicletas públicas o transporte intermunicipal, lo que limita su funcionalidad.

Tecnología limitada

- Fallas frecuentes en los validadores o lectores, que a veces no reconocen la tarjeta correctamente.
- Algunas tarjetas presentan desgaste rápido, lo que obliga a los usuarios a reemplazarlas y generar un gasto adicional.

Inconvenientes con saldo no utilizado

- Si un usuario pierde su tarjeta, el saldo acumulado no se puede recuperar fácilmente, lo que genera molestias y pérdida de dinero.
- No hay devolución del saldo en caso de que la tarjeta ya no sea utilizada por el usuario.

Falta de flexibilidad en pagos electrónicos

- Aunque se han introducido avances, como la recarga en línea, el proceso no siempre es eficiente o accesible para todos los usuarios, en particular para quienes no están familiarizados con las tecnologías digitales.

Riesgo de clonación o pérdida de datos

En 2016, las autoridades en Bogotá desmantelaron una red criminal dedicada a la clonación de tarjetas de transporte público en sistema de transporte Transmilenio y SITP. Este grupo se especializaba en manipular los datos de las tarjetas del transporte masivo para replicar en otras tarjetas electrónicas utilizadas por los usuarios.

Una vez clonadas, estas tarjetas eran vendidas a precios significativamente más bajos. Con esta operación ilícita, lograron defraudar al sistema de transporte público por un monto superior a los 27 mil millones de pesos colombianos**.**

El impacto de estas actividades no solo representó un perjuicio económico considerable para el sistema, sino que también afectó la sostenibilidad del modelo de transporte masivo, cuyo financiamiento depende en gran medida de los ingresos por la venta de pasajes. Además, este caso destacó las vulnerabilidades en los sistemas tecnológicos utilizados para el recaudo y la necesidad

de implementar medidas más robustas de seguridad cibernética y controles para evitar el robo de información personal.

Tras el escándalo generado por la clonación de tarjetas en la capital del país, el distrito analizo la situación y saco de circulación las tarjetas monedero de color azul y tarjeta cliente frecuente de color roja.

Pero después se observó que las tarjetas personalizadas eran utilizadas de forma indebida para la reventa ilegal de pasajes en distintos puntos de la ciudad. Este problema generó preocupación entre las autoridades, quienes comenzaron a implementar medidas de control y vigilancia para evitar el uso fraudulento de las tarjetas y preservar la integridad del sistema de transporte público.

- Desde julio del 2018 a julio de 2019 la policía ha decomisado 1963 tarjetas y emitido 111 comparendos y así mismo recaudo Bogotá ha bloqueado 1552 tarjetas que presenta conductas irregulares con el uso.
- En agosto del 2022. La policía ha identificado más 250 puntos en la ciudad dedicados a la venta ilegal de pasajes del SITP y Transmilenio.
- En enero del 2023. La policía ha incautado más 100 tarjetas Tú llave destinadas a la reventa de pasajes.
- En mayo del 2024 La policía recuperó 71 tarjetas del SITP que eran usadas para venta ilegal de pasajes en Bosa.

7.6 En otros países se regula de esta manera

En Estonia, luego de separase de la unión soviética y de enfrentar infinidad de ataques cibernéticos en el 2007, se volvió pionero en el despliegue de Blockchain para proteger su infraestructura de datos. Actualmente tiene el 99% de sus servicios digitalizados como salud, Justicia, negocios y servicios Públicos. Desde entonces, se ha implementado por clientes más exigentes del mundo, incluidos numerosos gobiernos y empresas líderes en telecomunicaciones, aeroespacial, defensa, energía, servicios financieros y seguros.

Además, mediante la implementación de la “X-Road”, una plataforma segura de intercambio de datos, los ciudadanos tienen control sobre quién puede acceder a su información personal y en qué circunstancias, promoviendo la transparencia y el respeto a la privacidad.

El compromiso de Estonia con la ciberseguridad ha sido pionero, especialmente desde los ataques cibernéticos de 2007, que impulsaron la creación del Centro de Excelencia de Cooperación en Ciberdefensa de la OTAN en Tallin. Gracias a estos esfuerzos, Estonia es hoy un referente global en protección de datos y un modelo para otros países interesados en construir una infraestructura digital segura y efectiva.

En el año 2022, el ministerio de las tecnologías de la información y las comunicaciones (MINTIC) público un documento llamado Guía de Referencia de Blockchain para Adopción e Implementación de Proyectos en el Estado Colombiano. Es un documento orientado a facilitar la comprensión y aplicación de la tecnología Blockchain en entidades públicas del país. Su objetivo principal es promover el uso de esta tecnología como una herramienta estratégica para mejorar la transparencia, seguridad, eficiencia y confianza en los procesos gubernamentales.

Los casos de uso implementados con esta tecnología en el país son:

Contrato Inteligente, Agencia nacional de tierras:

- Vigilancia de los documentos de procedimientos de adjudicación de predios “judicial-restitución”
- Trazabilidad, uso y modificación de estos documentos
- Se garantiza el vínculo entre propietario y predio plasmado
- Se garantiza la integridad de las resoluciones

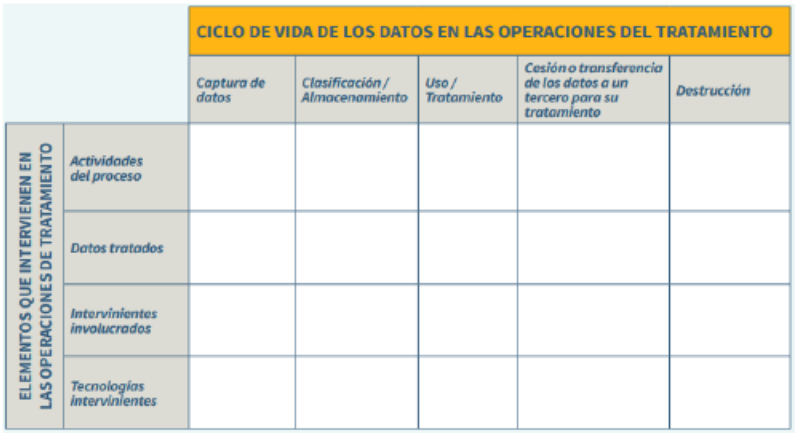
Contrato inteligente Trazabilidad de los diplomas

- Validar la autenticidad de los documentos
- Validar las personas asociadas a los actos administrativos del estado
- Se logró reducir la falsificación documentos y alteración de credenciales mediante la inserción de condenas de bloque

De acuerdo a lo mencionado y cumpliendo con el objetivo de la guía, podemos sugerir la protección de datos con este sistema. Teniendo cuenta que esta guía el Mictic al desarrollo basada en la experiencia de Estonia.

Las principales característica y herramientas en la protección de datos de Estonia y de la Unión Europea son:

EIPD significa **Evaluación de Impacto en la Protección de Datos**. Es una herramienta clave establecida en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, diseñada para identificar y minimizar riesgos en el tratamiento de datos personales.



		CICLO DE VIDA DE LOS DATOS EN LAS OPERACIONES DEL TRATAMIENTO				
		Captura de datos	Clasificación / Almacenamiento	Uso / Tratamiento	Cesión o transferencia de los datos a un tercero para su tratamiento	Destrucción
ELEMENTOS QUE INTERVIENEN EN LAS OPERACIONES DE TRATAMIENTO	Actividades del proceso					
	Datos tratados					
	Intervinientes involucrados					
	Tecnologías intervinientes					

Figura 8. Guía ciclo de vida de los Datos

En la figura anterior se muestra un ejemplo de una guía. Es esencial incorporar material gráfico que facilite la identificación de los elementos principales de manera clara y concisa. Una estrategia efectiva para lograrlo es el uso de diagramas, los cuales no solo simplifican la comprensión de información compleja, sino que también permiten visualizar relaciones, procesos y conceptos de forma estructurada.

Los diagramas pueden actuar como herramientas clave para sintetizar información, resaltar puntos críticos y comunicar ideas de manera más eficiente, mejorando así la interpretación y el análisis de los datos presentados.

Para estas actividades, además de documentar los motivos por los que se llega a la conclusión de que tienen un riesgo, se realiza un análisis de mínimos que simplifica el proceso de análisis de riesgos. Para empezar, se necesitan describir de manera adecuada las actividades de tratamiento.

El responsable de asegurar que se cumplen todas las normas desde que se recogen los datos hasta que se destruyen, con las fases que se muestran a continuación

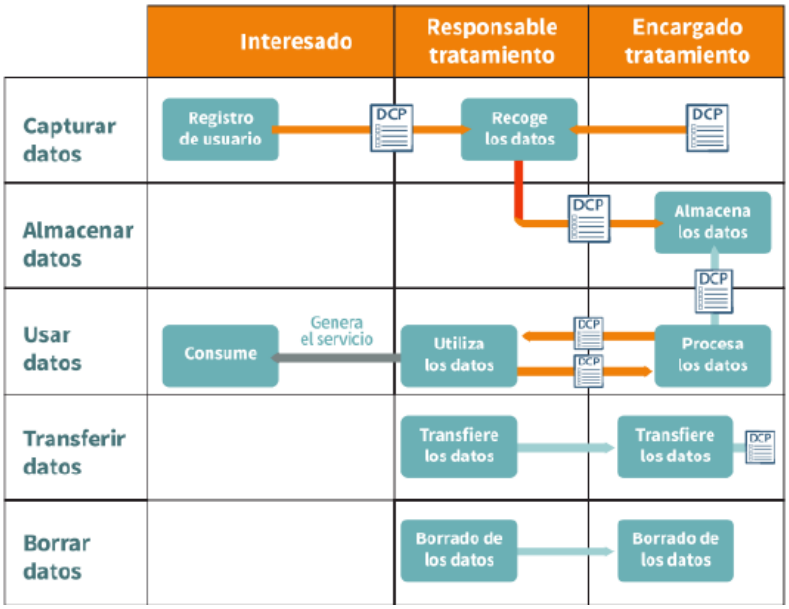


Figura 9. Ciclo de vida de los datos, recolección hasta su destrucción

En la figura anterior se observa de forma clara las responsabilidades de cada persona en el proceso, usuario interesado, responsable y encargado del tratamiento de datos. También se visualiza el flujo de información, desde el registro del usuario hasta el posible borrado de datos, incluyendo el almacenamiento, uso y transferencia de los mismos, que pueden ser realizados por el responsable o el encargado.

El proceso inicia desde la recolección de datos hasta su eliminación final. Este diagrama proporciona una representación visual clara de cada fase involucrada, permitiendo una comprensión detallada de cómo los datos se gestionan y procesan a lo largo de su ciclo de vida.

La agencia Nacional española en materia de protección de datos tiene estructurado sus fichas técnicas y diagramas en materia de protección de datos desde el registro del usuario hasta el posible borrado de datos, incluyendo el almacenamiento, uso y transferencia de los mismos, que pueden ser realizados por el responsable o el encargado.

Software para simular el diseño de un Evaluación de Impacto

Figura 10. Herramienta PIA, Evaluación de Impacto de la privacidad

En la figura anterior se observa una de las herramientas usadas por la Comisión Nacional de Informática y Libertad La entidad francesa (CNIL). Esto les ha permitido mitigar los riesgos asociados a los datos en los procesos de recolección durante la implementación de tecnologias.

Privacy Impact Assement (**PIA**) consiste en una guía creada para cumplir la normativa y una aplicación para poder hacer la EIPD. Además de formularios para rellenar, cuenta con una serie de conceptos del RGPD que se pueden ir mirando a la hora de realizar una EIPD.
Con estas herramientas podemos mejora la ley actual 1581del 2012, ayudando a mitigar los riesgos que pueden tener los datos personales.

8 Regulación actual del internet de las cosas en Colombia

8.1 Desarrollo legislativo

Como se evidenció previamente, el avance jurisprudencial en torno al derecho de protección de datos personales en el ámbito financiero ha sido notable. Aunque estos precedentes jurisprudenciales representaron logros significativos. En este contexto, 16 años después de la emisión de la Sentencia T-414 de 1992, el Congreso de la República de Colombia y el artículo 1526 de la Constitución Política, incorporó por medio de leyes estatutarias las garantías delineadas por la Corte Constitucional.

Estas leyes serán abordadas en orden cronológico de su promulgación: la ley sectorial 1266 de 2008, la Ley General de Protección de Datos Personales 1581 de 2011.

8.2 Problemática actual derecho a la privacidad

El rápido avance de las nuevas tecnologías ha llevado a que la información personal de los usuarios se encuentre en un delicado equilibrio entre su uso eficiente y la transgresión del derecho a la privacidad. El consentimiento es crucial al autorizar la recopilación y utilización de datos, tanto de forma expresa como mediante una información completa proporcionada con antelación.

La falta de conocimiento por parte de los consumidores sobre qué datos se recopilan y cómo se utilizan, poniendo en riesgo derechos fundamentales. La transgresión del derecho a la privacidad surge cuando las empresas utilizan los datos de formas no previstas, cuando la información recopilada excede el propósito original.

El Internet de las cosas plantea desafíos, ya que la cantidad de datos recopilados puede exponer la privacidad a problemas como la interceptación o el monitoreo malicioso. La falta de control sobre los datos personales una vez recopilados y la necesidad de eliminar o prohibir su uso posterior, en este contexto, la falta de consentimiento informado eficazmente se presenta como el factor más significativo en las vulneraciones al derecho a la privacidad relacionadas con el Internet de las cosas.

8.3 Habeas Data

El “hábeas Data” se rige actualmente como una herramienta de protección preventiva de la libertad, instrumento que en ocasiones va ligado a disposiciones especiales para los bancos de datos. En América Latina hay una tendencia particular que rige el Habeas Data como un instrumento de garantía consagrado en la constitución estatal” (Zuñiga, 1997).

(N, Remolina, 1994) señala que el Habeas Data es una institución jurídico de litigio especial que tiene por objeto específico: el acceso a la información, garantizando el derecho de una persona a saber qué tratamientos se realizan sobre sus datos; (datos de mora de una persona o de antecedentes penales, cuando ya ha solventado la deuda u obtenido la rehabilitación); corregir datos inexactos, corregir información errónea y eliminar la información denominada confidencial que, aunque sea correcta, una persona todavía tiene derecho a solicitar su eliminación.

Después de consagrarse el derecho de hábeas data en la Constitución Política, el legislativo promulgó la Ley 1266 de 2008, “que establece disposiciones generales sobre el hábeas data y regula su manejo de la información contenida en bases de datos personales. Especialmente la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”, cuya aplicación se vio limitada.

8.4 Constitución Política de 1991

El derecho al Habeas Data, según la Constitución Política de 1991, se presenta como un derecho fundamental autónomo, aunque fundamentado en el derecho a la intimidad. Este derecho incluye la facultad del individuo de ejercer un control permanente sobre los datos personales utilizados por los recolectores de datos (Constitución Política de la República de Colombia, 1991).

El Habeas Data ha evolucionado como un derecho autónomo en Colombia, permitiendo a los individuos conocer, rectificar, autorizar, suprimir y limitar el uso de sus datos personales. Respaldado por la libertad de expresión y el derecho a la información, garantiza la corrección de datos inexactos, asegurando el control y protección de la información conforme a los principios de libertad, dignidad humana y responsabilidad social.

8.5 Ley de protección de datos 1266 del 2008

La expedición de la ley 1266 representó un avance en materia regulatoria del Habeas Data, su implementación no fue la adecuada frente a todo lo que se refiere al manejo y protección de datos personales, todavía existen grandes brechas, lo que hace que los problemas aumenten por la falta de regulación; La problemática en la gestión de bases de datos en diferentes organizaciones (públicas y/o privadas) ha llevado a la necesidad de desarrollar nuevas leyes que regulen los datos personales de forma general e integral en muy diversos ámbitos, tanto comerciales como financieros (Ley 1266 de 2008, 2008).

Por lo anteriormente expuesto, en el año 2012, el Congreso expide la Ley 1581 “que establece disposiciones generales en materia de protección de datos personales”, con el objetivo de desarrollar derechos constitucionales que corresponden a todas las personas. En este sentido, en 2012, el congreso aprobó la Ley 1581, “que establece normas generales en materia de protección de datos personales”, con el objetivo de desarrollar derechos constitucionales que corresponden a todas las personas.(Ley 1581 de 2012, 2012)

Otra desventaja de esta ley es que no incluye en sus definiciones ni principios el llamado "derecho al olvido", adoptado internacionalmente por la necesidad constante de proteger la privacidad de los ciudadanos, cuando se les busca en internet, por su popularidad es actualmente la principal fuente de acceso a información.

Lo anterior impide que se ejerza en su totalidad el derecho de cancelación de datos que supone la destrucción de los datos almacenados en registros o bancos de datos dado que no contempla los llamados motores de búsqueda dentro de la definición legal de registro o banco de datos, quedando expuesta la información personal de las personas sin que consientan en ello, aun cuando se haya solicitado su eliminación de la base de datos que originalmente los recopiló.

Es así como ‘‘en la práctica, el derecho al olvido en Internet no es otra cosa que una definición de política pública que declara a los motores de búsqueda como responsables de bases de datos, lo que permite que los titulares de datos personales puedan hacer efectivo su derecho a cancelación de estos datos respecto del buscador. Otro punto para considerar es que la ley dentro del ámbito de datos personales distingue entre datos sensibles y datos puramente personales, pueden ser públicos o privados (Ortíz & Viollier, P80, 2021).

Artículo 1. Esta ley regula el derecho constitucional de las personas a conocer, actualizar y rectificar sus datos personales en bancos de datos, garantizando las libertades y derechos relacionados con la recolección, tratamiento y circulación de información, conforme a los artículos 15 y 20 de la Constitución Política (Ley 1581 de 2012, 2012).

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 los bancos de datos y en archivos de entidades públicas y privadas (Constitución Política de La República de Colombia, Art. 15, 2024).

Artículo 12. Requisitos especiales para fuentes. Las fuentes deberán actualizar mensualmente la información suministrada al operador, sin perjuicio de lo dispuesto en el Título III de la presente ley.(Ley 1266 de 2008, Art. 12, 2008)

Artículo 20. Derecho a la liberta de opinión información y presan**.** Se garantiza a toda persona la liberta de expresar y difundir su pensamiento y opiniones la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva (Constitución Política 1 de 1991, Art. 20, 1991)**.**

8.6 Ley de protección de datos personales 1581 del 2012

El contexto histórico del nacimiento de la ley 1581 del 2012, data del año 1991, del artículo 15 de la constitución Política de Colombia 1991, el objetivo de esta ley es desarrollar el derecho constitucional que tiene todas las personas a conocer, actualizar y ratificar la información que se hayan recogido en base de datos, banco de datos y en archivos de entidades públicas y privadas" cuando el responsable o encargado no establecido en el territorio nacional le será aplicable la legislación colombiana (Ley 1581 de 2012).

Aunque esta ley contiene principios y garantías protegiendo a los usuarios frente al tratamiento de datos personales, otorgándoles derechos como el de acceso, modificación, bloqueo y cancelación de datos a quien sea responsable para proteger el derecho a la privacidad de personas naturales y jurídicas.

También constituyó un gran avance en su momento para mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo en el territorio Nacional.

Hoy en día con el avance de la transformación digital, la industria 4.0 y la expansión del comercio electrónico se ha producido un acelerado intercambio de información haciendo que la ley no cubra todos los aspectos tecnológicos.

Existe un grave problema con el control y tratamiento de datos personales en que, a veces, la falta de información de los organismos encargados de recopilar datos produce que las personas no saben de haber firmado contratos por prestar su consentimiento dada la magnitud del desarrollo de las nuevas tecnologías.

La falta de control e información genera desconocimiento que los consumidores ni siquiera se enteran de su derecho a la privacidad está siendo vulnerado permitiendo que aquellos organismos dedicados al almacenamiento y tratamiento de datos personales pasen desapercibidos debido a la falta de certeza en el flujo de información.

El organismo administrativo a cargo del control de esta actividad y el principio, en definitiva, es la superintendencia de industria y comercio a través de una Delegatura para la Protección de Datos Personales.

8.7 Decreto 1377 del 2013

El Decreto 1377 de 2013 de Colombia fue emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) como una reglamentación complementaria de la Ley 1581 de 2012, conocida como la Ley de Protección de Datos Personales. Esta ley fue diseñada para garantizar la protección de la privacidad de los ciudadanos en un contexto en el que el tratamiento de datos personales se ha incrementado considerablemente debido al avance tecnológico y la digitalización. El Decreto 1377 establece disposiciones adicionales y define procedimientos específicos para asegurar la correcta implementación de la Ley 1581, con el objetivo principal de resguardar los derechos de los titulares de los datos en cuanto a su recolección, almacenamiento, uso, circulación y supresión.

El decreto regula aspectos clave como la obtención del consentimiento previo, expreso e informado de los titulares de los datos, así como la obligación de las entidades responsables de implementar políticas de seguridad adecuadas para proteger la información personal. Además, establece las condiciones bajo las cuales las bases de datos pueden ser recopiladas y gestionadas, aclarando el alcance y los límites del tratamiento de datos sensibles, como la información relacionada con la salud, creencias religiosas, opiniones políticas, entre otros.

También se incluye el derecho de los titulares a acceder, actualizar y rectificar sus datos personales, garantizando así un control más directo sobre la información que se recopila sobre ellos. Asimismo, el Decreto 1377 de 2013 introduce mecanismos de transparencia y responsabilidad para las entidades que manejan datos personales, al tiempo que regula la creación de registros de bases de datos, asegurando que toda recopilación de datos esté debidamente registrada ante la autoridad competente (Decreto 1377 de 2013).

A pesar de que el Decreto 1377 establece medidas claras para la protección de datos personales, en algunos aspectos puede resultar ambiguo, lo que podría generar dificultades de interpretación y aplicación. Por ejemplo, la definición exacta de "consentimiento" y los procedimientos adecuados para obtenerlo pueden variar entre diferentes entidades, lo que puede llevar a inconsistencias en su implementación. Esto puede crear incertidumbre para las empresas y las autoridades en cuanto a cómo cumplir con las disposiciones del decreto, además de dificultar la aplicación efectiva de la ley en escenarios prácticos.

El Decreto también depende en gran medida de la Autoridad Nacional de Protección de Datos Personales para establecer y supervisar políticas de protección, pero la capacidad y recursos de esta entidad pueden ser limitados en cuanto a la cobertura y la rapidez con que se aborden las violaciones. Esto puede crear cuellos de botella y retrasos en la respuesta a los incidentes de violación de datos personales, reduciendo la eficacia de la legislación.

8.8 Ley de acceso a la información pública: Ley 1712 de 2014

La Ley 1712 de 2014 fortalece la rendición de cuentas y la lucha contra la corrupción al obligar a las entidades a ser más transparentes y facilitar la participación ciudadana. Además, busca equilibrar el derecho a la información con la protección de la privacidad y otros derechos fundamentales. Esta ley promueve una gestión pública más abierta y accesible, reconociendo la importancia de la información como un bien público esencial para la democracia y el desarrollo social.

El artículo 6 de dicha norma introduce dos categorías clave en la noción de datos públicos:

"c) Información pública clasificada. Se refiere a la información que, estando en posesión o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica. Su acceso puede ser negado o excepcionado, siempre y cuando se cumplan circunstancias legítimas y necesarias, así como los derechos particulares o privados consagrados en el artículo 18 de esta ley;

e) Información pública reservada. Se trata de la información que, estando en poder o custodia de un sujeto obligado en su calidad de tal, está excluida de acceso por parte de la ciudadanía debido al perjuicio a los intereses públicos y en cumplimiento de todos los requisitos establecidos en el artículo 19 de esta ley"(Ley 1712 de 2014)*.*

Datos abiertos. Se refieren a todos aquellos datos primarios o no procesados, presentes en formatos estándar e interoperables que facilitan su acceso y reutilización. Estos datos están bajo la custodia de entidades públicas o privadas que desempeñan funciones públicas y se ponen a disposición de cualquier ciudadano de manera libre y sin restricciones, con el objetivo de que terceros puedan reutilizarlos y crear servicios derivados de los mismos." (Ley 1712 de 2014)

Estas clasificaciones respaldan las excepciones al derecho de acceso a la información pública, permitiendo a las entidades denegar la divulgación de información a terceros cuando dicha revelación pueda afectar los derechos individuales o el interés público.

ANÁLISIS REGULATORIO EN COLOMBIA CUADRO QUE AGRUPEN ASPECTOS TÉCNICOS DE IOT				
ASPECTO	**Ley 1266 de 2008**	**Ley 1581 de 2012**	**Ley 1712 de 2014**	**GDPR (UE)**
ÁMBITO DE APLICACIÓN	También conocida como Ley de Habeas Data Financiero. Regulación del manejo de información crediticia, comercial, financiera y de servicios.	Aplica a todas las entidades, públicas y privadas, que realicen tratamiento de datos personales en Colombia.	También conocida como Ley de Transparencia y Acceso a la Información Pública, regula el derecho de acceso a la información pública en Colombia.	Datos personales en la UE y entidades fuera de la UE que procesan datos de la UE.
PRINCIPIOS	Calidad de los datos Autorización del titular.	Legalidad, Finalidad Libertad, seguridad.	Publicidad Transparencia Participación.	Legalidad. Transparencia Minimización de datos Integridad.
DERECHOS DEL TITULAR/INDIVIDUO	Acceso Rectificación Actualización	Acceso, Rectificación, Actualización, Supresión y Revocación del consentimiento.	Acceso a la información pública. Promoviendo la participación ciudadana	Amplios derechos que incluyen acceso, rectificación, supresión, portabilidad, restricción del tratamiento, oposición y derecho al olvido.
CONSENTIMIENTO	Autorización del titular requerida	Previo, expreso e informado del titular, excepto en casos especificados por la ley (como la ejecución de un contrato o la obligación legal)	No aplica específicamente.	Consentimiento explícito, libre y específico del titular de los datos. El consentimiento debe ser verificable y puede ser retirado en cualquier momento
SEGURIDAD DE LA INFORMACIÓN	Confidencialidad y protección de datos.	Medidas técnicas y administrativas.	No aborda seguridad de datos personales.	Seguridad por diseño y por defecto.
TRANSFERENCIA INTERNACIONAL	No regula explícitamente.	Requiere nivel adecuado de protección.	Requiere nivel adecuado de protección.	Permite transferencias a países con decisiones de adecuación. Si no hay adecuación, se pueden usar cláusulas contractuales estándar
EVALUACIÓN DE IMPACTO DE PRIVACIDAD	No aplica.	No aplica.	No aplica.	Requiere para tratamientos de alto riesgo.
NOTIFICACIÓN DE BRECHAS	No regula explícitamente.	No regula explícitamente.	No regula explícitamente.	Obligatoria dentro de 72 horas.
SANCIONES	Multas y medidas correctivas.	Multas y medidas administrativas.	No aplica	Multas de hasta 20 millones de euros o el 4% del ingreso global anual.

Tabla 4. Leyes de protección datos en Colombia VS otras regulaciones

En el cuadro anterior se presenta un análisis comparativo entre la normativa colombiana y la Unión Europea. Este estudio evidencia diferencias significativas, tanto en el ámbito de aplicación como en los derechos reconocidos a los titulares de la información. Mientras que la normativa europea, establece un enfoque más amplio y riguroso en la protección de datos personales, la normativa colombiana, aunque alineada con principios internacionales, presenta ciertas limitaciones en cuanto a su alcance y nivel de detalle. Estas diferencias reflejan las prioridades y enfoques regulatorios de cada región, lo que resalta la necesidad de fortalecer la armonización normativa para fomentar la protección integral de los derechos de los titulares en un mundo cada vez más globalizado.

9 El derecho comparado: El lugar al que realmente queremos ir

9.1 Definición derecho comparado

Es una disciplina jurídica que se ocupa del estudio y análisis de las distintas normativas, sistemas legales y principios jurídicos existentes en diferentes países o culturas. Su objetivo es identificar similitudes y diferencias entre las diversas tradiciones legales y, a partir de ahí, extraer conclusiones que puedan enriquecer la comprensión y el desarrollo del derecho en distintos contextos.

Un ejemplo de su aplicación es el uso del derecho comparado para estudiar cómo otros países han abordado cuestiones específicas, como el derecho de familia o protección de datos, regulación de tecnologías como IoT y, a partir de ese análisis, adaptar o aplicar soluciones similares en cada país en el contexto legal.

9.2 Regulación europea al internet de las cosas

La Unión Europea (UE) es una organización política y económica conformada por 27 países europeos que cooperan en diversas áreas, como economía, política, medio ambiente, comercio y derechos humanos. Su objetivo principal es promover la integración y el desarrollo sostenible, asegurando la paz, la prosperidad y la estabilidad en la región.

La Unión Europea no solo es una unión económica, sino también un proyecto político que busca la cooperación estrecha entre naciones, basándose en valores como la democracia, la igualdad y los derechos humanos.

Logros importantes

- Creación del mercado único, que permite la libre circulación de personas, bienes, servicios y capital.
- Normativas ambientales pioneras a nivel global.
- Pionera en derechos digitales y protección de datos con leyes como el GDPR

Un ejemplo es Estonia hace parte de la UE, y es pionera en el despliegue de tecnología Blockchain, el 99% de sus servicios están digitalizados, actualmente trabaja de la mano con la OTAN.

Estados Unidos apenas está comenzando a regular el ámbito del Internet de las Cosas (IoT), centrando sus esfuerzos principalmente en la seguridad empresarial. Sin embargo, aún quedan

aspectos pendientes como garantizar el consentimiento informado de los consumidores para el uso de sus datos, fomentar la transparencia sobre cómo se maneja la información, y otorgar a las agencias reguladoras la facultad de sancionar a las empresas que incumplan la normativa.

10 Leyes de la Unión Europea

La Unión Europea comienza a regular el Internet de las Cosas desde una cierta base de desconfianza frente a las empresas y los desarrolladores de aparatos electrónicos, por lo que se debe comprender, con base a escepticismo, que el Estado debe favorecer y proteger a las personas frente a estas nuevas tecnologías, por lo que se dice que en Europa “la regulación se considera fundamental para proteger la equidad y competencia”(Feldgen, 2008).

Una manera de proteger esta equidad y competencia que se mencionaba anteriormente es por medio de la Comisión Europea, que es una de las instituciones de la Unión Europea, encargada de regular estos asuntos promoviendo investigaciones, controlando el desarrollo y fijando políticas en todos los países miembros del bloque.

Estas políticas tuvieron un giro dramático en el continente el año 2014 con la sentencia del Caso Costeja, cuyo litigio finalmente decanto por una protección más dura al derecho a la privacidad de las personas, en su esfera del derecho al olvido cibernético, el cual lo podemos definir como el derecho “a que la información publicada en línea en Internet no permanezca fija e intangible, ya que todas las personas tienen una segunda oportunidad como también a la protección de los datos personales, ya que Google tuvo que borrar todas las referencias al caso de embargo que afectaba al señor Costeja (Ángela, 2020).

Este caso impulsó también la actualización de la antigua Directiva 95/46 de la UE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, la cual se mantenía vigente desde el 24 de octubre de 1995 pero con las nuevas tecnologías se consideró que había quedado obsoleta, por lo que fue cambiada en 2018 por el Reglamento (UE) 2016/619 del Parlamento Europeo.

Ahora mejor conocido como Reglamento General de Protección de Datos, desde ahora RGDP por *sus siglas, el que plantea en el considerando 6 que "La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa* (Parlamento Europeo y Del Consejo, 2016/619).

El reglamento protege el derecho a la privacidad en relación a las nuevas tecnologías como el Internet de las cosas, y el derecho a protección de datos personales, como también la esfera de aplicación como el derecho al olvido, en el sentido explicado.

En lo que respecta al Internet de las Cosas, esta misma regulación se basa en el principio de que "los datos personales de cada persona pertenecen a cada ciudadano" (Feldgen, 2018). Estos datos almacenados por la empresa también requieren aprobación previa y se basa en los siguientes motivos de acuerdo con el artículo 7 de esta circular.

- Demostrar que el consentimiento se dio
- Se podrá retirar el consentimiento en cualquier momento
- Se tendrá que evaluar si el consentimiento se dio libremente

Otro asunto importante es que el reglamento asegura la transparencia del trato de la información, esto según el artículo 12 que establece que el responsable de tener la información tendrá que facilitar en cualquier momento su derecho al acceso a la información al interesado (Ley 1581 de 2012, Art. 12, 2012).

Además, dentro de otros tipos de regulaciones, (Directiva 2013/40, 2013), la cual habla sobre los ciberataques y las infracciones a los sistemas que contienen la información, desde el articulo 9 hasta el 11, se ven las sanciones para aquellos que vulneran los sistemas electrónicos como en casos de hackeos y otros tipos de vulneraciones, esto es importante para asegurar un correcto funcionamiento del IoT y para poder mantener la seguridad dentro de los sistemas o "nubes" que mantienen almacenada toda la información y privacidad de las personas que tienen los productos, de igual manera, este reglamento ayuda a estandarizar el sistema de ciberseguridad de todos los países miembros de la UE.

Es necesario mencionar que el desarrollo investigativo del IoT no solo es para regularlo, sino que también para hacer un análisis de mercado, ya que recientemente fue publicado por la Comisión

Europea un reporte para el Consejo y el Parlamento Europeo sobre una investigación sectorial sobre el Internet de las cosas del consumidor, reporte que fue comenzado en 2020 y publicado durante el año 2022.

Como apartados importantes se confirma el crecimiento del IoT en el mundo, aumentando de 105,7 billones de euros a aproximadamente 404,6 billones de euros al año 2030, además se puede observar que las principales plataformas que ocupan las personas fuera de los televisores y teléfonos inteligentes en Europa son las asistentes de voz, siendo las principales Alexa de Amazon, la asistente de Google y Siri de Apple (European Commission, 2022).

En este mismo reporte se señalan grandes preocupaciones en diferentes ámbitos, una de ellas es la imposibilidad de utilizar en un mismo dispositivo, celular o computadora, diferentes asistentes de voz al mismo tiempo, lo que podría generar prácticas monopólicas de las empresas ya que obligarían al consumidor de marcas a usar el asistente de voz de su misma línea.

Lo más importante surge en la información, pues como se expresó una gran preocupación por la cantidad de información que pueden almacenar las grandes empresas que poseen asistentes de voz, ya que los posicionarían en un lugar privilegiado en el mercado, aprovechándose de la información que estos captan para publicitar otros dispositivos de su marca.

Debemos mencionar que la Unión Europea, aunque tiene una de las regulaciones más desarrollado frente a temas de amenazas que puede tener el IoT al derecho a la privacidad, en todas sus esferas, aún hay un largo camino por delante para lograr una mejor regulación del acceso a la información privilegiada que las empresas pueden llegar a utilizar para posicionarse dentro de los mercados.

Es por esto que la Comisión Europea para el periodo de 2021 a 2027, está invirtiendo aproximadamente €95.5 Millones de euros en investigación, innovación y desarrollo de las tecnologías emergentes relacionadas al IoT, todo esto bajo la creación del programa Horizon Europeo, dentro de este programa también se tiene en consideración de que el IoT debe ser la clave para concretar la transformación digital en aquellos sectores importantes de la sociedad en que la digitalización aún no se da del todo como lo son la industria de la agricultura, la energía y la movilidad (Unión Europea, 2021).

11 La regulación a la privacidad en España

La regulación de la privacidad proviene desde la propia Constitución, que establece claramente en el artículo 18, el derecho a la privacidad e incluye 4 esferas fundamentales como son:

1. Primero que nada, se garantiza el derecho al honor, a la integridad de la persona, de la familia y a la propia imagen, lo que en nuestro país llamamos Derecho a la Honra.

2. En segundo lugar, se garantiza la inviolabilidad del domicilio

3. En tercer lugar, el secreto de las comunicaciones, incluidos los mensajes postales, telégrafos y teléfonos.

4. Finalmente, solo la ley limita el uso de la informática para garantizar la cercanía personal y familiar del ciudadano y cumplir con sus derechos (Constitución Española. Art, 18, 1978).

El numeral 4 es el de nuestro interés, porque regula la informática para garantizar la intimidad personal y familiar, este número será el derecho a la intimidad y la protección de los datos digitales, esto hace que la diversidad del derecho a observar en general haciendo una diferenciación del derecho a la intimidad, visto de una forma más general que se desarrolla en los puntos anteriores, que podríamos definirlo “como la esfera de protección que rodea la vida más privada del individuo frente a injerencias ajenas, con la salvedad de los supuestos previstos en la ley”(López Jiménez, 2013).

Estos derechos proporcionan un punto de partida para la regulación, pero cabe señalar que los dos derechos identificados anteriormente son diferentes de lo que podríamos considerar derechos de privacidad, que pueden incluir todos los datos relacionados con un individuo, ya sea de carácter sensible (López Jiménez, 2013). No son contradictorios, pese a las diferencias entre ambos derechos, por lo que se incluyeron en la Constitución española de 1978.

Junto al artículo 18 numeral 1 y 4, como lo mencionó el Tribunal Constitucional español en la sentencia STC 292/2000, que afirmó que "el objeto de protección del derecho fundamental a la protección de datos no se limita a los datos privados de una persona sino también a todo tipo de información personal " datos íntimos o no, cuyo conocimiento o utilización por terceros puede afectar a sus derechos, fundamentales o no, por cuanto se refieren no sólo a la integridad personal, protegidos en el artículo 18 numeral 1 datos personales.

Esto afecta, por tanto, también a los datos personales disponibles públicamente, ya que están a disposición del público, si son accesibles a cualquier persona, sin privar al interesado de ningún derecho de tratamiento, ya que ello garantiza su derecho a la protección de datos"(STC 292/2000, FJ°5, 2021).

Se resuelve el problema entre estas dos leyes, mencionamos que España es uno de los países europeos, en el que, en términos de regulaciones sobre derechos de seguridad digital para las perspectivas de seguridad Digital, creando una ley de datos protectores y garantiza los derechos digitales en 2018 Ley orgánica de protección de datos personales y garantía de los derechos digitales (LOPDGDD), esta es la adaptación al reglamento GDPR, por lo que los principios de la antigua regulación de la UE tendrán lugar después de 2016/679, esta es la base legal para ajustar el procesamiento de datos personales de las empresas esta ley actualiza según la protección de datos.

Los puntos principales de LOPDGDD son los siguientes:

1. primero debe existir consentimiento explícito y verificable por parte del usuario (Artículo 6), para menores de edad el consentimiento sólo se otorga a partir de los 14 años (Artículo 7).
2. Obligación de proporcionar información a las partes relevantes (Artículo 11), incluidos los derechos de acceso (Artículo 13), corrección (Artículo 14), eliminación (Artículo 15), restricciones al procesamiento (Artículo 16), portabilidad y oposición (Artículos 17 y 18).
3. Asegurar la seguridad de la información recibida (Artículo 5).

Finalmente, debe mencionarse que esta ley orgánica también se adapta a la comunicación de brechas de seguridad, que deben transferirse a las víctimas y agencias españolas para proteger los datos en un máximo de 72 horas. Como el artículo 34, creando el número de delegados de protección de datos, que es parte de la ley más precisa en comparación con las regulaciones generales de Europa, las organizaciones deben tener un delegado para proteger los datos.

Algunas organizaciones son escuelas, centros de formación, colegios e instituciones financieras, redes que ejecutan servicios de transmisión. Información electrónica, así como proveedores de servicios de una compañía de información, preparando grandes registros de usuarios de servicios a gran escala (LOPDGDD 3/2018, 5 de Diciembre, Art. 34, 2018)

Esto es crucial para evitar casos como el de Cambridge Analytica, que protagonizó el mayor escándalo de violación de privacidad y datos personales de la última década (Chan Rosalie, 2019).

12 El internet de las cosas en España

España fue uno de los primeros países en desarrollar la tecnología IoT, y en 2005 se fundaron pequeñas empresas relacionadas con IoT, pero la diferencia se hizo realmente notoria a partir de 2010, cuando “empezó”, el auge de las ciudades inteligentes en España, se dio lugar al nacimiento de RECI (Red Española de Ciudades Inteligentes)” (Vega, 2015). RECI abarca ciudades de 50.000 habitantes o más, empezando por las 27 ciudades españolas más grandes en 2012 y terminando con 89 ciudades en 2022.

El objetivo que mencionaron es "compartir experiencias y trabajar juntos por el desarrollo". un modelo de gestión sostenible y mejorar la calidad de vida de las personas, centrándose en aspectos como el ahorro energético, la movilidad sostenible, el gobierno electrónico, el cuidado humano y la seguridad” (Vega, 2015).

Cabe destacar que, en el año 2012, el Instituto para la Diversificación y Conservación de la Energía, dependiente del Ministerio de Industria, Turismo y Comercio, atribuyo 3 características a las ciudades inteligentes:

- No daña el medio ambiente
- Utilizar las tecnologías de la información y la comunicación como herramienta de gestión.
- Tomar el desarrollo sostenible como objetivo final

Por último, las ciudades inteligentes españolas también cuentan con la Red de Innovación Urbana, también conocida como RIU, (Moreno, 2018), "uno de los objetivos es promover la integración de las tecnologías de la información y las comunicaciones en el desarrollo urbano, transición al modelo de ciudad inteligente"(Moreno, 2018), por lo que el desarrollo de las ciudades inteligentes en Iberia avanza a pasos agigantados respecto al nuestro.

En otras áreas de la tecnología IoT, en España la tecnología surgió debido a la alta demanda académica de temas de investigación, por lo que las empresas se centraron en el almacenamiento en la nube, centrándose en la investigación académica. Este desarrollo temprano ha ayudado a "mejorar la reputación internacional de España en el sector IoT, contando el país con empresas de estándares globales y operadores de Wi-Fi como actores clave para proporcionar al país la conectividad inicial necesaria en ubicaciones específicas". como en plazas, aeropuertos, etc, otros

lugares públicos”(Vega, 2015). Se espera que el crecimiento de las empresas de IoT aumente con el paso de los años y no se centre únicamente en determinados aspectos.

Finalmente, lo importante es que tenemos que mencionar el estudio de las características del uso de dispositivos IoT en la población española, realizada para 2021, que nos muestra. IoT proporciona diferentes aplicaciones en España, cuyos grupos de edad son aplicaciones más populares en Internet y en realidad son dispositivos electrónicos relacionados con la tecnología. Los estudios muestran que en España el 85% de las personas conocen dispositivos equipados con tecnología IoT.

Si se divide por grupos de generaciones, resulta que el que más sabe sobre dispositivos o sistemas conectados a Internet: 35-44 años (22,37%) , seguido por el de 45 a 54 años con un 22,19%, lo que sorprende porque se podría pensar que el grupo de edades que más conoce las nuevas tecnologías sería el de la nueva generación que han convivido con el Internet desde que han nacido pero la generación de 16 a 24 años es el segundo menos familiarizado con los dispositivos IoT: sólo el 14,16% (Quintana, 2021).

Los dispositivos más utilizados en el país son los asistentes de voz virtuales como Alexa de Amazon, Siri de Apple y Google Home, con un promedio del 18,1%, ya que alrededor de 5.941.055 personas utilizaron estos dispositivos. Con lo que señalamos en el capítulo anterior respecto al análisis de mercado realizado por la Comisión Europea. En segundo lugar, se encuentran los dispositivos conectados a Internet con un 10,8%, los sistemas de seguridad del hogar con un 9,5% y finalmente los sistemas de gestión de energía con un 8,4% (Quintana, 2021).

Así, el Internet de las Cosas en España ha crecido rápidamente debido al crecimiento de industrias que comenzaron a apostar por esta tecnología a principios de siglo, cuando recién se estaba creada oficialmente, además de crear una gran red de ciudades que Ahora están enfocados en crear ciudades más inteligentes en todo el país, además de gestionar adecuadamente estas nuevas tecnologías, gracias al liderazgo de la Unión Europea, creare leyes para evitar vulneraciones de la privacidad por medio de la tecnología sean menores y tengan sanciones a quienes las incumplan.

13 Regulación del IoT en el Reino Unido

En todo el continente del reino unido, el Internet de las cosas ha crecido rápidamente, el IoT crece a pasos agigantados un ejemplo de esto es, al finalizar el 2020, “ya se habían instalado alrededor de 53 millones de medidores inteligentes en hogares del Reino Unido”. (Noto, La Diega, 2016).

Por este motivo, el gobierno desea proteger a los consumidores de los riesgos de privacidad que puede suponer, motivo por el cual desde mediados de 2010 el gobierno del Reino Unido ha buscado promover y gestionar el Internet de las Cosas, aumentando la inversión pública para garantizar que este sector de Internet se desarrolle como lo hizo en 2015, cuando “el gobierno del Reino Unido anunció una financiación de 40 millones de libras esterlinas para la industria de IoT para centrarse en la atención sanitaria, la asistencia social y las ciudades inteligentes (Ofgem, 2015).

En términos de regulación de IoT, el primer enfoque regulatorio adoptado por el gobierno del Reino Unido fue en 2014, cuando el Asesor Científico Jefe del gobierno del Reino Unido llevó a cabo la Revisión IoT, que recomendó que la regulación debería tener "límites mínimos" necesarios para el desarrollo de Internet de las cosas (Tanczer & M., 2019).

Esta publicación es la base para que el Reino Unido inicie una política regulatoria flexible para mantenerse al día con los cambios tecnológicos, así como con la inversión, como se mencionó arriba, con el establecimiento de IoT UK en 2015, un programa de tres años que informa sobre los logros de IoT en el país y es parte de la inversión gubernamental.

Posteriormente en el 2018, el Departamento de Digital, Cultura, Medios y Deportes emitió el Código de prácticas sobre seguridad de Internet de las cosas para los consumidores, basado en las regulaciones de la Unión Europea (en ese momento, el Reino Unido todavía era parte de la Unión Europea), el cual se creó por parte del el Departamento de Digital, Cultura, Medios y Deportes, que en sus propias palabras establece “lo que se considera buenas prácticas para la seguridad de IoT” (DDCMS, 2018), como parte de las decisiones toman.

Las acciones que se tomaron para aumentar la seguridad de esta tendencia tecnología (IoT) son las siguientes:

1. No debe existir una contraseña predeterminada en el dispositivo: Esto significa que los dispositivos electrónicos habilitados para IoT no tendrán una contraseña predeterminada de fábrica, por lo que se requerirán otros medios para autenticar el producto.

2. Las empresas que proporcionan dispositivos y servicios conectados a Internet deben proporcionar una persona de contacto o un número público que pueda revelar vulnerabilidades en sus productos para que se puedan tomar medidas correctivas rápidamente y corregir estas vulnerabilidades.

3. El proceso de actualizaciones debe ser con intervalos de tiempo más cortos para garantizar que su dispositivo tenga menos vulnerabilidades de seguridad.

Este Código de prácticas pretende ser aplicable a la industria, el mundo académico, las organizaciones de consumidores y otras agencias gubernamentales internacionales. Posteriormente, en enero de 2020, se publicó la respuesta del Departamento a una consulta abierta encaminada a mejorar el código, cuyo desarrollo se inició en mayo de 2019 y finalizó en junio del mismo año, y se publicaron los comentarios de las empresas reguladas y el impacto que había tenido la norma. Propuesta de reglamento para estos dos años de aplicación (DDCMS, 2020)

Finalmente, debemos mencionar que el Reino Unido anterior al Brexit también estaba sujeto al Reglamento 2016/679, conocido como GDPR, de forma general a través de la Ley de Protección de Datos de 2018, que el país implementó para cumplir con este reglamento de la UE. Sin embargo, en el caso de Brexit, se entiende que el RGPD ya no se aplica en el Reino Unido, lo que significa que ya no es válida ninguna ley que lo rija, pero el RGPD sigue incorporado a la legislación del Reino Unido mediante una data *protecction act*, siendo esto un total retroceso a la regulación del derecho a la privacidad en Internet.

14 Regulación del IoT en Estados Unidos

Como se ha comentado en el apartado sobre la Unión Europea, donde se menciona que la regulación del IoT comienza con un nivel de desconfianza en las empresas respecto al uso de los datos, lo contrario ocurre en Estados Unidos, donde según Feldgen, "los estadounidenses se preocupan más por el gobierno no ". interfiera en su vida privada.

Para la gente de estados unidos es mucho más importante tener la libertad de alcanzar objetivos y ejercer el derecho a elegir para que el Estado satisfaga las necesidades básicas de todos los ciudadanos, porque dicha regulación para los ciudadanos es incompatible con la innovación"(Feldgen, 2018).

Esto significa que para 2020 no habrá ninguna regulación federal en Estados Unidos. En ese mismo año se aprobaron la Ley Pública 116-207, conocida como Ley de Mejora de la Ciberseguridad en el Internet de las Cosas de 2020, que detalla, "futuros requisitos de seguridad que deben cumplir las entidades de propiedad o controladas por el gobierno federal". Personas conectadas a sus sistemas informáticos" (Roberts. Weidenslaufer, 2015)

Esta ley comienza definiendo qué es el Internet de las Cosas, afirmando que es "la extensión de la conectividad a Internet a dispositivos físicos y todo tipo de objetos cotidianos" (Gibson Dunn, 2021), esto es curioso porque esta definición no incluye los dispositivos electrónicos tradicionales como ordenadores, smartphones o tablets (Roberts & Weidenslaufer, 2015).

Según un estudio jurídico Gibson Dunn, este proyecto de ley autoriza al *National Institute of Standard and Technology* (Desde ahora NIST), a desarrollar estándares y pautas de seguridad para el uso y manejo adecuado de todos los dispositivos electrónicos de Internet de las Cosas que tiene el gobierno federal y están conectados a su sistema de información (Gibson Dunn, 2021). Además, el NIST "debe revisar y actualizar sus estándares cada cinco años para mantenerse actualizado sobre nuevas cuestiones relacionadas con los datos que se generan (Roberts & Weidenslaufer, 2021).

Además, de conformidad con la Sección 4-2 de la Ley de 2020, la NIST debe ser coherente en sus esfuerzos para abordar posibles vulnerabilidades de seguridad de IoT y debe cumplir con las siguientes consideraciones para los dispositivos habilitados para IoT:

1. Que puedan tener un desarrollo con seguridad
2. Gestión de identidad
3. Actualizaciones de versiones
4. Gestión de configuración

Además, se deben considerar estándares, directrices y mejores prácticas relevantes desarrolladas por el sector privado, agencias y asociaciones público-privadas (Ley Pública 116-207, Secciones 4-1 y 2, 2020).

Finalmente, es importante señalar que a partir del 5 de diciembre de 2022, todas las agencias gubernamentales tienen prohibido renovar contratos de adquisición con empresas cuyos dispositivos de IoT no cumplan con los estándares y pautas del NIST, de conformidad con la Sección 7(a)(1) y la Sección 7.(d) La Ley establece igualmente que todas las prohibiciones especificadas en la Ley entrarán en vigor dos años después de la publicación del anuncio y se harán en la fecha indicada anteriormente (Ley Pública 116-207, Artículo 7a 1 y Artículo 7d, 2020).

Es importante señalar que la primera ley estatal que regula la privacidad de la información en línea, la Ley del Estado de California No. 327 de 2018, fue aprobada en 2018 pero a partir del 1 de enero de 2020, muchos la consideran como un hilo importante en la implementación de regulaciones de IoT en los Estados Unidos.

Esta ley cobra importancia por el contexto histórico y geográfico del estado de California, que ha sido la “Meca” de la tecnología desde finales del siglo pasado, es la sede de Silicon Valley y es el lugar donde se desarrollan las operaciones de las empresas más grandes de tecnología. De ahí que las regulaciones para establecer estándares mínimos de seguridad para los dispositivos conectados a Internet se hayan vuelto claras y necesarias para las mayores empresas tecnológicas del mundo, como Facebook, Google y Apple.

La ley de California se agregó a la Parte 4 del Título 3 del Código Civil del mismo estado con secciones importantes como exigir a los fabricantes de dispositivos conectados a Internet que proporcionen medidas de seguridad adecuadas, tales como:

- ¿Que sean apropiadas para la naturaleza y funciones del dispositivo?
- Adecuados a la información que recogen, contienen y transmiten.

- Estén diseñados a proteger el dispositivo y toda la información contenida en el dispositivo contra el acceso no autorizado, la destrucción, el uso, la modificación y la divulgación (SB/327, 1798.91.04 a, 2018).

La ley exige que todos los dispositivos que se conecten fuera de la red local estén equipados con funciones de autenticación con características de seguridad adecuadas. Además, la contraseña predeterminada es exclusiva de este dispositivo y este dispositivo incluye una función de seguridad que requiere que el usuario cree un nuevo método de autenticación antes de otorgar acceso al dispositivo por primera vez (SB/327, 1798.91.04 a, 2018).

En resumen, con la ayuda de esta regulación, debe decirse que esta norma tiene contradictores, los expertos en ciberseguridad como Robert Graham, dice que la ley es "a menudo mala, porque se basa en un análisis superficial de la ciberseguridad y la piratería y que hay poco para mejorar la seguridad e impone costos y genera daño de la innovación (Porcelli, 2018).

También argumentó que tratar de resolver el problema con parches o actualizaciones constantes del dispositivo no es una solución porque no hay garantía de que las compañías de Internet proporcionen a los consumidores soluciones como esa o, peor aún, el consumidor actualizará el dispositivo, especialmente cualquier cosa que esté en el dispositivo. que no sean teléfonos, tabletas o computadoras porque simplemente se instalan donde se usarán y los usuarios “no ven notificaciones o no reciben notificaciones apropiadas cuando se aplican parches” (Porcelli, 2018).

En resumen, se puede decir que Estados Unidos recién está comenzando a regular el Internet de las Cosas, regulando a las empresas principalmente desde una perspectiva de seguridad, pero aún necesita gestionar cuestiones básicas como el consentimiento para proporcionar información personal, el consumo, la transparencia en el uso de información, y qué reguladores pueden imponer sanciones a las empresas si no cumplen con la ley.

15 Comparación entre la unión europea y Latinoamérica

El Reglamento General de Protección de Datos (RGPD) (Unión Europea, 2022), se ha convertido en un catalizador de cambios a nivel mundial, siendo considerado por muchos como una revolución en el ámbito de la protección de datos. Sin embargo, es importante reconocer que el RGPD no surge de la nada, sino que es el producto de más de cuatro décadas de evolución en la regulación de la protección de datos personales en la Unión Europea.

Su influencia trasciende las fronteras europeas, extendiéndose hacia otras regiones, entre ellas Latinoamérica. La implementación directa del RGPD y su alcance tienen un impacto global, obligando tanto a instituciones públicas como privadas en todo el mundo, incluyendo aquellas en Latinoamérica, a cumplir con sus rigurosos requisitos.

Sin embargo, surge la pregunta sobre cuáles son las principales innovaciones y cambios introducidos por este reglamento. Además, es pertinente analizar el estado de la protección de datos personales en Latinoamérica, así como la disponibilidad de los mecanismos y recursos necesarios para facilitar esta transición. Es esencial considerar cómo estas nuevas regulaciones impactan en las leyes latinoamericanas de protección de datos que existían antes de la implementación del RGPD. (Unión Europea, 2022).

¿Se están adaptando estas normativas locales para alinearse con los estándares europeos? ¿Qué estrategias son necesarias para fomentar una mayor armonización entre las leyes de protección de datos de la Unión Europea y las de Latinoamérica? En este sentido, es crucial explorar cómo la Unión Europea y Latinoamérica pueden convertirse en aliados estratégicos en la protección de datos personales. ¿Qué acciones pueden llevarse a cabo para promover una colaboración más estrecha entre ambas regiones en este ámbito? ¿Cómo pueden desarrollarse estrategias comunes que beneficien a ambas partes y fomenten una cultura de protección de datos más robusta a nivel internacional?

Latinoamérica y el Caribe cuentan con una población aproximada de 670 millones de habitantes distribuidos en 46 países. Varios de estos países, como Argentina, Uruguay, México, Perú y Colombia, entre otros, desarrollaron sus leyes de protección de datos personales a partir de los años 2000. Estas leyes estuvieron muy influenciadas por la visión de la Unión Europea sobre el derecho a la vida privada, plasmada en la Directiva Europea 95/46/CE.

Sin embargo, es importante destacar que, de los países latinoamericanos con leyes de protección de datos, solo Argentina y Uruguay eran considerados seguros para la transferencia de datos personales. En la época pre-RGPD, países como Ecuador, Venezuela, Bolivia y Brasil no contaban con una ley de protección de datos personales.

La idea de crear el RGPD surgió en enero de 2012, cuando la Comisión Europea propuso una reforma a la ("Directiva 95/46/CE," 1995) con dos objetivos: reforzar la protección del derecho a la privacidad de los datos personales e impulsar la economía digital en la Unión Europea. Dada la transformación económica, social y cultural que las tecnologías de la información trajeron desde 1995, este planteamiento fue muy coherente.

El principal problema de la ("Directiva 95/46/CE," 1995) era la falta de aplicación directa, lo que resultaba en una notable falta de homogeneización en las leyes de la Unión. Curiosamente, en ese mismo año, mientras la Unión Europea preparaba el camino hacia el RGPD, países latinoamericanos como Colombia promulgaban su propia ley de protección de datos.

Desde la entrada en vigor del RGPD el 25 de mayo de 2016, casi todos los países latinoamericanos han iniciado un proceso de reforma de sus leyes de protección de datos para cumplir con el RGPD. Resulta curioso que Brasil fue el primero en desarrollar una ley de protección de datos alineada con el RGPD, conocida como la Ley General de Protección de Datos (LGPD).(General Personal Data Protection Act (LGPD), 2018)

Aquellos países que carecían de regulaciones, como Ecuador o Paraguay, están actualmente en proceso de desarrollo y aprobación de sus propias leyes de protección de datos personales. Este progreso regional demuestra que Latinoamérica se ha convertido en un aliado estratégico importante de la Unión Europea en este ámbito.

En el caso de Ecuador, ha sido un proceso largo y con varios intentos fallidos. Un análisis legal detallado revela que existen normas dispersas en varios cuerpos legales, incluida la Constitución ecuatoriana, que intentaban regular la protección de datos personales, incluso sin una definición legal de datos personales en el ordenamiento jurídico.

El nuevo anteproyecto de ley ecuatoriana de protección de datos personales se desarrolló de acuerdo con el RGPD, lo cual es muy alentador (General Personal Data Protection Act (LGPD), 2018).

El RGPD define los datos personales como toda información que concierne a una persona física identificada o identificable (denominada "el interesado"); se considerará identificable a toda persona cuya identidad pueda determinarse, ya sea directa o indirectamente, especialmente a través de un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos que sean característicos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Esta definición de datos personales revela el enfoque técnico adoptado por el RGPD, que se basa en la gestión de riesgos, un lenguaje universal utilizado en el sector de la seguridad de la información. ¿Por qué una disciplina jurídica adoptaría una naturaleza principalmente técnica? La respuesta radica en la necesidad de establecer mecanismos efectivos para su cumplimiento en el contexto transnacional de un mundo dominado por las tecnologías de la información y la comunicación.

La Directiva 95/46/CE (“Directiva 95/46/CE,” 1995) ya introducía la noción de gestión de riesgos, aunque de forma superficial. El RGPD incorpora el enfoque proactivo del ámbito de la seguridad de la información, convirtiéndose en una normativa legal valiosa y proactiva que desafía la naturaleza tradicionalmente reactiva del derecho.

Es fundamental establecer la responsabilidad del responsable del tratamiento respecto a cualquier procesamiento de datos personales realizado por él mismo o en su nombre. En particular, el responsable debe cumplir con la obligación de implementar medidas apropiadas y efectivas, y debe ser capaz de demostrar la conformidad de sus actividades de procesamiento según el reglamento europeo, incluida la eficacia de las medidas. Estas medidas deben tener en cuenta la naturaleza, el alcance, el contexto y los fines del procesamiento, así como el riesgo para los derechos y libertades de las personas físicas. (Considerando 74 Del RGPD).

Los principios de seguridad y protección en el procesamiento de datos establecidos incluyen: confidencialidad, integridad, disponibilidad, resiliencia y trazabilidad.

Vamos a definir una descripción corta de los principios.

Confidencialidad: Se refiere a la prevención del acceso, divulgación y uso no autorizado de los datos.

Integridad: Se trata de prevenir cambios no autorizados en los datos, manteniendo su exactitud y consistencia.

Disponibilidad: Garantiza que los datos estén accesibles cuando se necesiten y por quienes estén autorizados a acceder a ellos.

Trazabilidad: Consiste en registrar las acciones realizadas en el tratamiento de datos, proporcionando una prueba para auditorías y seguimiento.

Resiliencia: Es la capacidad de un sistema informático para resistir ataques y mantener la funcionalidad ante eventos adversos.

Los primeros tres principios han sido y continúan siendo fundamentales en la gestión de riesgos de ciberseguridad. Aunque la resiliencia y la trazabilidad puedan parecer principios nuevos, en realidad han sido considerados implícitamente por los especialistas en ciberseguridad desde hace tiempo. El RGPD establece medidas preventivas de seguridad en su artículo 32, especificadas en los literales a y b.

El mayor desafío de las leyes latinoamericanas es adoptar el enfoque de gestión de riesgos, ya que tradicionalmente lo han aplicado la mayoría de las empresas desde la perspectiva de proteger sus activos patrimoniales, y no desde la óptica de derechos y libertades. El RGPD establece que tanto el responsable como el encargado del tratamiento de datos deben tomar medidas de seguridad adecuadas. Estos responsables y encargados suelen ser instituciones públicas o privadas.

Por tanto, es fundamental comprender la gestión de riesgos, y me atrevo a afirmar que como sociedad aún no comprendemos completamente. Muchas de las pequeñas y medianas empresas (Pymes) de la región, consideramos que muchas carecen de la infraestructura y los recursos humanos necesarios para implementar las medidas técnicas y organizativas requeridas para cumplir con lo establecido en el RGPD y realizar una gestión eficiente de riesgos y evaluaciones de impacto.

La mejor manera de entender qué es la gestión de riesgos es a través de una analogía. Esta práctica se originó en las décadas de 1970 y 1980, centrada en los riesgos financieros y los seguros. Los primeros modelos surgieron en los años 90, siendo especialmente destacados el Riskmetrics y el Creditmetrics.

La gestión de riesgos en ciberseguridad surgió en la misma década, principalmente como respuesta a los ataques informáticos, y asumiendo tres funciones fundamentales: comprender las capacidades y conocimientos de los atacantes, evaluar la eficacia de las herramientas de seguridad, y mitigar los riesgos identificados.

La Unión Europea se enfrenta a un gran desafío al apostar por una normativa jurídica que se alinea con el estado actual y el futuro de las tecnologías emergentes. Este enfoque está contribuyendo a la evolución de la industria de la ciberseguridad. El cambio de paradigma se produce al aplicar la gestión de riesgos a los derechos y libertades. Si tomamos como ejemplo una rama relacionada de la seguridad de la información, como la seguridad ocupacional, podemos entender que los modelos de gestión de riesgos se establecen para proteger ciertos derechos, como el uso de señales para advertir sobre el riesgo de resbalones en suelos mojados, con el fin de proteger el derecho a la vida del individuo.

En la gestión de riesgos de ciberseguridad, los datos personales tienden a considerar como un activo empresarial, dejando de lado el derecho a la protección de la privacidad del individuo. Esto ha llevado a que la industria actual se base en gran medida en la explotación de datos, con diversos propósitos, ya sean comerciales por parte de empresas o de vigilancia por parte de gobiernos. Es importante recordar que los datos son el recurso principal de la próxima revolución industrial, ya que impulsan la economía digital y son esenciales para cualquier proceso de análisis de datos y aprendizaje automático.

Actualmente, muchas empresas se dedican a desarrollar software de gestión de riesgos, evaluación de impacto y herramientas de ciberseguridad. Estas empresas también están actualizando sus metodologías para asegurarse de que sus productos sean herramientas efectivas para los responsables y encargados del tratamiento de datos.

El papel de estas empresas es fundamental, ya que tienen la responsabilidad empresarial de cumplir con los requisitos de seguridad de sus clientes. Por lo tanto, podemos ver que el RGPD ha impulsado la evolución de la industria de la ciberseguridad, convirtiendo el conocimiento y la gestión de riesgos de derechos y libertades en una de las áreas más demandadas a nivel global. Esta convergencia entre la protección de datos y la ciberseguridad contribuye significativamente a hacer que el ciberespacio sea más seguro.

Si examinamos los resultados del primer año de aplicación del RGPD, encontramos cifras bastante reveladoras. Hasta febrero de 2019, se habían reportado aproximadamente 5,900 incidentes en la Unión Europea. Este aumento puede atribuirse al crecimiento de los dispositivos móviles y al auge de Internet, pero también es evidente que la obligación de notificar a las autoridades ha tenido efectos positivos.

Antes de la implementación del RGPD, las empresas solían mantener en secreto los incidentes de seguridad, ya que podían tener consecuencias significativas para la reputación y credibilidad de la empresa ante sus clientes. Pero las instituciones públicas y las privadas que antes no priorizaban la seguridad y privacidad de sus clientes están obligadas a mejorar sus procesos internos, capacitar adecuadamente a su personal y usar tecnología adecuada para mitigar los riesgos.

Desde otra perspectiva, considerando la realidad de Latinoamérica, es importante reconocer que muchos profesionales latinoamericanos en seguridad de la información han sido formados y certificados según metodologías desarrolladas en Estados Unidos, como las de EC-Council, el instituto SANS o el ISC2. Asimismo, los estándares de seguridad de la información, como la familia ISO/IEC 27000, mantienen un enfoque previo a la RGPD que, aunque es valioso, podría necesitar actualizaciones en un futuro cercano.

Por lo tanto, la cooperación de la Unión Europea para desarrollar o adaptar metodologías de evaluación de riesgos basadas en la RGPD, que sean ajustables a las leyes de los países latinoamericanos, es esencial. Además, los países latinoamericanos pueden beneficiarse de la experiencia europea adquirida durante este primer año de implementación de la RGPD, lo que les permitirá capacitar a sus profesionales, empresas y sobre todo generar conciencia en la población sobre la importancia de proteger sus datos personales.

Teniendo en cuenta que en la región latino América todavía no existe algún proceso de integración jurídico en dicha área, solo la orientación establecida en el reglamento General de protección de datos (RGPD) que han adoptado algunos países de la región y que pueden suponer numerosas variantes.

Algunos ejemplos incluyen el principio de protección de la privacidad desde el diseño y por defecto, las certificaciones, las notificaciones de violaciones de datos, el rol del Oficial de Protección de Datos y las sanciones administrativas por incumplimiento.

Por ejemplo, en la nueva ley brasileña de protección de datos, la multa puede ser de hasta el 2 % de la facturación de una empresa, en lugar del 4 % previsto en el RGPD. De manera similar, en el nuevo anteproyecto de ley en Argentina, el consentimiento también puede ser tácito bajo ciertas circunstancias.

El panorama, sin embargo, también es alentador. En la economía digital se destacan tres grandes protagonistas: Estados Unidos, China y la Unión Europea en conjunto. Dado que Estados Unidos y China tienen estándares mucho más bajos de protección de datos personales, la Unión Europea, a través del RGPD, desempeña un papel crucial en la regulación de tecnologías emergentes como la inteligencia artificial, la biotecnología, el blockchain, IoT y la computación cuántica.

Cuadro comparativo leyes más importantes regulación IoT por cada país				
Aspecto	**Unión Europea**	**Estados Unidos**	**China**	**Japón**
Fecha de entrada en vigor	25 de mayo de 2018	1 de enero de 2020	1 de noviembre de 2021	30 de mayo de 2017, con enmiendas posteriores
Legislación	Reglamento General de Protección de Datos (GDPR) - Unión Europea	Ley de Privacidad del Consumidor de California (CCPA)	Ley de Protección de Datos Personales (PIPL) - China	Ley de Protección de Datos de Japón (APPI)
Alcance	Todas las empresas que procesan datos de residentes en la Unión Europea, independientemente de dónde se encuentren ubicadas.	Aplica a empresas que operan en California o que manejan datos de residentes de California, con ciertos umbrales de ingresos o cantidad de datos procesados.	Aplica a entidades que procesan datos personales de individuos en China, incluso si las entidades están ubicadas fuera del país.	Afecta a las empresas que manejan información personal de individuos en Japón, incluyendo entidades extranjeras que operan en Japón.
Características principales	Consentimiento Derecho al olvido Portabilidad de datos Notificación de violaciones de datos	Derecho a conoce Derecho a eliminar Derecho a optar por no participar Protección de menores	Consentimiento informado Transferencia internacional Derechos del individuo	Consentimiento informado Transferencias internacionales Derechos de los individuos
Multas	Las infracciones pueden resultar en multas de hasta el 4% de la facturación global anual de una empresa o 20 millones de euros, lo que sea mayor.	sanciones significativas por violaciones de privacidad y seguridad	Multas de hasta 50 millones de yuanes o el 5% de los ingresos anuales de la empresa.	Las infracciones pueden resultar en sanciones y multas administrativas

Tabla 5. Leyes en materia de protección de datos global

En la tabla anterior se puede observar un análisis de las regiones más avanzadas en el despliegue de tecnologías, así como aquellas que han implementado regulaciones eficaces en torno a estas innovaciones. Estas regiones no solo han logrado un progreso significativo en el ámbito tecnológico, sino que, al mismo tiempo, han establecido marcos regulatorios robustos que les han permitido posicionarse como potencias tecnológicas a nivel global.

Su enfoque proactivo hacia la regulación ha sido fundamental para fomentar la innovación, atraer inversiones y establecer modelos a seguir para otras regiones en términos de adopción de nuevas tecnologías. El RGPD no se limita al ámbito territorial de la Unión Europea. Se aplica a cualquier organización, dentro o fuera de la UE, que procese datos personales de ciudadanos europeos, siempre que ofrezca bienes o servicios o monitoree su comportamiento.

El RGPD permite el tratamiento de datos personales bajo diferentes bases legales, como el consentimiento, la ejecución de contratos, intereses legítimos, cumplimiento de obligaciones legales, entre otros.

Cuadro comparativo leyes más importantes regulación IoT por cada país				
Aspecto	**Canadá**	**Brasil**	**Reino Unido**	**Sudáfrica**
Fecha de entrada en vigor	Julio de 2000, con enmiendas posteriores	18 de septiembre de 2020	25 de mayo de 2018, junto con el **GDPR**	1 de julio de 2020
Nombre de la ley	Ley de Protección de Datos Personales y Documentos Electrónicos (PIPEDA)	Ley de Protección de Datos de Brasil (LGPD)	Ley de Protección de Datos Personales (DPA)	Ley de Protección de Información Personal (POPIA)
Alcance	Aplica a las organizaciones comerciales que operan en Canadá y que recopilan, usan o divulgan datos personales en el curso de actividades comerciales.	Aplica a cualquier operación de procesamiento de datos realizada en Brasil o que involucre datos de individuos en Brasil.	Se aplica a la recopilación y uso de datos personales en el Reino Unido	Aplica a todas las entidades que procesan datos personales en Sudáfrica
Características principales	Consentimiento Acceso a datos Notificación de violaciones de datos	Consentimiento explícito Derechos de los titulares de datos. Autoridad nacional	Principios de procesamiento de datos Derechos del individuo Transferencias internacionales	Consentimiento Derechos de los individuos Notificación de violaciones de datos
Multas	Hasta 10 millones de dólares o el 2% de la facturación global para las empresas. Las multas individuales oscilan entre $5,000 y $100,000 CAD, con sanciones que aumentan por reincidencia e infracciones graves.	multas de hasta el 2% de los ingresos de la empresa en Brasil, limitadas a 50 millones de reales por infracción.	multas de hasta el 4% de la facturación global anual o 17.5 millones de libras esterlinas	Las infracciones pueden resultar en multas o penas de prisión

Tabla 6. Leyes en materia de protección de datos Global

Algunas de las regiones que se observan en la tabla anterior han desarrollado sus marcos regulatorios basándose en las normativas europeas, lo que refleja un enfoque alineado con los estándares internacionales en materia de protección de datos y tecnologías emergentes.

El RGPD no solo establece un estándar elevado dentro de la UE, sino que también ha influido en otras normativas globales, como la Ley de Privacidad del Consumidor de California (CCPA) en Estados Unidos y la Ley General de Protección de Datos (LGPD) en Brasil. Su enfoque proactivo y amplio lo posiciona como un referente en la protección de datos personales.

16 Conclusiones

La ley de protección de datos en Colombia se basa principalmente en un único base legal para el tratamiento de datos (el consentimiento). Sus principios y derechos son bastante tradicionales, pues están fundamentados en la Constitución Política de 1991. Además, la normativa no aborda de manera adecuada los retos que plantea el entorno digital y las nuevas tecnologías de Internet.

El concepto de dato personal está estrechamente relacionado con la identificación de una persona. Según la normativa colombiana los datos se clasifican en categorías que incluyen: públicos, semiprivados, privados y sensibles.

A diferencia de otras regulaciones, tienen 5 o más bases legales para regular la protección de datos, el concepto de dato personal es mucho más amplio, se aleja del paradigma del dato personal que incluye más información como dirección IP, cookies, huellas digitales entre otros.

Las brechas de seguridad que involucran datos personales deben ser notificadas a la autoridad competente dentro de los quince (15) días hábiles siguientes a su detección. En otras regulaciones más avanzadas, como el Reglamento General de Protección de Datos (RGPD), se exige la notificación a la autoridad de control se realice a más tardar 72 horas después de que se tenga conocimiento de la brecha de seguridad.

Los procesos como la creación de guías, manuales y el diseño de roles específicos, como el del oficial de protección de datos, con funciones claramente definidas, están estrechamente vinculados al despliegue de cualquier tecnología que procese datos. Este enfoque se está adoptando cada vez más en diversos países como modelo para fortalecer sus políticas de protección de datos y mejorar la seguridad en el manejo de la información.

Lo anteriormente mencionado es preocupante ya que el avance de las tecnologías es mucho más acelerado que los procesos legislativos. Por ejemplo, si mañana se aprobara un proyecto de ley para actualizar la ley existente, es muy probable que este quede desactualizado rápidamente, poniendo en riesgo la protección de la vida privada de las personas.

El avance de las tecnologías como mencionamos anteriormente afecta a nivel mundial. Según las legislaciones analizadas, la única normativa que se actualiza de manera uniforme y adecuada es la

vigente en la Unión Europea. Esta legislación proporciona herramientas efectivas para sancionar a las empresas que incurren en malas prácticas y vulneran el derecho a la privacidad.

La regulación estadounidense en materia de Internet de las cosas presenta falencias al enfocarse en los dispositivos que utiliza el gobierno federal. Básicamente es una regulación que busca controlar el tratamiento de datos personales y la privacidad de las personas provenientes del Estado.

La mayoría, las empresas más grandes del mundo relacionadas con el IoT son de origen estadounidense. No regular correctamente a estas empresas afecta la privacidad y datos personales, no solo afecta a Estados Unidos, sino a todo el mundo. Un ejemplo claro es el uso de datos personales para obtener decisiones políticas en Estados Unidos, como ocurrió en unas elecciones presidenciales.

Es necesario una mayor inversión en investigación y desarrollo de la tecnología del IoT. Esto es una solución para lograr una mejor regulación, a medida que se incrementa el conocimiento sobre el IoT, es posible que se puedan llegar a nuevos y mejores modelos regulatorios.

El Internet de las cosas puede parecer invasivo en nuestra esfera de privacidad, esto no debe suponer una amenaza para el derecho a la privacidad siempre que se regule de manera eficaz y efectiva. Es crucial respetar el debido proceso de recopilación y tratamiento de datos personales, utilizarlos solo para el fin que fueron recolectados.

Sin embargo, el legislador colombiano ha tratado de incluir el ordenamiento jurídico disposiciones de seguridad directamente aplicables al tratamiento de grandes volúmenes de datos, como la obligación de anonimizarían, ya contemplada en la regulación europea.

La protección de datos personales en Colombia se fundamentó principalmente: la Ley Estatutaria 1266 del año 2008, que aborda el habeas data financiero y la Ley Estatutaria 1581 del año 2012, que regula el habeas data de manera más amplia.

Por lo tanto, siempre se debe cumplir esta legislación y los principios que contempla para asegurar la protección de datos personales. cuando el encargado o responsable del tratamiento de datos realice recolección, uso, almacenamiento o cualquier otro tipo de tratamiento de datos personales de un titular en el territorio nacional.

En cuanto al estado actual de la protección de datos personales en Colombia, el camino hacia un nivel adecuado aún es largo. Colombia necesita mayor precisión en sus normativas de protección de datos personales.

La Ley 1581 de 2012, por ejemplo, ofrece un marco muy genérico. Para la protección de datos personales específicamente en el uso del Internet de las cosas (IoT) y otras tendencias como inteligencia artificial (IA) o algoritmos que realizan tratamientos de datos personales.

El Estado colombiano debe prepararse mediante la implementación de normas específicas y eficientes que respondan a las realidades sociales actuales. Es preciso fortalecer la implementación del principio de trasparencia en las empresas que realizan tratamiento de datos personales.

La Superintendencia de industria y comercio (SIC), como autoridad, debe procurar evitar la vulneración de habeas data mediante la vigilancia constante y eficiente a las empresas que realizan tratamiento de datos personales (TDP).

La cooperación de todos es fundamental, especialmente teniendo en cuenta la brecha tecnológica que existe entre Colombia y la Unión Europea.

Por lo tanto, es fundamental comprender que en esta transición hacia la industria 4.0, no solo se trata de promover conocimientos técnicos, sino también de que las mentes más brillantes de las Ciencias Sociales comprendan que este nuevo orden mundial debe ser diseñado y regulado desde su campo.

La Unión Europea ha avanzado significativamente en el desarrollo de políticas para proteger los datos de sus ciudadanos en el campo de las tecnologías como la protección de datos personales, Internet de las cosas, ciberseguridad, blockchain, biotecnología y la inteligencia artificial.

17 Referencias

Ángela, M. B. (2020). Los derechos digitales en Europa tras la entrada en vigor del Reglamento de Protección de Datos Personales. *Scielo*. http://dx.doi.org/10.4067/S0718-52002020000200121Berrone, P., & Ricart, J. E. (2022). Cities in Motion 2022. *IESE - Cities in Motion*, 27.

Chan, R., Smith, A., & Rosenberg, M. (2019). *Escándalo de datos de Facebook-Cambridge Analytica*. Wikipedia. https://es.wikipedia.org/wiki/Escándalo_de_datos_de_Facebook-Cambridge_Analytica

Cheta, S., & Ashton, K. (2023). *Los orígenes del IoT*. Aplicaciones Tecnologicas. https://at3w.com/blog/iot-internet-of-things-tecnologia-proteccion-contra-rayo-tomas-tierra/#:~:text=Los orígenes del IoT,-El primer objeto&text=Aunque esta máquina de refrescos,fue una tostadora%2C en 1990.

Considerando 74 Del RGPD. Constitución Española. Art, 18 (1978). https://www.boe.es/eli/es/c/1978/12/27/(1)/con

Constitución Política 1 de 1991, Art. 20. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125

Constitución Política 1 de 1991 Asamblea Nacional Constituyente, Art. 230 (1991). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125

Constitución Política de La República de Colombia, Art. 15 (2024). http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Constitución Política de La República de Colombia (1991). http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Corral Talciani, H. (2000). *Configuración Jurídica del derecho a la Privacidad*. Dianet. file:///F:/PERFIL/Descargas/Dialnet-ConfiguracionJuridicaDelDerechoALaPrivacidadIIConc-2650218.pdf.

DDCMS. (2018). *Code of Practice for Consumer IoT Security*. DDCMS. (2020). *Government response to the "Regulatory proposals for consumer Internet of Things (IoT) security" consultation*. https://www.gov.uk/government/publications/secure-by-design

Decisión (Ue) 2016/619 Del Parlamento Europeo y Del Consejo (2016). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016D0619

Decreto 1377 de 2013 (2013). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Directiva 2013/40 (2013). https://www.boe.es/doue/2013/218/L00008-00014.pdf

Directiva 95/46/CE. (1995). *Departamento de Derecho Internacional*. https://www.oas.org/es/sla/ddi/docs/Directiva-95-46-CE.pdf

Echavarría, J., Villamizar, M., & González, J. (s. f.). (n.d.). *El Proceso Colombiano de Desindustrialización.* https://www.banrep.gov.co/docum/ftp/borra361.pdf

El Habeas Data En Colombia (1994). https://repositorio.uniandes.edu.co/server/api/core/bitstreams/9bcf47ab-2bbe-4801-b059-b9f780dc8a55/content

Feldgen. (2018). Internet de las cosas: La tecnología como aliada de la sostenibilidad. *InformeTICfacil.Com*. https://www.informeticplus.com/internet-de-las-cosas-la-tecnologia-como-aliada-de-la-sostenibilidad-eae-business-school#:~:text=Internet de las cosas%3A La,la sostenibilidad (EAE Business School)&text=El informe ofrece una visión,nivel de Latinoamérica

Fernadez, R. (2023). Previsión de la inversión en Internet de las cosas a nivel mundial de 2018 a 2023. *Statista*. https://es.statista.com/estadisticas/1117893/internet-de-las-cosas-gasto-a-nivel-mundial/

Fernandez, R. (2023). Dispositivos conectados (Internet de las cosas) a nivel mundial de 2015 a 2027. *Statista*. https://es.statista.com/temas/6976/el-internet-de-las-cosas-iot/#editorsPicks

General Personal Data Protection Act (LGPD) (2018). https://lgpd-brazil.info/

Hernández, G. (2011). *Historia de las computadoras*. https://www.uv.mx/personal/gerhernandez/files/2011/04/historia-compuesta.pdf

Herrera Carpintero, P. (2016). *El derecho a la vida privada y las redes sociales en Chile*. Revista Chilena de Derecho y Técnología. https://www.rchdt.uchile.cl/index.php/RCHDT/article/view/41268

Ince. (2022). *El panorama de la ciberseguridad IoT en 2024*. https://1nce.com/es-es/recursos/noticias/blog/panorama-de-la-ciberseguridad-de-las-iot

Ley 1266 de 2008, Art. 12 (2008). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Ley 1266 de 2008, Art. 3, Función Publica (2008). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Ley 1266 de 2008 (2008). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Ley 1581 de 2012, Art. 12 (2012). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ley 1581 de 2012, Art. 19, Autoridad de Protección de Datos (2012). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ley 1581 de 2012 (2012). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

LEY 1712 DE 2014 (2014). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

Ley Estatutaria 1581 de 2012, Art. 5, Gobierno de Colombia (2012). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ley Orgánica 3/2018, de 5 de Diciembre, de Protección de Datos Personales y Garantía de Los Derechos Digitales, Art. 34 (2018). https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

López Jiménez, D. (2013). Los códigos tipos como instrumento para la protección de la privacidad en el ámbito digital: apreciaciones desde el derecho Español. *Scielo*. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-52002013000200015&lng=es&nrm=iso&tlng=es

Luis, S. (2021). *Medición avanzada AMI ¿qué significa para Colombia?* https://bismark.net.co/medicion-avanzada-ami-que-significa-para-colombia/

Moreno, C. (2018). Ciudad inteligente y ciudad sostenible. *Anavam*, 31. http://anavam.com/wp-content/uploads/2018/06/Artículo-JUN.pdf

Noto, La Diega, G. (2016). Cloud of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom. *OECD*, 2016.

www.oecd.org/bookshopOfgem. (2015). *Ofgem announces £62.8 million to deliver smarter energy network for consumer*. https://www.ofgem.gov.uk/publications/ofgem-announces-ps628-milliondeliver-smarter-energy-network-consumers

Ortíz, M., & Viollier. (2021). Repensando el derecho al olvido y la necesidad de su consagración legal en Chile. *Revista Chilena de Derecho y Técnología*, 80.

Porcelli, A. M. (2018). Un hito jurídico sobre Internet de las Cosas: la Ley de California n° 327 del año 2018. *Scielo*. https://doi.org/10.1590/2317-6172201953

Protección de Datos Personales (2021). https://www.oas.org/es/sla/cji/informes_culminados_recientemente_Proteccion_Datos_Personales.

Quintana, C. (2021). Caracterización del uso de dispositivos IoT en la población española. In *Gobierno de España*. https://docta.ucm.es/rest/api/core/bitstreams/8ccbe295-2c17-4872-a9a0-702a876b76fa/content

Registro Nacional de Bases de Datos, RNBD., Protección de Datos Personales (2015). https://www.sic.gov.co/registro-nacional-de-bases-de-datos

Resolución 12192 Del 1 de Abril de 2020, Facebook (2020). https://www.sic.gov.co/decisiones-de-apelación-2020#:~:text=Resolución 12192 del 1 de abril de 2020.&text=El Principio de Responsabilidad Demostrada,la información de sus usuarios.

Resolución 30412 Del 23 de Junio de 2020 (fotógrafo). https://www.sic.gov.co/decisiones-de-apelación-2020#:~:text=Resolución 30412 del 23 de,la Ley 1581 de 2012).

Resolución 40072 de 2018. https://gestornormativo.creg.gov.co/gestor/entorno/docs/resolucion_minminas_40072_2018.htm

Roberts, R., & Weidenslaufer, C. (2015). Internet de las Cosas (IoT) Regulación federal de Estados Unidos y del Estado de California. *Biblioteca Del Congreso Nacional de Chile*. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/32180/1/BCN_internet_de_las_cosas_2021.pdf

Rose, K., Scott, E., & Lyman, C. (2015). *La Internet de las Cosas*. Internet Society. https://www.internetsociety.org/es/resources/doc/2015/iot-overview/

SB/327, 1798.91.04 a, 2018. (2018). California to Regulate Security of IoT Devices. *JonesDay*. https://www.jonesday.com/en/insights/2018/10/california-to-regulate-security-of-iot-devices

Sentencia No. T-414 de 1992 (1992). https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm

STC 292/2000, FJ. 5 (2021). https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276

Superintendencia de Industria y Comercio. (n.d.). *Resolución 1321 de 2019*. https://agoramercatorum.uexternado.edu.co/resolucion-1321-de-2019-de-la-superintendencia-de-industria-y-comercio-relevante-en-materia-de-proteccion-de-datos/

Tanczer, L., & M., B. (2019). The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. *SSRN*, 41. file:///F:/PERFIL/Descargas/ssrn-3385548.pdf

Telefónica. (n.d.). *Smart Cities*. https://www.ie.edu/business/centros/Proyectos/Informe Smart Cities ESPweb.pdf

Unión Europea. (2021). *Horizonte Europa: Nuevo programa marco de la ue*. Gobierno de España. https://www.horizonteeuropa.es/que-es

Unión Europea. (2022). Reglamento general de protección de datos. RGPD. *YourEurope*. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

Universidad del Norte. (2018). *Sistemas de medición avanzada en Colombia: beneficios, retos y oportunidades*.
https://www.redalyc.org/journal/852/85259689012/html/#B9

Vega, D. (2015). Red Española de Ciudades Inteligentes. *RECI SmartCities*.
https://www.linkedin.com/posts/danielvegadiaz_red-española-de-ciudades-inteligentes-reci-activity-7029779162487828480-XxDD/?trk=public_profile_like_view

Warren, & Brandeis. (1890). *The Right to Privacy*. Harvard Law Review.
https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Wikipedia. (2021). *Precursor del Internet de las Cosas*. ¿Quién Acuñó El Término IoT?
https://es.wikipedia.org/wiki/Internet_de_las_cosas#:~:text=A.-,¿Quién acuñó el término IoT%3F,mientras trabajaba en Procter %26 Gamble.

Zuñiga, F. (1997). *Derecho a la Intimidad y Habeas Data*. Dianet.
https://dialnet.unirioja.es/descarga/articulo/5085312.pdf

enel La medición Inteligente,Mediodres AMI.
https://www.enel.com.co/es/medicion-inteligente.html

mia, Bogotá extrena la medición inteligente de agua.
https://www.acueducto.com.co/wps/portal/EAB2/Home/general/sala-de-prensa/boletines/detalle/boletin+mia

Aaepd, Agencia Española de Protección de datos
https://www.aepd.es/

Tullave, Ahora puedes recargar tu llave desde plataformas digitales
https://www.tullaveplus.gov.co/

El tiempo, Asi clonavan las tarjetas d etransmilenio.
https://www.eltiempo.com/bogota/clonacion-de-tarjetas-de-transmilenio-43493

Smart cities, La transformación digital de las ciuda.
https://www.ie.edu/business/centros/Proyectos/Informe%20Smart%20Cities%20ESPweb.pdf

El panorama de la ciberseguridad IoT en 2024.
https://1nce.com/es-es/recursos/noticias/blog/panorama-de-la-ciberseguridad-de-las-iot
5200201300020015&lng=es&nrm=iso&tlng=es