# UNIVERSIDAD MAYOR DE SAN ANDRÉS

## FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

## CARRERA DE DERECHO

## PETAENG

# TRABAJO DIRIGIDO

## “BASES JURIDICAS FUNDAMENTALES PARA PLANTEAR UNA FUTURA LEY ESPECÍFICA DE PROTECCIÓN DE DATOS PERSONALES EN NUESTRO PAÍS”

POSTULANTE: José Luis Chana Durán

TUTOR: Dr. Oscar Ricardo Chuquimia

LA PAZ – BOLIVIA

2022

## DEDICATORIA

*Este trabajo está dedicado a Dios por permanecer siempre a mi lado en toda circunstancia.*

*A mis padres, aunque no se encuentran presentes, dieron todo su esfuerzo para mi formación profesional.*

*Al Dr. Oscar Ricardo Chuquimia por su orientación y apoyo permanente en la realización y conclusión del presente Trabajo Dirigido.*

**AGRADECIMIENTOS**

*Agradecer a Dios por darme las fuerzas y sabiduría necesaria para seguir mis estudios profesionales.*

*A mi familia por su apoyo constante e incondicional; a mi hijito Pablo que es la motivación constante de seguir adelante.*

*A las autoridades de la Carrera de Derecho y del PETAENG, al Dr. Oscar Ricardo Chuquimia, tutor del presente trabajo y a la planta de docentes que coadyuvaron con mi formación profesional.*

# ÍNDICE GENERAL

**CAPITULO II**

**MARCO CONCEPTUAL**

CAPITULO III

MARCO TEORICO

CAPÍTULO IV

MARCO NORMATIVO

**CAPÍTULO V**

**ANÁLISIS DE LOS HECHOS**



**CAPITULO VI**

**PROPUESTA DE LA INVESTIGACIÓN**

**CAPITULO VII**

**CONCLUSIONES Y RECOMENDACIONES**

# ÍNDICE DE GRÁFICOS

## INDICE DE CUADROS

# INDICE DE ANEXOS

## RESUMEN

El presente trabajo dirigido aborda un tema fundamental en nuestros días, la protección de los datos de carácter personal frente al crecimiento desmesurado de la Tecnología de la Información, el internet, la comunicación y en contraposición la carencia de una normativa acorde a este avance tecnológico en nuestros días.

De inicio, se efectúa un análisis de la protección de datos y el derecho a la privacidad desde su orígen, evolución histórica como un derecho fundamental de la persona, su ámbito de aplicación, así como el conjunto de principios que deben respetar los responsables y encargados del tratamiento y protección de la información.

La investigación desarrollada tiene muchísima importancia por ser un derecho inherente a la privacidad e intimidad de la persona, el cual es vulnerado de manera constante y en diferentes espacios; además siendo una temática de creciente actualidad, se busca contribuir con toda la información necesaria y los respaldos jurídicos suficientes que favorezcan a plantear soluciones a los vacíos legales existentes en nuestra normativa de manera específica.

En esta investigación se efectúa un análisis histórico de la protección de los datos de carácter personal, del derecho a la intimidad y privacidad, los conceptos y definiciones relacionadas a los datos, su tratamiento y los principios que rigen la regulación jurídica de los mismos; asimismo se realiza un análisis comparativo de la legislación sobre la protección de los datos personales tanto en Europa como en América.

Se realiza un estudio evolutivo acerca de la incorporación y reconocimiento del Habeas Data en las normas constitucionales en los países, sobre todo de Latinoamérica, tomando en cuenta sus características, principios, alcances e implicaciones jurídicas.

Con la finalidad de establecer un sustento teórico al campo jurídico de la protección de datos personales se realiza una revisión bibliográfica acerca de las teorías que la sustentan, debido a que es necesario unificar las visiones distintas existentes en este campo y de esta manera encaminar hacia una única visión teórica que sea lo suficientemente versátil para proteger los derechos que se pretenden, como en el caso del Data Privacy.

Como un sustento normativo internacional se lleva adelante un estudio de las normas a las cuales los países del mundo están adscritos, como la Declaración Universal de los Derechos Humanos, la Convención Americana sobre Derechos Humanos o Pacto de San José, Red Iberoamericana de Datos Personales y el Reglamento General de Protección de Datos (RGPD). Complementariamente se hace un desglose de la normativa nacional, desde la Constitución Política del Estado Plurinacional de Bolivia, leyes y normas sectoriales que regulan y amparan los derechos a la protección de la información y de datos personales.

Se realiza un estudio de la legislación comparada, describiendo de manera concisa las leyes promulgadas en Europa, Estados Unidos y los países de Latinoamérica, estos sirven de base para plantear una futura ley de protección de datos en nuestro país.

En la actualidad como ya se mencionó cobra gran importancia la incorporación de las tecnologías modernas de comunicación, el internet, las redes sociales, etc., que cobran suma importancia y por el hecho de que son medios de generación de datos deben estar necesariamente regulados en una ley específica al respecto.

Con la finalidad de obtener información primaria, y contar con datos reales acerca de la percepción de la población sobre la protección de los datos y las normas actuales que las regulan, se realiza una encuesta en base a un muestreo y se aplica un cuestionario a 50 personas de edades diferentes, desde los 18 hasta los 60; el cuestionario realizado consta de 10 preguntas. Los resultados de la encuesta aplicada de manera muy evidente, nos dan a conocer la importancia y necesidad de regular la protección de los datos en nuestro país en base a una Ley específica.

Siendo Bolivia uno de los países que aún no cuenta con una legislación integral y completa sobre protección de datos personales, en el presente trabajo se ve por necesario realizar una propuesta de anteproyecto de Ley de Protección de Datos Personales en Bolivia.

# INTRODUCCIÓN

La sociedad y la tecnología han evolucionado a un ritmo vertiginoso en los últimos años. Nos encontramos en la era de las telecomunicaciones, en la que el manejo y el intercambio de datos personales se han tornado en una práctica cotidiana en la que interviene el Estado, como sector público, y el sector privado, representado por las empresas. En ambos casos, los datos personales son utilizados para actividades relacionadas, sobre todo, con la venta de bienes y servicios.

Todos los días usamos aplicaciones móviles y el navegador de internet para diversas actividades como comunicarnos, mantenernos informados, realizar compras y ventas, entretenernos, efectuar operaciones bancarias, trabajar, entre otras. Claramente, vivimos en un mundo interconectado.

Como usuarios reconocemos fácilmente las ventajas de vivir conectados. No obstante, existe otro aspecto que no siempre es evidente porque sucede detrás de nuestras pantallas. Hablamos del uso y tratamiento de nuestros datos personales.

Este tipo de prácticas comporta nuevos riesgos para los ciudadanos, por cuanto las leyes nacionales han establecido normas y procedimientos con la finalidad de buscar un debido tratamiento de la información que se encuentra en las bases de datos. Existe la necesidad de perfeccionar dichas disposiciones y de que las mismas respondan a las necesidades particulares que surgen en una sociedad cada vez más globalizada.

Por ello, hace algunos años los gobiernos y activistas empezaron a preocuparse sobre el uso de los datos personales. En muchas partes del mundo (incluida América Latina) los países cuentan, desde hace varios años, con leyes generales de protección de datos, que ponen límites a la recolección y análisis de

información personal y reconocen derechos a los usuarios para evitar abusos y controlar el funcionamiento de la tecnología.

Sin embargo, como la tecnología avanza y cada vez estamos más interconectados, las leyes suelen quedar desactualizadas. La Unión Europea entendió esta situación y emitió un Reglamento General de Protección de Datos Personales ("RGPD" en adelante) que cuenta con nuevas y más sofisticadas herramientas para garantizar un uso adecuado de los datos personales más allá de los límites geográficos, porque la atención primordial está puesta en el interés y los derechos de los usuarios.

Bolivia es uno de los países que aún no cuenta con una ley general de protección de datos personales, aunque en la Constitución Política del Estado está garantizado la protección de los derechos a la privacidad, intimidad, honra, honor, propia imagen y dignidad; sin embargo, aún carece de una ley con características integrales.

Es necesario tener en cuenta que cada día se originan nuevas formas de recolección y procesamiento de datos, como puede evidenciarse en la esfera de las tecnologías de la información y la comunicación. Gracias a internet es cada vez más fácil recopilar la información que representa un gran valor para el comercio electrónico, entre otros usos en línea, situación que, a falta de regulación, ha derivado en una problemática delincuencial. De modo que es fundamental salvaguardar la intimidad como derecho fundamental, proteger la vida privada de las personas y garantizar el pleno ejercicio de sus derechos al momento de utilizar determinados datos.

A pesar de que el uso y manejo de la información no es un tema nuevo en Bolivia, se ha observado que las políticas definidas acerca de protección han resultado insuficientes, al exceder los medios de control y administrativos

gubernamentales. Por ello, podría afirmarse que no es solo el Estado el encargado de proteger a los sujetos de eventuales delitos, por cuanto es la misma persona quien, con sus acciones, puede decidir la información personal que debe ocultarse total o parcialmente para mantener su reserva o cederla a voluntad para determinados fines.

A partir del siglo XVIII, con la aparición de los derechos humanos podría considerarse que inició un proceso de reconocimiento que luego se vería reflejado en diferentes constituciones nacionales como un derecho individual o de primera generación, en especial, la libertad personal. Un ejemplo de ello es Bolivia, que adopta el derecho de habeas data como un derecho fundamental autónomo, distinguible de otras garantías como la intimidad y el buen nombre, que puede ser tutelado en el ámbito interno con sujeción a las normas nacionales o mediante instrumentos internacionales.

En el presente trabajo de investigación, precisamente, se ha efectuado una investigación bibliográfica para determinar la evolución histórica de la protección de datos personales a nivel internacional y nacional.

La relación estrecha entre la protección de datos personales y los derechos a la intimidad y privacidad llevaron a efectuar un análisis profundo sobre la importancia de plantear normas y leyes de protección de la información de los usuarios y registrada en archivos y bancos de datos públicos y privados.

Sin embargo, se puede evidenciar el uso indiscriminado de la información personal que va en detrimento de nuestra privacidad, honor e intimidad personal y familiar. Los datos personales requieren que se regule el uso que se hace de estos, por lo tanto, se pretende que su utilización tenga un propósito que se considere legal y legítimo.

En la era digital en la que vivimos, la obtención, así como el almacenamiento de datos personales son aspectos muy importantes. Los avances tecnológicos relacionados con el análisis de información personal han llegado a un grado de avance que es probable que exista más información sobre una persona, en distintos tipos de archivos de lo que uno pueda imaginarse.

Los hechos y sucesos de la vida de un individuo se almacenan en un banco de datos o archivo, se genera una información que requiere ser protegida de la discriminación y del riesgo de daño a su intimidad, dignidad y honor, siendo capaz el titular de saber quién tiene su información, para qué propósito e incluso oponerse a la tenencia de la misma en manos de un banco de datos, base importante en la autodeterminación.

En la actualidad, las y los bolivianos cuentan con leyes que tocan algunos temas de datos personales, pero lo hacen de manera incompleta y no integral.

Existe una normativa general y sectorial de protección de los datos personales que protege los datos personales, desde la Constitución Política del Estado Plurinacional, Código Civil, Ley general de Telecomunicaciones y TIC, moduladas por sentencias constitucionales; pero se requiere la protección de los datos personales mediante una ley específica, ya que se considera a estos como bienes jurídicos que demandan protección. Además, se debería concretizar con la creación de una entidad encargada de la protección de datos, a través de sistemas de protección de los mismos como las Agencias de Protección de Datos similar a la de otros países, o Autoridades encargadas de la protección de datos personales, con todos sus atributos y responsabilidades.

Por tanto, la presente investigación aborda la problemática a partir de los hechos y ejemplos reales suscitados en nuestro país. A nivel internacional, el caso de

Cambridge Analytica aceleró a varios países y para actualizar y generar nuevas leyes para proteger a sus ciudadanos contra la violación de la privacidad y el usufructo no consentido de sus datos personales. La Unión Europea, Argentina y ahora Ecuador, están entre ellos. En éste último se generó una normativa altamente participativa con la sociedad civil. Dentro de poco, Bolivia será el único país de la región que no cuenta con una Ley de protección de datos personales.

Se efectúa en el primer capítulo un análisis histórico y evolutivo de la protección de datos, la privacidad y la intimidad, mediante el método deductivo, desarrollando los antecedentes históricos en Europa, Estados Unidos y Latinoamérica.

En el segundo capítulo está referido al marco conceptual donde se definen los conceptos fundamentales respecto a la presente investigación, partiendo de los derechos humanos como base legal de aplicación en todo el mundo considerando que los Derechos Humanos son las libertades fundamentales que tiene una persona por el simple hecho de haber nacido, sin los cuales no se puede vivir como tal. El significado e importancia de la privacidad, intimidad, honor, dignidad intrínsecos en el individuo y que están directamente relacionados a la protección de datos como prácticas, salvaguardas y principios fundamentales puestos en ejercicio para proteger la información personal y asegurar que se mantengas en control de ella. Se hace un estudio descriptivo de los tipos de datos personales, los tipos que existen así como el tratamiento de ellos. En el tercer capítulo se realiza un estudio de las teorías básicas sobre la protección de datos a nivel mundial, el derecho a la privacidad, así también la importancia del habeas data y su incorporación de las leyes y constituciones del mundo Uno de los derechos que se ha desarrollado con el avance la tecnología es el que tiene el ciudadano a estar correctamente informado acerca de los datos que y son manejados por el poder público o privado. El capítulo cuarto se desarrolla el marco

normativo, partiendo de la Declaración Universal de los Derechos Humanos, que en su artículo 12, hace referencia a que toda persona debe ser protegida ante injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia, así como de ataques contra su honra y reputación, también se toma en cuenta las diferentes convenciones, redes y reglamentos de protección de datos a nivel mundial como el RGPD; asimismo se efectúa una descripción de la normativa nacional sobre protección de datos, las leyes y los decretos promulgados por el gobierno nacional, así como las legislaciones sectoriales, concluyendo con un análisis descriptivo de la legislación comparada.

En el quinto capítulo se efectúa un análisis de los hechos; tomando en cuenta todos los antecedentes teóricos mencionados.

Se realiza además una prueba de campo aplicando encuestas y entrevistas a la población objeto de estudio, según el muestreo planteado y entrevistas a profesionales, sobre la situación actual de nuestro país en cuanto se refiere a la protección de datos personales. Esta información es considerada primaria debido a que las respuestas obtenidas de las personas abordadas reflejan el conocimiento y conciencia real, de las normas que tienen nuestro país, los procedimiento y formas de tratamiento o finalmente que leyes de protección son los que conocen y en las que se ampara nuestra sociedad.

Con toda la información primaria y secundaria, en el sexto capítulo se realiza una propuesta de un anteproyecto de ley de protección de datos personales para nuestro país.

El presente trabajo de investigación cierra con el séptimo capítulo con las conclusiones y recomendaciones principales.

## 1. ENUNCIADO DEL TEMA DEL TRABAJO DIRIGIDO

**“BASES JURIDICAS FUNDAMENTALES PARA PLANTEAR UNA FUTURA LEY ESPECÍFICA DE PROTECCIÓN DE DATOS PERSONALES EN NUESTRO PAÍS”**

## 2. IDENTIFICACIÓN DEL PROBLEMA

Bolivia aún no cuenta con una ley general de protección de datos personales, por lo que se requiere desarrollar un análisis jurídico profundo al respecto para establecer las bases jurídicas fundamentales y esenciales para plantear a futuro una ley específica de protección de datos personales.

Al efectuar la revisión de la normativa nacional, desde la Constitución Política del Estado Plurinacional, la sentencia constitucional 0965/2004-R, Ley General de Telecomunicaciones y Tecnologías de la información y Comunicación, otras leyes y reglamentos, vemos que los legisladores son muy conscientes de la necesidad de colocar mecanismos de seguridad, límites al tratamiento y hasta otorgar derechos cuando se trata de datos de carácter personal.

Se puede evidenciar que no existe una visión normativa integral sobre datos personales y su respectiva protección. Cada norma contiene artículos que mencionan temas de datos personales, pero desde su propio enfoque, que en algunos casos puede resultar descoordinado hasta contradictorio. Es como intentar armar un rompecabezas de los datos personales con las piezas incompletas.

Al ver en detalle los artículos de las normas citadas y otras, se puede percibir que en sí mismos también se encuentran incompletos. Algunos no incluyen todos los derechos relacionados a la protección de datos personales, no incorporan mecanismos de seguridad, y en otros tampoco se hace mención a todos los principios fundamentales de protección de la privacidad, intimidad y/o reputación.

Compartir información personal puede implicar muchos beneficios. En algunos casos incluso es necesario hacerlo para cumplir con nuestras tareas cotidianas y para mantenernos en contacto en la sociedad moderna. Pero ello implica un riesgo. La información personal revela mucho acerca de cada uno de nosotros, de los pensamientos, y de la vida en general. Esta información puede ser fácilmente utilizada en contra y eso es especialmente peligroso en el caso de individuos y comunidades vulnerables, como, por ejemplo, periodistas, activistas, defensores de derechos humanos y miembros de grupos marginalizados y oprimidos. Es por ello que esta información debe ser protegida de manera muy estricta

Por este mismo hecho, los casos de abuso de la información personal de los usuarios de internet no pasan de ser simplemente hechos noticiosos, sobre todo en países donde no existe una ley de datos personales, como es el caso de Bolivia. La inexistencia de un marco normativo hace que no se puede ir más allá y cuestionar esos hechos ante las instituciones locales, quedando usuarios y usuarias sin acceso a protecciones y reparaciones básicas por abuso de su información de carácter personal.

## 3. PROBLEMATIZACIÓN

Como ya se ha manifestado nuestro país aún no cuenta con una ley de protección de datos personales. Lo que tiene, actualmente, son normas de diversos sectores

que contienen referencias al tratamiento de datos personales. Al analizarlas encontramos que, si bien hay una conciencia de tener que legislar sobre datos personales, no hay una visión normativa integral ni un desarrollo conceptual completo.[1]

Actualmente se habla mucho sobre datos personales. Recientemente, hubo escándalos internacionales por la obtención y utilización fraudulenta de datos personales en elecciones y en redes sociales. De la misma manera, se generaron grandes discusiones normativas cuando el Reglamento de Datos Personales de la Unión Europea entró en vigencia y otros países (incluida buena parte de los países del continente americano) comenzaron a discutir la actualización o creación de leyes al respecto.[2]

A pesar de esto, los casos de abuso de la información personal de los usuarios de internet no pasan de ser “hechos noticiosos” en países donde no existe una ley de datos personales, como es el caso de Bolivia.

La inexistencia de un marco normativo hace que no se puede ir más allá y cuestionar esos hechos ante las instituciones locales, quedando usuarios y usuarias sin acceso a protecciones y reparaciones básicas por abuso de su información personal. Esto debe cambiar.

Por esta razón se debe impulsar la creación de una ley de protección de datos personales en Bolivia, a través de un proceso de diálogo sobre lo que los distintos actores involucrados entienden por datos personales, de manera que los derechos de los usuarios queden en el centro de la discusión.

[1] Arroyo, V. (2019). Guía para una ley de protección de datos personales en Bolivia. https:/www.accessnow.org.
[2] Idem

## 4. DELIMITACIÓN DEL TRABAJO DIRIGIDO

### 4.1. DELIMITACIÓN TEMÁTICA

La delimitación temática especifica se la considera al estudio y análisis de la normativa vigente y la necesidad de plantear una ley de protección de los datos personales, el tema de investigación requiere de un conjunto de elementos teórico conceptuales de carácter jurídico relacionados básicamente con el Derecho Civil, Derecho Informático y especialmente el Derecho Constitucional, por tanto, es de carácter jurídico.

### 4.2. DELIMITACION ESPACIAL

A efecto de cumplir con la rigurosidad de una investigación científica en ciencias sociales la investigación se delimitará espacialmente para efectos de toma de muestra y otros a área del Municipio Urbano de La Paz, Macrodistrito Max Paredes, Distrito 7. Todo del Gobierno Municipal de La Paz.

### 4.3. DELIMITACIÓN TEMPORAL

A fin de realizar revisión documental y otros se tomará un lapso temporal de 10 años del 1 de enero 2018 al 1 de enero de 2021.

## 5. FUNDAMENTACIÓN E IMPORTANCIA DEL TEMA

Las normas actuales en nuestro país, presentan vacíos que requieren ser resueltas jurídicamente.

No existe una norma específica para las personas particulares quienes sufren la vulneración de sus derechos por la publicación de imágenes sin autorización que se dan a a través del internet. Si usan las redes sociales para buscar información está bien, pero no podemos usar el internet para dañar la imagen de una persona o violar la dignidad de las mismas.

Lastimosamente, en Bolivia no tenemos una ley de protección de datos personales y eso es muy lamentable en esta época, donde las personas exponemos cada vez más nuestros datos e imágenes y no se garantiza un tratamiento correcto de los mismos. No existe, por lo que se debe elaborar una Ley de Protección de Datos Personales.[3]

En la actualidad nuestras normas requieren ser nuevamente revisadas y actualizadas según las necesidades y cambios, sobre todo, tecnológicos.

La tecnología avanza a ritmo acelerado que ha dejado muy por detrás aquellos principios jurídicos de protección a la invención y creación del hombre.

Cuando navegamos o usamos aplicaciones vamos dejando rastros de información. Esa información puede revelar quienes somos y cómo usamos la tecnología.

Estos datos personales también son analizados por quienes nos brindan servicios en Internet para diversos fines que incluyen desde brindar una mejor experiencia de uso hasta clasificarnos discriminatoriamente. Esta situación se presenta y repite todo el tiempo.

[3] Durán, Ch.M. (2018). *Normativa sobre protección de datos personales en Bolivia*. https://medium.com › normativa-sobre-datos-personales

En la actualidad, las y los bolivianos cuentan con leyes que tocan algunos temas de datos personales, pero lo hacen de manera incompleta y no integral.[4]

Por lo tanto, la regulación debe ser capaz de poner límites en cuanto a la recolección, el uso y procesamiento de datos personales; establecer sanciones al uso indiscriminado de datos; restringir tratamientos automatizados de datos por parte de empresas que puedan abusar de ellos a través de: vigilancia masiva o dirigida, micro segmentación de perfiles para el posicionamiento publicitario, creación de noticias falsas, u otros mecanismos, que van en contra del derecho de privacidad y de libertad de expresión.[5]

## 6. OBJETIVOS

### 6.1. OBJETIVO GENERAL

Establecer las bases jurídicas fundamentales referidas a la protección de datos personales con el propósito de plantear a futuro una ley específica de protección de datos de carácter personal, acorde al tiempo actual.

### 6.2. OBJETIVOS ESPECÍFICOS

- Efectuar un análisis de la evolución de la normativa referida a la protección de datos e imágenes de las personas que se difunden a través de las redes sociales.

[4] Arroyo, V. (2019). *Guía básica sobre datos personales para Bolivia.* https:/www.accessnow.org.
[5] Leon, C.C., Quiroz, E., Foronda, A. (2018). *Protección de Datos Personales y Derechos Digitales*.http://library.fes.de

- Analizar las normas nacionales actuales que regulan y sancionan la protección de datos e imágenes y de personas que se publican a través del internet y que vulneran sus derechos adquiridos.

- Efectuar un estudio comparativo de la legislación nacional e internacional sobre la protección de datos de las personas en concordancia con el desarrollo tecnológico.

- Desarrollar un análisis de la normativa actual de protección de datos personales, en torno a la era digital.

- Plantear una propuesta de ley de regulación y protección de datos personales en el marco del desarrollo tecnológico actual.

## 7. METODOS Y TECNICAS A UTILIZAR EN EL TRABAJO DIRIGIDO

Conforme los lineamientos de la presente investigación se utilizó métodos científicamente aceptados para la investigación en ciencias sociales en ese sentido se utilizó los siguientes métodos:

### 7.1. MÉTODOS ESPECÍFICOS

#### 7.1.1. MÉTODO BIBLIOGRÁFICO

En un sentido amplio, el método de investigación bibliográfica es el sistema que se sigue para obtener información contenida en documentos. En sentido más específico, el método de investigación bibliográfica es el conjunto de técnicas y estrategias que se emplean

para localizar, identificar y acceder a aquellos documentos que contienen la información pertinente para la investigación.

El método documental o bibliográfico consiste en la captación por parte del investigador de datos aparentemente desconectados, con el fin de que a través del análisis crítico se construyan procesos coherentes de aprehensión del fenómeno y de abstracción discursiva del mismo, para así valorar o apreciar nuevas circunstancias.[6]

### 7.1.2. MÉTODO ESTADÍSTICO

Método Estadístico es un proceso de obtención, representación, simplificación, análisis, interpretación y proyección de las características, variables o valores numéricos de un estudio o de un proyecto de investigación para una mejor comprensión de la realidad y una optimización en la toma de decisiones. El Método Estadístico en las Ciencias sociales se convierte en una herramienta poderosa de precisión científica en la medida en la que se combine con los métodos cualitativos y se emplee de acuerdo a las necesidades y al sano criterio.

Con la utilización de este método, en el presente trabajo a partir de la obtención de datos primarios, a través de la aplicación de encuestas a la población de a pie sobre la base de un muestreo estadístico y los resultados obtenidos cuantitativamente se podrá inferir las acciones futuras a tomar. Los datos tabulados con la información directa servirán como base informativa de la condición acerca de la necesidad e importancia de plantear una normativa acorde a la realidad actual.

[6] Botero, B.A. (2003). La metodología documental en la investigación jurídica: alcances y perspectivas. thttps://dialnet.unirioja.es

### 7.1.3. MÉTODO JURIDICO TELEOLÓGICO

Este método consiste en tele significa fin, lógico: pensamiento, cuando hablamos del método teleológico se habla desentrañar el fin normativo, espíritu de la ley, el objetivo que persigue una disposición. El punto de contacto entre el método histórico evolutivo y método teleológico es que al analizar las necesidades históricas, se ve obligado a evaluar su pensamiento, y al evaluarlo tiene que extraer cual fue su propósito o finalidad norma. A la luz del método teleológico el derecho autentico es el que se vive de modo real por la gente y que se aplica en las sentencias y en las resoluciones. Ninguna ley puede ser entendida como mandato sin conocer las condiciones y necesidades del pueblo en que se aplica.

El método teleológico distingue entre ciencias de la naturaleza y ciencias de la cultura. En esta última se encuentra la ciencia del derecho, la cual utiliza los valores o fines para elaborar e interpretar los conceptos jurídicos.[7]

Con la aplicación de este método se determinará el interés jurídicamente protegido y se establecerá la naturaleza socio jurídica con relación a la importancia de la protección de datos de carácter personal en nuestro país.

## 7.2. MÉTODOS GENERALES

Se utilizará el método deductivo en la presente investigación, por el razonamiento mental que conduce de lo general a lo particular y permite extender los conocimientos que se tienen a una clase determinada comportamiento de la sociedad en general. Es un razonamiento que consiste en partir de un principio general conocido para llegar

[7] Melian, V.J (2003). *Métodos de la Ciencia Jurídica*. https://accedacris.ulpgc.es

a otro principio supuesto o equivalente con objeto de extraer consecuencias y aplicaciones, por medio del razonamiento para deducir comprobaciones.

El proceso de deducción va de lo general a lo particular, e implica sistematizar conocimiento y establecer inferencias que se aplican a varias situaciones y casos pertenecientes a un conjunto.[8]

En el presente trabajo se efectuará un análisis deductivo a partir de las normas generales a nivel internacional y también de la normativa nacional que nos permitirá considerar la regulación específica de la protección de datos de carácter personal, a través de una mejor organización, estructura y propuesta jurídica.

## 8. TECNICAS A UTILIZARSE EN EL TRABAJO DIRIGIDO

Las técnicas de investigación son procedimientos y recursos de que se vale la ciencia para conseguir su fin. Sin embargo, el nivel del método o de los métodos no tienen nada en común con el de las técnicas, entendiéndose, las técnicas como procedimientos operativos rigurosos, así en correlación al método ya descrito las técnicas a utilizarse serán:

- La revisión bibliográfica de material relacionado al tema mediante fichaje bibliográfico.
- La entrevista a abogados.
- La toma de encuestas a la población objeto de estudio.

[8] Villabella. A.C.M. (2015). *Los Métodos en la Investigación Jurídica*. https://archivos.juridicas.unam.mx

# CAPÍTULO I

# MARCO HISTÓRICO

## 1.1. LA PROTECCIÓN DE DATOS A LO LARGO DEL TIEMPO

### 1.1.1. La antigua Grecia

Los griegos tenían un concepto distinto de lo que era la privacidad, para los griegos lo importante era la ciudad, la polis, la comunidad; el individuo era ciertamente algo secundario.

Los griegos no lograron configurar un derecho a la intimidad con el contenido y con la interpretación que de él se realiza en la actualidad. Sin embargo, es en la sociedad helénica en donde podemos encontrar las primeras manifestaciones de intimidad a partir de la meditación y la contemplación, prácticas que fueron valoradas por entenderse que a través de la reflexión se alcanzaba una plena vida interior, lo que representaba una íntima relación con el ser divino. Para el mundo helénico, el hombre alcanzaba la sabiduría y el fundamento de su individualidad solo mediante la reflexión y el pensamiento interior. Sócrates decía “conócete a ti mismo”.

El derecho a la intimidad sí se manifestó en estos tiempos, pero fue eficazmente reprimido por la existencia de la vida común y la participación en la vida de la polis, a la cual los ciudadanos estaban obligados.[9]

### 1.1.2. Roma

[9] Zaballos, E. (2013) La protección de datos personales en España: evolución normativa y criterios de aplicación. (Memoria-grado Doctor). Universidad Complutense de Madrid, Madrid España. Recuperado de https://eprints.ucm.es/22849.Madrid, España

En Roma se dan cuenta que no siempre tiene que ser asi, de hecho, se dan cuenta porque ellos tienen esclavos, se dan cuenta que ellos pueden poseer el cuerpo de un esclavo, pero no su mente, la mente del esclavo sigue siendo libre, que sigue haciendo, pensando, creyendo, etc., lo que quiera. Entonces se dan cuenta que hay un hombre interior y un hombre exterior; ese hombre interior es la primera vez que se le da forma, eso quedamos en llamarlo hoy en día privacidad.[10]

En estos tiempos, la concepción mística religiosa de la intimidad, caracterizada por el mundo griego como la búsqueda de una comunión con lo divino, desaparece. Roma, a diferencia de Grecia, realizará la distinción entre lo público y lo privado84. El mundo romano también entendió a la intimidad como una necesidad de cada individuo de conocerse a sí mismo y a su esencia personal, pero en general el derecho romano trató con desprecio a la intimidad, a partir de una serie de referencias normativas que declaraban ilegales los matrimonios de personas de edad avanzada porque se estimaban inútiles, o la configuración del adulterio como un delito de acusación pública.

Ahora bien, sea como fuere, lo cierto es que la idea de intimidad adquiere mayor significación en el mundo romano que aquella que le había reconocido el mundo griego, dejando a salvo la filosofía epicúrea como un importante antecedente helénico.

### 1.1.3. Surgimiento del Cristianismo

Durante el imperium de Augusto nació Jesús “el Cristo”, y este hecho modificó la historia de la humanidad de tal manera que dividimos los tiempos históricos en “antes” y “después” de Cristo.

[10] UNIVERSITAT POLITÉCNICA DE VALENCIA (2016, enero 28 ). Historia de la Protección de Datos Personales. www.youtube.com/watch?v=S7uXyCyOwyw

Si analizamos el concepto de intimidad en el mundo cristiano, encontramos en el Nuevo Testamento, en el Evangelio de San Mateo, un reconocimiento a la intimidad como la manifestación de Dios en la propia vida interior.[11]

La libertad religiosa es una manifestación de la intimidad, la publicación del Edicto de Milán en el año 313, acordada por Emperadores Constantino y Licinio dio a los cristianos, como a todos los demás la libertad de seguir la religión que cada cual quiera. Suprimió por completo la acusación pública de adulterio, al entender que era indigno para los matrimonios verse perturbados por la audacia de extraños.

### 1.1.4. Edad Media

Con San Agustín, el hombre es considerado como portador de valores eternos. Llega Santo Tomas quien se da cuenta que cuando el hombre está rezando, tiene un momento de intimidad que debe ser sagrado porque es su comunicación con Dios, eso de la intimidad se remite al pater familias, solamente el padre de familia tiene privacidad, la familia es su único ser que goza de esa privacidad, no el individuo.[12]

Debe tenerse en cuenta que la intimidad es un valor que se había ido consolidando sólo desde el predominio de la clase social burguesa y la aparición del individualismo, desde aproximadamente el fin de la Baja Edad Media, que da paso al "Renacimiento" y el "Humanismo", términos decididamente ambiguos que apenas si sirven para

[11] Zaballos, E. (2013) La protección de datos personales en España: evolución normativa y criterios de aplicación. (Memoria-grado Doctor). Universidad Complutense de Madrid, Madrid España. Recuperado de https://eprints.ucm.es/22849.Madrid, España

[12] UNIVERSITAT POLITÉCNICA DE VALENCIA (2016, enero 28). Historia de la Protección de Datos Personales. www.youtube.com/watch?v=S7uXyCyOwyw

describir la evolución de dos o tres siglos desde el “otoño de la Edad Media” descrito por HUIZINGA 11 , hasta la plena Edad Moderna.[13]

### 1.1.5. Edad Moderna

En esta edad los filósofos de la “razón” aparte de los conceptos de la “libertad negativa” donde se reconoce al individuo en una esfera íntima y en concreto con Jacobo Rousseau nos habla de la intimidad desde el ámbito de la persona.

Aquí se produce un cambio de mentalidad en el hombre, que a partir de entonces llamamos con justicia “moderno”. Por eso, seguramente la palabra más acertada para referirse a este conjunto de fenómenos es “Modernidad”. La autoafirmación del individuo produce el individualismo, y éste, la demanda de intimidad como un bien deseable, que termina siendo protegido por el ordenamiento jurídico. Por otro lado, “el comercio es cálculo”, como dijo Constant, y los burgueses capitalistas de la Edad Moderna necesitan más y más información para poder calcular si un negocio u operación son suficientemente rentables. El capitalismo a la postre acaba llevando al tratamiento masivo de datos personales, cuando los empresarios comienzan a ofrecer bienes y servicios al gran público. Y, sobre todo, el estado moderno es el vector impulsor más decisivo para el tratamiento de datos de carácter personal.

El Estado moderno, que es esencialmente un Estado burocrático, ejerce su dominio, además de con la fuerza cuando es preciso, a través del conocimiento. Ciertamente,

[13] Huerta, P. P. (2017). La génesis del derecho fundamental a la protección de datos personales. (Tesis Doctoral) Universidad Complutense de Madrid, Madrid. Recuperado de https://eprints.ucm.es/43050//1/T38862.pdfA

en estas transformaciones se encuentran las bases de la evolución que acaba conduciendo a la aparición de la protección de datos en la segunda mitad del siglo XX.[14]

### 1.2. ORIGEN DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

Los factores más importantes que han provocado la necesidad de la protección de datos personales han sido la protección a la dignidad humana, la preocupación jurídica por la intimidad y el honor y, el impacto social producido con la aparición de los ordenadores. Además, otro factor importante en Europa continental, fue el activo rechazo a la barbarie nazi y a los totalitarismos de la primera mitad del siglo XX, que aprovecharon todo tipo de información personal para llevar a cabo la persecución y exterminio de determinados colectivos de personas.

### 1.3. ANTECEDENTES EN ESTADOS UNIDOS

El origen más claro del campo de la protección de datos lo encontramos en Estados Unidos en el ensayo publicado como artículo en la Harvad Law Review como "The Right to Privacy" por Warren y Brandeis en 1890, donde se establece lo que ahora se considera la definición más aceptada sobre la privacy. La privacidad se entiende de forma general como aquel derecho a ser dejado solo o a no ser molestado, “the right to be let alone”. Por ello, se puede observar que la privacidad se fundamenta en el anonimato, el secreto, teniendo como pilares la autonomía, individualidad el desarrollo de la personalidad, y la inviolabilidad de la dignidad personal.[15]

---

[14] Huerta, P. P. (2017). La génesis del derecho fundamental a la protección de datos personales. (Tesis Doctoral) Universidad Complutense de Madrid, Madrid. Recuperado de https://eprints.ucm.es/43050//1/T38862.pdfA

[15] Nisa, A. J. (2020). Origen Jurídico Histórico de la Protección de Datos. https:// elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la

Asimismo, históricamente mucho más atrás en 1763, nos encontramos con el autor de la cita del clásico aforismo inglés “a man’s house as his castle” (la casa de cada uno es su castillo) de William Pitten. Un principio básico del Derecho inglés el cual otorga a cada ciudadano como individuo la protección de su hogar como aquel lugar donde se da la máxima protección personal. La pretensión de William Pitten en 1763 fue la reivindicación de la protección personal del individuo frente al poder del Monarca en cualquier lugar, incluido en la más humilde morada.[16]

Pero no fue hasta algunos años después en 1905 cuando la Corte Suprema de Georgia aplicó claramente desde un punto de vista jurídico por primera vez el concepto protección de datos y privacidad.

El caso Pavesick & New England Life Insurance Company: Aquí se reconoce la existencia del derecho a la propia imagen y el derecho a la intimidad de la vida privada; todo ello bajo el fundamentado jurídico de que ese derecho es un derecho innato que surge a la luz de las leyes naturales. La sentencia indica que la libertad personal abarca tanto el derecho a la vida pública como un derecho correlativo a la intimidad al mismo nivel de protección que el primero y de carácter inviolable. A partir de aquí todo fue un incremento de derechos en la esfera de la privacidad y protección de datos en los años posteriores en los Estados Unidos.

### 1.4. ANTECEDENTES EN EUROPA

Respecto a Europa y hasta mitad del siglo XX las únicas referencias fueron de carácter filosófico, donde podemos encontrar a de Benjamín Constant De Rebecque, Jeremy Bentham, Thomas Hobbes, John Looke o Robert Price. Los países europeos que fueron

[16] Nisa, A. J. (2020). Origen Jurídico Histórico de la Protección de Datos. https:// elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la

precursores de la protección de datos en europea fueron Reino Unido y Alemania principalmente, debido a su fecha y contenido regulado. La primera de todas fue el Reino Unido la cual comenzó su debate en 1961 cuando Lord Mancroft presentó un proyecto de ley cuyo objetivo era la regulación y protección de la privacidad.[17]

Tras más de 23 años de debates, la Comunidad Europea en esa época aprobó el Convenio para la Protección de las Personas con respeto al Tratamiento Automatizado de Datos de Carácter Personal, de 28 de enero de 1981.

Por otro lado, nos encontramos con Alemania, la cual inició la andadura legal en la protección de datos personales con la Ley de Hesse una ley promulgada por el Land de Hesse en 1970 donde regulaba ciertos aspectos sobre el secreto de las comunicaciones o el derecho sobre el control de datos. Posteriormente en 1977 se aprobó a nivel federal en Alemania una ley contra el uso ilícito de los datos personales y la protección de datos. Adelantándose en fecha de entrada en vigor a Reino Unido, aunque este último llevara más años debatiendo legalmente sobre dicha temática. Asimismo, también existen otras legislaciones sobre la materia como la Sueca de 1973, entre otras. A partir de aquí progresivamente fueron publicándose diferentes legislaciones en la materia en todos los países.[18]

La realidad de esta época nos muestra que llevó casi un siglo desde que en Estados Unidos se comenzó a legislar hasta que Europa comenzó a realizar la misma tarea.

[17] Idem

[18] Nisa, A. J. (2020). Origen Jurídico Histórico de la Protección de Datos. https:// elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la

La falta de un consenso para entender la necesidad de creación de una legislación de bases sobre protección de la privacidad que permita posteriormente en base a la misma desarrollar diferentes legislaciones de protección en base al ámbito de actuación, es una carencia que arrastramos hasta el día de hoy y que se suple reformando la norma. La refundición para la creación de una norma base es necesaria, y la creación de específicas un paso necesario ante la invasión en todos los ámbitos del ser humano por parte de la Inteligencia Artificial y el IOT, gracias al Data Mining.

### 1.5. DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS

La Declaración Universal de los Derechos Humanos fue firmada en Nueva York el 10 de diciembre de 1948, otros derechos de los ciudadanos se han ido sumando a estos primeros derechos de 1948, en este sentido se habla de los derechos humanos de segunda y tercera generación. Entre los derechos humanos de tercera generación se encuentra el derecho a la protección de datos de carácter personal.

El Derecho a la protección de datos ha tenido un intenso desarrollo normativo desde que justamente en la Declaración Universal de los Derechos del Hombre, tuviese su primer antecedente en su artículo 12:

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

En una primera fase normativa, la protección de los datos de carácter personal estaba vinculada al uso de la informática y a la “afectación de una serie de datos o conocimientos precisos que resultaban referibles a la esfera de intimidad del sujeto”, pero muy

pronto se produjo la distinción entre privacidad e intimidad, de manera que todo tratamiento de datos y recolección de los mismos en un archivo quedaba amparado por la normativa en materia de protección de datos de carácter personal.[19]

### 1.6. ANTECEDENTES EN AMÉRICA LATINA

A diferencia de la Unión Europea, en américa Latina no existe un tratado internacional que regule el derecho a la protección de datos personales. Podría pensarse que en el numeral 45 de la Declaración de Santa cruz de la Sierra, del 15 de noviembre de 2003, se encuentra el fundamento para su reglamentación, en virtud de que representantes de veintiún países reunidos en la XIII cumbre iberoamericana de Jefes de Estado y de Gobierno, celebrada en Bolivia, manifestaron su preocupación frente a la protección de datos personales como un derecho fundamental de las personas y destacaron la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La antigua, por la que se creó la Red iberoamericana de Protección de Datos, abierta a todos los países de dicha comunidad.

En materia mercantil, mediante pronunciamiento emitido en 1996 por la Uncitral y denominado “Model Law on Electronic commerce” (relativo al comercio electrónico), frente a la validez del contrato electrónico la ONU intentó dar garantía al marco legal y adaptar los requisitos legales existentes para aumentar la seguridad del proceso. Expresó que no se puede negar el efecto legal o la validez al contrato o su aplicabilidad por presentar la información en formato digital.

[19] Mayorga, J.T.C.,Garcia,J.M. (2019). Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos. https://dialnet.unirioja.es

Mediante el pronunciamiento “Model Law on Electronic Signatures”, de 2001, este organismo estableció, entre otros aspectos, que la firma electrónica debía ser considerada igual a la firma original sin perjuicio de producto tecnológico en particular, en aras de garantizar la autenticidad y seguridad de las partes por cuanto las firmas digitales constituyen una herramienta esencial en las transacciones y un elemento imprescindible en el comercio electrónico.

De otra parte, dada la importancia de los pronunciamientos de la Organización para la cooperación y Desarrollo Económico (OCDE) en cuanto a protección de datos, es preciso considerar que el comité de Política del consumidor de este organismo inició en 1998 el desarrollo de un conjunto de lineamientos generales para proteger a los consumidores en el comercio electrónico y eliminar barreras en el mismo; culminó en 1999 con la expedición de la “Recomendación del consejo de la OCDE relativo a los lineamientos para la protección al consumidor en el contexto del comercio electrónico”.

Uno de los objetivos de la OCDE es promover políticas para la expansión de la economía y del empleo que permitan la estabilidad financiera de los países miembros y así el desarrollo de la economía mundial.

Luego, la asamblea General de la OEA, al considerar la creciente importancia de la privacidad y la protección de datos personales, así como la necesidad de fomentar y proteger el flujo transfronterizo de información en américa, aprobó declaraciones y resoluciones que se compilaron en el documento OEA 5232/11, junio 2011, entre las que se halla la Resolución 2661 (XLI-O/11) sobre el acceso a la información pública y protección de datos personales.

El papel de la OEA es determinante en la protección de datos en la región, puesto que los países que la conforman deben adoptar sus disposiciones sobre la materia en un escenario un poco más global, dado su ámbito de aplicación.

Si la OEA adopta medidas estratégicas, beneficiará a todos los países latinoamericanos y logrará que nos convirtamos en un lugar en donde se pueda invertir sin reserva en negocios que involucran transferencia de datos personales desde diversas partes del mundo. Esto hará que América Latina sea más competitiva frente a otros sitios del globo terráqueo respecto de nuevos y más significativos negocios en TIC e información personal.

Pese a que no existe un tratado, los países latinoamericanos sí han realizado esfuerzos en aras de regular la protección de los datos personales, hacer efectivo el derecho de habeas data y otorgar reconocimiento constitucional a las normas estatales adoptadas.[20]

[20] Rojas, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. https:// novumjus.ucatolica.edu.co/article/download/652/670

# CAPÍTULO II

# MARCO CONCEPTUAL

## 2.1. DEFINICIONES CONCEPTUALES EN EL ÁMBITO DE LA PROTECCIÓN DE DATOS

### 2.1.1. Derechos Humanos

Los Derechos Humanos se definen como universales, indivisibles e interdependientes. El 10 de diciembre se celebra el Día Internacional de los Derechos Humanos, una jornada en la que se rememora la proclamación de la Declaración Universal de los Derechos Humanos (DUDH), adoptada por la Asamblea General de la ONU en su resolución 217 A (III), de 1948.

Tras la DUDH se han adoptado una serie de tratados internacionales sobre derechos humanos y otros instrumentos que han desarrollado el marco jurídico internacional aplicable.[21]

Los Derechos Humanos son las libertades fundamentales que tiene una persona por el simple hecho de haber nacido, sin los cuales no se puede vivir como tal.

Fueron creados por la Asamblea General de las Naciones Unidas en 1948 y están agrupados en la Declaración Universal de los Derechos Humanos. En total, los seres humanos gozamos de 30 derechos.

**1. Características de los Derechos Humanos**

[21] Ministerio de Asuntos Exteriores. (2016). Derechos Humanos en el Mundo. www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/DerechosHumanos/Paginas/Derec

Todos los Derechos Humanos comparten las mismas características:

**a. Son universales:** Todos los seres humanos, sin distinción alguna, cuentan con los mismos Derechos Humanos.

**b. Inderogables:** Los Derechos Humanos están fuera del debate democrático. Por ello, no pueden ser alterados por los Estados.

**c. Inalienables:** Los Derechos Humanos no pueden ser renunciados, ignorados o desconocidos por las personas y los gobiernos. Adicionalmente, ningún ser humano puede ser obligado a renunciar a sus Derechos.

**d. Imprescriptibles:** Los Derechos Humanos no pierden vigencia, ya que se ejercen de manera permanente.

**e. Indivisibles:** Todos los Derechos Humanos tienen la misma importancia y jerarquía. Forman un conjunto de derechos que garantizan las libertades fundamentales de los individuos.

**f. Interdependientes:** Los Derechos Humanos esta relacionados entre sí y dependen del cumplimiento de todos los Derechos para su funcionamiento.

**2. Categorías de los Derechos Humanos**

a. **Derechos Civiles:** Son aquellos Derechos Humanos relacionados a la vida cotidiana del individuo. Algunos ejemplos de los Derechos Civiles son: Derecho a la vida, Derecho a practicar una religión, Derecho a una nacionalidad.

b. **Derechos Políticos:** Son los Derechos que promueven y garantizan la participación de los ciudadanos en la toma de decisiones políticas de los países. Algunos ejemplos de los Derechos Políticos son: Derecho a votar, Derecho a formar partidos políticos, Derecho a estar inscrito en un registro electoral.

c. **Derechos Económicos:** Son los Derechos Humanos que promueven la participación de los individuos en las actividades económicas, laborales y profesionales. Algunos ejemplos de los Derechos Económicos son: Derecho a un trabajo, Derecho a la propiedad privada, Libertad de crear una empresa.

**d. Derechos Sociales:** Son los Derechos Humanos que promueven el bienestar y seguridad social. Algunos ejemplos de los Derechos Sociales son: Derecho a la educación, Derecho a la salud, Derecho a la alimentación.

**e. Derechos Culturales:** Son los Derechos que promueven la participación del individuo en los beneficios dela vida cultural de la comunidad y a nivel nacional. Algunos ejemplos de los Derechos Culturales son: Derecho a conocer y preservar la identidad histórica, Derecho a participar en la música, arte, literatura, danza entre otros.[22]

Los derechos humanos son y deben ser observados y respetados por todas las instituciones públicas y privadas, dado que son la base de una convivencia social armónica dentro del Estado de derecho. Uno de los derechos fundamentales que deben tomar en cuenta las instituciones es la protección de los datos personales de los ciudadanos. Es vital preservarlos incólumes ante la voracidad de la tecnología y las redes sociales, que hoy por hoy son el medio de comunicación global. Ante este panorama, se vulnera más el derecho a la intimidad de las personas.[23]

[22] FUNDEMAS. (2014). Qué son los derechos humanos?. https;//fundemas.org/index.php?option=com_content&view=article&id=387&Itemid=80. El Salvador, C.A.

[23] Milenio, Diario, S.A. (2014). Derecho Humano a la Protección de Datos Personales. (https:// www.milenio.com/opinion/varios-autores/derechos-humanos/derecho-humano-a-la-proteccion-de

### 2.1.2. Data privacy

Data Privacy pretende proteger los datos privados de la utilización indebida regulando su correcto uso, recolección, borrado total o parcial, así como almacenaje y tratamiento de los mismos. El Data Privacy es el derecho a proteger.

### 2.1.3. Data Protection

Por el contrario, el Data Protection serían los métodos o políticas de seguridad todo ello a nivel técnico y regulado legalmente; establecidas para asegurar la correcta protección del Data Privacy. Data Protection la herramienta que se usa para proteger, objeto a proteger vs herramienta a usar.

### 2.1.4. Derecho a la Privacidad

El término “privacidad” es una palabra que no puede ser usada sin relacionarla al tema de protección de datos personales.

Aparece por primera vez en 1890 en Estados Unidos en el famoso artículo “The right to privacy” de los autores Samuel D. Warren y Louis D. Brandeis. En este artículo, se hace un pronunciamiento respecto de los cambios que sufren las sociedades desde el punto de vista económico, político y social, cambios que implican el reconocimiento de derechos, como lo son el derecho a la privacidad y a la protección de información personal.

Warren y Brandeis enfocan su artículo en un derecho que garantiza la protección a las personas respecto de su vida privada, en contra de las injerencias de los medios de información, como lo era la prensa. Este derecho “the right to privacy”, fue resumido a “the right

to be let alone", derecho que de alguna manera también se había previsto en la regulación francesa en materia de prensa sin que se hiciera referencia exacta al concepto de privacidad o derecho a ser dejado solo.

Posteriormente, en 1960 William L. Prosser establece cuatro tipos de "torts" (agravios) a la privacidad, los cuales derivaron de los precedentes establecidos por los tribunales de Estados Unidos, y que habían tomado como referencia el derecho establecido en el artículo de Warren y Brandeis.

Este derecho a la privacidad o a ser dejado sólo, según fue comprendido por los franceses, fue planteado por los autores sin conocer las implicaciones y precedentes que fijaría en su aplicación e interpretación, pues la mayoría de las cortes de Estados Unidos lo reconocieron, al grado de que la Suprema Corte de dicho país lo consideró como derecho con protección constitucional. No sobra mencionar que este derecho tiene al día de hoy una relevancia trascendental en Estados Unidos como parte de un nuevo concepto de privacidad en relación a su seguridad nacional, pero que sin embargo también resulta ser uno de los derechos más controvertidos pues Estados Unidos es considerado uno de los países que más indaga sobre la información de las personas. Basta con mencionar, como ejemplo, la conocida "lista negra" del ex presidente Bill Clinton que no es otra cosa sino una lista en donde se incluyen los nombres de personas y empresas que según ese país se encuentran relacionados con el narcotráfico.

### 2.1.5. Derecho a la Dignidad

La "Carta de los Derechos Fundamentales de la Unión Europea" de 2000, regula el Derecho a la Privacidad en sus artículos 1, 7,8, 10, 11 y 12 que respectivamente expresan:

Artículo 1:“La dignidad humana es inviolable. Será respetada y protegida.”[24]

La dignidad de la persona es el rasgo distintivo de los seres humanos respecto de los demás seres vivos, la que constituye a la persona como un fin en si mismo, impidiendo que sea considerada un instrumento o medio para otro fin, además de dotarlo de capacidad de autodeterminación y de realización del libre desarrollo de la personalidad. La dignidad es así un valor inherente a la persona humana que se manifiesta a través de la autodeterminación consciente y responsable de su vida y que exige el respeto de ella por los demás.

La dignidad del hombre, como ente ético-espiritual, puede, por su propia naturaleza, consciente y libremente, autodeterminarse, formarse y actuar sobre el mundo que lo rodea. A su vez, la dignidad es la categoría que corresponde al ser humano por estar dotado de inteligencia y voluntad, distinto y superior a todo lo creado, que establece un tratamiento en toda circunstancia concordante con la naturaleza humana.

La dignidad de la persona se constituye en el valor supremo y en el principio jurídico que constituye la columna vertebral básica de todo el ordenamiento constitucional y es fuente de todos los derechos fundamentales, irradiando todo el sistema jurídico el que debe interpretarse y aplicarse conforme a las condiciones en que dicha dignidad se realice de mejor forma.

La dignidad de la persona humana consiste en el hecho de que, cada ser humano es humano por fuerza de su espíritu, que lo distingue de la naturaleza impersonal y que lo capacita para, con base en su propia decisión, volverse consciente de sí mismo, de

[24] Villalta, Ana. E. (2017). La privacidad y la protección de datos personales. https://www.oas.org/es/sla/cji/docs/informes_culminados_recientemente_Proteccion_Datos_Personales_C

autodeterminar su conducta y dar forma a su existencia y al medio que lo rodea. Todo individuo humano es un ser que desarrolla su libertad autonoma, autodeterminando su conducta.

La dignidad de la persona humana consiste en el valor y pretensión de respeto intrínseco y simultáneamente social, al cual pertenece cada ser humano por su condición humana.

Podemos sostener la primacía de la dignidad de la persona sobre los derechos fundamentales, ya que estos tienen su fuente y fundamento en la primera, debiendo rechazarse el ejercicio de cualquier derecho que suponga un atentado a ella. La dignidad de la persona constituye una barrera insuperable en el ejercicio de los derechos fundamentales. La dignidad humana se constituye en una barrera o límite inmanente a toda reforma constitucional, que pretenda desconocerla, suprimirla, degradarla o desnaturalizarla. La dignidad del ser humano es el minimum invulnerable que todo ordenamiento y operador jurídico debe asegurar y garantizar, sin que nunca pueda legitimarse un menosprecio del ser humano como persona digna.[25]

### 2.1.6. Derecho a la Intimidad

El derecho a la intimidad consiste en la defensa de la persona en su totalidad a través de un muro que prohíbe publicar o dar a conocer datos sobre temas como la religión, la política o la vida íntima. Todo el ser humano tiene derecho absoluto a mantener su vida privada y bajo ningún concepto, esto no puede ser revelado ni siquiera a una persona muy cercana, ni al tutor legal, en caso de que sea menor de edad.

[25] Nogueira, H. (2007). El derecho a la propia imagen como derecho fundamental implícito, fundamentación y caracterización. www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122007000200011.

La intimidad es la parte de la vida de una persona que no ha de ser observada desde el exterior, y afecta sólo a la propia persona. Se incluye dentro del “ámbito privado” de un individuo cualquier información que se refiera a sus datos personales, relaciones, salud, correo, comunicaciones electrónicas privadas, etc.

El derecho que poseen las personas de poder excluir a las demás personas del conocimiento de su vida privada, es decir, de sus sentimientos y comportamientos. Una persona tiene el derecho a controlar cuándo y quién accede a diferentes aspectos de su vida particular.

El origen del concepto jurídico de intimidad es anglosajón y en concreto procede del derecho norteamericano.

El primer antecedente es la definición contenida en la obra "The Elements of Torts", del Juez Thomas A. Cooley, en la que se recogía la idea en estos términos: «the right to be let alone», que podríamos traducir como el derecho a ser dejado en paz.

En 1890 Samuel Warren y Louis Brandeis publican en la Harvard Law Review un artículo titulado «The Right to Privacy». En él se definía el nuevo derecho en los siguientes términos:

«Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society […] Now the right to life has come to mean the right to enjoy life, - the right to be let alone».

Desde esta idea primaria, la lucha por el reconocimiento de un ámbito de privacidad inherente a toda persona ha sido una constante en la evolución de las sociedades democráticas. Por esta razón, desde los años sesenta y setenta del pasado siglo, la posibilidad

de injerencias en la intimidad de las personas se ha ido incrementando de forma constante y espectacular, planteando a su vez nuevos retos para el Derecho que no puede ser ajeno a una realidad que evoluciona constantemente.

### 2.1.7. Derecho al Honor

Alude a la consideración de la persona en cuanto a su integridad de ser humano, intrínseca al principio de dignidad. Para que se produzca una lesión del derecho al honor es necesario que se afecte a esta dignidad, al reconocimiento que los demás tienen de la persona, de su integridad moral o de su consideración social. Su principal peligro proviene de ataques de particulares.[26]

Desde este punto de vista, el honor y la intimidad, no se superponen, sino que más bien se relacionan, pudiéndose ver atacados de manera conjunta o separada: no siempre la violación de la intimidad supone un descrédito del honor o viceversa y puede ocurrir que el descrédito se lleve a cabo mediante una lesión al derecho a la intimidad, cuando se revelen datos atinentes a la intimidad de la persona.

### 2.1.8. Derecho a la propia imagen

Puede ser definido, también de forma autónoma a los dos anteriores, como la garantía del individuo frente a los intentos de un tercero de captar, reproducir o publicar su imagen sin autorización. La imagen protege, según el Tribunal Supremo español, “la representación gráfica de la figura humana mediante un procedimiento mecánico de reproducción, lo que puede incidir en la esfera de un derecho de la personalidad de inestimable

[26] Escobar, G. (2004). Los Derechos Fundamentales y las Telecomunicaciones. https://ebuah.uah.es/xmlui/bitstream/handle/10017/454/Los%20derechos%20fundamentales%20y%20la

valor para el sujeto y el ambiente social en que se desenvuelve, incluso en su proyección contra desconocidos sujetos.[27]

## 2.2. PROTECCIÓN DE DATOS

La protección de datos se refiere a las prácticas, salvaguardas y principios fundamentales puestos en ejercicio para proteger la información personal y asegurar que se mantengas en control de ella. En pocas palabras, cada persona debe tener la posibilidad de decidir si desea o no compartir ciertos datos, quién puede tener acceso a ellos, por cuanto tiempo, por qué razones, tener la posibilidad de modificarlos y mucho más.

Los gobiernos tienen un interés de seguridad en garantizar la protección de datos personales. En 2015, un grupo de delincuentes robaron una cantidad de 21,5 millones de registros de la Oficina de Administración de Personal de EE. UU. que contenían información personal sumamente sensible de los empleados federales y de los miembros de su familia. Este tipo de ataques suceden cada vez con mayor frecuencia en todo el mundo, por lo tanto, los países deben tomar medidas para proteger la información de las personas de forma eficiente.

## 2.3. DATOS PERSONALES

Dato Personal es cualquier tipo de información vinculada a una persona que puede utilizarse para identificar, directa o indirectamente, a esa persona.[28]

Los datos personales son cualquier información que permite identificar a una persona. El nombre, los apellidos, la fecha de nacimiento, la dirección del domicilio, la dirección

[27] Idem
[28] Delgado, I. (2020). Protección de datos personales Bolivia. https://www.protecciónde datos. bolivia.bo

de correo electrónico, el número de teléfono, el número de RUC, el número de la placa del vehículo, la huella digital, el ADN, una imagen, el número del seguro social, etc. son datos que identifican a una persona, ya sea directa o indirectamente.

Entendemos por “dato personal” toda información relativa a personas físicas identificadas o identificables. Por tanto, debemos entender que la protección de los datos personales se refiere exclusivamente a la privacidad e intimidad de las personas físicas, pero no de las personas jurídicas. Además, otro concepto clave en la definición de dato personal es que el mismo nos proporcione una información acerca de la persona a la que se refiere, y que exista una asociación entre la información proporcionada y el interesado. La asociación entre la información referida a una persona física y dicha persona en concreto es el aspecto determinante para que podamos afirmar la existencia de un dato personal a los efectos de nuestro régimen jurídico.

Según la Comisión Europea, se entiende por datos personales cualquier información sobre una "persona física viva identificada e identificable".[29]

Cualquier información, por tanto, que sirva para identificar personalmente a una persona, constituye para el regulador europeo un dato de carácter personal. Ejemplos de datos personales serían los siguientes:

- Nombre y apellidos
- El domicilio postal personal
- El correo electrónico personal
- Cualquier documento de identificación nacional personal

[29] Sumup. (2021). Privacidad y protección de datos ¡Qué es la privacidad y protección de datos? .https://debitoor.es/glosario/privacidad-y-proteccion-de-datos-personales

- Los datos de localización (como los del teléfono móvil personal)
- La dirección IP personal
- El identificador de una cookie (un pequeño archivo que recopila información de navegación de un usuario en un sitio web)
- El identificador de la publicidad del teléfono
- Los datos de un hospital o médico sobre sus pacientes.

No se consideran datos personales la siguiente información:

- ✓ El correo electrónico corporativo
- ✓ El número de registro mercantil
- ✓ Cualquier dato anónimo.

### 2.4. EL CONTROLADOR DE DATOS

Es la persona física o jurídica, entidad pública o privada, organismo u organización que solo o conjuntamente se encarga del almacenamiento, el procesamiento, el uso, la protección y la difusión de los datos y en algunas circunstancias pueden convertirse en recopiladores de datos.

### 2.5. EL PROCESADOR DE DATOS

Es la persona física o jurídica, entidad pública o privada, organismo u organización que solo o conjuntamente procesa los datos en cuestión, abarcando toda

operación o conjunto de operaciones que se realizan con datos personales, como recopilación, registro, almacenamiento, recuperación, divulgación o transferencia.[30]

## 2.6. LA AUTORIDAD RESPONSABLE DE LA PROTECCIÓN DE DATOS

Es la que se encarga de establecer y hacer cumplir leyes, normas, requisitos relativos a la protección de datos personales a fin de mantener una uniformidad; esta autoridad puede variar según la legislación de los Estados Miembros.

## 2.7. TITULAR DE LOS DATOS

Es la persona cuyos datos personales se recopilan, procesan, almacenan, utilizan o difunden, es decir, es la persona a quien corresponden los datos personales.

## 2.8. TIPOS DE DATOS

### 2.8.1. Datos personales sensibles

Están constituidos por: Los datos biométricos que por sí mismos pueden identificar a la persona, como la huella digital, la retina, el iris; Datos referidos al origen racial y étnico; Ingresos económicos; Opiniones o convicciones políticas, religiosas filosóficas o morales; la afiliación sindical; Información relacionada a la salud o a la vida sexual. Estos datos requieren de especial protección y solamente pueden ser objeto de tratamiento con el consentimiento expreso y por escrito del titular de los datos.[31]

[30] Villalta, A. E. (2017). La privacidad y la protección de datos personales. www.oas.org/es/sla/cji/docs/informes_culminados_recientemente_Proteccion_Datos_Personale.
[31] Delgado, I. (2020). Protección de datos personales Bolivia. https://www.protecciónde datos. bolivia.bo

### 2.8.2. Datos personales no sensibles

Son aquellos que se refieren a un sujeto individualizado y son relativos a su fuero interno o íntimo sin llegar a ser información puramente sensible. Identifican su personalidad, nombre y apellido, domicilio, números identificatorios (cédula, pasaporte, etc.). Esta clase de datos personalísimos pertenecen, en principio, a la persona física que los genere, detente y, por ende, pueda disponer de ellos, no deben ser objeto de manipulación, tratamiento o divulgación de ningún tipo.

### 2.8.3. Datos íntimos o privados

Son datos que se caracterizan porque le pertenecen al titular y son únicamente de su interés; sólo pueden ser obtenidos con su consentimiento, por orden de autoridad judicial y para salvaguardar la vida de la persona cuando ésta se encuentre en incapacidad física o jurídica. Los ejemplos más comunes son creencias religiosas, orientación sexual o afecciones a la salud.[32]

### 2.8.4. Datos biométricos

Por definición común, los datos biométricos son aquellos rasgos físicos, biológicos o de comportamiento de un individuo que lo identifican como único del resto de la población. Aquellos sistemas informáticos en los que se mide algún dato biométrico, como parte del proceso de identificación y/o autentificación de un sujeto, son conocidos como sistemas de seguridad biométrica o simplemente sistemas biométricos.

La siguiente lista son algunos ejemplos de datos biométricos:

[32] Soto, C. C., Espinosa, C. A., Ducuara, C. (2018). Protección de datos personales en los servicios de internet. Universidad Católica, Colombia. Recuperado de https://repository.ucatolica.edu.co

- Huellas dactilares
- Geometría de la mano
- Análisis del iris
- Análisis de retina
- Venas del dorso de la mano
- Rasgos faciales
- Patrón de voz
- Firma manuscrita
- Dinámica de tecleo
- Cadencia del paso al caminar
- Análisis gestual
- Análisis del ADN

Por definición y por su propia naturaleza, los datos biométricos son datos personales, sin embargo, la interrogante es ¿Cuál es la aplicación de las leyes de protección de datos personales con respecto a los datos biométricos?

### 2.8.5. Datos públicos

Se define los datos públicos como todos aquellos datos que tienen un interés general, como por ejemplo el número de cédula, sentencias judiciales, etc.

### 2.8.6. Datos semiprivados

Son datos que, aun teniendo carácter privado, son de interés únicamente del titular y a un grupo determinado de personas, las cuales pueden consultar la información con autorización del titular. El ejemplo más frecuente es el historial crediticio de una persona.

Es semiprivado el dato que no tiene naturaleza íntima, reservada o pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.[33]

### 2.8.7. Datos anonimizados o disociados

Existen también otros tipos de datos que, por la forma en la que son obtenidos o procesados, reciben otras denominaciones. En este grupo tenemos a los datos anónimos y anonimizados o disociados. Estos son datos que en principio permiten identificar a personas pero que gracias a mecanismos de anonimización o disociación terminan teniendo poca o nula relación con la persona que antes identificaban. Estos procesos son utilizados por ejemplo en investigaciones científicas donde, con el fin de proteger la identidad de las personas que participaron en el estudio, se elimina de los conjuntos de datos personales la información que permita la identificación. Sin embargo, esta práctica no quita que los principios de protección de los datos personales, que veremos más adelante, deban ser aplicados, en especial el de minimización de la recolección y análisis de datos; ya que existen procedimientos técnicos para revertir la anonimización y volver a identificar a las personas, en algunos casos.

### 2.8.8. Los metadatos

Estos son los llamados “datos sobre los datos”, puesto que son datos que se obtienen al analizar otros conjuntos de datos. Esto incluye, por ejemplo, algunos datos de navegación en internet e información sobre comunicaciones entre personas (a qué hora se mandó un SMS, en qué ubicación GPS se tomó una foto, etc). Si bien estos datos por sí solos

[33] Rojas, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales.https://novumjus.ucatolica.edu.co/article/download/652/670

no identifican a una persona, un análisis conjunto de los mismos sí podría hacerlo ya que nos brinda información importante y detallada sobre una persona. Por ejemplo, las redes sociales generan registros de visitas, reacciones (likes), compras en línea, entre otros. Al analizar y estudiar estos datos podemos conocer los gustos y preferencias de los usuarios de esas redes sociales; deducir donde viven, trabajan, van de vacaciones y quiénes son sus familiares y amigos.[34]

## 2.9. BANCO DE DATOS

Se designa al banco de datos como un sistema automático de acumulación, conservación, elaboración y registro de datos de cualquier naturaleza.

Aquel conjunto de archivos conexos o relacionados y organizados en función de su comunicación a una determinada población de usuarios. Los bancos de datos son un conjunto de datos e informaciones recogidas, acumuladas y clasificadas por cualquier medio. Se trata de una pluralidad de datos agrupados en un mismo conjunto, que pueden estar en diversos formatos, como son el (cada vez menos) tradicional soporte en papel impreso, o en un soporte digitalizado (o electrónico), almacenado y accesible mediante los medios que ofrece la técnica digital.[35]

### 2.9.1. Banco de datos públicos y privados

[34] Arroyo, V. (2019). Guía básica sobre datos personales para Bolivia. www.accessnow.org/cms/assets/uploads/2019/03/Guia-Basica-Proteccion-de-Datos-Bolivia.pdf

[35] Perez, R. M. (2011). La regulación para el acceso a datos en los registros públicos y privados en Bolivia. 2011. https://repositorio.umsa.bo/xmlui/handle/123456789/14189

Esta clasificación no se refiere a la posibilidad de acceso público o privado, sino por la circunstancia de si están administrados por organismos públicos o por empresas privadas esta última debe tener en mira la publicada de aquéllos datos.

## 2.10. FICHERO

Un fichero es un conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. De esta definición podemos extraer que si bien existe la necesidad de una organización u ordenación de los datos, por contra, no se requiere que el fichero esté automatizado.[36]

Uno de los puntos más importantes para poder comprender la definición del concepto de fichero es la existencia de un conjunto organizado en los datos personales en él incluidos. Debemos tener en cuenta que sobre este concepto gira gran parte de las obligaciones impuestas por la normativa en materia de protección de datos de carácter personal.

### 2.10.1. Fichero Físico

Un fichero es un conjunto organizado de informaciones almacenadas en un soporte común. A dicha definición será necesario añadirle el calificativo de físico y, por tanto, ser conscientes que éstos pueden encontrarse en múltiples soportes: Ficheros en papel, aquellos contenidos en una determinada aplicación informática, aquellos conformados por un conjunto de archivos informáticos etc.

[36] Zaballos, E. (2013) La protección de datos personales en España: evolución normativa y criterios de aplicación. (Memoria-grado Doctor). Universidad Complutense de Madrid, Madrid España. Recuperado de https://eprints.ucm.es/22849.Madrid, España

Por tanto, en una organización es habitual encontrar decenas o centenares de ficheros físicos que contienen datos personales ya que éstos se encuentran en aplicaciones y archivos informáticos que contienen datos personales y que suelen generar a su vez una gran cantidad de pequeños ficheros creados por los responsables de cada área para variadas finalidades.

### 2.10.2. Fichero Lógico

Un fichero lógico es un fichero o conjunto de ficheros físicos, que contienen el mismo tipo de datos, y que son tratados para una misma finalidad o finalidades compatibles.

Las claves para llevar a cabo correctamente la identificación de los ficheros lógicos y la agrupación de los ficheros físicos en estas categorías pueden resumirse en dos:

1. Finalidad. Los ficheros lógicos se identifican en función de la finalidad. Para cada finalidad señalaremos la existencia de un fichero lógico y será necesario cumplir con las exigencias de la LOPD.
2. Nivel de seguridad. El objetivo de la agrupación de ficheros físicos en ficheros lógicos es registrar un solo fichero y aplicarle unas medidas de seguridad homogéneas. Por ello, es conveniente que a los ficheros físicos agrupados en un fichero lógico les sea aplicable un mismo nivel de seguridad de acuerdo con lo establecido por el Reglamento de desarrollo de la LOPD.[37]

Una vez realizada la agrupación, la identificación de los tratamientos de la información debe completarse de la siguiente manera:

[37] Zaballos, E. (2013) La protección de datos personales en España: evolución normativa y criterios de aplicación. (Memoria-grado Doctor). Universidad Complutense de Madrid, Madrid España. Recuperado de https://eprints.ucm.es/22849.Madrid, España

1. Determinación de las aplicaciones y sistemas que tratan los ficheros: ubicación física, responsables, etc.
2. Determinación de los encargos del tratamiento, así como de las cesiones.

### 2.10.3. Ficheros públicos y privados

- **Ficheros de titularidad privada:** Los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.
- **Ficheros de titularidad pública:** Los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

## 2.11. TRATAMIENTO DE DATOS PERSONALES

Cuando hablamos de tratamiento de datos personales nos estamos refiriendo a cualquier operación o procedimiento técnico, sea o no automatizado, que permita, entre otras cosas, la recogida, conservación, modificación, consulta, o cancelación de estos datos. En este sentido tomaremos como referencia la clasificación propuesta por Davara Rodriguez, que

distingue, dentro de los mismos, las siguientes fases: Toma de datos, Tratamiento de datos y Utilización y en su caso la comunicación de los mismos. [38]

El tratamiento de los datos personales tiene un paso previo consistente en la recogida de datos y otro posterior en la utilización de los resultados obtenidos como consecuencia de ese tratamiento. La definición de estas fases debe servir como esquema previo para el análisis de tratamientos complejos, y nos permitirá sistematizar el estudio de la materia, así como identificar los riesgos y obligaciones asociados a cada uno de ellos.

## 2.12. INFORMATICA

La informática es la disciplina que estudia el tratamiento automático de la información utilizando dispositivos electrónicos y sistemas computacionales.

El origen de las investigaciones sobre los tratamientos de información y la computación comienza alrededor de 1930, el término “informática”, es atribuible al ingeniero francés Philippe Dreyfus que utilizó “informatique” por primera vez en 1962, como acrónimo de las palabras “information” y “automatique”.

Lo que hoy en día conocemos comúnmente como “informática” está conformado por muchas técnicas y áreas de conocimiento, que van desde la gestión de negocio, el almacenamiento de información, el control de procesos o las comunicaciones.

En lo relativo a la evolución de la informática a lo largo del siglo XX, puede afirmarse que ha tendido al diseño de técnicas y sistemas cada vez más compatibles,

[38] Zaballos, E. (2013) La protección de datos personales en España: evolución normativa y criterios de aplicación. (Memoria-grado Doctor). Universidad Complutense de Madrid, Madrid España. Recuperado de https://eprints.ucm.es/22849.Madrid, España

acompañadas del progresivo abaratamiento de los costes de los componentes y los equipos informáticos.

Estos dos han sido los factores clave en la aparición de la denominada "Sociedad de la Información", modelo en el que la Informática está presente de manera masiva en todos los ámbitos de la Sociedad, y muy especialmente en las actividades económicas, así como en el propio tejido social.

Por otra parte, y como afirma Márquez Lobillo, no podemos afirmar que el proceso de informatización de la sociedad haya concluido, sino que probablemente nos encontremos en el inicio de modelos y formas de convivencia que podemos anticipar solo en parte.[39]

## 2.13. PROTECCIÓN DE DATOS Y DERECHO INFORMATICO

La protección de datos personales se ubica dentro del campo de estudio del Derecho Informático. Se trata de la garantía o la facultad de control de la propia información frente a su tratamiento automatizado o no, es decir, no sólo a aquella información albergada en sistemas computacionales, sino en cualquier soporte que permita su utilización: almacenamiento, organización y acceso.

## 2.14. RECURSO DE HABEAS DATA

El derecho fundamental al habeas data es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión,

[39] Zaballos, E. (2013) La protección de datos personales en España: evolución normativa y criterios de aplicación. (Memoria-grado Doctor). Universidad Complutense de Madrid, Madrid España. Recuperado de https://eprints.ucm.es/22849.Madrid, España

exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales.[40]

## 2.15. TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

El sistema europeo cuenta con una legislación que rige la recolección de datos personales por el Gobierno y las entidades privadas; el sistema estadounidense sigue un criterio que facilita que los sectores económicos regulen los datos personales recabados por organizaciones privadas y la regulación estatal de los datos recogidos por el Estado; en varios países de américa Latina se sigue el concepto del habeas data, que permite a las personas acceder a sus propios datos personales y otorga el derecho a corregir información errónea.

En este sentido, para la efectiva protección de los datos personales en cuanto a la transferencia entre diferentes países, se debe contar con instrumentos dentro del marco de tratados internacionales ratificados por las partes, de modo que, cuando un país receptor de datos no proporcione mayor o igual protección adecuada que los de la legislación del país emisor, se entiende que la transferencia de datos está prohibida, por cuanto no garantiza el debido tratamiento de los mismos.

No obstante, existen excepciones a estas reglas y dos de las más recurrentes son, en primer lugar, cuando el titular de la información autoriza de modo expreso la

[40] Rojas, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. https://novumjus.ucatolica.edu.co/article/view/652

transferencia internacional de los datos y en segundo lugar, cuando la transferencia se requiere para el cumplimiento de una obligación legal o contractual.[41]

Pues bien, en cuanto a estándares internacionales para la transferencia de datos, se considera que la persona natural o jurídica de carácter público o privada encargada o responsable de la administración de los mismos debe celebrar un acuerdo con el tercero del país a quien eventualmente se le suministren dichos datos, en aras de mantener las garantías de protección y de uso para los fines que autorizó el titular y no podrán destinarse a fines diferentes.[42]

### 2.16. CIBERESPACIO

Es una construcción metafísica compuesta por hardware digital, los datos que éste hardware crea y administra, y los humanos que producen y consumen la información contenida en los datos y que interactúan con el hardware. Se reconoce a los humanos como responsables de la dinámica del sistema, así como lo son los datos y la tecnología.

### 2.17. CIBERIDENTIDAD

Hace referencia al conjunto de características de las personas que las diferencian de otras, en el ciberespacio.

### 2.18. CIBERSEGURIDAD

[41] Rojas, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. https://novumjus.ucatolica.edu.co/article/view/652
[42] Idem

Conjunto de medidas y acciones tomadas para evitar el acceso no autorizado, la manipulación o destrucción de datos cibernéticos; incluyendo tecnologías, políticas y procedimientos para asegurar algo en el ciberespacio.

### 2.19. GEOLOCALIZACIÓN

Es un conjunto de tecnologías que tienen como fin la utilización de la información relacionada con la ubicación geográfica del mundo real.

### 2.20. NUBE

Es un modelo que traslada la información de los usuarios a un conjunto de servidores a los que se accede a través de una red, frecuentemente internet.

### 2.21. RIESGO DE SEGURIDAD DIGITAL

Describe una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital, resultante de la combinación de vulnerabilidades y amenazas en el ambiente digital. El riesgo de Seguridad digital puede debilitar el logro de objetivos económicos y sociales.

### 2.22. RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

### 2.23. TRANSMISIÓN Y TRANSFERENCIA DE INFORMACIÓN.

Basándose en el principio de Responsabilidad demostrada, la transmisión hace referencia a que el responsable de la información determina el tratamiento de los datos personales por parte del encargado; mientras que en la transferencia el encargado decide el tratamiento que le dará a los datos personales que le ha entregado el emisor.

# CAPÍTULO III

# MARCO TEÓRICO

## 3.1. TEORÍAS SOBRE LA PROTECCIÓN DE DATOS

Todo campo jurídico necesita de un sustento teórico, este se lleva a cabo por una serie de teorías que tienen como objetivo unificar diversos criterios sobre una única visión interpretativa. La teorización en el ámbito jurídico es necesaria porque unifica visiones distintas y ayuda a caminar hacia una única visión teórica que sea lo suficientemente versátil pero férrea como para proteger los derechos que se pretenden. La imposibilidad de la existencia de una única teoría en cualquier campo es el poder que enriquece al derecho y permite conseguir nuevas perspectivas que ayuden a evolucionar las normas conforme la sociedad y que esos derechos de ese campo jurídico evolucionen.

Para el caso del Data Privacy, que es como se debería llamar, existen cuatro grandes teorías, dos europeas y dos de Estados Unidos.

### 3.1.1. La Sphärentheorie o Teoría de las esferas o círculos concéntricos

La teoría de las esferas o círculos concéntricos fue desarrollada por Heinrich Hubmann en 1957 la cual divide el contenido de la intimidad según Hubmann en tres grandes esferas. La primera de ellas abarca el círculo más amplio y es la esfera privada, ésta tiene dentro todos los datos referidos a noticias y expresiones que la persona no desea que trasciendan de forma pública y la denomina, privatsphäre. La segunda de las esferas es la que enmarca a los datos referidos a temas confidenciales la vertravensphäre, que se encuentra dentro de la primera esfera. La tercera de las esferas es la que protege los datos que se

consideran lo más secreto del individuo la gehimsphäre, que se encuentra a su vez dentro de la segunda.

La primera de las esferas la privatsphäre ubica los datos relacionados con todas aquellas relaciones y conductas que, siendo privadas, se desenvuelven en espacios públicos y tienen una mayor trascendencia social, es la esfera primera, mayor y contiene el mayor número de datos.

Los datos que se recogen dentro de esta esfera son datos que el sujeto o desea que sean de conocimiento público o no tiene inconveniente en que sean conocidos.

La segunda de las esferas vertravensphäre, que se encuentra dentro de la primera, es la esfera que enmarca todos los datos referidos a conductas, decisiones u opiniones. Todas ellas se generan en espacios privados o en zonas privadas. En la vertravensphäre el titular del derecho podría si lo considera adecuado y es voluntad suya renunciar a la privacidad de esta información y darla a conocer. Es la esfera confidencial y abarca lo que el sujeto comunica a otra persona de su confianza.

La tercera esfera es la gehimsphäre es la esfera donde se custodian los datos más íntimos o secretos del individuo y no se debería poder renunciar a su derecho de privacidad ni con la voluntad del propio individuo propietario de dichos datos. En esta esfera nadie accede a estos datos, pues sólo los conoce el individuo.[43]

### 3.1.2. La Teoría del Mosaico

[43] Nisa,J. (2020). Origen jurídico histórico de la protección de datos: evolución de las diferentes teorías jurídicas que la han protegido. https://elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la-protegido

La Teoría del Mosaico fue creada por Fernando Madrid Conesa en 1984. La Teoría del Mosaico venía a rebatir la Teoría Alemana de las Esferas bajo la calificación de férrea, poco adaptable y demasiado cartesiana en lo que a clasificación de datos se refiere, carecía de falta de transversalidad. La Teoría del Mosaico considera los datos como conceptos relativos, todo depende de quién sea el receptor de los datos, estableciéndose una relatividad entre privado y público respecto a la privacidad de datos.

El principal baluarte de esta teoría radica en el hecho de que los datos tienen un valor ambivalente dependiendo del lugar donde se encuentren tratándose. El resultado de un dato examinado de forma aislada puede resultar irrelevante para el derecho a la intimidad y no es el mismo que examinado en conjunción con otros datos "irrelevantes" los cuales puestos todos en conjunto pueden formar un mosaico de la personalidad de un ciudadano.

Asimismo, esta teoría se basa en el planteamiento conceptual sobre la polivalencia de la protección de los datos en consonancia con quien sea el receptor de los mismos y en perspectiva respecto al derecho a la intimidad. El principal revelador de si el dato debe ser protegido o no es el derecho a la intimidad, con lo que encontramos una limitación protectora como más adelante podremos observar.[44]

### 3.1.3. La Teoría del Right to Privacy

La Teoría del Right to Privacy o Theories of the Common Law of Torts son teorías basadas en la Tort Law o Ley de Agravios, existentes en los países del Common Law.

[44] Nisa,J. (2020). Origen jurídico histórico de la protección de datos: evolución de las diferentes teorías jurídicas que la han protegido. https://elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la-protegido

La principal de las Teorías son las diversas teorías existentes alrededor del Tort Law la cual posteriormente ha dado con la Teoría del Right to Privacy que no es otra que una teoría algo más concreta del Tort Law. Las Theories of the Common Law of Torts se basan en el Tort Law que es la parte del derecho perteneciente al derecho civil en el Common Law que se ocupa del enjuiciamiento de aquellos actos no enmarcables como penales, incumplimientos contractuales o delictivos en los que un individuo o persona jurídica es perjudicada y necesita ser resarcida económica o moralmente, se encuentra dentro del Grounds of Action in Civil Law.

El Tort Law se divide en tres secciones, el wrongs against the person, Wrongs against property y Wrongs against people or property. Las Theories of the Common Law of Torts son teorías de Data Privacy sin una formulación doctrinal como tal y basadas directamente en el derecho positivo complementadas por la diferente generación de jurisprudencia basada tanto en derecho natural como derecho positivo en dicha materia.

La Teoría del Right to Privacy fue formulada en 1960 por William Prosser y divide la privacidad en cuatro estadios:

- Intrusión en la soledad de la vida de una persona o en sus asuntos privados, protegido mediante la acción intrusion on an individual's privacy.
- Divulgación de datos íntimos que afecten al individuo dueño de los mismos, protegido mediante la acción public disclosure of private facts.
- Publicidad de dichos datos de forma que puedan desprestigiar a la persona frente a la opinión pública, protegido mediante la acción putting an individual in a false light in the public eye.
- Apropiación del nombre de la persona, voz o imagen, protegido mediante la acción appropiation of some elements of an individual's personality.

Todo ello debe ser visto bajo el prisma básico de una serie de requisitos que debe cumplir todo dato privado para ser reclamada su protección. Los requisitos son el deber de una obligación legal de privacidad o negligencia, que conlleve un incumplimiento que genere una responsabilidad, por una razón concreta que haya causado a su vez un daño que sea demandable y demostrable.

### 3.1.4. La Restricted Access/Limited Control (RALC) Theory of Privacy

Es una teoría del autor Herman Tavani en el año 2007. El autor considera al resto de teorías bajo una clasificación propia como no intrusivas, seclusivas, limitativas o de control teórico y las considera ineficaces desde un punto de vista jurídico teórico al faltarle elementos del resto de teorías.

El RALC coge los puntos clave de cada una de esas teorías y las intenta unificar en una sola. La RALC realiza una diferencia entre aspectos descriptivos de la norma y aspectos puramente normativos con la finalidad de poder conocer cuáles son los datos realmente necesarios a ser protegidos y bajo que herramientas. El RALC indica que no es lo mismo perder la privacidad e invasión de la privacidad, siendo únicamente el segundo el que tiene derecho a ser protegido. Asimismo, el autor indica que se debe diferenciar entre la gestión de la privacidad y la justificación de los datos privados y situaciones privadas naturales y situaciones privadas normativas, siendo de nuevo sólo protegidas las derivadas de violaciones de datos de situaciones privadas normativas, por carecer las situaciones privadas naturales de ámbito normativo protector.

En el RALC se otorga al concepto dato una tangibilidad como si de un objeto físico se tratase, al entender que puede haber privacidad sin tener el control de la información,

y que porque alguien tenga acceso a una información privada no significa que tenga el control de la misma.[45]

## 3.2. ANÁLISIS LEGAL DE LAS TEORÍAS SOBRE PROTECCIÓN DE DATOS Y SU SITUACIÓN ACTUAL

Las teorías sobre Data Privacy expuestas son las cuatro grandes teorías actuales. Todas ellas no se encuentran “vigentes”, desde un punto de vista doctrinal puesto que estamos hablando de cuestiones teóricas.

La teoría de las esferas es una teoría que se considera desfasada y desplazada por la teoría del mosaico.

La teoría del mosaico es la teoría actual sobre Data Privacy más aceptada y sobre la que se basa muchas legislaciones de diferentes ordenamientos jurídicos. La segunda más usada es la teoría Right to Privacy o Tort Law Theories, sobre todo en Estados Unidos y países del Common Law.

Una teoría jurídica debe contener y ser identificables, los siguientes puntos que podríamos llamar metodología de construcción teórico jurídica:

- Ámbito de actuación
- Ámbito de aplicación
- Tipología de aplicación
- Tipología de protección

[45] Nisa,J. (2020). Origen jurídico histórico de la protección de datos: evolución de las diferentes teorías jurídicas que la han protegido. https://elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la-protegido

- Marco Teórico

Por lo que respecta a las teorías actuales con más relevancia en el data privacy, cabe decir que tanto en la Teoría de Mosaico como en la Teoría del Right to Privacy, ambas carecen de un ámbito de aplicación correctamente desarrollado. La teoría del mosaico se circunscribe a la violación de los datos íntimos asimilando como el mismo concepto el data Privacy y el data Intimacy, los cuales son distintos, pues no pueden ser equivalentes entre sí. La fundamentación protectora del data privacy sobre exclusivamente los datos íntimos de una persona es ceñir a una parcela muy concreta de datos una teoría que pretende dar cobertura teórico jurídica al ámbito del Data Privacy en general.

Asimismo, en el caso de la Teoría del Right to Privacy, la cosa es diferente pues carece de prácticamente todos los elementos al estar construida desde la concreción a la abstracción y no de la abstracción a la concreción que sería lo correcto. Además, el hecho de que pertenezca al Common Law no la exime de la necesidad de cumplimiento de los elementos necesarios para una correcta teoría. La Teoría del Right to Privacy no tiene ámbito de aplicación concreto, ni desarrollado, ni tampoco una tipología de actuación acorde a ese ámbito, carece de un desarrollo del tipo de aplicación, aunque si disfrute de una tipología de protección muy concreta. La realidad nos muestra que realmente no se podría enmarcar como una teoría en sí, sino un compendio de recursos jurídicos con una serie de puntos en común.

## 3.3. COMPONENTES

### 3.3.1. Ámbito de actuación

El ámbito de actuación es el lugar en el derecho positivo donde se quiere actuar con la teoría que se pretende formular. En este sentido, puede decirse que es el campo del

derecho en su aspecto más amplio sin concreciones específicas sobre en el que se pretende actuar para su posterior modificación legislativa o creación.

### 3.3.2. Ámbito de aplicación

El ámbito de aplicación, sin embargo, es la descripción específica teórica desglosada del ámbito de actuación. Aquí se va a concretar dependiendo del ámbito de actuación una descripción teórica de todos los elementos básicos sobre el que se sustenta la teoría para su posterior incorporación al derecho positivo.[46]

### 3.3.3. Tipología de aplicación

La tipología de aplicación es el grueso de la teoría puesto que es el desarrollo de todos los aspectos teóricos en base al ámbito de actuación y ámbito de aplicación, aplicados a una serie de tipologías jurídicas sobre la que se teoriza. La tipología de aplicación es el desarrollo práctico de los conceptos jurídicos que se quiere que posteriormente se incorporen al derecho positivo que se encuentre dentro del ámbito de aplicación correspondiente, describiendo las diferentes naturalezas jurídicas de las tipologías de aplicación que se desarrollen.

### 3.3.4. Tipología de protección

La tipología de protección son las herramientas jurídicas que se deben usar, actuales si ya existen o nuevas para el caso que no existan, con la finalidad de aplicar correctamente la tipología de protección en el derecho positivo. El marco teórico es el conjunto

[46] Nisa,J. (2020). Origen jurídico histórico de la protección de datos: evolución de las diferentes teorías jurídicas que la han protegido. https://elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la-protegido

del ámbito de actuación, el ámbito de aplicación, la tipología de protección y la tipología de aplicación. Todos estos elementos, son los necesarios para poder evaluar el correcto y eficiente desempeño en el ámbito del derecho positivo de una teoría.

## 3.4. DERECHO A LA PRIVACIDAD

El término “privacidad” es una palabra que no puede ser usada sin relacionarla al tema de protección de datos personales.[47]

Si deseamos saber cómo y cuándo se gestó lo que hoy entendemos por «privacidad» (privacy) hemos de remontarnos a finales del siglo XIX y situarnos en Estados Unidos. Es allí donde comenzó a tenerse una noción legal de derecho a la intimidad o right to privacy que, a través del tiempo, acabaría tomando la forma del derecho a la intimidad tal y como lo conocemos hoy.

Para ser más precisos, el nacimiento del concepto de privacy suele situarse en la publicación del artículo «The Right to Privacy», firmado por los juristas norteamericanos Samuel Warren y Louis Brandeis.

### 3.4.1. Derecho a la privacidad en el Derecho Norteamericano

En Estados Unidos, el derecho emana de la Constitución, las leyes y reglamentos y el common law, una suerte de jurisprudencia o derecho creado por decisiones de los tribunales. Una de las nociones más importantes del common law son los llamados torts,

[47] López, J. (2014). Antecedentes internacionales en materia de privacidad y protección de datos personales. https://publicaciones.eafit.edu.co/index.php/ejil/article/view/2849/2626

que podrían definirse como un agravio o ilícito civil cometido por una persona legalmente responsable que causa un perjuicio, un daño o una pérdida a un tercero.[48]

### 3.4.2. Common Law

El Common Law es el sistema jurídico vigente en Inglaterra y en la mayoría de los países de tradición anglosajona, pero también da nombre a toda una tradición jurídica o familia del Derecho.[49]

En sentido estricto podemos decir que es el sistema jurídico creado en Inglaterra tras la conquista normanda (1066). Se llamó common (común) porque pasó a ser el Derecho de aplicación general en todo el reino por parte de los tribunales del rey, los cuales seguían un mismo conjunto de principios y reglas jurídicas.

En un sentido más amplio se habla de Common Law para referirse a aquel sistema legal basado, primordialmente, en las decisiones adoptadas por los tribunales, en contraste con los sistemas de Derecho Civil (o tradición romano-germánica), como el nuestro, donde la principal fuente de Derecho es la Ley.

#### 3.4.2.1. Características

El Common Law, está formado por un conjunto de normas no escritas (unwritten) y no promulgadas o sancionadas (unenacted). Se fundamenta, por tanto, en el Derecho de carácter eminentemente jurisprudencial.

---

[48] Cazurro, V. (2020). Antecedentes y fundamentos del derecho a la protección de datos. www.marcialpons.es/libros/antecedentes-y-fundamentos-del-derecho-a-la-proteccion-de-datos/9788

[49] Gamez, R. (2021). Qué es el Common Law. https://traduccionjuridica.es/que-es-el-common-law

De ahí el dicho comúnmente utilizado por los juristas anglosajones de Remedies precede rights, que podría traducirse por «la acción crea el derecho», y que hace referencia a que son las acciones o los procedimientos judiciales interpuestos antes los tribunales los que dan pie a las decisiones de los jueces que, a su vez, crean el Derecho.

#### 3.4.2.2. Fuentes del Common Law

Pero, no solo del precedente vive el Common Law. Existen también otras fuentes creadoras de Derecho como son la ley (que, poco a poco, va ganando importancia), la costumbre y la doctrina. Éstas son las principales fuentes del Derecho anglosajón:

Judicial Precedent o Case Law: similar a lo que nosotros llamamos jurisprudencia.

Legislation o Statutory Law: las leyes, que pueden ser leyes parlamentarias (Act of Parliament) y disposiciones de tipo reglamentario y la legislación delegada (Delegated legislation) emanada del gobierno central o local, como las órdenes ministeriales (ministerial orders) y las ordenanzas municipales (local by-laws).

Custom: la costumbre, como los usos mercantiles (law merchant)

Books of authority: la doctrina.[50]

### 3.4.3. El modelo Europeo

Tras la II Guerra Mundial, con el doble objetivo de proteger los derechos humanos y las libertades públicas, y promover una mayor unidad entre los Estados europeos, se fundó en 1949 el Consejo de Europa, un organismo internacional formado inicialmente por

[50] Gamez, R. (2021). Qué es el Common Law. https://traduccionjuridica.es/que-es-el-common-law

diez Estados y que ahora integra ya a casi cincuenta. Un año más tarde, el 4 de noviembre de 1950, se firmó en el seno del Consejo de Europa el que ha sido hasta ahora su instrumento más importante: el Convenio Europeo de Derechos Humanos (CEDH).

### 3.5. EL PRINCIPIO DE LA PRIVACIDAD DESDE EL DISEÑO

El principio es “importado” desde Canadá, donde fue desarrollado en los años 90 por la Dra. Ann Cavoukian Esta mujer no sólo fue una de las pioneras en advertir que la privacidad tenía que ser un factor tan importante como la seguridad en el tratamiento automatizado de la información personal, sino que, sobre todo, mostró al mundo la “privacidad desde el diseño” como una herramienta idónea para atender esa necesidad.

La finalidad de este principio es incluir la noción de privacidad en la propia tecnología, consiguiendo alternativas técnicas que garanticen el pleno respeto a la privacidad de los ciudadanos, sin disminuir la plena funcionalidad del proyecto. Esto es, apuesta por un progreso tecnológico respetuoso con la privacidad y, que pueda llegarse a conseguir el win-win con plena funcionalidad de negocio y privacidad.

Cavoukian propone extender a la privacidad el mismo planteamiento de “design-thinking” que ha dado lugar a la revolución tecnológica actual: “observar el mundo con ojos de diseñador” desde un planteamiento integral y transversal en el que nada se debe dar por sentado. Bajo esta nueva perspectiva, siempre que se traten datos personales, la privacidad debe protegerse por defecto y desde su mismo diseño en cualquier tecnología informática,

modelo organizativo, arquitectura física, ecosistema informático conectado, e incluso modelos de gobierno o gobernanza.[51]

Pero, gracias al impulso de esta mujer, el concepto evolucionó a nivel internacional y fue tenido en consideración por la Comisión Europea en la elaboración de su propuesta de RGPD, en el que finalmente fue incluido. De este modo, la Unión Europea ha adoptado formalmente un importante principio internacional, formulándolo como obligación en el RGPD.

### 3.6. HABEAS DATA

Uno de los derechos que se ha desarrollado con el avance la tecnología es el que tiene el ciudadano a estar correctamente informado acerca de los datos que y son manejados por el poder público o privado. Una de las amenazas que era imposible hace pocos años fue precisamente la que provendría de la información computarizada y las redes electrónicas que almacenan datos referentes a las personas y que ayuda con pavor, a que en el Estado moderno no sean los ciudadanos los que controlan al Estado, sino que sea éste el que controla a los ciudadanos.

Varias naciones han incorporado una garantía especial la de Hábeas Data o también llamada acción de protección de la privacidad sobre los datos personales, para una más útil defensa de los mismos.

#### 3.6.1. Antecedentes del Habeas Data

[51] Cortes, S. (2019). Protección de datos: sus orígenes y la privacidad desde el diseño. https:// mujeresenelsectorpublico.com/proteccion-de-datos-sus-origenes-y-la-privacidad-desde-el-diseno

El desarrollo conceptual del derecho a la intimidad personal tiene lugar en la experiencia de los Estados Unidos y en el Reino Unido, desde fines del siglo pasado cuyo punto crucial fue la definición del derecho a la privacidad como “The right to be alone”; es decir, el derecho a ser dejado en soledad, elaborado por el Juez Cooley.

Este concepto fue desarrollado por los Jueces Warren y Braendeis buscando proteger a la persona frente a datos o actos de índole personal, que se ponen en conocimiento del público o de terceros sin el consentimiento del afectado. Aproximadamente desde 1960, como consecuencia del vertiginoso desarrollo tecnológico que se traduce en nuevos sistemas informáticos, tanto en los Estados Unidos y Gran Bretaña se empiezan a promover proyectos legislativos que da un nuevo giro o extensión al derecho a la privacidad; se refieren a la protección de la libertad y esfera personal frente a posibles excesos del registro informatizado o difusión de datos e informaciones vinculados a aspectos reservados o íntimos. A la Data Protección Act Británica de 1984 en Gran Bretaña. En Estados Unidos se llegó así, finalmente, a la Privacy Act Norteamericana del 31 de diciembre de 1974, el Habeas Data en Norteamérica también es conocido como el derecho a la autodeterminación informativa, que se define como el derecho que tiene toda persona a solicitar judicialmente la exhibición de los registros públicos o privados en los cuales están incluidos sus datos personales o los de su familia, con la finalidad de tener conocimiento de su exactitud; también para requerir la rectificación o la supresión de los datos inexactos u obsoletos. En cambio, en Europa el derecho a la autodeterminación informativa se fue consolidando progresivamente como un derecho autónomo. Destaca Alemania el primer texto de protección de datos correspondió al “Lan de Hesse” de Alemania, como el primer país europeo donde se elaboró el primer texto de protección de datos personales hacia aproximadamente 1970, el cual se constituye en el primer antecedente del Convenio

para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal del 28 de enero de 1981.[52]

El Habeas Data es una herramienta destinada a controlar el uso de los datos que se tienen sobre las personas. Un mecanismo de protección de los derechos inherentes a la dignidad informativa de las personas lo es el Habeas Data, es la garantía que le permite a toda persona (determinada o determinable) a solicitar judicialmente la exhibición de los registros, banco de datos, archivos, en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud, a requerir la rectificación, la supresión de datos inexactos u obsoletos o que impliquen discriminación.

El Habeas Data, protege el derecho a la intimidad personal y familiar, defiende la privacidad o la dignidad humana, es el derecho a la información, vela por la tutela del honor, preserva la imagen o perfil personal, derecho a la identidad, derecho a la autodeterminación informativa.

### 3.6.2. Etimología del Habeas Data

La palabra Habeas Data ha tenido una explicación etimológica generalizada y homologada en los Estados Latinoamericanos y principalmente en Brasil donde nace la institución con dicho nombre. El término “Habeas” proviene de los términos latinos: “Habeo” o “Habere” y cuya múltiple significación sería: tener, gozar, disfrutar, exhibir, presentar, tomar, aprehender, traer, trasladar, transportar, entre otros términos sinónimos. La mayoría de los doctrinales inciden más en el significado de la posesión de algo o de alguien y por eso argumentan que Habeo o Habere, significa aquí tengas en posesión, otros insisten en el

[52] Perez, R.M. (2011). La regulación para el acceso a datos en los registros públicos y privados en Boivia. https:// repositorio.umsa.bo/xmlui/handle/123456789/14189.

significado exhibitorio del término: “He aquí del documento, el dato, el registro requerido” algunos otros, enfatizan en que significa: “conserva o guarda tu” y hay quienes prefieren resaltar la función de aprehensión en forma poco ortodoxa, al decir: “que el sujeto a que los datos refieren pueda verlos, acceder a los mismos”.

Con relación al término: “Data” discutible y discutido al menos desde el punto de vista del uso terminológico y como adición del “Habeas” pues en castellano Data significa “fecha o tiempo antiguo”; en cambio, en inglés significa toda forma, hecho o suceso que identifique información alguna de algo o alguien.

En informática o computación es cualquier unidad, digito o cifra de información que pueda estar representada en sonido, video, texto o imágenes. Data: es el acusativo plural de datum, que en los diccionarios más modernos definen como representación convencional de hechos, conceptos o instrucciones de forma apropiada para la comunicación y procesamiento por medios automáticos.

En consecuencia, Habeas Data significa que se posean los datos o los registros. Ahora bien, qué importancia actual tiene este desfase lexical en la institución jurídica que conocemos como “Habeas Data” donde se une una palabra latina a otra de origen inglés, para producir una sola que nos da como resultado una institución que se ha venido generalizando en todo el mundo y se entiende como tener, poseer, gozar, disfrutar, exhibir, presentar, tomar, aprehender, traer, trasladar, transportar los datos o informaciones de la persona (natural o jurídica) o de sus bienes, institución jurídica que algunos autores reducen a las acciones de “acceder, tener y exhibir los datos personales”.

### 3.6.3. Concepto del Habeas Data

El Habeas Data es una garantía constitucional, que tutela, fundamentalmente, el derecho a la vida privada, y es una forma de derecho de acceso a la información pública, en la medida en que garantiza el acceso de las personas a los registros o bases de datos públicos o privados que contengan información que les concierna.[53]

La traducción literal desde Latín de Habeas Data que es tener los datos. El nombre es completamente apropiado, para él describe su naturaleza muy exactamente. El Habeas Data es un derecho Constitucional otorgado en varios países Latinoamericanos. La muestra varia de país a país, pero en general, es él ideado para proteger, por medio de una queja individual presentada, la imagen, privacidad, honor, información autodeterminación y libertad de información de una persona.

El derecho de Habeas Data puede ser planteado por un ciudadano contra algún registro para descubrir que información es guardada sobre su persona. La persona puede pedir la rectificación, actualización o nivelación, la destrucción de los datos personales archivados si el registro es público o privado.

El concepto de Hábeas Data, literalmente significa “presenten o traigan los datos”, viene a significar: traigan el dato y sométanlo al tribunal.

Sin embargo, el verdadero origen es desconocido, aunque el Hábeas Data debe significar que cada persona “tiene sus datos”.

Hábeas Data es una garantía constitucional de carácter procesal para la protección de los datos personales, aquellos que forman parte del núcleo esencial del derecho

[53] Durán, W. (2006). Contenido y Alcances del Habeas Data en Bolivia. www.corteidh.or.cr/tablas/R08047-12.pdf

a la privacidad o la intimidad de una persona, frente a la obtención, almacenamiento y distribución ilegal, indebida o inadecuada por entidades u organizaciones públicas o privadas. [54]

### 3.6.4. Objetivos del Habeas Data

En relación a esta garantía, se desprenden los derechos: derecho de acceso, derecho de conocimiento, derecho a la actualización, rectificación, eliminación o anulación de datos.

Estos derechos confirman el objetivo básico del HÁBEAS DATA: evitar que el uso incorrecto de la información pueda lesionar el honor, el buen nombre y el ámbito de la privacidad de la persona como consecuencia de la difusión de esos datos erróneos, incompletos o inexactos estos como derechos subjetivos incorporados en la Constitución Política del Estado Plurinacional.

De una manera perspectiva analítica y reflexiva se señala que los objetivos del Habeas Data son:

- Acceder a la información de su interés o a conocer datos sobre su persona que se encuentran en archivos o registros.
- Actualizar información o datos personales contenidos en archivos o registros, el objetivo es evitar que se siga tomando en cuenta como verdadera o vigente una situación actualmente inexistente, pues se considera que el no hacer notar este cambio dentro del actual estado de cosas puede ocasionar graves perjuicios a la persona cuya información no ha sido puesta al día, el objetivo de actualización de la

[54] Medinaceli, K. (2018). El Tratamiento de los Datos Sanitarios en la Historia Clínica Electrónica: Caso Boliviano. https://www.aepd.es/sites/default/files/2019-10/tratamiento-de-datos-sanitarios.pdf

información está dirigido a poner al día los datos que puedan tenerse acerca de una persona.

- Rectificación de informaciones o datos inexactos, con la corrección o modificación se busca la eliminación de información falsa de datos que ni antes ni ahora se ajustan a la verdad.
- Exclusión o supresión de datos sensibles que, por su carácter personal o privado, deben ser regulados con el objeto de almacenamiento o registro a fin de salvaguardar la intimidad personal o la eventual no discriminación.

El rol del Habeas Data es el de evitar que los datos que libremente facilitamos para que fuesen incluidos en un fichero, sean trasladados sin nuestro consentimiento a otros bancos de datos.

### 3.6.5. Principios del Habeas Data

1. **Principio de Justificación Social:** Solo permite la recolección de datos con propósitos generales y para usos específicos socialmente aceptables.
2. **Principio de Limitación de la Recolección:** Se establece expresamente la limitación de recolectar información sensible: raza, religión, salud, costumbres sexuales, opiniones políticas, uso de estupefacientes, etc., donde debe ser solamente autorizada por el titular de los datos a dar dicha información, saber para que se solicita, donde se encuentra almacenado y solamente dicha persona titular tiene a: el acceso, rectificación o eliminación y oponerse de la información sea registro publico o privado.
3. **Principio de Calidad o Fidelidad de la Información:** La información acumulada debe ser cierta a fin de que no produzca una imagen equivocada o falsa de la persona.

4. **Principio de Especificación del Propósito o la Finalidad:** La finalidad con que se recolectan los datos debe ser previamente declarado, no pudiendo con posterioridad hacer uso de ellos para fines distintos a los que se señaló para su recolección.
5. **Principio de Confidencialidad:** Solo por mandato judicial previa acreditación y justificación o por consentimiento del propio sujeto de la información, los terceros pueden acceder a los datos almacenados.
6. **Principio de Salvaguarda de Seguridad:** El responsable de los archivos y registros tiene la obligación de adoptar todas las seguridades que sean necesarias para impedir que se pierda, se destruya o haya acceso a la información almacenada.
7. **Principio de la Política de Apertura:** La existencia, fines, usos y métodos de operación de los registros de datos personales deben ser de conocimiento público y privado.
8. **Principio de Limitación en el Tiempo:** Los datos deben ser cancelados una vez alcanzada la finalidad por la cual fueron recolectados, salvo casos excepcionales.
9. **Principio de Control:** La legislación debe prever un organismo de control responsable del cumplimiento de los principios enunciados.
10. **Principio de Participación Individual:** Toda persona tiene derecho a acceder a los registros de datos donde se halle almacenada información sobre su vida personal o familiar.

### 3.6.6. Clasificación del Habeas Data

1. **Habeas Data Informativo:** Es aquél, de acuerdo con Sagüés, utilizado por quien procura recabar información. Se divide a su vez en subtipos como el exhibitorio, previsto para conocer que se registró; finalista, destinado a determinar para qué y para quién se realizó el registro; y autorial, cuyo sentido es el averiguar quién obtuvo los datos incluidos en el registro. Como fácilmente puede verse, incidimos nosotros, aquí lo que parece procurarse es darle una adecuada tutela a derechos como los de acceso a los diferentes bancos de datos que pudiesen existir.[55]
2. **Habeas Data Aditivo:** Aquí lo que se va a buscar es agregar más datos a aquellos que figuren en el registro respectivo, ya sea actualizando datos que no responden al actual estado de cosas (subtipo actualizador) o incorporando a alguno que no fue oportunamente incluido (subtipo inclusivo). Va de la mano con la actualización como parte de la autodeterminación informativa.
3. **Habeas Data Rectificador o Correctivo:** Destinado a modificar o sacar informaciones falsas, inexactas o imprecisas de un banco de datos. Sin duda busca tutelar el aspecto denominado modificación o corrección.
4. **Habeas Data Reservador:** Su finalidad es asegurar que un dato legítimamente registrado sea solamente proporcionado a quienes estén legalmente autorizados para ello. La protección de la confidencialidad como parte de la autodeterminación informativa está claramente detrás de este tipo de Hábeas Data.
5. **Habeas Data Exclutorio o Cancelatorio:** Tiene por objeto eliminar la información del registro, donde se encuentre registrados, cuando por algún motivo no deba mantenerse, su razón de ser es la eliminación de aquella información sensible,

[55] Perez, R. (2011). La regulación para el acceso a datos en los registros públicos y privados en Boivia. https:// repositorio.umsa.bo/xmlui/handle/123456789/14189.

información que en mérito a su misma naturaleza no debiera estar en algún o algunos de los bancos de datos. Este tipo está relacionado con los datos sensibles.

## 3.7. DERECHOS SOBRE LOS DATOS

### 3.7.1. Control sobre los datos

El término que se utiliza en esta materia es el de “derecho a la protección de los datos personales”. Aquí cabe una aclaración, puesto que a simple vista parecería que se quiere proteger el dato; sin embargo, el concepto va más allá. No se está hablando de proteger el dato, sino a la persona que está detrás del dato, es decir a la persona a la cual ese dato identifica o hace identificable. Por lo tanto, a fin de generar esa protección se le brindan herramientas para que controle la información que está relacionada a su persona.

Dicho control sobre los datos personales es entendido por una parte de la doctrina jurídica como un ejercicio de autodeterminación informativa, esto es, la libertad de decidir sobre la propia información. Lo cual permite que la persona pueda, por ejemplo, conocer de qué forma y con qué finalidades se están tratando sus datos personales y así evitar daños económicos y sociales, entre otros.

Es así que debemos mencionar la expresión básica del control de nuestros datos personales: el consentimiento como una expresión explícita, informada, que hacemos de manera libre a fin de dar nuestra aprobación a un tercero para que realice tratamiento de nuestros datos personales.

### 3.7.2. Derecho a la Información

Este derecho nos garantiza poder obtener información sobre el tratamiento de nuestros datos directamente del ente responsable del tratamiento, sin demoras ni trámites burocráticos. Esto incluye, entre otros, el derecho a saber quiénes, cómo, con qué fines y por cuánto tiempo recolectan y analizan nuestra información.

### 3.7.3. Derecho de acceso

Este derecho nos permite conocer de primera mano si un ente privado o de gobierno tiene o trata nuestros datos. Este derecho incluye el de obtener una copia de ese archivo. Por ejemplo, si quieres ejercer este derecho podrías pedir a tu centro de salud el historial de las visitas médicas que realizaste y este centro deberá entregarte una copia de dicho historial.

### 3.7.4. Derecho a la rectificación

Este derecho fue pensado en consonancia a otro principio que es el de exactitud y del que hablaremos más adelante. Los datos que se manejen deben ser exactos, por lo tanto, se nos da la posibilidad de corregir y actualizar los datos personales que estén almacenados en bases de datos. Por ejemplo, podríamos querer actualizar nuestro estado civil o el registro de deudas que figura en servicios de información crediticia.

### 3.7.5. Derecho a revocar el consentimiento o cancelación

Como comentamos líneas arriba, una de las expresiones base de la protección de los datos personales es el consentimiento. Así como damos nuestro consentimiento para que nuestros datos sean tratados, también podemos retirar dicho consentimiento cuando el

tratamiento sea excesivo, no pertinente, inadecuado, entre otros. Ello significa que el responsable del tratamiento deberá dejar de tratar nuestros datos personales.

### 3.7.6. Derecho de supresión

Este derecho garantiza que luego de terminado el uso de un servicio, podamos solicitar que el responsable elimine todos los datos personales que nos conciernen. En marcos regulatorios como el RGPD, también puede reclamarse la eliminación cuando el responsable de los datos los haya usado ilegalmente.[56]

### 3.7.7. Derecho al olvido

Este derecho está lleno de controversias. El derecho al olvido apareció en un caso judicial ante la Corte Europea de Justicia y consiste en que la persona puede pedir que se disocie de los buscadores en internet aquella información personal que ya no sea relevante. Si bien parece una causa noble, la misma ha generado ciertas discusiones. La más importante de ellas es con respecto al derecho a la información: al disociar dicha información se reducen las posibilidades que otras personas puedan conocer hechos que eventualmente puedan resultar de interés público.

### 3.7.8. Derecho a la oposición

Este derecho permite a las personas oponerse a la recolección o tratamiento de su información personal ante ciertos casos puntuales, que cada legislación determina en función de objetivos de política pública. Ejemplo de esto son los casos en los que podemos

[56] Perez del Castillo, R., Quiroz, E. (2019). Guia básica sobre datos personales para Bolivia. https://www.accessnow.org.

oponernos previamente al tratamiento de nuestros datos con fines de marketing o si se hace para la toma automatizada de decisiones que nos conciernen.[57]

### 3.7.9. Derecho a la portabilidad

Este es un nuevo derecho que se incluyó recientemente en el RGPD. Según este derecho, tenemos el poder movilizar nuestros datos personales de una base de datos a otra. Ello puede implicar solicitar al responsable del tratamiento una copia o el original de toda nuestra información en un formato compatible que permita trasladarla a otro proveedor de servicios. En algunos casos también puede pedirse que el responsable del tratamiento de datos haga ese traslado por nosotros. Por ejemplo, se podría solicitar a un banco que mueva todos nuestros datos a otro banco. Así, no perderíamos historial de nuestros movimientos financieros, ni de los créditos que obtuvimos.

### 3.7.10. Derecho a la explicación

Este también es otro derecho que fue plasmado por primera vez en el RGPD. Cabe resaltar que no hay un artículo en específico asignado a este derecho, sino que proviene de la interpretación de varios. Este derecho nos permite obtener explicaciones sobre las decisiones que se realizan mediante el tratamiento automatizado de nuestra información personal. Es el caso de las decisiones que se toman mediante sistemas de inteligencia artificial o algoritmos.[58]

[57] Perez del Castillo, R.,Quiroz, E. (2019). Guia básica sobre datos personales para Bolivia. https://www.accessnow.org.
[58] Idem

## 3.8. PROTECCIÓN DE LOS DATOS PERSONALES

### 3.8.1. Rol del Estado

El principal actor llamado a garantizar nuestros derechos es el Estado. En ese sentido, el Estado debe promover mecanismos que nos permitan controlar nuestros datos personales. Uno de estos mecanismos es el contar con una ley general sobre la materia, otro factor adicional son políticas públicas para capacitar a la población sobre los derechos que tiene, e inclusive el Estado podría trabajar mano a mano con las empresas para asegurar que respeten los derechos de las personas. Claramente, el Estado puede implementar un sinfín de mecanismos. En los siguientes puntos hablaremos de dos de ellos.

### 3.8.2. Marco Normativo - Enfoque desde el usuario y principios

Varios países en la región de América Latina cuentan con una ley general sobre protección de datos personales. Algunas de estas leyes fueron elaboradas hace más de una década y naturalmente a la fecha requieren actualizaciones debido a la evolución tecnológica y el enfoque actual del uso de datos en la economía digital. Esto último se debe básicamente a la forma en que están planteadas estas leyes, es decir, el enfoque que se utilizó.

Anteriormente, las leyes de protección de datos seguían el principio de territorialidad de las normas, que dice que las normas se aplican dentro del territorio de un Estado. De esta manera, se decidía qué ley se aplicaba de acuerdo a donde se encontraba el responsable del tratamiento y/o su base de datos. Por ejemplo, si el responsable y/o la base de datos estaban en Bolivia entonces se aplicaba la ley de Bolivia. Siguiendo el ejemplo, el problema surgió cuando esas bases comenzaron a tener responsables de tratamiento o estar

situadas fuera de Bolivia. Internet y la transmisión de datos personales a servidores que están situados fuera del país presentan un desafío en este sentido.

En este contexto, la Unión Europea propuso un nuevo enfoque: desde el usuario. Ello significa que no importa dónde los datos personales de esa persona estén almacenados o donde esté el responsable del tratamiento. Por consiguiente, se optó por una mirada extraterritorial de la aplicación de las normas. De esta manera, se aplicará las leyes de donde se encuentre el usuario.

### 3.8.3. Principios más usados

Otro punto importante es la inclusión de principios. Algunas leyes en la región ya incluyen principios rectores. Lo cual es bueno y debe repetirse en las nuevas propuestas legislativas. Ello porque los principios son fundamentos y límites básicos que se mantienen en el tiempo. Principios más usados:

#### 3.8.3.1. Lealtad y legalidad

Los datos personales deben ser procesados de manera justa y legal; lo que implica que exista una ley, y que el tratamiento de datos se realice de una manera justa y transparente, para que podamos informarnos sobre cómo las entidades recopilan, usan y almacenan nuestros datos personales.

#### 3.8.3.2. Limitación de la finalidad

Los datos personales deberán ser tratados solo para fines específicos y legítimos. El propósito debe ser explícito, y de duración limitada.

#### 3.8.3.3. Minimización de Datos

El tratamiento de datos personales debe limitarse a lo que sea suficiente, pertinente y no excesivo en relación con una finalidad específica y definida.

#### 3.8.3.4. Exactitud

Los datos personales deben ser precisos y, cuando corresponda, deben ser actualizados. Recordamos aquí el derecho que tenemos de rectificación.

#### 3.8.3.5. Conservación Limitada

Los datos personales procesados por cualquier propósito no deben ser mantenidos por más tiempo del necesario.

#### 3.8.3.6. Derechos de los usuarios

Los datos personales deben ser tratados respetando nuestros derechos.

#### 3.8.3.7. Integridad y confidencialidad

Los datos personales deben ser tratados de forma segura, protegiéndolos contra accesos no autorizados o ilegítimos, pérdida accidental, destrucción o daño de los mismos.

#### 3.8.3.8. Adecuación

Los datos personales no deben ser transferidos a un país o territorio tercero, a menos que el país o territorio en cuestión garantice un nivel adecuado de protección para nuestros derechos en relación al tratamiento de los datos personales.

### 3.9. AUTORIDAD COMPETENTE

Además de contar con una ley general sobre datos personales, los Estados también deben crear una autoridad con capacidad de hacer cumplir la norma legal. Se recomienda que esta autoridad sea independiente en todo sentido, para que pueda realizar investigaciones, fiscalizaciones y pueda sancionar a cualquier entidad sea esta pública o privada. Asimismo, esta autoridad debe contar con mecanismos robustos de control que le permitan actuar sin retraso.

La importancia de contar con una autoridad de protección de datos adecuada se puede ver en Chile y Brasil, países donde existe legislación, pero no se cuenta con una autoridad independiente, haciendo que la ley y sus disposiciones se queden en el papel.[59]

### 3.10. SUJETOS O ROLES QUE INTERVIENEN EN LA PROTECCIÓN DE DATOS

1. **El Interesado.** La persona física de la que se trata información que la identifica o hace identificable.
2. **El Responsable del Tratamiento.** La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, (corresponsables) determine los fines y medios del tratamiento.
3. **El Encargado del Tratamiento.** La persona física o jurídica, autoridad pública, servicio u otro organismo que trata datos personales por cuenta del responsable del tratamiento.
4. **El Delegado de Protección de Datos.** Persona contratada por el responsable del tratamiento, para informarle y asesorarle, supervisar el cumplimiento de lo dispuesto en

[59] Perez del Castillo, R., Quiroz, E. (2019). Guia básica sobre datos personales para Bolivia. https://www.accessnow.org.

el Reglamento, Cooperar con la autoridad de control, y actuar como punto de contacto con esta.

5. **La Autoridad de Control.** En España, existe una autoridad de control nacional, la Agencia española de Protección de Datos, siendo competente en el territorio de su Estado para ejercer los poderes y desempeñar las funciones que se le confiere Reglamento General de Protección de Datos.

# CAPÍTULO IV

# MARCO NORMATIVO

## 4.1. DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS

La Declaración Universal de los Derechos Humanos, en 1948, señala el derecho a la intimidad en su artículo 12, referido a que toda persona debe ser protegida ante injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia, así como de ataques contra su honra y reputación. así inició un recorrido normativo en aras de garantizar el derecho a la protección de datos. Este precepto fue ratificado en el artículo 17 del Pacto internacional de Derechos civiles y Políticos, adoptado por la asamblea General de las Naciones Unidas en la Resolución 2200 a (XXi), de 16 de diciembre de 1966, como un refuerzo a la Declaración Universal de los Derechos Humanos de 1948 y años más tarde fue introducido en el artículo 11 de la Convención Americana de Derechos Humanos de 1969, celebrada en San José, Costa Rica del 7 al 22 de noviembre del mismo año.

## 4.2. CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS O PACTO DE SAN JOSÉ, DE 22 DE NOVIEMBRE DE 1969

Regula el Derecho de Rectificación o Respuesta, en su artículo 14 que literalmente expresa:

1. Toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentados y que se dirijan al público en general, tiene derecho a efectuar por el mismo Órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley.

2. En ningún caso la rectificación o la respuesta eximirán de las otras responsabilidades legales en que se hubiese incurrido.

3. Para la efectiva protección de la honra y la reputación, toda publicación o empresa periodística, cinematográfica, de radio o televisión tendrá una persona responsable que no esté protegida por inmunidades ni disponga de fuero especial.[60]

### 4.3. ORGANIZACIÓN DE NACIONES UNIDAS (ONU)

En 1948, adopta el documento conocido como Declaración Universal de Derechos Humanos, en la que el artículo 12 señala que las personas tienen derecho a la protección de la ley de sus datos personales.[61]

### 4.4. APROXIMACIÓN GENERAL A LA REGULACIÓN DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN IBEROAMÉRICA

Iberoamérica no tiene una tradición tan arraigada en materia de protección de datos personales como podamos encontrar en Europa o Estados Unidos. Esto es consecuencia directa, de una parte, del escaso nivel de desarrollo que las Tecnologías de la Información alcanzaron en estos países, sobre todo en las décadas de los 70 y 80, años en los que, como hemos visto, en Europa se estaba formando la que hemos denominado “conciencia de protección de datos”. Por otra parte, este factor en algunos casos combinó con la existencia de regímenes totalitarios poco receptivos al reconocimiento de los derechos fundamentales que sirvieron como base para desarrollar el derecho a la protección de datos personales.

---

[60] Villalta, A. E. (2017). La privacidad y la protección de datos personales. www.oas.org/es/sla/cji/docs/informes_culminados_recientemente_Proteccion_Datos_Personale.

[61] Sanchez, Gabriel., Rojas, I. (2018). Leyes de protección de datos personales en el mundo y la protección de datos biométricos – parte I. https://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo.

Esta situación comenzó a cambiar hacia finales de la década de los ochenta, cuando empezaron a surgir voces exigiendo protección en este ámbito. En este sentido, fue la Constitución Brasileña de 1988, el primer texto fundamental que reguló la materia adoptando un procedimiento basado en la acción del “Habeas Data”. Se trataba de una acción concebida como una protección constitucional contra los abusos del poder y las ilegalidades cometidas por los administradores y encargados de gestionar datos personales para los poderes públicos. A través de la acción de Habeas Data, los interesados pueden solicitar la exhibición de sus datos personales a la autoridad responsable de su registro y si fuere procedente, exigir su supresión, rectificación o actualización. En concordancia con este primer antecedente, "Habeas Data" es la denominación que mejor representa a los temas de protección de datos personales en Iberoamérica, coloquialmente hablando, si bien desde un punto de vista estrictamente técnico con este término nos estamos refiriendo a una garantía procesal constitucional. El Habeas Data fue posteriormente adoptado por otras constituciones como es el caso de Argentina, Perú, Paraguay y Ecuador.

En términos generales, el Habeas Data es un procedimiento abreviado, para el que se establecen plazos cortos. Su tramitación es competencia de los órganos de justicia. De todas formas, y examinando el Habeas Data desde la perspectiva del nivel de protección que establece la Directiva, debe entenderse que, en general, nos encontramos ante un procedimiento que no garantiza un nivel de protección comparable.

### 4.5. RED IBEROAMERICANA DE DATOS PERSONALES

En junio de 2003, en el marco del Encuentro Iberoamericano de Protección de Datos celebrado en La Antigua (Guatemala), y a iniciativa de la Agencia Española de Protección de Datos, se creó la Red Iberoamericana de Protección de Datos. La idea consistía

en la creación de un foro abierto a la incorporación de los países iberoamericanos, con el propósito de potenciar las iniciativas de intercambio de experiencia entre los miembros y de reforzar la colaboración en materia de protección de datos. En noviembre del mismo año, la Declaración de Santa Cruz de la Sierra (Bolivia), firmada tras la XIII Cumbre de Jefes de Estado y de Gobierno de Iberoamérica, recogió en su artículo 45 el reconocimiento expreso de la protección de datos como derecho fundamental y la labor de la Red Iberoamericana. En estos momentos, la Red cuenta con la representación de entidades de control de 17 países.

Entre los objetivos de la Red destaca el impulso para la elaboración de los instrumentos normativos necesarios para garantizar la protección del derecho a la protección de datos personales en aquellos países de la Comunidad Iberoamericana que aún no hayan afrontado su regulación.

### 4.6. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)

El Reglamento General de Protección de Datos (RGPD) es un conjunto de regulaciones que aborda la forma en que las empresas deben recopilar y tratar los datos personales en internet.

El RGPD es la nueva regulación sobre protección y tratamiento de datos que afecta a todas las empresas y autónomos que operan en la UE, tengan o no residencia comunitaria.

El reglamento entró en vigor el 24 de mayo de 2016, pero será de obligado cumplimiento a partir del 25 de mayo de 2018.[62]

La necesidad de respetar los derechos de privacidad y protección de datos del individuo está detrás de la nueva regulación, de modo que se garantice que toda la información de carácter personal que se reúna sea con consentimiento y pueda ser retirada por el usuario en cualquier momento.

El RGPD se ha introducido como reglamento para unificar el modo en que las empresas recopilan y tratan los datos de sus usuarios en cualquiera de sus sitios web o servicios online.

Los cambios en los métodos de recopilación online de datos sobre personas han dado lugar a la necesidad de un enfoque actualizado para el tratamiento de datos en términos de negocios.

Si bien existen regulaciones vigentes en todos los países de la UE, la cobertura, el cumplimiento y las sanciones difieren enormemente entre países. El RGPD homologa y unifica cada elemento de las distintas regulaciones nacionales así como el método en que las empresas deben recopilar y tratar los datos personales dentro de la UE.

El RGPD tiene como objetivo aumentar la transparencia de cómo los sitios web y las empresas manejan los datos personales que se recopilan a partir de la navegación web y servicios que ofrecen a los usuarios.

[62] Herranz, A. (2018). GDPR/RGPD: qué es y cómo va a cambiar internet la nueva ley de protección de datos. https://www.xataka.com/legislacion-y-derechos/gdpr-rgpd-que-es-y-como-va-a-cambiar-internet-la-nueva-ley

También exige que cualquier fuga que ponga en peligro el conocimiento a terceros de cualquier tipo de información personal recopilada sea informada a las autoridades correspondientes dentro de las 72 horas posteriores a la fuga, de modo que se pueda minimizar la exposición y el potencial daño.

La nueva regulación prioriza los derechos de la persona y obliga a las empresas a informar por qué y cómo utilizan los datos personales.

Cada usuario, según el RGPD, deberá aceptar los términos y condiciones modificados para muchos de los servicios online que ya tienen contratados. La mayoría de las compañías también deberá hacer público su política de privacidad, así como un documento que detalle cómo se procesarán los datos (Acuerdo de Procesamiento de Datos).

El RGPD amplía y protege los derechos individuales relativos a los datos personales. Es decir, que la nueva regulación supone:

• La obligación de dar consentimiento y el derecho a eliminar dicho consentimiento para recibir newsletters.

• El derecho a poder exportar todos los datos personales almacenados por cualquier empresa.

• El "derecho al olvido".

• La obligación de una empresa a ofrecerle toda la información sobre cómo trata los datos personales.

Si una persona tiene una pequeña empresa o sitio web, entonces también queda obligado por la nueva regulación. Si un sitio web utiliza cookies, requiere un inicio de sesión o si envía una newsletter a sus usuarios, deberá implementar la nueva regulación.

## 4.7. NORMATIVA NACIONAL SOBRE PROTECCIÓN DE DATOS PERSONALES

### 4.7.1. El Recurso de Habeas Data en Bolivia

El hábeas data, como una vía procesal instrumental de protección al derecho a la autodeterminación informática, fue incorporado al sistema constitucional boliviano mediante la Ley 2631 de Reforma de la Constitución de 20 de febrero de 2004.

Ley 2410 Declaratoria de Necesidad de Reforma se propuso ampliar el catálogo de los derechos fundamentales previsto en el artículo 7 de la Constitución, con la inclusión de otros derechos fundamentales, entre ellos, el derecho a la intimidad y privacidad, imagen, honra y reputación.

En la Ley 2410 Declaratoria de Necesidad de Reforma, en el capítulo referido a las garantías constitucionales, se propuso instituir el Habeas Data como vía jurisdiccional expedita para que toda persona pueda acceder, objetar u obtener la eliminación o rectificación de sus datos personales registrados en bancos de datos o archivos públicos o privados. A este efecto la Ley 2410 se propuso modificar el texto del artículo 23 de la Constitución.

En efecto, el constituyente boliviano, al sancionar la Ley 2631 de fecha 20 de febrero de 2004, en el marco de la Ley 2410 de fecha 1.º de agosto de 2002, entre otras disposiciones, reforma el artículo 23 del texto de la Constitución. [63]

[63] Medinaceli, K. (2016). El Tratamiento de los Datos Sanitarios en la Historia Clínica: Caso Boliviano. https://www.aepd.es/sites/default/files/2019-10/tratamiento-de-datos-sanitarios

### 4.7.2. La Acción de Protección de Privacidad

El Estado Plurinacional de Bolivia ha reformado su Constitución en el año 2009, oportunidad en la que ha incluido una nueva garantía constitucional de protección a la intimidad y a los datos personales, a la que denominó “acción de privacidad”.

En esta constitución se ha ampliado el catálogo de los derechos civiles y políticos; es así que en el artículo 21.2. se han consagrado los derechos a la privacidad e intimidad, honra, honor, propia imagen y dignidad. En coherencia con ello, se ha consolidado la garantía constitucional jurisdiccional que protege el derecho a la intimidad y privacidad, en su dimensión positiva de conocer, objetar u obtener la eliminación o rectificación de los datos de la vida íntima o privada de la persona o sus familiares, mismos que son obtenidos, almacenados y distribuidos por bancos de datos públicos o privados por cualquier medio físico, electrónico, magnético e informático. El Constituyente ha cambiado el nombre de la garantía constitucional jurisdiccional, denominándola Acción de Protección de Privacidad en reemplazo del Recurso de Hábeas Data.

Probablemente por su reciente mutación constitucional, Bolivia todavía no ha desarrollado legislativamente el instituto de la protección de los datos personales en una ley específica. Por este motivo, ante la carencia de normas infra constitucionales, la protección genérica de la intimidad o la protección específica de los datos de carácter personal debe ser complementada por otras normas análogas o genéricas que indirectamente puedan hacer referencia al tema.[64]

### 4.7.3. Constitución Política del Estado

[64] Durán, M. (2018). Normativa sobre protección de datos personales en Bolivia. https://medium.com/@mrduranch/normativa-sobre-datos-personales-en-bolivia-ece7a61f50b0

En este sentido, la Constitución Política del Estado de Bolivia expresa en el Capítulo Tercero, referido a los Derechos Civiles y Políticos, Sección I sobre Derechos Civiles, artículo 21º: que “Las bolivianas y los bolivianos tienen los siguientes derechos: A la privacidad, intimidad, honra, honor, propia imagen y dignidad.

Más adelante, la Carta Magna de Bolivia se ocupa nuevamente del derecho a la intimidad y en particular del derecho a la protección de los datos personales, en el Título IV referido a las Garantías Jurisdiccionales y Acciones de Defensa, en cuyo Capítulo Segundo dedicado a las Acciones de Defensa propiamente dichas, en su Sección III, se encuentra el artículo 130, que textualmente expresa:

I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.
II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa.

A continuación, el artículo 131.

I. La acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional
II. Si el tribunal o juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado. Esta sentencia tiene efecto ejecutivo, ya que textualmente el apartado III del artículo 131 expresa:

"La decisión se elevará, de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución".

III. La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo con lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme lo dispuesto por este artículo quedará sujeta a las sanciones previstas por la Ley.

La ley fundamental boliviana establece en el artículo 109 punto I, que "Todos los derechos reconocidos en la Constitución son directamente aplicables y gozan de iguales garantías para su protección", con lo cual queda claro que, al estar el derecho a la protección de los datos personales reconocido en la Carta Magna, es de aplicación operativa y no programática. Sin embargo, de legeferenda, se plantea la sanción de una ley específica sobre el tema.

El derecho a la intimidad también se encuentra contenido por la protección al secreto de la correspondencia y de los papeles privados, que la Constitución Política del Estado contempla en el art. 25 del texto reformado.

También el artículo 35 es muy claro al expresar que "Las declaraciones, derechos y garantías que proclama esta Constitución no serán entendidas como negación de otros derechos y garantías no enunciados que nacen de la soberanía del pueblo y de la forma republicana de gobierno". El derecho a la protección de los datos personales no es una

creación posmodernista del derecho positivo, sino un descubrimiento basado en la necesidad humana de proteger su dignidad, libertad e intimidad de cada persona.[65]

El derecho a la protección de datos personales existe aun cuando en Bolivia faltan leyes que desarrollen la Constitución, dada su calidad de derecho humano y personalísimo.

Aun así, es conveniente su pronta incorporación en el derecho positivo infra constitucional para dar una mayor protección a los habitantes de Bolivia, a los efectos de que cuenten con garantías constitucionales y leyes específicas que protejan su intimidad y sus datos personales. También sería importante para las relaciones exteriores de Bolivia, ya que una incorporación legislativa seria y completa sobre este tema, le permitiría cumplir con las exigencias de una normativa equivalente requerida por la Unión Europea y otros Estados que se preocupan por este derecho. Una legislación que se precie de completa y seria sobre protección de datos personales, debe incluir la creación de un organismo de control o autoridad de aplicación en la materia. [66]

Así como los autores mencionados realizan el análisis sobre la normativa nacional, en este caso en la Constitución Política de nuestro país, los artículos citados precisan con claridad los derechos a la intimidad, privacidad e incluso la acción de protección a la privacidad que también está establecida en esta ley fundamental, lo que hace posible, sobre esta base jurídica, encaminar o formular una ley específica de protección de datos personales.

---

[65] Saltor, C. E. (2013). La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina. (Memoria grado Doctor). Universidad Complutense de Madrid. Madrid-España. Recuperado de https://eprints.ucm.es

[66] Idem

## 4.8. LEGISLACIÓN SECTORIAL

### 4.8.1. Código Civil

Normativa de 6 de agosto de 1975, determina en los siguientes artículos:

Artículo 15°.- (Nulidad) Son nulas toda confesión y toda manifestación de voluntad obtenidas por procedimientos lesivos a la personalidad.

Artículo 16°.- (Derecho a la imagen)

1. Cuando se comercia, publica, exhibe o expone la imagen de una persona lesionando su reputación o decoro, la parte interesada y, en su defecto, su cónyuge, descendientes o ascendientes pueden pedir, salvo los casos justificados por la ley, que el juez haga cesar el hecho lesivo.

2. Se comprende en la regla anterior la reproducción de la voz de una persona.

Artículo 17°.- (Derecho al honor) Toda persona tiene derecho a que sea respetado su buen nombre. La protección al honor se efectúa por este Código y demás leyes pertinentes.

Artículo 18°.- (Derecho a la intimidad) Nadie puede perturbar ni divulgar la vida íntima de una persona. Se tendrá en cuenta la condición de ella. Se salva los casos previstos por la ley.

El código civil también establece en los artículos mencionados los derechos de las personas, en cuanto se refiere a la imagen, privacidad, intimidad, honor, etc., otorgando cobertura y protección y que los usuarios pueden acudir en su defensa; sin embargo, también son normas que requieren ser incluidas en un marco legal específico de protección de datos de carácter personal.

### 4.8.2. Ley № 1488 de 14 de abril de 1993. Ley de Bancos y Entidades Financieras

Artículo 86°.- Las operaciones bancarias en general estarán sujetas al secreto bancario. No podrán proporcionarse antecedentes relativos a dichos operaciones sino a su titular, o a la persona que lo represente legalmente.

Artículo 87°.- El secreto bancario será levantado únicamente.

1. Mediante orden judicial motivada, expedida por un juez competente dentro de un proceso formal y de manera expresa, por intermedio de la Superintendencia.
2. Para emitir los informes ordenados por los jueces a la Superintendencia en proceso judicial y en cumplimiento de las funciones que le asigna la Ley.
3. Para emitir los informes solicitados por la administración tributaria sobre un responsable determinado, que se encuentre en curso de una verificación impositiva y siempre que el mismo haya sido requerido formal y previamente; dichos informes serán tramitados por intermedio de la Superintendencia.
4. Dentro de las informaciones que intercambian las entidades bancarias y financieras entre sí, de acuerdo a reciprocidad y prácticas bancarias.
5. Para emitir los informes de carácter general que sean requeridos por el Banco Central de Bolivia.

De manera sectorial, las entidades bancarias y financieras de administración tributaria, etc, tienen normas que regulan de forma particular el tratamiento de los datos o

informes de los usuarios, sin embargo, esta normativa no tiene injerencia en otros campos públicos o privados por ende su aplicación es restringida.

### 4.8.3. Código Penal

Modificado por la Ley Nº 1768, de 10 de marzo de 1997 (Artículos 363 Bis y 363 ter.). Delitos Informáticos.

Artículo 363 Bis. (MANIPULACIÓN INFORMÁTICA). El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno (1) a cinco (5) años y con multa de sesenta (60) a doscientos (200) días.

Artículo 363 Ter. (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS). El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un (1) año o multa hasta doscientos (200) días.[67]

El código penal boliviano establece según lo descrito en estos dos artículos sanciones a los delitos informáticos, por manipulación informática, alteración, acceso y uso indebido de datos. Sin embargo, se circunscribe tan solo a estos delitos de manera específica, por lo que su análisis se reduce al ámbito sectorial.

[67] Durán, M. (2018). Normativa sobre protección de datos personales en Bolivia. https://medium.com/@mrduranch/normativa-sobre-datos-personales-en-bolivia-ece7a61f50b0

### 4.8.4. Ley N° 2026 de 14 de octubre de 1999. Código del Niño, Niña y Adolescente.

Artículo 10°.- (Reserva y resguardo de identidad) Las autoridades judiciales y administrativas tienen la obligación de resguardar la identidad de los niños, niñas y adolescentes que se vean involucrados en cualquier tipo de procesos, salvo los casos expresamente previstos por este Código.

Los medios de comunicación cuando publiquen o transmitan noticias que involucren a niños, niñas o adolescentes, no pueden identificarlos nominal ni gráficamente, ni brindar información que permita su identificación, salvo determinación fundamentada del Juez de la Niñez y Adolescencia, velando en todo caso, por el interés superior de los mismos.

El incumplimiento de esta disposición dará lugar a la acción legal correspondiente.

Artículo 229°.- (Prohibición de registro) Los organismos policiales no podrán registrar en sus archivos datos personales del adolescente que incurra en una infracción.

El registro judicial de infracciones será reservado y sólo podrá certificar antecedentes mediante auto motivado.

Como se puede apreciar en los artículos 10 y 229 del Código del Niño, Niña y Adolescente, esta normativa protege la intimidad y la privacidad pero solamente de niñas, niños y adolescentes de manera “aislada”; obviamente este Código establece estos articulados bajo el criterio del interés superior del niño, respaldados por la Convención sobre los Derechos del Niño, pero su cobertura se reduce a estos grupos etáreos.

### 4.8.5. D.S. N° 28168 de 18 de mayo de 2005. Acceso a la Información del Poder Ejecutivo

ARTÍCULO 19.- (PETICIÓN DE HABEAS DATA).

I. Toda persona, en la vía administrativa, podrá solicitar ante la autoridad encargada de los archivos o registros la actualización, complementación, eliminación o rectificación de sus datos registrados por cualquier medio físico, electrónico, magnético o informático, relativos a sus derechos fundamentales a la identidad, intimidad, imagen y privacidad. En la misma vía, podrá solicitar a la autoridad superior competente el acceso a la información en caso de negativa injustificada por la autoridad encargada del registro o archivo público.

II. La petición de Habeas Data se resolverá en el plazo máximo de cinco (5) días hábiles. En caso de negativa injustificada de acceso a la información, la autoridad jerárquica competente, adicionalmente tendrá un plazo de quince (15) días hábiles para proporcionar la información solicitada.

III. La petición de Habeas Data no reemplaza ni sustituye el Recurso Constitucional establecido en el Artículo 23 de la Constitución Política del Estado. El interesado podrá acudir, alternativamente, a la vía administrativa sin que su ejercicio conlleve renuncia o pérdida de la vía judicial. El acceso a la vía judicial no estará condicionado a la previa utilización ni agotamiento de esta vía administrativa.

El D.S. N° 28168 de 18 de mayo de 2005, plantea este recurso de petición de habeas data con la finalidad de hacer valer los derechos de las personas en cuanto soliciten información, rectificación, actualización o eliminación de sus datos registrados en cualquier medio, esta es otra norma que ampara los derechos de las personas al ser un recurso

específico de protección de los datos de carácter personal. Es muy importante este recurso legal, sin embargo, también su aplicación es de carácter sectorial.

### 4.8.6. Ley N° 3131 de 8 de agosto de 2005. Ley del Ejercicio Profesional Médico

Artículo 3°.- (Principios)

c) En el ejercicio profesional médico, inclusive en la enseñanza de la medicina, el secreto médico es inviolable salvo las excepciones previstas en la presente Ley.

Articulo 4°.- (Definiciones)

SECRETO MÉDICO: Toda información identificada durante el acto médico sobre el estado de salud o enfermedad del paciente, su tratamiento y toda otra información de tipo personal, debe mantenerse en secreto, inclusive después de su muerte, para salvaguarda de la dignidad del paciente.

Artículo 12°.- (Deberes del Médico) Son deberes del profesional médico:

k. Guardar el secreto médico, aunque haya cesado la prestación de sus servicios.

Dentro de los deberes del médico, establecidos en el artículo 12 de la Ley 3131, se rescatan los relacionados con la información, consentimiento del paciente, secreto médico. — Respetar el consentimiento expreso del paciente, cuando rechace el tratamiento u hospitalización que se le hubiera indicado. — Informar al paciente, o responsables legales, con anterioridad a su intervención, sobre los riesgos que pueda implicar el acto médico. — Guardar el secreto médico, aunque haya cesado la prestación de sus servicios. [68]

Artículo 13°.- (Derechos del Paciente) Todo paciente tiene derecho a:

c) La confidencialidad.

[68] Medinaceli, K. (2016). El Tratamiento de los Datos Sanitarios en la Historia Clínica Electrónica: Caso Boliviano. https://www.aepd.es/sites/default/files/2019-10/tratamiento-de-datos-sanitarios.pdf

d) Secreto médico.

g) Reclamar y denunciar si considera que sus derechos humanos han sido vulnerados durante la atención médica.

i) Respeto a su intimidad.[69]

Asimismo, dentro de los deberes del paciente, éste debe comunicar de manera veraz y completa sus antecedentes de salud, personales y familiares (artículo 14). [70]

Es obligación del médico registrar en la historia clínica la información brindada al paciente respecto al diagnóstico, tratamiento y pronóstico de la enfermedad; este registro debe ser suscrito por el paciente, familiar, pariente o representante legal (artículo 14).

En el sector de salud también la normativa nacional ha tenido el cuidado de establecer artículos que protegen el derecho a la intimidad y privacidad de los pacientes y de los mismos médicos cuando se refiere al secreto profesional. Esta ley respecto a los datos personales define con precisión los derechos de los pacientes y deberes de los médicos en torno a la privacidad de la información, pero también es una norma específica que no aborda otros intereses.

### 4.8.7. Ley N° 018 de 16 de junio de 2010, del Órgano Electoral Plurinacional

Artículos 72 (obligaciones); 74 (Registro y actualización de datos); 76 (Padrón Electoral); 77 (Lista de habilitados e inhabilitados), y 79 (acceso a información del Padrón Electoral).

---

[69] Durán, M. (2018). Normativa sobre protección de datos personales en Bolivia. https://medium.com/@mrduranch/normativa-sobre-datos-personales-en-bolivia-ece7a61f50b0

[70] Medinaceli, K. (2016). El Tratamiento de los Datos Sanitarios en la Historia Clínica Electrónica: Caso Boliviano. https://www.aepd.es/sites/default/files/2019-10/tratamiento-de-datos-sanitarios.pdf

Artículo 72. (OBLIGACIONES). El Servicio de Registro Cívico (SERECÍ) tiene las siguientes obligaciones:

1. Respeto irrestricto del derecho a la intimidad e identidad de las personas y los demás derechos derivados de su registro.

2. Garantizar la privacidad y confidencialidad de los datos registrados de las personas.

3. Velar por la seguridad e integridad de la totalidad de la información registrada.

Artículo 74. (REGISTRO Y ACTUALIZACIÓN DE DATOS).

I. El registro biométrico de datos que componen el Padrón Electoral es permanente y está sujeto a actualización.

II. La actualización de datos en el Padrón Electoral es permanente y tiene por objeto:

1. Registrar a las personas naturales, en edad de votar, que todavía no estuvieren registradas biométricamente tanto en el país como en el extranjero, sin restricción en su número y sin limitación de plazo.

2. Registrar los cambios de domicilio y las actualizaciones solicitadas por las personas naturales.

3. Asegurar que en la base de datos no exista más de un registro válido para una misma persona.

Artículo 76. (PADRÓN ELECTORAL). El Padrón Electoral es el Sistema de Registro Biométrico de todas las bolivianas y bolivianos en edad de votar, y de los extranjeros habilitados por ley para ejercer su derecho al voto. El Padrón Electoral incluye como mínimo, además de la información biométrica, los siguientes datos: nombres y apellidos, fecha de

nacimiento, sexo, grado de instrucción, domicilio, tipo de documento, número de documento, nacionalidad, país, departamento, provincia, municipio, territorio indígena originario campesino y localidad de nacimiento, asiento y zona electoral, recinto de votación.

Artículo 77. (LISTA DE HABILITADOS E INHABILITADOS).

I. Para cada proceso electoral, referendo y revocatoria de mandato, el Tribunal Supremo Electoral, a través del Servicio de Registro Cívico, elaborará la lista de personas habilitadas para votar y la lista de personas inhabilitadas, por cada mesa de sufragio.

II. Las listas de habilitados e inhabilitados, clasificadas por departamento, región, provincia, municipio, territorio indígena originario campesino, circunscripción uninominal, circunscripción especial, localidad, distrito, zona, recinto y mesa, según corresponda, contendrán como mínimo los siguientes datos:

1. Apellidos y nombres, en orden alfabético.
2. Sexo.
3. Número de documento de identidad personal.
4. Fotografía.
5. Recinto y número de la mesa electoral.

III. Las listas de inhabilitados e inhabilitadas, serán publicadas por lo menos cuarenta y cinco (45) días antes de la realización del acto de votación, con el fin de que los interesados tengan el derecho a realizar la representación del caso ante la autoridad competente.

IV. Serán inhabilitadas las personas que no hayan emitido su voto, de forma consecutiva, en dos procesos electorales, referendos o revocatorias de mandatos de alcance nacional, departamental, regional o municipal, o no hayan cumplido su obligación de ser

jurados electorales en uno de dichos procesos. Los mecanismos de habilitación e inhabilitación serán establecidos mediante Reglamento por el Tribunal Supremo Electoral.

Artículo 79. (ACCESO A INFORMACIÓN DEL PADRÓN ELECTORAL).

I. La información estadística del Padrón Electoral es pública. Las organizaciones políticas podrán solicitar una copia digital de la misma al Servicio de Registro Cívico.

La entrega de esta información se sujetará al calendario electoral establecido por el Tribunal Supremo Electoral. Las organizaciones políticas son las únicas responsables sobre su uso.

II. El Servicio de Registro Cívico, proporcionará anualmente datos demográficos y de residencia de las personas naturales al Consejo de la Magistratura para el sorteo de Jueces Ciudadanos.

III. El Servicio de Registro Cívico, proporcionará los datos solicitados de las personas naturales, a requerimiento escrito y fundamentado del Ministerio Público, de un Juez o de un Tribunal competente. Las autoridades requirentes, bajo responsabilidad, no podrán utilizar estos datos para ninguna otra finalidad.

IV. Las instituciones públicas podrán solicitar la verificación de identidad de personas naturales, previo cumplimiento de las condiciones y requisitos establecidos mediante Reglamento por el Tribunal Supremo Electoral.

La Ley N° 018 de 16 de junio de 2010, del Órgano Electoral Plurinacional en sus artículos precedentes da a conocer el procedimiento del uso o tratamiento de los datos personales de la población en edad de sufragar, sin embargo, toda la información proporcionada realmente es muy delicada y requiere un sistema de protección de los datos, de

tal manera que no haya vulneración a los derechos a la privacidad e intimidad de los votantes. Este aspecto se debería incluir en una norma específica de protección de datos personales.

### 4.8.8. Ley N° 164 de 8 de agosto de 2011, General de Telecomunicaciones, Tecnologías de la Información y Comunicación

Artículos 54 (derechos de los usuarios); 56 (inviolabilidad y secreto de las comunicaciones); 59 (obligaciones de los operadores y proveedores); 84 (reglamentación); 89 (correo electrónico personal); 90 (correo electrónico laboral), y 91 (comunicaciones comerciales publicitarias por correo electrónico o medios electrónicos)

Artículo 54. (DERECHOS DE LAS USUARIAS Y USUARIOS). Las usuarias o los usuarios de los servicios de telecomunicaciones y tecnologías de información y comunicación tienen derecho a:

1. Acceder en condiciones de igualdad, equidad, asequibilidad, calidad, de forma ininterrumpida a los servicios de telecomunicaciones y tecnologías de información y comunicación.

2. Elegir y cambiar libremente de operador o proveedor de los servicios y de los planes de acceso a los mismos, salvo las condiciones pactadas libremente en el contrato, las cuales deben ser explícitas, claras y previamente informadas a las usuarias y los usuarios.

3. Acceder a información clara, precisa, cierta, completa, oportuna y gratuita acerca de los servicios de telecomunicaciones y tecnologías de información y comunicación, a ser proporcionada por los operadores o proveedores de los servicios.

4. Acceder gratuitamente a los servicios de telecomunicaciones y tecnologías de información y comunicación en casos de emergencia, que determine la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.[71]

5. Recibir de forma oportuna, comprensible y veraz la factura mensual desglosada de todos los cargos y servicios del cual es usuario, en la forma y por el medio en que se garantice su privacidad.

6. Exigir respeto a la privacidad e inviolabilidad de sus comunicaciones, salvo aquellos casos expresamente señalados por la Constitución Política del Estado y la Ley.

7. Conocer los indicadores de calidad de prestación de los servicios al público de los proveedores de telecomunicaciones y tecnologías de información y comunicación.

8. Acceder gratuitamente a las guías telefónicas a nivel nacional y a un servicio nacional gratuito de información de voz, sobre sus contenidos.

9. Solicitar la exclusión, sin costo alguno, de las guías de usuarias o usuarios disponibles al público, ya sean impresas o electrónicas. Las usuarias o usuarios podrán decidir cuáles datos personales se incluyen, así como comprobarlos, corregirlos o suprimirlos.

10. Suscribir contratos de los servicios de telecomunicaciones y tecnologías de información y comunicación de acuerdo a los modelos de contratos, términos y condiciones, previamente aprobados por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.

11. Ser informado por el proveedor oportunamente, cuando se produzca un cambio de los precios, las tarifas o los planes contratados previamente.

12. Recibir el reintegro o devolución de montos que resulten a su favor por errores de facturación, deficiencias o corte del servicio.

---

[71] Durán, M. (2018). Normativa sobre protección de datos personales en Bolivia. https://medium.com/@mrduranch/normativa-sobre-datos-personales-en-bolivia-ece7a61f50b0

13. Ser informado sobre los plazos de vigencia de las ofertas y promociones de los servicios.

14. Obtener respuesta efectiva a las solicitudes realizadas al proveedor.

15. Ser informado oportunamente de la desconexión o corte programado de los servicios.

16. Reclamar ante los proveedores de servicios y acudir ante las autoridades competentes en aquellos casos que la usuaria o usuario considere vulnerados sus derechos, mereciendo atención oportuna.

17. Recibir protección del proveedor del servicio sobre los datos personales contra la publicidad no autorizada por la usuaria o usuario, en el marco de la Constitución Política del Estado y la presente Ley.

18. Disponer, como usuaria o usuario en situación de discapacidad y persona de la tercera edad facilidades de acceso a los servicios de telecomunicaciones y tecnologías de información y comunicación, determinados en reglamento.

19. Exigir la protección de la niñez, adolescencia y juventud en la prestación de los servicios.

20. Recibir servicios que no causen daños a la salud y al medio ambiente, conforme a normas establecidas.

21. Participar en los mecanismos de control social.

22. Otros que se deriven de la aplicación de la Constitución Política del Estado, Tratados Internacionales, las leyes y demás normas aplicables.

Artículo 56. (INVIOLABILIDAD Y SECRETO DE LAS COMUNICACIONES).

En el marco de lo establecido en la Constitución Política del Estado, los operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación, deben garantizar la inviolabilidad y secreto de las comunicaciones, al igual que la protección de los datos personales y la intimidad de usuarias o usuarios, salvo los contemplados en guías telefónicas, facturas y otros establecidos por norma.

Artículo 59. (OBLIGACIONES DE LOS OPERADORES Y PROVEEDORES).

1. Someterse a la jurisdicción y competencia de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.

2. Proveer en condiciones de igualdad, equidad, asequibilidad, calidad, de forma ininterrumpida, los servicios de telecomunicaciones y tecnologías de información y comunicación.

3. Proporcionar información clara, precisa, cierta, completa, oportuna y gratuita acerca de los servicios de telecomunicaciones y tecnologías de información y comunicación, a las usuarias o los usuarios.

4. Proporcionar información clara, precisa, cierta, completa y oportuna a la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.

5. Proveer gratuitamente los servicios de telecomunicaciones y tecnologías de información y comunicación en casos de emergencia, que determine la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.

6. Entregar en servicios de modalidad post-pago de forma oportuna, comprensible y veraz, la factura mensual desglosada de todos los cargos y servicios del cual es proveedor, en la forma y por el medio en que se garantice la privacidad de la usuaria o del

usuario y facilitar los medios de pago por los servicios prestados. En servicios de modalidad pre-pago o al contado, entregar la factura según corresponda.

7. Entregar gratuitamente y anualmente a las usuarias o los usuarios de servicios de telefonía, guías telefónicas impresas o electrónicas y un servicio gratuito de información de voz, sobre su contenido, así como, excluir sin costo alguno, a las usuarias o los usuarios que así lo soliciten.

8. Suscribir contratos de los servicios de telecomunicaciones y tecnologías de información y comunicación de acuerdo a los modelos de contratos, términos y condiciones, previamente aprobados por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.

9. Efectuar el reintegro o devolución de montos que resulten a favor de las usuarias o los usuarios por errores de facturación, deficiencias o corte del servicio, con los respectivos intereses legales.[72]

Artículo 84. (REGLAMENTACIÓN). El reglamento referido a firmas y certificados digitales comprenderá:

1. Los requisitos, funciones, procedimientos, convenio de partes, obligaciones, cese de la entidad certificadora autorizada, responsabilidad de las entidades certificadoras autorizadas ante terceros, sanciones, resolución de controversias y otros.

2. La publicidad, seguridad e integridad en el uso de la firma digital.

3. Las definiciones, principios y procedimientos relativos al tratamiento de los datos personales.

[72] Durán, M. (2018). Normativa sobre protección de datos personales en Bolivia. https://medium.com/@mrduranch/normativa-sobre-datos-personales-en-bolivia-ece7a61f50b0

Artículo 89. (CORREO ELECTRÓNICO PERSONAL).

A los efectos de esta Ley el correo electrónico personal se equipara a la correspondencia postal, estando dentro del alcance de la inviolabilidad establecida en la Constitución Política del Estado. La protección del correo electrónico personal abarca su creación, transmisión, recepción y almacenamiento.

Artículo 90. (CORREO ELECTRÓNICO LABORAL).

Cuando una cuenta de correo electrónico sea provista por la entidad empleadora al dependiente como medio de comunicación, en función de una relación laboral, se entenderá que la titularidad de la misma corresponde al empleador, independientemente del nombre de usuario y clave de acceso que sean necesarias para su uso, debiendo comunicarse expresamente las condiciones de uso y acceso del correo electrónico laboral a la empleada o empleado.

Artículo 91. (COMUNICACIONES COMERCIALES PUBLICITARIAS POR CORREO ELECTRÓNICO O MEDIOS ELECTRÓNICOS).

Mediante reglamento se establecerán, las condiciones de las comunicaciones comerciales publicitarias realizadas por medio de correo electrónico o cualquier otro medio electrónico, sin perjuicio de la aplicación, en los casos que corresponda, de la normativa vigente en materia comercial sobre publicidad y protección a las usuarias o usuarios.

La Ley N° 164, General de Telecomunicaciones, Tecnologías de la Información y Comunicación también establece de manera sectorial los parámetros legales de cobertura y protección de datos o de información, derechos de los usuarios, la inviolabilidad y secreto de

las comunicaciones; determina aquellas obligaciones de los operadores y proveedores en cuanto al acceso a la tecnología de las comunicaciones. Todos estos aspectos legales brindan cobertura y protección al usuario en cuanto al servicio prestado y al mecanismo de uso de las comunicaciones. También es otra norma que contribuye a establecer una normativa integral de protección de datos personales.

#### 4.8.9. Ley N° 1080, de 11 de Julio de 2018, de Ciudadanía Digital.

Artículo 11°.- (Prohibiciones y sanciones) El uso indebido, suplantación, alteración, modificación o venta de credenciales, datos o información, serán sancionados conforme a normativa vigente.

Artículo 12°.- (Protección de datos personales y seguridad informática)

1. Las y los servidores y funcionarios de las instituciones previstas en la presente Ley, utilizarán los datos personales y la información generada en la plataforma de interoperabilidad y ciudadanía digital únicamente para los fines establecidos en normativa vigente.
2. El incumplimiento de la anterior previsión, será sujeto a responsabilidad por la función pública; para el caso de instituciones privadas que presten servicios públicos delegados por el Estado, el ente que ejerza supervisión respecto a sus funciones deberá establecer los mecanismos pertinentes a fin de dar cumplimiento a esta norma.

Esta ley es muy importante en la actualidad, por el mismo hecho del avance de la tecnología, existe mayor riesgo de vulneración de datos de carácter personal, así como a la privacidad, por lo que debería ser actualizada constantemente; también debe ser incluida en la

nueva normativa legal de protección de datos personales actualizada y evaluada constantemente por un sistema de control de información insertada en esta normativa.

### 4.8.10. D.S. N° 27443, de 8 de abril de 2004 . Reglamento a la Ley de Código Niño, Niña y Adolescente (Ley Nº 2026)

Artículo 13°.- (Discapacidad)

1. El Viceministerio de la Juventud, Niñez y Tercera Edad diseñará, en coordinación con las instancias del Poder Ejecutivo responsables de la formulación de políticas públicas, los programas y proyectos específicos para la prevención, detección oportuna, tratamiento e integración social de niños, niñas y adolescentes con discapacidad y las ejecutará a través de las Prefecturas y los Gobiernos Municipales.

2. Las entidades públicas o privadas acreditadas que brindan atención especializada a niños, niñas y adolescentes con discapacidad, enviarán anualmente, a través de las Instancias Técnicas Gubernamentales, al Viceministerio de la Juventud, Niñez y Tercera Edad, la nómina de la población atendida para la organización de una base de datos departamental y nacional.

Artículo 23°.- (Registro)

1. Todo niño, niña o adolescente, ingresado en un centro de acogimiento público o privado, debe tener un registro desde el momento de su ingreso con datos que permitan identificar su situación personal y familiar, así como la orden judicial de acogimiento y las correspondientes resoluciones de Guarda; al momento de su egreso esta información será actualizada. Los registros deberán consolidarse en una base de datos a cargo de la Instancia

Técnica Gubernamental, que servirá para la elaboración de un sistema de información nacional a cargo del Viceministerio cabeza de sector.

Este sector es muy vulnerable dentro de nuestra sociedad, muchas veces las niñas, niños o personas de la tercera edad, aún con más razón si presentan discapacidad, son excluidos por su condición, por este hecho se los debería tomar muy en cuenta y con prioridad en cualquier modificación o tratamiento de la ley de protección de datos personales; por este mismo hecho esta norma tendría que tener un carácter inclusivo.

#### 4.8.11. D.S. N° 2514 de 9 de septiembre del 2015.

El presente Decreto Supremo tiene por objeto:

a) Crear la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC;

b) Crear los Comités interinstitucionales de Simplificación de Trámites.[73]

ARTÍCULO 19.- (INTEROPERABILIDAD, DATOS E INFORMACIÓN).

I. La AGETIC coordinará con las entidades del sector público la implementación de servicios de interoperabilidad de Gobierno Electrónico, así como los datos e información que deben estar disponibles.

II. Se autoriza a las entidades públicas proporcionar a la AGETIC los datos e información que hubieran producido, recolectado o generado, por medios electrónicos o mecanismos de interoperabilidad, que ésta solicite mediante nota formal de su MAE, en el

[73] Durán, M. (2018). Normativa sobre protección de datos personales en Bolivia. https://medium.com/@mrduranch/normativa-sobre-datos-personales-en-bolivia-ece7a61f50b0

marco de la política general de Gobierno Electrónico, simplificación de trámites, transparencia, participación y control social y tecnologías de la información y comunicación.

III. El ente rector de Gobierno Electrónico determinará la política general y normativa específica de interoperabilidad e intercambio de información y datos entre las entidades del sector público.

El D.S. N° 2514 responde a los cambios modernos sobre la tecnología que se utiliza en el intercambio de información esta instancia AGETIC que coordinará con las entidades del sector público la implementación de servicios de interoperabilidad de Gobierno Electrónico, así como los datos e información que deben estar disponibles. Este procedimiento facilita el intercambio y rapidez en la comunicación y transferencia de información en el sector público. También debe ser un aspecto que constantemente debe ser actualizado y tomado muy en cuenta en sistemas de control modernos.

### 4.8.12. D.S. N° 3251 de 11 de julio de 2017. Plan de Implementación de Gobierno Electrónico y Plan de Implementación de Software Libre y Estándares Abiertos.

Artículo 4°.- (INTEROPERABILIDAD)

1. El COPLUTIC, en coordinación con la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación — AGETIC, podrá determinar la obligatoriedad por parte de las entidades públicas para compartir información mediante interoperabilidad, en el marco de las leyes y normas vigentes, así como disposiciones específicas de sectores estratégicos.

2. Las entidades públicas en el plazo de dos (2) meses de haber sido notificadas con la resolución del COPLUTIC, deberán habilitar a través de la AGETIC los accesos a la información objeto de la resolución.
3. Las entidades públicas que no cuentan con las condiciones técnicas para proporcionar la información objeto de la resolución, podrán solicitar ante la AGETIC la ampliación del plazo establecido en el Parágrafo precedente, previa justificación técnica de la entidad.
4. El Ente Rector del Gobierno Electrónico y Tecnologías de Información y Comunicación establecerá los mecanismos y condiciones de acceso a los datos disponibles en el marco del presente Artículo.
5. Las entidades del sector público, en el marco de sus funciones y atribuciones, sin perjuicio de la aplicación de lo establecido en el presente Artículo, podrán suscribir convenios de interoperabilidad, para garantizar el intercambio de información.[74]

Esta norma por lo descrito arriba, tiene cobertura al sector público en la transferencia de datos, mecanismos y condiciones de acceso, con un carácter obligatorio, lo que significa que toda la información generada es compartida en los procesos laborales u otros al interior de una entidad. Tienen por lo tanto que contar con mecanismos de control muy precisos que permitan resguardar la información proporcionada y que se evite la vulneración de derechos de los usuarios o personal perteneciente a una entidad estatal.

### 4.8.13. D.S. N° 3525 de 4 de abril de 2018

[74] COPLUTIC. (2017). Plan de Implementación de Gobierno Electrónico. https://repositorio.uasb.edu.bo:8080/bitstream/54000/1280/1/COPLUTIC-Gobierno%20electr%C3%B3n.

Artículo 4°.- (Definiciones) A efecto del presente Decreto Supremo se tienen las siguientes definiciones:

Archivo Digital:

Es el Archivo ordenado con soporte digital, que resguarda la totalidad de los datos, información, documentos y expedientes digitales recepcionados, generados y procesados por la entidad pública;

Acción de participación digital con el Estado: Es toda aquella interacción del administrado con el Estado, por medio de la cual se manifiestan quejas, propuestas y sugerencias;

Dato:

Cifra, letra, carácter, símbolo o palabra susceptible de ser generada, procesada o almacenada por medios informáticos;

Expediente Digital:

El expediente digital es el conjunto ordenado de datos, información y documentos digitales, vinculados sobre un determinado asunto, independientemente de la naturaleza de la información que contenga;

Registro de Orden Cronológico e Integridad de Documentos Digitales:

Es un registro de documentos y datos digitales que permite verificar posteriormente con grado de certeza la existencia y orden cronológico del registro de un documento o dato y la integridad del mismo.

Artículo 14°.- (Archivo digital)

Todo documento firmado digitalmente será plenamente válido en toda actuación administrativa, sea de ejecución o de control gubernamental o ante la vía judicial, conforme a lo establecido en el Artículo 78 de la Ley Nº 164, de 8 de agosto de 2011.

Los documentos firmados digitalmente deberán ser recepcionados y procesados obligatoriamente por todas las entidades del sector público y privado que presten servicios públicos delegados por el Estado.

La AGETIC, mediante Resolución Administrativa, definirá y actualizará los parámetros técnicos, estándares y formatos para la gestión documental digital.

Las entidades públicas y privadas que presten servicios públicos delegados por el Estado, mediante resolución expresa de la máxima autoridad, aprobarán un reglamento de gestión documental digital.

Artículo 16°.- (Registro de orden cronológico e integridad)

I. La AGETIC será responsable de implementar, gestionar y coordinar un registro descentralizado de orden cronológico e integridad de datos y documentos digitales.

II. Los datos consignados en el registro de orden cronológico e integridad de datos y documentos digitales, tendrán plena validez jurídica respecto a la integridad y temporalidad de los mismos, para asuntos judiciales y administrativos, incluyendo aquellos de ejecución y control gubernamental.

III. La AGETIC establecerá los lineamientos y condiciones técnicas para la implementación y uso del registro de orden cronológico e integridad de datos y documentos digitales.

IV. El uso del registro de orden cronológico e integridad de datos y documentos digitales, será potestativo para las entidades públicas y privadas que presten servicios públicos delegados por el Estado.[75]

En este D.S. principalmente se define los roles y responsabilidad de la AGETIC (Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación) tanto en el marco de las entidades públicas y privadas en gestionar y coordinar un registro descentralizado de orden cronológico e integridad de datos y documentos digitales. Dentro de este marco, podemos considerar que esta instancia es de crucial importancia al momento de registrar y transferir información digitalizada. En estos tiempos de avance tecnológico la normativa a este nivel deberá estar constantemente actualizada y adecuadas a los cambios que se dan tanto a nivel nacional como internacional.

#### 4.8.14. Sentencia Constitucional 0965/2004-R

Sucre — 23 de junio de 2004 establece la protección que brinda el Habeas Data, así como sus diversos tipos:

Siguiendo la doctrina del Dr. José Antonio Rivera Santivañez en su obra "Jurisdicción Constitucional", el hábeas data se define como el proceso constitucional de carácter tutelar que protege a la persona en el ejercicio de su derecho a la "autodeterminación informática".

Es una garantía constitucional que, sin desconocer el derecho a la información, al trabajo y al comercio de las entidades públicas o privadas que mantienen centrales de información o bancos de datos, reivindica el derecho que tiene toda persona a verificar qué

[75] Decreto Supremo Nº 3525. (2018). https://www.lexivox.org/norms/BO-DS-N3525.html.

información o datos fueron obtenidos y almacenados sobre ella, cuáles de ellos se difunden y con qué objeto, de manera que se corrijan o aclaren la información o datos inexactos, se impida su difusión y, en su caso, se eliminen si se tratan de datos o informaciones sensibles que lesionan su derecho a la vida privada o íntima en su núcleo esencial referido a la honra, buena imagen o el buen nombre.

Partiendo de los conceptos referidos, se puede inferir que el hábeas data es una garantía constitucional por lo mismo se constituye en una acción jurisdiccional de carácter tutelar que forma parte de los procesos constitucionales previstos en el sistema de control de la constitucionalidad. Es una vía procesal de carácter instrumental para la defensa de un derecho humano como es el derecho a la autodeterminación informática.

Como una acción tutelar, el hábeas data sólo se activa a través de la legitimación activa restringida, la que es reconocida a la persona afectada, que puede ser natural o jurídica. En consecuencia, no admite una activación por la vía de acción popular, es decir, no se reconoce la legitimación activa amplia.

- Acción Subsidiaria.

Tomando en cuenta sus fines y objetivos , así como la aplicación supletoria de las normas previstas por el art. 19 de la CPE, dispuesta por el art. 23 parágrafo V antes referido, se entiende que el hábeas data es una acción de carácter subsidiario, es decir, que solamente puede ser viable en el supuesto que el titular del derecho lesionado haya reclamado ante la entidad pública o privada encargada del banco de datos, la entrega de la información o datos personales obtenidos o almacenados, y en su caso, la actualización, rectificación o supresión de aquella información o datos falsos, incorrectos, o que inducen a discriminaciones,

y no obtiene una respuesta positiva o favorable a su requerimiento, o sea que la entidad pública o privada no asume inmediatamente la acción solicitada.[76]

Dentro de una nueva ley de protección de datos personales, el habeas data deberá estar incluido como un derecho fundamental al que pueden acudir las personas cuyos derechos sean vulnerados o acceder a información que requiera el usuario. El habeas data constituye por lo tanto un recurso fundamental en los procedimientos judiciales de protección de datos de carácter personal.

### 4.8.15. Sentencia Constitucional 1738/2010-R

Sucre, 25 de octubre de 2010.

Los derechos a la intimidad y privacidad como base de la protección de datos personales.

Del art. 130 de la CPE, se concibe que tanto las personas naturales y jurídicas tienen acceso a los derechos a la privacidad, intimidad, honra, honor, propia imagen y dignidad reconocido en el art. 21.1 de la CPE, entre uno de esos derechos esta la intimidad, que sin duda es uno de los bienes más susceptibles de ser lesionados o puesto en peligro por el uso de las nuevas tecnologías, por lo que se hace necesario colocar un límite a la utilización de la informática y las comunicaciones ante la posibilidad de que se pueda agredir a la intimidad de los ciudadanos y con ello se pueda coartar el ejercicio de sus derechos.

De todo lo anterior se tiene que tanto la intimidad como la privacidad son la base fundamental para la protección de todos los datos personales de las personas, que sólo le

[76] Durán, M. (2018), Normativa sobre protección de datos personales en Bolivia. https://medium.com/@mrduranch/normativa-sobre-datos-personales-en-bolivia-ece7a61f50b0

atingen a él o a ella, por lo que la vulneración de estos derechos afectan directamente a su imagen, honra y reputación.[77]

Esta norma pretende establecer un límite a la utilización de la informática y las comunicaciones por el riesgo de que se pueda agredir a la intimidad de los ciudadanos y coartar el ejercicio de sus derechos, se debe tomar en cuenta que tanto la intimidad como la privacidad son la base fundamental para la protección de los datos personales de los usuarios. En estos tiempos el riesgo es mayor por el devenir acelerado de la tecnología digital y la informática que hace tan complicado establecer un sistema de control y protección de la información de datos personales, lo que requiere un esfuerzo mayor de los legisladores para formular una ley específica que incluya todos estos detalles tecnológicos.

#### 4.8.16. Sentencia del Tribunal Constitucional sobre Recurso de Hábeas Data 1972/2011- 7 diciembre 2011-R Sucre

Establece que la cancelación de antecedentes en actividades de narcotráfico, debía ser a través de orden judicial.

Todos los antecedentes de una persona son parte de sus datos personales que podrían determinar una condición en la sociedad por lo que los procedimientos de cancelación u otros deberán ser tratados con mucho profesionalismo y basados en parámetros, normas, procedimientos y principios jurídicos precisos.

#### 4.8.17. Sentencia Constitucional Plurinacional 0090/2014-S1 Sucre, 24 de noviembre de 2014.

[77] Durán, M. (2018), Normativa sobre protección de datos personales en Bolivia. https://medium.com/@mrduranch/normativa-sobre-datos-personales-en-bolivia-ece7a61f50b0

La acción de protección de privacidad, constituye un medio procesal constitucional de protección de los datos personales, dirigido a la protección efectiva, inmediata y oportuna del derecho a la autodeterminación informática, en los supuestos en que éste sea transgredido por acciones u omisiones ilegales o indebidas. Por intermedio de ella, toda persona natural o jurídica, puede acudir a la jurisdicción constitucional, para demandar a los bancos de datos y archivos de entidades públicas o privadas, persiguiendo el conocimiento, actualización, rectificación o supresión de las informaciones o datos contenidos en éste, que se hubiesen obtenido, almacenado o distribuido en los mismos.

En la actualidad esta Sentencia Constitucional, a través de la protección de privacidad, con relación a la autodeterminación informática, favorece al usuario ya que puede demandar la vulneración que pueda sufrir por acciones u omisiones ilegales o indebidas. En la actualidad es un recurso de mucha utilidad porque constantemente se presentan hechos que dañan y vulneran la intimidad y la privacidad de muchas personas incluso autoridades públicas.

### 4.8.18. Sentencia Constitucional Plurinacional 0819/2015-S3

Sucre, 10 de agosto de 2015 Sobre la revictimización:

Lo anterior se evidencia del informe FGE/STRIA. GRAL./1/2015, emitido por el Ministerio Público y remitido ante este Tribunal, el cual señaló:

La Fiscalía General del Estado no cuenta con un área de informática dentro de un proceso penal que le permita identificar y neutralizar las imágenes de contenido denigrante o sexual que se encuentren circulando por internet; por lo que se puede evidenciar que al no contar con una unidad especializada, ni haber gestionado convenios nacionales e internacionales pertinentes, el Ministerio Público no puede garantizar de una manera real y

concreta los derechos de las víctimas ni de cualquier otra persona que vea derechos vulnerados en internet. [78]

Las obligaciones de proteger consisten en que el Estado y sus servidores públicos garanticen que terceros no vayan a interferir, obstaculizar o impedir el goce de esos derechos. Las obligaciones de asegurar suponen cerciorar que el titular del derecho acceda a éste cuando no puede hacerlo por sí mismo; y, las obligaciones de promover se caracterizan por el deber de desarrollar condiciones para que los titulares del derecho accedan al bien, es así que el Estado, servidores públicos y sociedad deben adoptar las medidas necesarias e idóneas para satisfacer el contenido de los derechos de manera que la igualdad y el ejercicio de los derechos no sea únicamente de manera formal, sino real y material.

Tomando en cuenta estas dificultades dentro de un proceso penal, para poder identificar y neutralizar imágenes denigrantes, se ve por necesario abordar este aspecto tan lacerante en la actualidad que daña la honorabilidad de una persona con normas o procedimientos mucho más avanzados y tecnificados que permitan proteger los derechos de las personas los cuales deberán considerarse en una nueva ley de protección de datos personales.

## 4.9. LEGISLACIÓN COMPARADA

## 4.10. PROTECCIÓN DE DATOS EN EUROPA

### 4.10.1. El Consejo de Europa

### 4.10.2. Las Resoluciones (73) 22 y (74) 29 del Comité de Ministros

[78] Durán, M. (2018), Normativa sobre protección de datos personales en Bolivia. https://medium.com/@mrduranch/normativa-sobre-datos-personales-en-bolivia-ece7a61f50b0

Formalmente, podemos considerar a las Resoluciones (73) 22 y (74) 29 del Comité de Ministros del Consejo de Europa como el punto de partida del estudio de una situación que fue altamente demorada por los legisladores; no obstante, es conveniente señalar que los principios y derechos que se recogían en aquellos escritos siguen teniendo vigencia y plena actualidad hoy en día, aunque, como es lógico, adecuados y adaptados a la evolución social y tecnológica.

A modo de ejemplo, el Comité de Ministros del Consejo de Europa recomendó a los Gobiernos de sus estados miembros, respecto de la creación de bancos de datos, tanto en el sector público como en el privado, tener en cuenta determinados aspectos, cuya finalidad era tomar precauciones contra todo abuso o mal empleo de la información; pueden ser resumidos de la siguiente forma:

1. La información debe ser exacta, mantenida al día, apropiada para el fin para el que fue almacenada y obtenida por medios legales.

2. Todo ciudadano tiene derecho a conocer la información almacenada sobre sí mismo.

Las personas que deban operar sobre las bases de datos tienen que estar bajo normas severas de conducta para el mantenimiento del secreto y para prevenir el mal uso de los datos.

4. La seguridad debe ser extremada al máximo para impedir el acceso a las bases de datos a personas no autorizadas o para evitar el desvío de la información, mal intencionadamente o no, hacia sitios no previstos.

5. Si la información va a ser utilizada con fines estadísticos, se revelará de tal forma que sea totalmente imposible relacionarla con ninguna persona en particular.

Casi coincidiendo en el tiempo, veía luz en los Estados Unidos, la llamada Ley de Privacidad que, en su Exposición de Motivos, decía que:

El Congreso estima que la privacidad de un individuo es afectada directamente por la captación, conservación, uso y difusión de información personal por entes y órganos federales. El creciente uso de ordenadores y de una tecnología compleja de la información, ha aumentado grandemente el detrimento que para la privacidad individual puede derivarse de cualquier captación, conservación, uso y difusión de información personal.[79]

### 4.10.3. El Convenio 108 del Consejo de Europa

La preocupación europea por un derecho que se ocupe del uso de las telecomunicaciones estuvo presente desde fines de la década de 1960. En la década del 70 se comenzó a debatir sobre la necesidad de una legislación que unificara pretensiones y especialmente que ofreciera un conjunto de medios de protección a derechos y libertades fundamentales. La legislación genérica de la Unión Europea es una legislación de mínimo; sin embargo, en materia de protección de datos, permitió que los Estados miembros fueran elevando progresivamente su nivel de protección.

Esta preocupación de las organizaciones supranacionales europeas en la protección de los derechos de la personalidad y en función de las lesiones que los efectos de la tecnología pueden producir en la sociedad, se formalizó en el Convenio Nº 108 del Consejo de Europa sobre la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, aprobado en 1981 y ratificado por España en 1984. El Consejo de

[79] Saltor, C.E. (2013). La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación Argentina. (Memoria Doctoral). Universidad Complutense de Madrid. Madrid España. Recuperado de https://eprints.ucm.es/22832/1/T34731.pdf

Europa es considerado el promotor de la tendencia legislativa en materia de protección de datos, superadora de los criterios que existían hasta ese momento, los cuales fueron luego receptados por muchas leyes y por algunas constituciones europeas.

El Convenio 108 fue pionero en materia de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales. Ciertamente, su contenido no es derecho directamente aplicable, ya que está compuesto por pautas a las que deben acomodarse las legislaciones internas de países que lo han ratificado. Uno de los documentos más importantes en materia de protección de datos personales que ha surgido en Europa fue el Convenio (108) del Consejo de Europa para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal, firmado en 1981 en Estrasburgo.

Los principios básicos establecidos por este convenio son los siguientes:

a) Calidad de los datos.

b) Obtención y tratamiento leal y legal de los datos.

c) Los datos se registrarán para finalidades determinadas y legítimas.

d) Los datos serán adecuados, pertinentes y no excesivos en relación con las finalidades que se recabaron y registraron.

e) Los datos serán exactos y puestos al día.

### 4.11. ANTECEDENTES EN EL DERECHO EUROPEO

En el derecho europeo podemos encontrar que ya a mediados de la década de 1960 se procura alcanzar una legislación de protección a los derechos y libertades fundamentales ante el desarrollo de las telecomunicaciones.

Así, podemos tomar como un primer antecedente en materia de protección de datos personales a la Conferencia de Juristas Nórdicos, celebrada en Estocolmo en mayo de 1967. Esta reunión científica tomó como referencia inmediata anteriores textos internacionales, tales como la Declaración Universal de los Derechos del Hombre, el Pacto Internacional sobre Derechos Civiles y Políticos, así como la Convención Europea sobre los Derechos del Hombre y viene a representar un precedente importante, al reconocer que el derecho a la vida privada es el derecho de una persona a ser dejada en paz, para vivir su propia vida con el mínimo de injerencias exteriores.

En otras partes del mundo se realizaron también reuniones científicas de gran importancia en el tema, tales como la Conferencia Internacional de los Derechos del Hombre celebrada en 1968 en Teherán, la cual, a pesar de no desarrollarse en Europa, influye en el derecho europeo, dado que recomienda a la ONU que proceda al estudio de las cuestiones planteadas con relación a los derechos del hombre que resulten afectados por el desarrollo de la técnica y la ciencia. En consecuencia, el 19 de diciembre de 1968 la ONU adopta la Resolución 2450, en la que se establece la necesidad de fijar límites a las aplicaciones de la electrónica por su injerencia en los derechos de la persona.

Se inicia así un período de intensos trabajos sobre la problemática que plantea el alcance de los progresos científicos y tecnológicos en los derechos de la persona, que concluye en 1983, con la aprobación por la Comisión de Derechos Humanos de un informe relativo al estudio de los principios rectores pertinentes, respecto de la utilización de los archivos informatizados de datos de carácter personal.

Siguiendo este proceso evolutivo, el 23 de enero de 1970 la Resolución 428 de la Asamblea Consultiva del Consejo de Europa se refiere a la intimidad como objeto de obligada protección, frente a la intromisión de la tecnología informática.

Es importante el antecedente mencionado, ya que en 1970 también se aprueba en Costa Rica la Convención Americana sobre Derechos Humanos, en la que nada se declara con respecto a los peligros que acosan a la humanidad, procedentes de la abusiva utilización de las modernas tecnologías de la información.

A partir de 1976 se inicia el auge del tratamiento supranacional de la protección dela intimidad frente a la informática. Efectivamente, a partir de 1977, la OCDE auspicia un "Encuentro sobre las corrientes internacionales de datos y la protección a la intimidad de las libertades individuales".

Durante 1967, debido a la preocupación por la evolución de las nuevas tecnologías de la información y sus efectos sobre la intimidad de las personas, se constituyó en el seno del Consejo de Europa una Comisión Consultiva para estudiar las tecnologías de la información y su potencial agresividad a los derechos de la persona, cuyo trabajo dio como resultado la Resolución 509 (en el año 1968) de la Asamblea del Consejo de Europa, sobre "los derechos humanos y los nuevos logros científicos y técnicos".

Luego, en 1970, el 23 de enero, la Resolución 428 de la Asamblea Consultiva del Concejo de Europa se refiere al Derecho a la Intimidad, como un objeto de obligada protección, frente a la intromisión de la tecnología informática.

En esta línea y asesorados por la Comisión Jurídica de la Asamblea Consultiva, en septiembre de 1973, los parlamentarios recomiendan al Comité de Ministros del Consejo de

Europa, que tengan en consideración la iniciativa de adoptar normas protectoras del derecho a la intimidad frente a los avances tecnológicos. Esta norma recomendó a los Gobiernos de sus Estados miembros, respecto de la creación de bancos de datos en el sector privado, considerar determinados aspectos tendientes a tomar precauciones contra todo abuso o mal empleo de la información. Un año más tarde, en septiembre de 1974, se realiza una recomendación similar respecto a la creación de bancos de datos en el sector público. [80]

### 4.11.1. Acuerdo de Schengen de 14 de junio de 1985

El Acuerdo de Schengen, firmado en Luxemburgo, constituye uno de los pasos más importantes en la historia de la construcción de la Unión Europea (UE) y también, aunque en forma indirecta, en la evolución del derecho a la protección de los datos de carácter personal. El acuerdo, firmado un 14 de junio de 1985 y en vigor desde 1995, tiene como objetivo finalizar con los controles fronterizos dentro del espacio de Schengen y armonizar los controles fronterizos externos. Al Acuerdo de Schengen se han adherido la mayoría de los Estados miembros de la Unión y algunos terceros países.

En el Título IV del Acuerdo Schengen encontramos disposiciones que organizan la coordinación del control entre los Estados firmantes; entre ellas, el Sistema de Información Schengen (SIS), sistema de información común que permite a las autoridades competentes de los Estados miembros disponer de información relativa a algunas categorías de personas y objetos. Esta información es compartida entre los estados participantes, que son mayoritariamente signatarios del Acuerdo de Schengen (AS), como Alemania, Francia, Bélgica, Países Bajos y Luxemburgo. Después de su creación, varios países se han unido al sistema;

[80] Saltor, C.E. (2013). La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación Argentina. (Memoria Doctoral). Universidad Complutense de Madrid. Madrid España. Recuperado de https://eprints.ucm.es/22832/1/T34731.pdf

Grecia, Austria, Islandia, Suecia, Suiza, Finlandia, Dinamarca, Italia, Portugal, España y Noruega, que firmaron el AS.

### 4.11.2. Directiva 95/46/CE

El 24 de octubre de 1995, luego de los antecedentes antes mencionados, se aprueba la Directiva europea 95/46/CE, relativa a la protección de las personas físicas en lo referido al tratamiento de los datos personales y a su libre circulación.

La Directiva es una disposición normativa de Derecho comunitario que vincula a los Estados de la Unión o, en su caso, al Estado destinatario en la consecución de resultados u objetivos concretos en un plazo determinado, dejando, sin embargo, a las autoridades internas competentes la debida elección de la forma y los medios adecuados a tal fin.

### 4.11.3. Directiva 58/2002/CE del Parlamento Europeo y del Consejo

La Directiva 2002/58/CE212 del 12 de julio de 2002, forma parte del grupo o paquete normativo de telecomunicaciones, conjunto de disposiciones legislativas destinado a regular el sector de las comunicaciones electrónicas y a modificar a la normativa existente en el sector de las telecomunicaciones. El mencionado paquete normativo de telecomunicaciones comprende cuatro directivas relativas al marco general, al acceso y a la interconexión, a la autorización y a las licencias, y al servicio universal.

En diciembre de 2009, este paquete normativo de telecomunicaciones fue modificado por medio de las Directivas conocidas como “Legislar mejor” y “Derechos de los ciudadanos”; también fue alterado con la instauración de un Organismo de Reguladores Europeos de Comunicaciones Electrónicas (ORECE).

### 4.11.4. Directiva 97/66/ CE

La Directiva 97/66/CE217 de 15 de diciembre de 1997 define su objeto en el art. 1º, dirigido a armonizar las disposiciones relativas a la protección de datos de los distintos Estados, con el objeto de garantizar un nivel equivalente de protección de las libertades y de los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que hace referencia al tratamiento de los datos personales en el sector de las telecomunicaciones.

El propósito de la Directiva radica en establecer las obligaciones y derechos, tanto de abonados como de proveedores, en el ámbito de las telecomunicaciones y de la protección de los datos personales.

### 4.11.5. Nuevas normas europeas

Internet ha cumplido veinte años desde su apertura al uso masivo y sus efectos, junto a otros fenómenos del mundo de las comunicaciones han potenciado la revolucionaria y vertiginosa evolución del uso de la tecnología.

El uso masivo de la web, de los buscadores y de las redes sociales son tan sólo algunos signos de una realidad de movimiento y cambio tecnológico a la que el Estado moderno y el derecho no deben desatender para dar adecuación permanente de su legislación. Europa, consciente de esta realidad, fue adecuando su legislación de protección de datos personales.

Algunas de las nuevas normas europeas que fueron adecuando el derecho a la protección de los datos de carácter personal al progreso del sector de las comunicaciones, son las siguientes:

**a) Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009,**

Por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) Nº 2006/2004 sobre la cooperación en materia de protección de los consumidores.

**b) Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006,**

Sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

**c) Directiva 2008/68/CE del Parlamento Europeo y del Consejo Europeo de 24 de septiembre de 2008,**

Por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores.[81]

[81] Saltor, C.E. (2013). La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación Argentina. (Memoria Doctoral). Universidad Complutense de Madrid. Madrid España. Recuperado de https://eprints.ucm.es/22832/1/T34731.pdf

### 4.11.6. Proyecto de la Comisión Europea del año 2012

La norma básica vigente de la UE en materia de protección de datos es la ya comentada Directiva 95/46/CE, adoptada en el año 1995 con un doble objetivo: defender el derecho fundamental a la protección de datos y garantizar la libre circulación de estos datos entre los Estados miembros.

### 4.11.7. Control ciudadano

Para reforzar los derechos de los ciudadanos a la protección de sus datos, la Comisión propone nuevas normas que:

a) Aumenten el control de los ciudadanos sobre sus datos.

b) Mejoren los medios que permiten a los ciudadanos ejercer sus derechos.

c) Refuercen la seguridad de los datos.

d) Acrecienten la responsabilidad de quienes tratan datos, concretamente.

### 4.11.8. Protección de datos en el mercado digital

Con el fin de potenciar la dimensión de mercado único de la protección de datos, la Comisión propone:

- Fijar las normas de protección de datos al nivel de la UE mediante un Reglamento directamente aplicable en todos los Estados miembros, lo que pondrá fin a la aplicación acumulativa y simultánea de distintas leyes nacionales de protección de datos;
- Simplificar el entorno regulador mediante una drástica reducción de los trámites burocráticos y la eliminación de determinadas formalidades.
- Ampliar la independencia y las facultades de las autoridades nacionales de protección de datos, habilitándolas para llevar a cabo investigaciones, adoptar decisiones

vinculantes e imponer sanciones efectivas y disuasorias, y obligar a los Estados miembros a que les faciliten los recursos suficientes para el desempeño de esas tareas.

- Crear un sistema de ventanilla única para la protección de datos en la UE: los responsables del tratamiento de datos de la UE tendrán como único interlocutor a una autoridad nacional de protección de datos, a saber, la del Estado miembro donde esté radicado el establecimiento principal.
- Crear las condiciones necesarias para una cooperación presta y eficaz entre autoridades nacionales de protección de datos, lo que incluirá la obligación para cualquiera de ellas de llevar a cabo investigaciones e inspecciones a petición de cualquier otra y el reconocimiento mutuo de sus decisiones.
- Crear un mecanismo de coherencia al nivel de la UE para asegurar que las decisiones de las autoridades nacionales de protección de datos que tengan mayor repercusión europea tengan plenamente en cuenta los puntos de vista de las demás autoridades de protección de datos interesadas y se ajusten plenamente al Derecho de la UE.
- Elevar el rango del Grupo de trabajo del artículo 29, convirtiéndolo en un Consejo Europeo de Protección de Datos a fin de mejorar su contribución a la aplicación coherente de la legislación en materia de protección de datos y de sentar unas sólidas bases de cooperación entre las autoridades de protección de datos, incluido el Supervisor Europeo de Protección de Datos, y potenciar las sinergias y la eficacia disponiendo que este último asuma las tareas de la Secretaría del Consejo Europeo de Protección de Datos.

#### 4.11.9. Globalización y protección de los datos

La globalización presenta desafíos que requieren de herramientas y mecanismos flexibles, especialmente para las empresas activas en todo el mundo. Pero también se hacen necesarias nuevas normas que garanticen al mismo tiempo la protección jurídica de los datos personales acorde a los nuevos tiempos. La Comisión propone las siguientes acciones:

- Adopción de normas claras que determinen en qué supuestos se aplica el Derecho de la UE a los responsables del tratamiento de datos establecidos en terceros países y que, en particular, especifiquen que siempre que se ofrezcan bienes y servicios a ciudadanos de la UE, o cuando se proceda a algún control de su comportamiento, serán de aplicación las normas europeas.
- Toda decisión de adecuación que la Comisión adopte se basará en criterios explícitos y claros.
- La circulación legítima de datos a terceros países se facilitará reforzando y simplificando las normas sobre transferencias internacionales de datos a los países no cubiertos por ninguna decisión de adecuación, y sobre todo racionalizando ciertas herramientas (como por ejemplo las normas corporativas vinculantes) y generalizando su uso, de forma que puedan aplicarse a los responsables del tratamiento de datos y dentro de los grupos de sociedades, lo que reflejará mejor el número de empresas que llevan a cabo actividades de tratamiento de datos, especialmente mediante computación en nube.
- Apertura de un diálogo y, cuando así proceda, negociaciones con terceros países (especialmente los socios estratégicos de la UE y los países de la Política Europea de Vecindad) y con las organizaciones internacionales

pertinentes (como el Consejo de Europa, la Organización para la Cooperación y el Desarrollo Económico, las Naciones Unidas) a fin de promover la adopción de unas normas de protección de datos exigentes e interoperables en todo el mundo.

## 4.12. LA PROTECCIÓN DE DATOS EN LA CONSTITUCIÓN EUROPEA

La Unión Europea también trató la protección de los datos personales en su Constitución aprobada por unanimidad por el Tratado de Roma, el 29 de octubre de 2004, por los jefes de Estado o de Gobierno de los Estados miembros de la Unión Europea. El Tratado de Roma establece una Constitución para Europa, por eso es más conocido como Constitución Europea o Tratado Constitucional, cuyo proyecto había sido aprobado el 18 de junio de 2003.

El 12 de enero de 2005, el Parlamento Europeo aprobó una resolución por 500 votos a favor, 137 en contra y 40 abstenciones, en la que recomendó a los Estados miembros que ratificaran la Constitución.

Entró en vigencia el primero de noviembre de 2006.

El Tratado confirma los avances logrados para garantizar la protección del derecho fundamental a la protección de datos personales.

El Artículo II-68 Protección de datos de carácter personal de la Constitución de Europa, expresa lo siguiente:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

## 4.13. LEY DE PROTECCIÓN DE DATOS EN ESPAÑA

El derecho a la protección de los datos personales surgió en España con la Constitución de 1978, ya que los constituyentes españoles de 1978 pensaron que el desarrollo de las nuevas tecnologías de la información y las telecomunicaciones era una amenaza para los derechos fundamentales de los ciudadanos. Para evitar el peligro que les representaba el desarrollo tecnológico de las TIC, incorporaron en la Constitución española, en el artículo 18.4, una garantía de protección a las personas frente a la informática. Esta norma, presente en la Constitución, tiene por objeto limitar el uso de la informática para garantizar el honor, la intimidad familiar y personal de los ciudadanos junto al pleno ejercicio de sus derechos.

Los constituyentes españoles tuvieron a la vista el artículo 35 de la Constitución Portuguesa de 1976 junto a las diferentes leyes ya existentes en algunos Estados europeos, de protección de datos y defensa de la intimidad frente a la informática, por ejemplo las danesas y alemanas, que incidieron en la actitud de los parlamentarios españoles desde los primeros debates sobre la nueva Constitución.

Cinco años más tarde, con el fin de garantizar los derechos y las libertades de las personas físicas, y en particular su intimidad frente a la utilización de la informática, se dio desarrollo legislativo al mencionado artículo 18.4 de la Constitución, por medio de la Ley

Orgánica 5/1992 sobre regulación del tratamiento automatizado de datos de carácter personal, promulgada en 1992.

Como consecuencia de los mandatos de la Directiva 95/46/CE, la LORTAD fue derogada y reemplazada en 1999 por la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) Nº 15/1999 vigente en la actualidad, que tuvo como principal objeto adecuar la legislación española a la mencionada Directiva.

Sin embargo, y aun a pesar de la exigente crítica de los doctrinarios españoles, no sería justo dejar de reconocer que tanto la LORTAD como la LOPD, son leyes que modelaron la legislación del mundo de habla hispana, y en especial la legislación en Sudamérica, en la materia.

La última sancionada es la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los Derechos Digitales.

### 4.14. LEY DE PROTECCIÓN DE DATOS EN ALEMANIA

Alemania cuenta con el antecedente de haber legislado la primera ley europea de las llamadas leyes de primera generación de protección de datos en el Estado de Hesse. Promulgada el 7 de octubre de 1970, esta norma provincial fue precursora en su tiempo y solitaria en su territorio.

En esta ley del Land de Hesse, se encuentra la primera referencia a un Comisario de Protección de Datos que sólo podrá ser cesado en su cargo, en caso de probarse ciertos supuestos de hecho que justificarán la separación del servicio, garantizando de esta forma su independencia, ya que la ley expresaba textualmente: “no estará sujeto a órdenes o

instrucciones de órgano alguno". En la actualidad existen leyes similares en múltiples Länder de la antigua RFA, normas que, siguiendo el antecedente de la antigua ley de Hesse, hacen gala de independencia y federalismo.

El Estado Federal Alemán tuvo que esperar casi siete años hasta que se promulgó, el 27 de enero de 1977, la Ley Federal para la protección contra el uso ilícito de Datos Personales.

En la actualidad, la ley de protección de datos en Alemania es la conocida BDSG de 20 de diciembre de 1990 que entrando en vigor el 1 de junio de 1991 sustituye a la de enero de 1977 y su objeto es "Proteger al individuo para que la utilización de los datos personales no comporte un atentado a su derecho a la personalidad".[82]

### 4.15. LEY DE PROTECCIÓN DE DATOS PERSONALES EN AUSTRIA

La República de Austria, miembro de la Unión Europea desde 1995, ratificó el Convenio del Consejo de Europa el 30 de marzo de 1988, el cual entró en vigor el 1 de julio del mismo año.

Austria ya había dictado su Ley de Protección de Datos Personales, conocida en alemán con el nombre de Datenschutzgesetz (DSG, 1978), el 18 de octubre de 1978. Más tarde, esta ley fue adaptada a través de modificaciones como la realizada por la decisión 609/1989 de la Corte Constitucional y últimamente a través de la Ley Federal de Protección de Datos de Carácter Personal (Bundesgesetzüber den Schutz personen bezogener Daten / Datenschutzgesetz 2000 - DSG 2000) dictada en el año 2000, se adaptó la legislación

[82] Saltor, C.E. (2013). La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación Argentina. (Memoria Doctoral). Universidad Complutense de Madrid. Madrid España. Recuperado de https://eprints.ucm.es/22832/1/T34731.pdf

austríaca en materia de protección de datos a la Directiva 95/46/CE de Parlamento y del Consejo de Europa.

Con respecto al derecho fundamental a la protección de los datos personales, el artículo 1º de la ley austríaca del año 2000, textualmente expresa: "(Disposición Constitucional). Derecho Fundamental a la Protección de Datos:

1. Todas las personas tienen el derecho al secreto de los datos personales que le conciernen, sobre todo en lo que respecta a su vida privada y familiar, en la medida en que exista un interés que merezca protección. Tal interés queda excluido cuando los datos no pueden estar sujetos al derecho al secreto debido a su disponibilidad general o porque no se puede regresar nuevamente a la protección de datos (afectado).
2. Los datos personales se deben utilizar a favor del interés vital del interesado o con su consentimiento, las restricciones al derecho al secreto sólo se permiten para salvaguardar los legítimos intereses primordiales de otro, es decir, en caso de una intervención de una autoridad pública, la restricción sólo se permitirá sobre la base de las leyes necesarias por las razones indicadas en el art. 8, párrafo 2 del Convenio Europeo de Derechos Humanos.

### 4.16. LEY DE PROTECCIÓN DE DATOS PERSONALES EN BÉLGICA

El Reino de Bélgica comenzó promulgando disposiciones específicas sobre protección de datos para ofrecer garantías a las personas que figuraban en determinados ficheros. De esta forma estableció una conciencia sobre protección de datos personales que formó la base para la posterior aceptación del ciudadano, de una legislación sobre principios y derechos a la autodeterminación informativa.

En materia de acuerdos internacionales, Bélgica suscribió el ya estudiado Convenio 108 del Consejo de Europa, ratificado el 28 de mayo de 1993, que entró en vigor el 21 de septiembre del mismo año.

La normativa sobre la protección de datos personales en Bélgica es la Ley del 8 de diciembre de 1992, modificada por la ley de Transposición (de fecha 11 de diciembre de 1998) de la Directiva 95/46/CE, que entró en vigor el 1 de septiembre de 2001.

La ley no distingue entre ficheros de titularidad pública y ficheros de titularidad privada, extendiendo su alcance a todos los archivos de datos de carácter personal relativos a personas físicas. Quedan fuera de su ámbito de aplicación los ficheros referentes a datos de personas jurídicas, los que mantienen las personas físicas para uso familiar, los que contienen datos públicos y los del órgano estatal destinado a la estadística oficial.

Los principios y derechos generalmente establecidos en estas normativas son recogidos en la legislación belga mediante los llamados derechos de acceso, rectificación y supresión.

La Autoridad de control en Bélgica es la Comisión para la Protección de la Vida Privada, la cual juega un papel muy importante con relación a los archivos de incumplimiento de obligaciones dinerarias. Los consumidores pueden dirigirse a la Comisión, una vez que reciben la notificación de su inclusión en uno de estos archivos, para que ésta investigue la legalidad de dicha inclusión y, en su caso, emita una recomendación dirigida al responsable del archivo.

### 4.17. LEY DE PROTECCIÓN DE DATOS DE DINAMARCA

El Reino de Dinamarca ratificó el Convenio del Consejo de Europa el 23 de octubre de 1989, entrando en vigor el 1 de febrero de 1990 y consecuentemente legisló sobre protección de datos personales, siendo su actual ley Nº 429246 del 31 de mayo de 2000, que entró en vigor el 1 de julio de ese año y recibió diferentes modificaciones.

En el capítulo I, en su artículo 1º, la ley 429 del año 2000 establece el ámbito de aplicación, expresando que abarcará el tratamiento de datos personales, total o parcialmente automatizado, y el tratamiento no automatizado de datos personales que forman parte de un sistema de base de datos.

El capítulo II se ocupa en el apartado 3 de las definiciones, entre las que destaca el concepto de dato personal como aquel dato relativo a una persona natural identificada o identificable.

En el año 2000 entró en vigor la nueva ley danesa de protección de datos, con el objetivo dar cumplimiento a la Directiva 95/46/CE sobre la protección de las personas con respecto al tratamiento de datos personales ya la libre circulación de estos datos.

La autoridad de control danesa es la Agencia de Protección de Datos Personales, llamada Data Surveillance Authority, su nombre puede traducirse como Autoridad de Vigilancia de los Datos, también conocida bajo el nombre genérico de inspección de registros, está compuesta por un presidente y seis miembros, nombrados por cuatro años por

el Ministro de Justicia y tiene como funciones velar por el cumplimiento y la correcta interpretación de las dos leyes. [83]

### 4.18. LEY DE PROTECCIÓN DE DATOS PERSONALES EN FRANCIA

En la República de Francia, la protección de los datos de carácter personal se encuentra reglada por la ley n° 78-17253 del 6 de enero de 1978 relativa a la informática, a los ficheros y a las libertades. Esta ley se aplicaba tanto a los archivos de titularidad pública como a los de titularidad privada, estableciendo para los de titularidad pública que sean creados mediante una ley o un acto reglamentario realizado tras informe motivado de la Comisión Nacional de la Informática y las Libertades.

La norma mencionada sufrió modificaciones en el año 2004 por imperativo de la Directiva europea 95/46/CE, del Parlamento y del Consejo Europeo, que ordenó a todos los Estados Miembros, incluso a Francia, modificar su legislación en materia de Protección de Datos personales.

La ley vigente, con las modificaciones de año 2004, cuenta con 72 artículos. La ley dedica su capítulo primero a enumerar unos principios y definiciones entre los que destaca la declaración de que “la informática deberá estar al servicio del ciudadano. Su desarrollo debe llevarse a cabo en el marco de la cooperación internacional. No debe perjudicar ni la identidad humana, ni los derechos humanos, ni la intimidad de las personas, ni las libertades individuales o públicas” (art. 1).

[83] Saltor, C.E. (2013). La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación Argentina. (Memoria Doctoral). Universidad Complutense de Madrid. Madrid España. Recuperado de https://eprints.ucm.es/22832/1/T34731.pdf

Esta posición es ratificada en el art. 2º in fine cuando expresa: “La persona afectada por el tratamiento de datos de carácter personal será aquélla a la se refieran los datos objeto de tratamiento”.

### 4.19. LEY DE PROTECCIÓN DE DATOS PERSONALES EN GRECIA

La Constitución de la República Helénica reconoce el derecho de toda persona a la privacidad y a la confidencialidad de las comunicaciones. La Carta Magna griega expresa textualmente en el artículo 9°: "la casa de cada persona es inviolable; es un santuario de la vida privada y familiar de la persona en el que ninguna búsqueda se efectuará, a excepción de aquellas que estén amparadas por la ley en la forma, el tiempo y en presencia de representantes del poder judicial. Los infractores de la disposición anterior serán sancionados por violar el asilo de la casa y por abuso de poder, siendo responsables de los daños y perjuicios causados a la víctima, según lo especificado por la ley".

La Constitución Helénica fue reformada en el año 2001, oportunidad en la que se incorporó al artículo antes mencionado, el derecho de la persona a la protección de su información personal. Así, el reformado artículo 9 actualmente expresa: "Todas las personas tienen derecho a ser protegidas de la recolección, procesamiento y uso, especialmente por medios electrónicos, de sus datos personales, según lo especificado por la ley"; también dispone en una segunda parte que "la protección de datos está garantizada por una autoridad independiente, que se establece y opera según lo especificado por la ley".

La modificación de 2001, además de agregar dos nuevas disposiciones a este artículo, establece una autoridad independiente que vigila los asuntos relacionados con las telecomunicaciones.[84]

## 4.20. LEY DE PROTECCIÓN DE DATOS PERSONALES EN HOLANDA

Luego de ratificar el Convenio del Consejo de Europa el 24 de agosto de 1993, que entró en vigor el 1 de diciembre del mismo año, Holanda modificó su legislación sobre la protección de datos personales el 23 de noviembre de 1999, en su sesión Nº 92 del período parlamentario 1999 - 2000 mediante la ley 25.892 de Protección de Datos Personales (Wetbescherming Persoonsgegevens) con el objetivo de adecuar su legislación a la Directiva Europea 95/46/CE.

La ley holandesa de protección de datos personales se aplica tanto a los archivos del sector público como a los del sector privado y a los automatizados como a los manuales, cuando estos últimos poseen una estructura lógica que permita una consulta metódica de sus datos. Como ya dijimos, esta norma vino a modificar la anterior ley holandesa de protección de datos personales de 1988, conocida como WPR (Wetpersoneneregistraties).

Se exige para la creación y mantenimiento de un archivo de titularidad pública un reglamento sobre el funcionamiento del tratamiento que se va a realizar y una declaración ante la autoridad de control denominada College Bescherming Persoonsgegevens (CBP), a fin de que pueda ser consultado por cualquier interesado. Diferente es el trámite para los archivos del

[84] Saltor, C.E. (2013). La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación Argentina. (Memoria Doctoral). Universidad Complutense de Madrid. Madrid España. Recuperado de https://eprints.ucm.es/22832/1/T34731.pdf

sector privado, ya que la declaración de los tratamientos se efectúa en un formulario, indicando las principales características.

### 4.21. LEY DE PROTECCIÓN DE DATOS PERSONALES EN IRLANDA

La República de Irlanda firmó el Convenio del Consejo de Europa, luego ratificado el 25 de abril de 1990, que entró en vigor el 1 de agosto del mismo año. La legislación nacional de Irlanda dictó la ley de protección de datos personales el 13 de julio de 1988, que entró en vigor el 19 de abril de 1989 y que fijó como objetivo la aplicación del acuerdo del Consejo de Europa e incluso el texto del convenio fue incorporado al texto de la ley como anexo. En el año 2003 Irlanda modificó la ley de 1988 para adaptar su legislación a la Directiva 95/46/CE. También se incorporó a la legislación irlandesa el Reglamento de la Privacidad Electrónica en el año 2011 (SI 336 de 2011) para regular la protección de datos de teléfono, e-mail, SMS y el uso de Internet. Este reglamento busca adaptar la legislación de Protección de Datos irlandesa a la Directiva de la UE 2002/58/CE (modificada por la Directiva 2006/24/CE y 2009/136/CE).

Se observa que la ley irlandesa ha seguido un sistema de inscripción y registro de archivos de tipo “selectivo”, dado que la inscripción sólo es obligatoria para los archivos del sector público y aquellos del sector privado pertenecientes a instituciones financieras, compañías de seguros, empresas de venta por correo y empresas que prestan información en materia de crédito. También deben registrarse aquellos bancos de datos específicamente indicados por procesar datos de carácter sensible sobre origen racial, opiniones políticas o religiosas u otras creencias, salud física o mental, vida sexual o condenas criminales.

## 4.22. LEY DE PROTECCIÓN DE DATOS PERSONALES EN ITALIA

Luego de ratificar el Convenio del Consejo de Europa firmado el 2 de Febrero de 1983, la República de Italia aprobó su ley de protección de datos personales con el Nº 675/96 de 31 de diciembre de 1996 (publicada en el Boletín Oficial de 8 de enero de 1997) luego modificada en mayo y julio de 1997 por las leyes 123/97 y 255/97, respectivamente.

Al igual que la legislación griega, esta ley italiana fue una de las últimas leyes europeas de protección de datos en dictarse. Entró en vigor el 8 de mayo de 1997 y su más reciente modificación fue realizada por la ley 467 del 28 de diciembre del año 2001. Esta ley contiene en su articulado a todos los principios y derechos en materia de protección de datos. Siguiendo la técnica legislativa europea, comienza con un capítulo primero de Principios Generales, donde plasma conceptos y definiciones a los efectos de su interpretación. En el artículo 1º, apartado 2º, inc. c) define al Dato Personal, expresando que es "cualquier información relativa a las personas naturales o jurídicas, entes o asociaciones que sean identificadas o identificables en forma directa o indirectamente por referencia a cualquier otra información, incluyendo los números de identificación personal". Podemos destacar en la ley italiana, que, en sintonía con la doctrina de su tiempo, extendió su protección no solo a las personas físicas, sino también a las personas jurídicas.

El artículo 30 de la ley italiana de protección de datos crea la institución del Garante per la Protezione dei Dati Personali y establece sus competencias. Es un órgano colegiado, autónomo, independiente, que se compone de cuatro miembros, elegidos por la Cámara de diputados y senadores de la República. El Garante dispone de un presidente que es elegido dentro del ámbito del cuerpo colegiado, y cuyo voto prevalece en caso de empate. El

presidente dura cuatro años, y no puede ser reelegido. Los miembros de esta institución deben ser personas de reconocida independencia y experiencia en el campo del derecho, de la informática y de las nuevas tecnologías de la información.

### 4.23. LEY DE PROTECCIÓN DE DATOS PERSONALES EN PORTUGAL

A partir del artículo 35288 de su Constitución Nacional de 1976, Portugal legisló sobre la protección de los datos personales el 9 de abril de 1991 mediante la ley 10/91 de "protección de datos personales frente a la informática". Esta norma omitió establecer en forma expresa las condiciones de licitud para el procesamiento de datos personales; tampoco exigió el consentimiento del afectado para poder tratar sus datos personales. Posteriormente, el 2 de septiembre de 1993 Portugal ratificó el Convenio del Consejo de Europa, que entró en vigor el 1 de enero de 1994 y a partir del cual se aprobó la ley 28/94 del 29 de agosto de 1994 que vino a incorporar medidas de refuerzo a la protección de datos personales en ya mencionada la ley 10/91.

Posteriormente, Portugal, obligado por las directivas europeas 95/46/CE y 97/66/CE, derogó sus leyes de protección de datos personales 10/91 y 28/94 para poner en vigencia la ley 67/98290 (que vino a transponer al derecho interno portugués la directiva 95/46/CE). También sancionó las leyes 68/98 y 69/98, esta última a los efectos de transponer a su derecho interno la Directiva 97/66/CE, relacionada con la protección de datos personales en el sector de las telecomunicaciones.

En su segundo artículo, la ley 67/98 enuncia un principio general, según el cual "el tratamiento de los datos personales debe procesarse de forma transparente y en un estricto respeto por la reserva de la vida privada, así como los derechos, libertades y garantías

fundamentales". Este punto de partida de la ley portuguesa es altamente positivo, dado que marca una línea rectora de interpretación y aplicación de los preceptos siguientes de la norma.

La legislación portuguesa sólo permite recoger datos personales tratados en forma lícita y con respeto al principio de buena fe, recogidos para finalidades determinadas, explícitas y legítimas, que sean relevantes, pertinentes y adecuados para la finalidad del procesamiento de datos autorizado por la autoridad de aplicación. Con respecto a la calidad de los datos, se exige que los datos sean exactos, correctos y actualizados.

La autoridad de control en Portugal es la Comisión Nacional de Protección de Datos (CNPD), cuya función es controlar la aplicación de la ley de protección de datos personales y el respeto por las garantías declaradas en el art. 35 de la Constitución. Esta comisión se compone de siete miembros de integridad y mérito reconocido, de los cuales el presidente y dos de los vocales son elegidos por la Asamblea de la República. El resto de los vocales se integra con dos magistrados que cuenten con más de diez años de antigüedad y dos personas particularmente competentes designadas por el Gobierno. El artículo 25º de la ley 67/98 establece que los integrantes de la Comisión duran cinco años en el cargo.

### 4.24. LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL REINO UNIDO

La historia del derecho a la intimidad, o privacy, tiene una gran influencia de la legislación anglo-americana.

La primera ley de protección de datos personales británica, la Data Protection Act, surge el 12 de julio de 1984 luego de un profundo debate en el cual primero es publicado el Libro Blanco sobre Informática e Intimidad (Computers and Privacy) en 1975303 y luego el informe Lindop (Lindop Report) en 1978.

La Ley de Protección de Datos (Data Protection Act) de 1984 fue una norma diferente a las restantes leyes de protección de datos personales vigentes en esos tiempos. Sus principios y reglas se caracterizaron por la generalidad y la flexibilidad, motivos por los cuales pudo ir adaptándose a la dinámica y a las necesidades del cambio tecnológico acontecido en las últimas décadas. Esta ley entró en vigor en forma progresiva, ya que el 12 de septiembre de 1984 comenzó a regir una parte y en una segunda etapa tomó vigencia la otra parte, el 11 de noviembre de 1987, hasta la sanción y promulgación de la Ley de Protección de Datos de 1998.

La Ley de Protección de Datos de 1998 se aplica tanto al sector público como al sector privado y exige la inscripción de los archivos en la Oficina del Comisionado para la Protección de Datos.

La anterior Ley de Protección de Datos de 1984 había creado la oficina del Registrador para la Protección de Datos (The Data Protection Registrar) y el Tribunal de Protección de Datos (The Data Protection Tribunal), dos órganos diferentes que tienen la misión de velar por el cumplimiento de la ley y la protección de los datos personales. Estos órganos de control cambiaron sus nombres con La ley de Protección de Datos de 1998, y el Tribunal de la Protección de Datos modificó su nombre por la denominación de Tribunal de la Información con la Ley de Libertad de Información (Freedom of Information) del año 2000.

La Ley de Protección de Datos de 1998 entró en vigencia en el Reino Unido de Gran Bretaña el 1 de marzo de 2000, revocando la Ley de Protección de Datos de 1984.

### 4.25. LEY DE PROTECCIÓN DE DATOS PERSONALES EN SUECIA

Suecia dictó su primera legislación sobre la protección de datos por medio de su Ley de Datos (The Data Act) número 1973/289 vigente a partir del 1 de julio de 1973, siendo modificada, primero en 1989 y luego remplazada en 1998 por la ley de Protección de Datos (The Personal Data Act) Nº 1998/204, que comenzó a regir plenamente a partir del 30 de septiembre de 2001.

El marco legislativo en materia de datos personales se completa en Suecia con la Ley de Información de Crédito (The Credit Information Act) promulgada en 1973 y la Ley de Recuperación de Deudas (The Debit Recovery Act) promulgada en 1974.

La ley sueca de protección de datos personales se aplica a todos los bancos o bases de datos personales, sean de titularidad pública como privada que se encuentren en el territorio de Suecia, y extiende su ámbito de aplicación también a los bancos de datos personales establecidos en un tercer país, que procese datos personales por medio de equipos situados en Suecia.

La autoridad de control sueca es la Datainspektionen (Junta de Inspección de Datos), autoridad pública que actúa a través de un equipo de empleados públicos, que en su mayoría son abogados, bajo la dirección de un Director. La función de este organismo público es proteger la intimidad de las personas en la sociedad de la información sin exigir prevenciones innecesarias que compliquen el uso de las nuevas tecnologías.[85]

## 4.26. LEY DE PROTECCIÓN DE DATOS PERSONALES EN NORUEGA

[85] Saltor, C.E. (2013). La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación Argentina. (Memoria Doctoral). Universidad Complutense de Madrid. Madrid España. Recuperado de https://eprints.ucm.es/22832/1/T34731.pdf

En el Reino de Noruega la protección de datos personales se encuentra regulada por la Ley sobre el Tratamiento de Datos Personales Nº2000-04-14-31320. Esta norma fue promulgada en el año 2000, entró en vigor el 1° de enero de 2001 y sufrió diferentes modificaciones, pero la más reciente data de junio del año 2009.

La autoridad de control es la Junta de Protección de Datos de Noruega. Tiene la tarea de ayudar a proteger la intimidad de las personas violada por el tratamiento de datos personales. Los datos personales serán tratados de acuerdo con las consideraciones básicas de política, tales como la necesidad de protección de la integridad personal y la privacidad.

### 4.27. PROTECCIÓN DE DATOS EN AMÉRICA

El derecho a la intimidad es el derecho núcleo desde el cual se desarrolla el derecho a la intimidad, aun cuando en su evolución se independiza, se hace autónomo y crece como un derecho nuevo, distinto, que ya no sólo protege los datos íntimos de una persona sino también aquellos que sin ser íntimos se refieren a ella.

Sobre la protección de los datos personales en América, diciendo que la protección del derecho a la intimidad en este continente fue incorporada en noviembre de 1969 por la Convención Americana sobre Derechos Humanos, también conocida como Pacto de San José de Costa Rica, en la cual encontramos diferentes normas que dan fundamento a los derechos relacionados con el derecho a la protección de los datos personales. Así, el artículo 1º compromete a los Estados firmantes a legislar contra la discriminación por motivos de raza, color, sexo, idioma, religión, opiniones políticas o de cualquier índole. Otros artículos contienen declaraciones que protegen la honra y la dignidad de las personas; así, el art. 11 enuncia en su inciso 1º, que “Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada,

en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación".

Luego llegará la incorporación del instituto del habeas data en la Constitución de la República Federativa de Brasil en 1988, con la cual se inicia en América un proceso de reformas constitucionales que incluirán una garantía constitucional específica para controlar los bancos de datos públicos y privados, a los efectos de proteger los datos de carácter personal y permitir la toma de conocimiento de la información personal almacenada en bases, archivos o bancos de datos públicos y privados.

EEUU y Canadá dictaron las primeras normas sectoriales de protección de datos personales en el continente americano en el siglo pasado. El resto de las naciones de América, todas más retrasadas en el uso de la tecnología que los países del norte, recién comenzaron a legislar sobre este tema en el presente siglo.

Las primeras leyes latinoamericanas sobre protección de datos personales surgieron en Chile (1999) y en Argentina (2000). Varios años más tarde lo hicieron Perú y México.

### 4.28. LEY DE PROTECCIÓN DE DATOS PERSONALES EN ESTADOS UNIDOS

La doctrina jurídica, las normas y la jurisprudencia de los EEUU de América son antecedentes fundadores en materia de protección de datos personales. Los juristas norteamericanos Samuel Warren y Louis Brandeis construyeron el moderno concepto jurídico de derecho a la vida privada (privacy law), al publicar un embrionario escrito en la revista de la Universidad de Harvard titulado The Right to Privacy.

La doctrina del derecho a la vida privada (Privacy Law), aportó una nueva interpretación de los precedentes judiciales del derecho de los EEUU, ya que antes de esta doctrina, se entendía que el Common Law solo protegía personas físicas o bienes materiales a través del derecho de propiedad.

Muchos años más tarde, se dictaron en los EEUU las primeras normas que buscaron proteger la información personal. La Freedom of Information Act (Ley de Libertad de la Información, FOIA) como la Fair Credit Reporting Act (Ley de Equidad Financiera de 1978) y la Privacy Act (Ley de protección de la Intimidad).

El sistema jurídico anglosajón ha preferido promulgar normas sectoriales en materia de protección de datos personales. Hoy encontramos en la legislación de los Estados Unidos de América las siguientes normas relativas a la registración y almacenamiento de datos:

a) Ley de Protección de la Intimidad de 1974 (Privacy Act): busca proteger la intimidad de las personas cuyos datos personales figuran en bancos de datos del gobierno.

b) Ley de protección de datos del sector de la educación: protege la información registrada en instituciones educativas públicas.

c) Ley de protección de la privacidad financiera Fair Credit Reporting Act de 1978: proporciona protección a los individuos, restringiendo el acceso del gobierno a las informaciones sobre los clientes de los bancos e instituciones financieras, estableciendo así un cierto grado de confidencialidad de los datos financieros personales.

d) Ley de libertad de información de 1966 (Freedom of Information Act): establece el derecho de las personas a acceder a los datos sobre ellos almacenados.

La ley de Libertad de Información (FOIA), es otra norma relacionada con el derecho a la información, es una forma de habeas data que permite el acceso a toda clase de documentación o archivo gubernamental.

e) Legislación Estatal. Además de las leyes federales ya mencionadas, cada Estado dicta sus propias leyes. En muchas de estas normas se exige que los datos sean relevantes, actualizados y precisos, además se prohíbe su difusión sin autorización. Falta legislación que regule las prácticas de las instituciones privadas respecto de sus bancos de datos de información personal.

Los EEUU carecen de un organismo de control en materia de protección de datos personales como los que existen en Europa. Como hemos explicado ut supra, el sistema jurídico norteamericano no legisla con leyes de alcance general u ómnibus; por el contrario, ha regulado la materia con diferentes leyes sectoriales.[86]

## 4.29. LEY DE PROTECCIÓN DE DATOS PERSONALES EN BOLIVIA

El Estado Plurinacional de Bolivia ha reformado su Constitución en el año 2009, oportunidad en la que ha incluido una nueva garantía constitucional de protección a la intimidad y a los datos personales, a la que denominó “acción de privacidad”, sobre la cual profundizaremos a continuación. Probablemente por su reciente mutación constitucional, Bolivia todavía no ha desarrollado legislativamente el instituto de la protección de los datos personales en una ley específica. Por este motivo, ante la carencia de normas infra

[86] Saltor, C.E. (2013). La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación Argentina. (Memoria Doctoral). Universidad Complutense de Madrid. Madrid España. Recuperado de https://eprints.ucm.es/22832/1/T34731.pdf

constitucionales, la protección genérica de la intimidad o la protección específica de los datos de carácter personal debe ser complementada por otras normas análogas o genéricas que indirectamente puedan hacer referencia al tema.

En este sentido, la Constitución Política del Estado de Bolivia expresa en el Capítulo Tercero, referido a los Derechos Civiles y Políticos, Sección I sobre Derechos Civiles, artículo 21º: que “Las bolivianas y los bolivianos tienen los siguientes derechos: 2. A la privacidad, intimidad, honra, honor, propia imagen y dignidad”

La Carta Magna de Bolivia se ocupa nuevamente del derecho a la intimidad y en particular del derecho a la protección de los datos personales, en el Título IV referido a las Garantías Jurisdiccionales y Acciones de Defensa, en cuyo Capítulo Segundo dedicado a las Acciones de Defensa propiamente dichas, en su Sección III, se encuentra el artículo 130 , que textualmente expresa:

> I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.
>
> II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa”.

A continuación el artículo 131 expresa que el procedimiento aplicable será el de la acción de amparo constitucional, y que en caso de que un juez o tribunal competente

declare procedente la acción de privacidad, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado. Esta sentencia tiene efecto ejecutivo, ya que textualmente el apartado III del artículo 131 expresa: “La decisión se elevará, de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución.

El derecho a la intimidad también se encuentra contenido por la protección al secreto de la correspondencia y de los papeles privados, que la Constitución Política del Estado contempla en el art. 25 del texto reformado.

También el artículo 35 es muy claro al expresar que “Las declaraciones, derechos y garantías que proclama esta Constitución no serán entendidas como negación de otros derechos y garantías no enunciados que nacen de la soberanía del pueblo y de la forma republicana de gobierno”.

El derecho a la protección de datos personales existe aun cuando en Bolivia faltan leyes que desarrollen la Constitución, dada su calidad de derecho humano y personalísimo. Aun así, es conveniente su pronta incorporación en el derecho positivo infra constitucional para dar una mayor protección a los habitantes de Bolivia, a los efectos de que cuenten con garantías constitucionales y leyes específicas que protejan su intimidad y sus datos personales.

### 4.30. LEY DE PROTECCIÓN DE DATOS PERSONALES EN BRASIL

La Constitución de la República Federativa de Brasil reformada en 1988 agregó a sus tradicionales garantías de mandato de seguridad y habeas corpus la acción de habeas data en el artículo 5º numeral LXXII del capítulo I.

Esta es la primera de las constituciones que nombró con la denominación de habeas data a una garantía constitucional concedida por los constituyentes para: “asegurar el conocimiento de informaciones relativas a la persona solicitante, que consten en registros de bancos de datos de entidades gubernamentales o de carácter público”, o “para la rectificación de datos cuando se prefiera hacerlo en proceso reservado (léase secreto) judicial o administrativo” (Art. 5º numeral LXXII).

Brasil incorporó en forma temprana el habeas data en su Constitución, motivos por los cuales su redacción es más limitada que el texto de las constituciones posteriores (Argentina, Perú, Venezuela, Colombia, Bolivia, etc.), y no garantiza el acceso a los bancos de datos privados. Esta limitación en la regulación del instituto del habeas data en Brasil, es criticada, y a falta de una nueva reforma constitucional, será el Congreso o la jurisprudencia quienes deberán permitir el acceso a los bancos o registros de datos privados y avanzar con reglamentaciones más efectivas.

El primer párrafo del artículo Art. 5º numeral LXXII de la Constitución de Brasil, garantiza a quienes lo soliciten, el acceso a la información de carácter personal referido a su persona, existente en registros o bancos de datos públicos. La segunda parte concede al solicitante la facultad de rectificar un dato a él referido, mal consignado en los registros o bancos de datos públicos.

En el mismo artículo 5º y directamente relacionados con el instituto del habeas data, también se encuentran los numerales XXXIII y LXXVII.

El numeral XXXIII del artículo 5º, se refiere al habeas data impropio y textualmente expresa que “todos tendrán derecho a recibir de los órganos públicos

informaciones de su interés particular, o de interés colectivo o general, que serán entregadas en los términos que establezca la ley, bajo pena de responsabilidad, excepto aquellas cuyo secreto fuere imprescindible para la seguridad de la sociedad y del Estado".

Por último, la Constitución contiene el numeral LXXVII del artículo 5º, que se refiere a la gratuidad del recurso de habeas data, y textualmente expresa que: "Son gratuitas las acciones de habeas corpus y habeas data en la medida en que la ley disponga los actos necesarios para el ejercicio de la ciudadanía. 1) Serán de aplicación inmediata las normas definidoras de los derechos y garantías fundamentales. 2) Los derechos y garantías indicados en esta Constitución no excluyen otros que deriven del régimen y principios adoptados por ella o de los tratados internacionales en que la República Federativa del Brasil sea parte".

La legislación sobre protección de datos personales en Brasil omitió crear una autoridad de control independiente que regule los registros y bancos de datos con facultades y potestades suficientes para dar protección efectiva a los datos personales.[87]

### 4.31. LEY DE PROTECCIÓN DE DATOS PERSONALES EN PERÚ

Siguiendo el antecedente de la Constitución brasileña de 1988, la Constitución Política del Perú de 1993 incorporó la garantía constitucional del habeas data, la cual fue reformada en 1995 con modificaciones al art. 200, inc. 3º)357, dentro del título que regula las Garantías Constitucionales. Los medios de comunicación y los organismos profesionales y gremiales del periodismo peruano plantearon su desacuerdo a la incorporación

[87] Saltor, C.E. (2013). La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación Argentina. (Memoria Doctoral). Universidad Complutense de Madrid. Madrid España. Recuperado de https://eprints.ucm.es/22832/1/T34731.pdf

del habeas data, al entender que la norma constitucional atentaba contra la libertad de expresión.

El enunciado constitucional expresaba textualmente que: “La acción de Habeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos que se refieren al artículo 2° incisos 5°, 6° y 7° de la Constitución”.

De esta forma, la Constitución peruana entendía que el habeas data era una garantía constitucional que venía a complementar los derechos del artículo 2° inciso 5° y 6°. Veamos su texto: Art. 2° - “Toda persona tiene derecho a Inc. 5°, a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. El secreto bancario y la reserva tributaria pueden levantarse a pedido del juez, del fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado. Inciso 6°, A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar. Por último, el inciso 7° expresaba que toda persona tiene derecho “al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propia. Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que este se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley.”

Actualmente, la Constitución Política del Perú reconoce el derecho fundamental a la autodeterminación informativa como una de las facultades que tienen las personas para

resguardar su propia información ante el registro, uso y revelación de los datos que considere sensibles y que no deberían ser difundidos. A partir de ahí, el legislador ha establecido un marco legal para desarrollar este derecho a través de la Ley de Protección de Datos Personales – Ley 29733 del 3 de julio de 2011 y de su reglamento, aprobado por Decreto Supremo 003-2013-JUS.[88]

### 4.32. LEY DE PROTECCIÓN DE DATOS PERSONALES EN NICARAGUA

La Constitución de la República de Nicaragua todavía no ha incorporado en forma expresa la acción de protección de los datos personales. De todas formas, como todas las Cartas Constitucionales americanas, protege al derecho a la intimidad. Su artículo 26º expresa textualmente que "Toda persona tiene derecho a su vida privada y a la de su familia", con lo cual es posible interpretar que el derecho a la intimidad en general se encuentra expresamente protegido por la constitución nicaragüense y en forma indirecta podemos extender esta protección a los datos personales y al derecho a la autodeterminación informativa.

### 4.33. LEY DE PROTECCIÓN DE DATOS PERSONALES EN PANAMÁ

Panamá buscó dar protección jurídica a los datos de carácter personal, primero por medio de la legislación, con la ley 6/2002 Nº 24.476 del 23/01/2002 y recién dos años más tarde con la incorporación de la acción de habeas data en su Constitución.

La Constitución de Panamá incorporó la acción de habeas data luego de ser reformada en el año 2004. Se encuentra en el artículo 44, cuyo texto expresa: "Toda persona podrá promover acción de habeas data con miras a garantizar el derecho de acceso a su

[88] Diaz, K., Escudero, S. (2019). Manual de Protección de Datos Personales. https:// www.defensoria.gob.pe/wp-content/uploads/2019/11/Manual-de-Protecci%C3%B3n-de-Datos-Pe

información personal recabada en bancos de datos o registros oficiales o particulares, cuando estos últimos pertenezcan a empresas que prestan un servicio al público o se dediquen a suministrar información. Esta acción se podrá interponer, de igual forma, para hacer valer el derecho de acceso a la información pública o de acceso libre, de conformidad con lo establecido en esta Constitución. Mediante la acción de habeas data se podrá solicitar que se corrija, actualice, rectifique, suprima o se mantenga en confidencialidad la información o datos que tengan carácter personal. La ley reglamentará lo referente a los tribunales competentes para conocer del habeas data, que se sustanciará mediante proceso sumario y sin necesidad de apoderado judicial".

El 26 de marzo de 2019 sanciona la ley N° 81 sobre Protección de Datos Personales.[89]

La Constitución panameña ha reunido en un mismo artículo, dentro de la acción de habeas data, a los derechos a la protección de los datos personales y al acceso a la información pública.

### 4.34. LEY DE PROTECCIÓN DE DATOS PERSONALES EN CANADÁ

La ley de Protección de la Información Personal y de los documentos electrónicos (conocida como la ley PIPEDA, Bill C-6) fue sancionada en Canadá el 13 de abril de 2000 y entró en vigencia el 1 de enero de 2001. Recientemente esta ley federal canadiense fue reformada en abril del año 2011, luego de un largo debate iniciado en el año 2008 sobre una reforma general a esta legislación de protección de datos personales canadiense y para ello la Oficina del Comisionado de Privacidad de Canadá, así como las comisiones

[89] ASAMBLEA NACIONAL REPÚBLICA DE PANAMÁ. (2019). Sobre protección de datos personales. https:// www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/2010/2019/2019_645_3008.pdf

pertinentes del Parlamento elaboraron sendos informes a partir de los cuales se sancionó la reforma.

La ley vigente legisla sobre la protección de datos personales y otorga nuevos derechos a las personas físicas para que puedan protegerse de la acumulación, uso o revelación (disclosure) de la información personal en la actividad comercial del sector privado. Canadá intentó alcanzar, con esta ley, los estándares jurídicos europeos para la protección de datos personales.

Canadá cuenta con dos leyes nacionales en relación a la privacidad y protección de datos:

- Privacy Act: Esta ley limita la recolección, uso y publicación de datos personales por parte de los organismos del gobierno.
- PIPED Act: Esta ley regula como el sector privado debe recolectar, usar y publicar datos de los usuarios.[90]

### 4.35. LEY DE PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA

Desde la década de 1980 encontramos antecedentes colombianos en materia de derecho a la protección de datos personales:

En 1986, la Universidad de los Andes elaboró un proyecto de ley de datos personales que sirvió de antecedente para proyectar una iniciativa parlamentaria de perfil permisivo sobre habeas data. Este proyecto parte de la licitud de construir bancos de datos de información personal, previa condición de ser comunicados a una autoridad de control, y tiene como objeto la tutela, por vía de un desarrollo legislativo, de los datos de las personas físicas y

[90] Athento. (2017). ¿Por qué Canadá es un país seguro para mis datos?. soporte.athento.com/hc/es/articles/115004366045--Por-qu%C3%A9-Canad%C3%A1-es-un-pa%C3

jurídicas frente a bancos de datos personales públicos y privados, ya sean manuales o informáticos.

En 1987, (cuatro años antes de ser sancionada la Constitución Política de Colombia de 1991) entraba en vigencia el Código Procesal Penal, que también abordaba la protección de la intimidad, dado que además de habilitar el uso de una acción de tutela y protección de las informaciones existentes en los bancos de datos, autoriza a los interesados a apelar a medidas procesales equivalentes en el marco de un proceso contencioso y a solicitar judicialmente el conocimiento, la actualización o rectificación de un banco de datos, puesto que el derecho a la información es de aplicación inmediata en Colombia .

Finalmente se consagra el derecho a la protección de los datos personales garantizado por el habeas data en la Constitución Política de la República de Colombia del año 1991 (luego reformada en diferentes oportunidades, siendo su última enmienda en el año 2005). En esta norma fundamental colombiana se consagró la protección de los datos de carácter personal en su art. 15. Posteriormente, en el año 2003, el texto del artículo fue modificado y quedó redactado de la siguiente forma:

ARTICULO 15 (Constitución Política de Colombia):

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.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Sin embargo, debido a los constantes avances tecnológicos y al uso de nuevas herramientas cibernéticas se creó la necesidad de regular en detalle aspectos relacionados con los datos personales. Por consiguiente, se dio nacimiento a la Ley 1581 de 2012, en la cual se expusieron los aspectos generales en dicha materia.[91]

### 4.36. LEY DE PROTECCIÓN DE DATOS PERSONALES EN CHILE

La Constitución Política de la República de Chile (aprobada en 1980 y reformada sustancialmente en 1989 y en 1991), no legisla en forma expresa sobre la protección de datos personales, sólo lo hace indirectamente en los artículos 19.4 y 19.12.

Concretamente el art. 19.4 garantiza a toda persona el respeto y protección a su vida privada, a su honra, a la de su familia y a la libertad de información.

El inciso 12° del artículo 19° de la Constitución consagra la libertad de emitir opinión y de informar sin censura previa, sin que pueda interpretarse que la libertad de informar implique la posibilidad de acceder o dar acceso a datos de carácter personal.

En base a los preceptos constitucionales mencionados, la jurisprudencia ha aceptado planteos de acciones judiciales de protección, para proteger los derechos afectados

[91] Aguilar, M.A. (2018). La Ley de Protección de Datos en Colombia: sus inicios y examen de sus principales postulados. https://repository.ucatolica.edu.co/bitstream/10983/23060/1/La%20Ley%20De%20Protecci%C3%B3n%20D

por el tratamiento de datos personales de los accionantes. Muchas de estas acciones fueron resueltas por la Corte Suprema de Justicia chilena.

La ley 19.628 sobre Protección de la Vida Privada publicada y vigente a partir del 28 de septiembre de 1999 es una consecuencia directa de la actividad judicial desarrollada sobre el tema. Esta norma fue parcialmente modificada en el año 2002 por la ley 19.812.

El objeto de la ley es el tratamiento de los datos de carácter personal realizado en registros o bancos de datos, por organismos públicos o por particulares. El artículo 1º exceptúa el tratamiento de datos que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regula por la ley a que desarrolla el artículo 19 inc. 12 de la Constitución Política.

La ley 19.628 protege los datos personales de las personas físicas o naturales sin comprender a los datos referidos a personas jurídicas.

El mayor defecto de la ley chilena radica en el órgano de control. Ya que mientras el derecho comparado en general (legislación europea, Argentina, etc.), crea una autoridad de aplicación y control especial sobre protección de datos personales, la Ley chilena de protección de la vida privada opta por un sistema de control judicial que, en el caso de organismos públicos, es fortalecido por un control cruzado con el Servicio de Registro Civil e identificación de las personas.

Recogiendo las recomendaciones que hizo la OCDE al país en el año 2010, el día 15 de marzo de 2017, se ingresó el proyecto de ley de protección de datos personales bajo el Boletín N° 11.14 4 - 07 (el “Proyecto” ), que ya se encuentra bastante avanzado en su primer trámite constitucional ante el Senado, siendo su última actividad de fecha 16 de marzo de 2020.

Si bien este proyecto no intenta derogar la LPVP, sí viene a modificar gran parte de su articulado, reforzando y reordenando algunos conceptos ya consagrados por la Ley N° 19.628, como también introduciendo ciertas novedades, como por ej:[92]

- Se refuerzan y amplían los derechos del titular de los datos (se consagran el Derecho de Acceso, Derecho de Rectificación, Derecho de Cancelación, Derecho de Oposición y se agrega el Derecho de Portabilidad).
- Se establece una regla de protección especial para el tratamiento de los datos personales de niños y adolescentes.

## 4.37. LEY DE PROTECCIÓN DE DATOS PERSONALES EN COSTA RICA

La República de Costa Rica es un país pluricultural de Centroamérica que limita al norte con la República de Nicaragua y al sur con la República de Panamá. Se destaca por ser una de las democracias más consolidadas de América.

Aun cuando la Constitución Política de la República de Costa Rica y los diversos tratados internacionales de protección de derechos humanos ratificados por el Estado, contemplan la protección de los derechos y libertades fundamentales, el derecho a la intimidad carece, de un mecanismo ágil y eficiente para su protección.

La protección jurídica de los datos de carácter personal o habeas data propiamente dicho, aún no se encuentra contemplada en la Constitución Política de la República de Costa Rica, ni en la legislación del Estado.

[92] Ortiz, O. (2020). Protección de datos personales en Chile. https://www2.deloitte.com/content/dam/Deloitte/cl/Documents/legal/2020/cl-protecci%C3%B3n-datos-pers

## 4.38. LEY DE PROTECCIÓN DE DATOS PERSONALES EN ECUADOR

La República de Ecuador incorporó en su reforma constitucional del año 1996, el artículo 30, dentro del cual expresa que: “toda persona tiene derecho a acceder a la documentación, bancos de datos e informes que sobre sí misma o sobre sus bienes consten en entidades públicas o privadas, así como conocer el uso que se haga de ellos y su finalidad. Igualmente podrá solicitar ante el funcionario o juez competente la actualización, rectificación, eliminación o anulación de aquellos, si fueren erróneos o afectaren ilegítimamente sus derechos. Se exceptúan los documentos reservados por razones de seguridad nacional”.

Posteriormente, la Constitución de la República de Ecuador, aprobada el 11 de agosto de 1998, ha incluido el recurso de habeas data como una garantía constitucional expresa, ubicada dentro de la Sección referida a las Garantías de los Derechos.

El artículo 94 otorga a toda persona el derecho a acceder a los documentos, bancos de datos e informes que sobre si misma o sobre sus bienes, consten en entidades públicas o privadas, así como para conocer el uso y el propósito que se haga de ellos. Las personas también pueden solicitar, ante el funcionario respectivo, la actualización de los datos, su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. El afectado puede demandar una indemnización, si la falta de atención le causare algún perjuicio.

El acceso a los datos personales que consten en los archivos vinculados con la defensa nacional, requiere un procedimiento especial que debe ser establecido por ley del Congreso.

El cuadro normativo de la protección de datos personales se completa en Ecuador con la Ley del Control Constitucional promulgada en 1997.

Lo más criticable de este sistema legal de protección de datos personales, es que la legislación ecuatoriana no ha creado una autoridad de aplicación y control en materia de protección de datos personales.

### 4.39. LEY DE PROTECCIÓN DE DATOS PERSONALES EN MÉXICO

En el año 2002, entra en vigencia en México la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y se crea el organismo supervisor de dicha ley: el Instituto Federal de Acceso a la Información y Protección de Datos. Su campo de vigilancia, en un comienzo sólo alcanzó a la Administración Pública Federal y a los organismos autónomos como el Instituto Federal Electoral (IFE), la Comisión Nacional de Derechos Humanos (CNDH) y el Banco de México.

En julio de 2007 se implementaron acciones con miras a consolidar la protección de datos personales en posesión de las empresas particulares, pero tuvieron que transcurrir tres años más, y tres modificaciones a artículos de la Constitución Mexicana (6°, 16° y 73°), junto con la transformación del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) para quedar como un organismo público descentralizado de la Administración Pública Federal con autonomía operativa, presupuestaria y de decisión, para recién llegar a la promulgación y posterior publicación, el 5 de julio de 2010, del decreto que expide la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP).

La LFPDPPP es de orden público y observancia general en toda la República y su objeto es la protección de los datos personales en posesión de particulares para regular su tratamiento legítimo, informado y controlado a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Basada principalmente en el modelo europeo, esta ley se compone de 69 artículos, agrupados en 11 capítulos, que cubren entre otros los siguientes temas:

a) Los derechos que otorga la ley, llamados en Méjico derechos ARCO, por medio de los cuales se otorgan las garantías y procedimientos para que cualquier persona pueda acceder, ratificar, corregir y/u oponerse a la existencia de registros con información sensible o no sensible.

b) El derecho al aviso de privacidad, conforme al cual la obtención de datos debe hacerse a través de medios lícitos y no fraudulentos

c) Tratamiento de datos. El tratamiento de los datos requiere la autorización del titular de los mismos (aviso de privacidad) y éstos sólo se podrán usar para el fin para el cual fueron recabados.

d) No cumplimiento. La verificación del cumplimiento de la LFPDPPP queda a cargo del IFAI, y puede iniciarse de oficio o a petición de parte. El no cumplimiento de la ley puede generar infracciones económicas o sanciones penales. Las multas varían desde los valores cercanos a los 500 dólares, hasta llegar al millón y medio de dólares estadounidenses.

e) Debido a la legislación mexicana y a los artículos transitorios de la ley es importante tener presente las siguientes consideraciones: El derecho ARCO se podrá ejercer a los dieciocho meses de la entrada en vigor de la ley, esto es a partir del 6 de enero de 2012.

f) Los avisos de privacidad se podrán expedir a más tardar un año después de la entrada en vigor de la ley, esto es, como máximo, el 6 de julio de 2011.

g) El reglamento de la ley se expedirá dentro de los siguientes doce meses a su entrada en vigor, esto es, antes del 6 de julio de 2011.

El IFAI hoy en día se enfrenta a amparos y confrontaciones con organismos de gran relevancia nacional, que incluso pueden llegar a la corte.

Finalmente México promulgó una legislación general sobre protección de datos personales a la que dio por nombre Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), publicada el 05 de julio de 2010, dicha ley está alineada con los preceptos originales que otras naciones, principalmente europeas.

## 4.40. LEY DE PROTECCIÓN DE DATOS PERSONALES EN PARAGUAY

La Constitución de la República de Paraguay introdujo la protección de los datos de carácter personal con la reforma constitucional del año 1992, en el capítulo de las garantías constitucionales, al receptar el recurso de habeas data en el artículo 135.

Este recurso fue calificado por la jurisprudencia como una garantía constitucional tendiente a tornar efectivas algunas previsiones constitucionales, tales como el derecho a la intimidad, la inviolabilidad del patrimonio documental y la comunicación privada o la protección de la dignidad y de la imagen privada de las personas.

La Constitución define como sujeto activo del recurso de habeas data a toda persona, expresión entendida tanto por la jurisprudencia como por la doctrina, con alcance a todas las personas tanto físicas como jurídicas.

Entonces, el recurso de habeas data otorga a toda persona los siguientes derechos:

a) a acceder a la información que sobre la persona del accionante, o sobre sus bienes, obren en registros oficiales o privados de carácter público;

b) a conocer el uso que se haga de los mismos y su finalidad.

c) a solicitar, ante el magistrado competente, si los datos fuesen erróneos o afectaren ilegítimamente los derechos del afectado: la actualización, la rectificación, o la destrucción de los mismos.

El punto más criticable de la legislación paraguaya de protección de datos personales es la ausencia de una autoridad de aplicación y control en la materia. Por el contrario, ha dejado estas competencias en manos del Juzgado en lo Civil y Comercial, en trámite sumario, es decir que se ha pronunciado a favor del sistema del control judicial de la aplicación de la ley 1682 y toda otra normativa referida a la protección de datos personales.

### 4.41. LEY DE PROTECCIÓN DE DATOS PERSONALES EN URUGUAY

Uruguay es el único país del Mercosur que no ha incluido en su Constitución el recurso garantía de habeas data para proteger jurídicamente los datos personales de las personas que habitan su territorio nacional. De esta forma se apartó también de la tendencia iberoamericana en esta materia; sin embargo, la Constitución de la República Oriental del Uruguay contiene normas que, sin referirse expresamente a los datos personales, son el fundamento para la protección jurídica de los derechos a la privacidad, a la intimidad, a la autodeterminación informativa, a la protección de los datos personales, a la honra y a la propia imagen en Uruguay.

La protección de los datos personales está implícita en el ordenamiento jurídico de Uruguay, a partir del texto de los artículos 7, 10, 72 y 332 de la Constitución uruguaya, los cuales, además de establecer una normativa marco en la materia, consagran los principios generales como fuente de derecho.

Uruguay necesita legislar una norma específica y de carácter general en materia de protección a los datos personales y a la vida privada de las personas. La ausencia de una norma de tales características en el derecho uruguayo, crea una importante distancia jurídica con el resto del Mercosur, con gran parte de Iberoamérica y en particular con la Unión Europea en materia de protección de datos personales.

Uruguay ha crecido considerablemente en sus exportaciones y es una economía en expansión que necesita estar cada vez más conectada con el mundo y transferir datos (muchos de carácter personal) a países que exigen legislaciones equivalentes para permitir la transferencia internacional de datos.

Desde el año 2010 los referentes políticos uruguayos han comenzado a acordar una nueva reforma a la Constitución, oportunidad en la cual podría debatirse la consagración constitucional del recurso de habeas data.

### 4.42. LEY DE PROTECCIÓN DE DATOS PERSONALES EN VENEZUELA

La República Bolivariana de Venezuela ha incluido el habeas data en su Constitución del año 2000, luego ha realizado una enmienda constitucional el 15 de febrero del año 2009, pero a la fecha no ha realizado un desarrollo legislativo infraconstitucional, específico en materia de protección de datos personales.

La Asamblea Nacional Constituyente del año 2000 expresaba en la exposición de motivos de la Constitución que: “Se reconoce por vez primera en el constitucionalismo venezolano, el habeas data o derecho de las personas de acceso a la información que sobre sí mismas o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley. El habeas data incluye el derecho de las personas de conocer el uso que se haga de tales registros y su finalidad, y de solicitar ante el tribunal competente su actualización, rectificación o destrucción, si fuesen erróneos o afectasen ilegítimamente sus derechos”.

La Constitución venezolana atribuye la facultad de interponer las acciones de habeas data, entre otros recursos y acciones de inconstitucionalidad, al Defensor del Pueblo en el artículo 281 inciso 3º.

### 4.43. LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL SALVADOR

La Constitución de la República de El Salvador no incluye al habeas data, pero se lo puede considerar implícito en otros artículos de la misma Carta Magna o en Tratados Internacionales a los cuales esta nación se encuentra adherida. A modo de ejemplo podemos mencionar al artículo 2° de la Constitución, cuando protege el derecho al honor, a la intimidad personal y familiar, y a la propia imagen.

La Constitución salvadoreña también establece implícitamente el procedimiento del amparo en el artículo 247, cuando textualmente expresa que ante una violación a los derechos que otorga la Constitución (por ejemplo, el ya mencionado artículo 2°), toda persona puede pedir amparo ante la Sala Constitucional de la Corte Suprema de Justicia.

En otras palabras, podemos decir que los derechos reconocidos, tanto implícita como explícitamente por la Constitución, deben ser garantizados a toda persona por el sólo hecho de estar incluidos en la Ley Fundamental, independientemente de que exista o falte una ley reglamentaria o dela naturaleza del legitimado pasivo.

### 4.44. LEY DE PROTECCIÓN DE DATOS PERSONALES EN ARGENTINA

En la República Argentina, el derecho a la protección de los datos de carácter personal comenzó a ser reconocido en el año 1994, al ser incorporado a la Constitución Nacional, luego de la Reforma aprobada ese año.

Los reformadores de la Carta Fundamental tomaron como fuente, en este instituto, a la Constitución de Brasil, que en el año 1988 había incorporado el habeas data a su texto constitucional. También recurrieron al derecho comunitario europeo, al derecho comparado, a la doctrina de los diferentes autores, nacionales y extranjeros, y a la jurisprudencia en materia de derecho a la intimidad y autodeterminación informativa.

En el año 2000 fue promulgada la Ley Nacional 25.326 de Protección de los Datos de Carácter Personal.

Esta Ley 25.326 de Protección de Datos Personales tomó como modelo, casi textual, a la LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de Datos), Ley española del año 1992. Pero paradójicamente, casi como una trampa cronológica, un año antes, en 1999, España había derogado la LORTAD para promulgar y aprobar la LOPD (Ley Orgánica de Protección de Datos de Carácter Personal).

Luego llegó la creación de la Dirección Nacional de Protección de Datos de Carácter Personal, autoridad en la materia, la jurisprudencia sobre habeas data y sobre protección de datos de carácter personal, junto con la reglamentación de la nueva ley.

De acuerdo con la Constitución Argentina, la Ley de Protección de Datos Personales 25.326 (PDPA) se sancionó en 2000 para proteger la privacidad de los datos personales y ofrecer acceso a los usuarios a cualquier información sobre ellos almacenada en los registros y en las bases de datos públicas y privadas. La Agencia de Acceso a la Información Pública (AAIP) de Argentina, perteneciente a la Jefatura del Gabinete de Ministros, es responsable de aplicar esta legislación.

La PDPA se alinea con el modelo de información legislativa europeo para la protección de la privacidad de datos, y Argentina fue el primer país en Latinoamérica en lograr una calificación de "idoneidad" para las transferencias de datos de la UE.[93]

[93] Mazzoli, R. (2021). Ley de Protección de Datos Personales (PDPA) de Argentina. https:// docs.microsoft.com/es-es/compliance/regulatory/offering-pdpa-argentina

# CAPÍTULO V

# ANÁLISIS DE LOS HECHOS

## 5.1. ANÁLISIS SEGÚN LA INVESTIGACIÓN REALIZADA

Por toda la investigación realizada, la protección de datos personales es un tópico legal de suma importancia no solo a nivel nacional sino a nivel internacional. La mayoría de los países a través de la evolución de sus leyes y el estudio de la realidad identifican los aspectos que se tienen que cambiar, modificar, o actualizar con la mira de proteger la información y los datos personales de sus ciudadanos.

En la actualidad y en todo ámbito se habla bastante sobre datos personales. Se tuvo reportes de escándalos internacionales por la obtención y utilización fraudulenta de datos personales en elecciones y en redes sociales. De la misma manera, se generaron grandes discusiones normativas cuando el Reglamento de Datos Personales de la Unión Europea entró en vigencia y otros países comenzaron a discutir la actualización o creación de leyes al respecto.

A pesar de todo esto, los casos de abuso de la información personal de los usuarios de internet no pasan de ser hechos noticiosos en países donde no existe una ley de datos personales, como es el caso de Bolivia.

Por no poseer un marco normativo deriva en el hecho que no se pueda ir más allá y cuestionar esos hechos ante las instituciones locales, quedando usuarios y usuarias sin acceso a protecciones y reparaciones elementales por abuso de su información personal. Esta situación debe cambiar de manera inmediata.

En la actualidad, las y los bolivianos cuentan con leyes que tocan algunos temas de datos personales, pero lo hacen de manera incompleta y no integral. Por ello, se requiere establecer un proceso de construcción en la formulación de una ley centrada en una visión completa y con los derechos de los usuarios en el centro de la discusión.

En este sentido, cabe recalcar que, siendo el derecho un instrumento privilegiado de la construcción de este nuevo espacio, resulta evidente que la investigación jurídica debe, en primer lugar, tomar un adecuado conocimiento de los fenómenos técnicos y sociales, para, luego, proceder al estudio de las normas que salen al encuentro de esa nueva realidad, pese a que el propio dinamismo del cambio tecnológico impide, en muchas ocasiones, el que podamos tener una visión completa y acabada de todos y cada uno de los problemas a que puede dar lugar.

La temática requiere abordarla de manera integral, por tal motivo el presente trabajo plantea recabar información de carácter primario a través de encuestas y entrevistas dirigidas a la ciudadanía.

## 5.2. ENCUESTAS REALIZADAS

1. Edad:

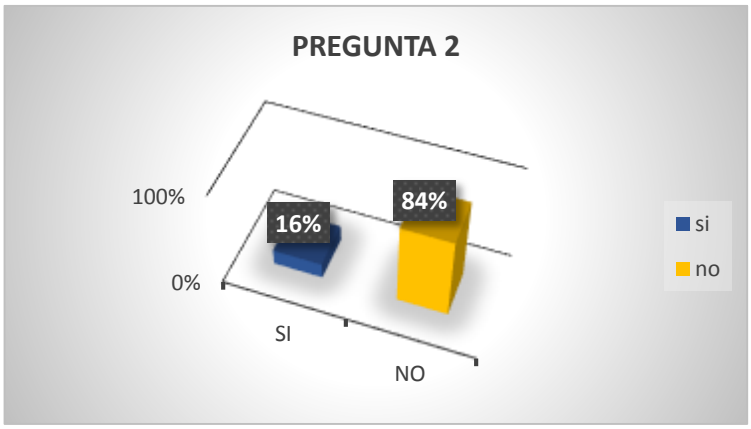
**CUADRO N° 1**

| RANGO-EDAD | 10 a 20 | 21 a 30 | 31 a 40 | 41 a 50 | 51 a 60 |
|---|---|---|---|---|---|
| ENTREVISTADOS | 6 | 24 | 10 | 6 | 4 |

Se ha llevado adelante la encuesta dirigida a la población de la ciudad de La Paz con la finalidad de obtener una información primaria, real y actual sobre el conocimiento y percepción que tienen acerca de la protección de los datos personales. El rango de edad está distribuido desde los 18 años hasta los 60, según el cuadro N°1 detallado arriba.

2. ¿Cuál(es) son dato(s) personal(es)?

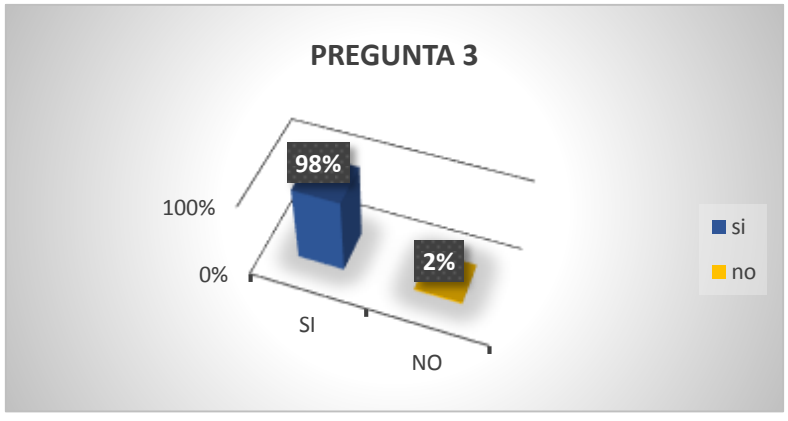
**GRÁFICO N° 1**




Sobre la pregunta 2, de la encuesta realizada, existe un porcentaje alto de personas que afirman no tener un concepto preciso de lo que son los datos personales, es un panorama que nos lleva a inferir realmente que se debe trabajar la formulación de una ley desde abajo, es decir con el concurso de toda la población.

3. ¿Considera que la protección de sus datos personales constituye un derecho fundamental?

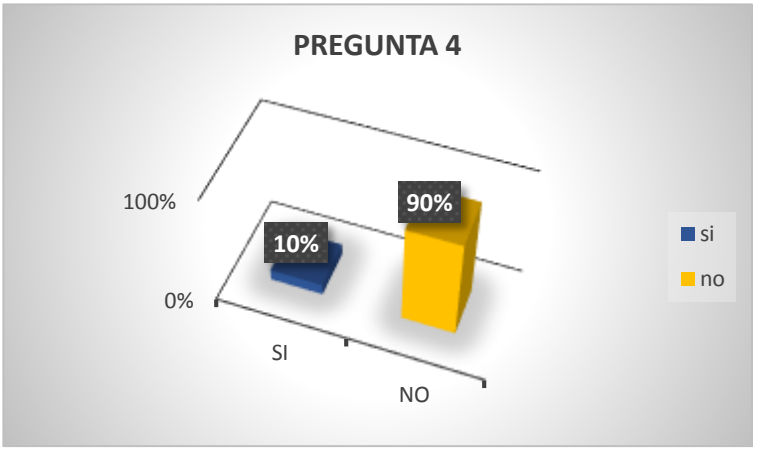
**GRÁFICO N° 2**



El 98% de los encuestados respondió positivamente a la pregunta 2 lo que implica que tiene conciencia real sobre el ejercicio de sus derechos personales.

4. ¿Conoce de alguna ley que proteja sus datos personales?

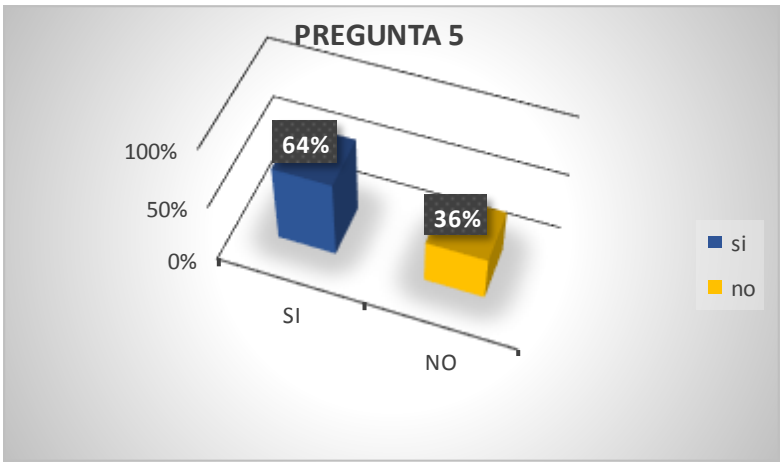
**GRÁFICO N° 3**




Acerca de la pregunta planteada en el numeral 4, el 90% de los encuestados indica no tener conocimiento sobre una ley concreta que proteja sus datos personales; el 10% restante manifiesta conocer leyes de protección de sus datos personales, pero dan a conocer normativas sectoriales.

5. Sabe usted que sus datos personales que proporciona a los diferentes registros públicos y privados tienen que estar protegidos conforme a su identidad personal, intimidad, privacidad, honor, imagen?

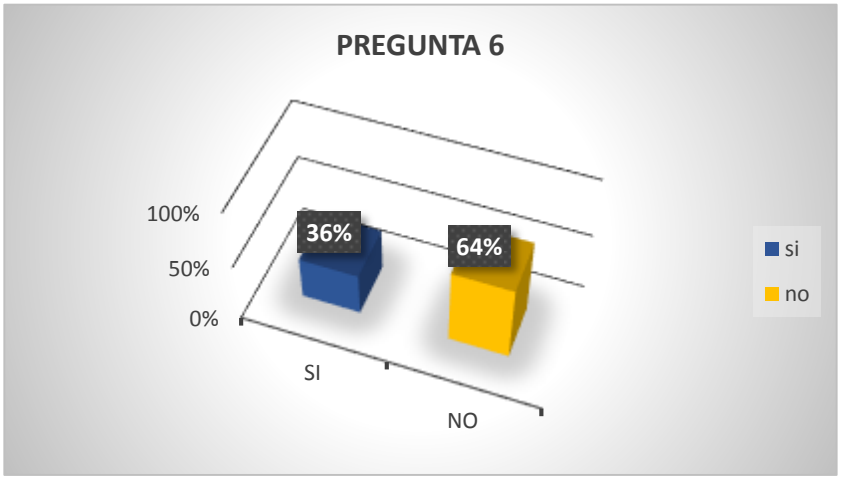
**GRÁFICO N° 4**




En la pregunta 5 acerca de los registros públicos y privados y su debida protección, un 64% afirma que sus datos tendrían que estar protegidos debidamente y un 36% indica que no es necesario la debida protección. Esta respuesta nos presenta un panorama de que una parte de la población no le da la debida importancia a la protección de sus datos personales o desconoce los procedimientos de protección.

6. ¿Conoce en qué consisten los derechos (Información, Acceso, rectificación, cancelación, supresión, olvido y oposición) aplicable a sus datos personales.

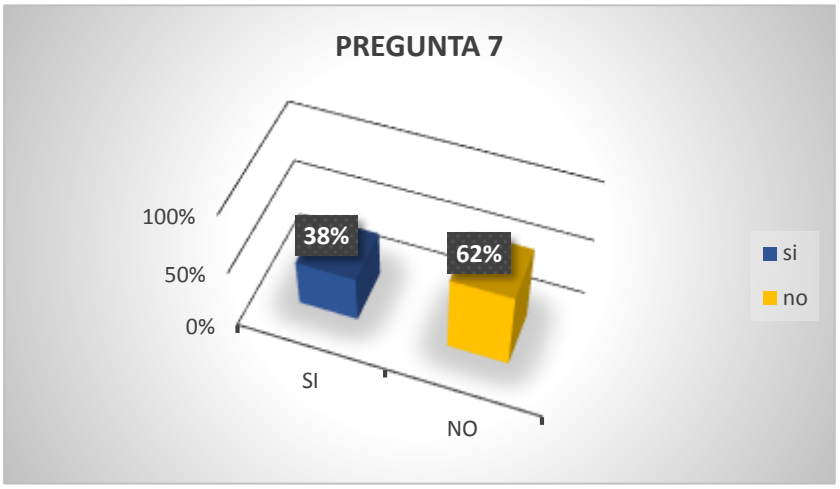
**GRÁFICO N° 5**



Con relación a la pregunta 6 el 64% señala no tener conocimiento acerca de sus conocimientos sobre sus derechos a la protección de datos personales, el restante 36% afirma conocer sus derechos relacionados a la protección de datos.

7. ¿Alguna empresa o entidad le ha pedido consentimiento para el uso de sus datos personales? (ejemplo: empresas de telefonía, seguros, bancos)

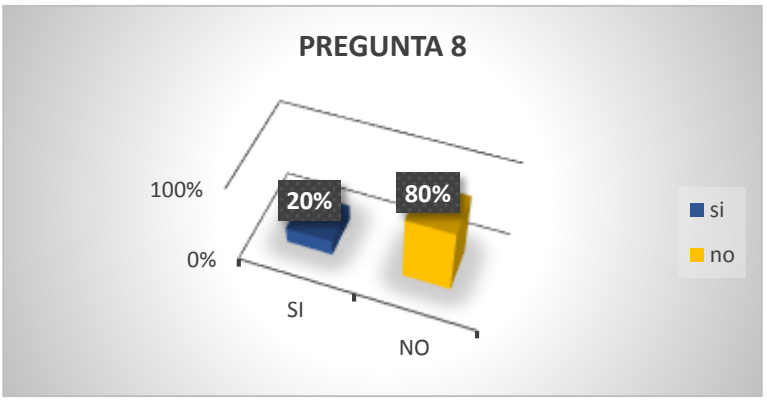
**GRÁFICO N° 6**




Con respecto a la pregunta N° 7, relacionado al consentimiento para el uso de datos personales, el 62% indica no haber proporcionado sus datos a ninguna institución que la haya solicitado, el 38% restante señala si haber proporcionado información al respecto. Esta información nos muestra como la población no tiene una real conciencia de los momentos en que está dando a conocer su información íntima o privada.

8. ¿Conoce usted alguna institución encargada de fiscalizar el acceso a datos personales y si estos tienen un control y sanción para aquellos que atenten contra su honor, privacidad, imagen, intimidad y puedan ser denunciados y sancionados ante autoridad competente?

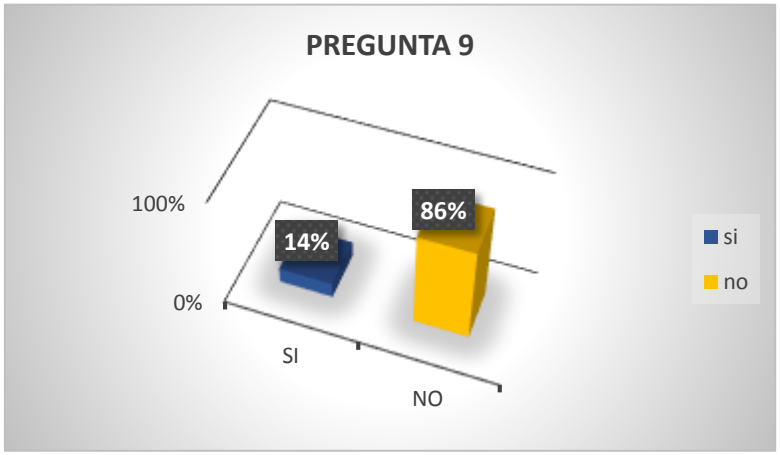
**GRÁFICO N° 7**




Acerca de la pregunta N° 8 planteada a la población el 80% expresó no tener conocimiento sobre una instancia o institución fiscalizadora sobre la protección de datos el restante 20% afirma si tener conocimiento al respecto. Esto implica que un gran porcentaje tiene claridad acerca de la necesidad de que se instaure una oficina específica de control de datos personales.

9. Sabe usted cuando debe presentar el recurso de acción de protección de privacidad, o conocido también como el habeas data?

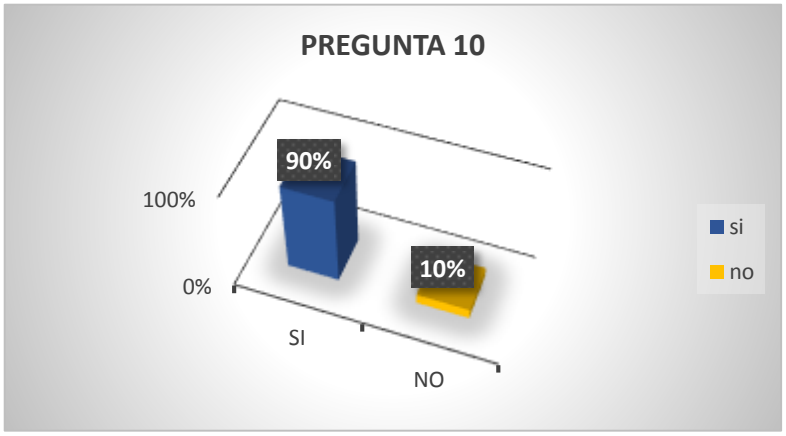
**GRÁFICO N° 8**



El 86% de los encuestados indica no tener conocimiento sobre este recurso de habeas data en cuanto a la protección de datos personales; el 14% afirma conocer esta acción de protección de privacidad. La mayor parte de las personas sin embargo no tienen conocimiento sobre esta acción en materia de protección de datos personales, lo que nos muestra que la mayor parte de la población ignora sobre sus derechos personales y cuanto hace falta trabajar y socializar a todo nivel de la población.

10. ¿Considera usted importante y necesario que sus datos personales deben ser protegidos, en el sistema informático y la tecnología actual?

**GRÁFICO N° 9**




Con respecto a la pregunta N° 10, el 90% afirma que si es necesario e importante que sus datos personales sean protegidos y el 10% considera que no. Los porcentajes que se pueden apreciar nos llevan a realizar un análisis en el sentido de que realmente la mayoría considera que los datos personales son de real importancia en cuanto su protección, aún más considerando que estamos viviendo una época con auge de la tecnología y la informática y el riesgo de vulneración es mayor.

## 5.3. ENTREVISTAS

Como otra técnica aplicada en la investigación fueron las entrevistas realizadas con profesionales y abogados de quienes se ha recabado información actualizada sobre los conceptos y criterios técnicos jurídicos que tienen ellos sobre la protección de los datos personales y la situación actual en nuestro país.

Algunos de los entrevistados dan a conocer de manera taxativa que nuestro país tiene a la constitución como la norma básica y fundamental de protección de nuestros datos personales, asimismo las normas sectoriales son aquellas que contienen aquellos articulos referentes a la protección de la información privada otorgada a las distintas instituciones que la requieren.

Se puede acudir a la constitución a requerimiento personal para solicitar información u otra acción sobre nuestros datos personales y mediante el juez está autorizado legalmente para dar respuesta a este requerimiento.

Otro grupo de profesionales, abogados, se inclina por que se tengan mecanismos de control adecuados que eviten la vulneración de los derechos de los usuarios. Se tiene que realizar el control efectivo para establecer o identificar las instituciones o instancias donde se vulneran con mayor frecuencia los derechos a la intimidad de las personas.

Otras opiniones con toda certeza afirman que a diario usamos aplicaciones móviles y el navegador de internet para diversas actividades, para comunicarnos, mantenernos informados, realizar compras y ventas, entretenernos, efectuar operaciones bancarias, trabajar, entre otras. Definitivamente, vivimos en un mundo interconectado.

Como usuarios nos damos cuenta fácilmente las ventajas de vivir conectados. No obstante, existe otro aspecto que no siempre es evidente porque sucede detrás de nuestras pantallas, se habla del uso y tratamiento de nuestros datos personales.

En muchas partes del mundo (incluida América Latina) los países cuentan, desde hace varios años, con leyes generales de protección de datos, que ponen límites a la recolección y análisis de información personal y reconocen derechos a los usuarios para evitar abusos y controlar el funcionamiento de la tecnología. Sin embargo, como la tecnología avanza y cada vez estamos más interconectados, las leyes suelen quedar desactualizadas; se requieren nuevas y más sofisticadas herramientas para garantizar un uso adecuado de los datos personales más allá de los límites geográficos, porque la atención primordial está puesta en el interés y los derechos de los usuarios.

# CAPÍTULO VI

# PROPUESTA DE LA INVESTIGACIÓN

## 6.1. JUSTIFICACIÓN PARA PLANTEAR UNA LEY DE DATOS PERSONALES EN BOLIVIA DE MANERA ESPECÍFICA

Bolivia es uno de los países que aún no cuenta con una ley específica de protección de datos personales. Al momento, solo se cuentan con leyes que tocan algunos temas de datos personales, pero lo hacen de manera incompleta y no integral.

La protección de datos de carácter personal es un derecho que tienen todos y cada uno de los ciudadanos y que los mismos no sean utilizados por el acceso de terceros y al mismo tiempo corran el riesgo de ser manipulados sin la autorización debida del titular.

La falta de fiscalización hace que se efectúen negocios con bases de datos. Esta situación, es aún peor en países donde ni siquiera hay ley de protección de datos que permita fiscalizar estos negocios. Por ejemplo, en Bolivia, también hay uso no autorizado de bases de datos personales por parte de particulares; la venta o cesión de bases de datos personales de supermercados, empresas de seguros, entre otros está a la orden del día.

Los datos personales, al revelar información importante de los usuarios, son muy valiosos para distintas finalidades y actores. Es por ello que resulta de mucha importancia que, como usuarias y usuarios, se tenga conocimiento de esta situación y se conozcan los derechos para no ser las próximas víctimas de un tratamiento indebido de los datos personales.

Hoy en día, los datos personales son elementos imprescindibles para llevar acabo cualquier tipo de acto o actividad dentro de nuestra sociedad; por ejemplo actos

judiciales, financieros, de identificación, actos laborales, actividades donde se involucran servicios médicos y otros.

Es evidente en la actualidad que la difusión de información por internet es una realidad, y que así mismo, tiene gran aceptación en la población, sin embargo, al encontrarse esta información en Internet, están sujetos a ataques cibernéticos por hackers o piratas informáticos, los cuales se aprovechan de vulnerabilidades que pueda tener el sistema y efectuar ataques a estos sitios.

Todos los sistemas informáticos de entidades públicas contienen una cantidad considerable de datos e información referente a su actividad, asimismo contiene datos personales de los empleados y de las personas que se someten a determinado tratamiento.

La legislación boliviana no puede permanecer ajena a la falta de medidas legales que exijan a las entidades públicas contar con los requisitos de seguridad de información y a su vez debe regular una protección de datos personales ante los avances tecnológicos del internet, por lo que será imprescindible, exigir de manera obligatoria la existencia de los sistemas de controles de seguridad de información adecuados para la creación de los sitios web con el fin de proteger, los datos personales registrados.

En tal sentido se hace necesario la intervención del Estado para que se garantice no solamente el derecho de los ciudadanos de estar informados y de transparentar sus acciones gubernamentales, asimismo garantizar jurídicamente el derecho a la protección de datos personales respetando los principios de protección de los mismos.

Es fundamental crear mecanismos de control o el establecimiento de un organismo de protección de los datos personales para que regule de manera efectiva el uso

que pueda hacerse de los datos personales, además de ser una instancia para hacer valer los procedimientos jurídicos, como sucede en muchos países de Europa fundamentalmente.

Muchos sistemas de información ofrecen sus servicios al público, abriendo las puertas a la difusión o mal uso de las informaciones sensibles. Por esta razón, resulta indispensable establecer normas jurídicas que garanticen la protección al Derecho a la Privacidad y la Intimidad de los usuarios.

Se hace imprescindible crear un marco jurídico más amplio y eficiente que proteja los datos e información que proporcionen los ciudadanos no sólo a los sitios web de las empresas, sino sobre todo a los órganos gubernamentales, a los registros públicos y privados cuyos servicios se ofrecerán completamente en línea como va sucediendo actualmente.

La inclusión de la Acción de Protección a la Privacidad o también conocido como el Habeas Data, tan moderno en la Constitución Política del Estado de Bolivia, es un gran adelanto en dirección hacia la modernidad y el reconocimiento a la imperiosa necesidad de proteger la intimidad y los datos de las personas.

Nuestro país no puede quedar al margen de la imperiosa necesidad de establecer nuevas garantías que surgen a propósito del desarrollo tecnológico virtual y sus repercusiones en los derechos y garantías de los ciudadanos, el propósito de regular el acceso a los datos personales en los registros públicos y privados tiene por objeto brindar adecuada protección de los datos personales de los ciudadanos de Bolivia y que estén a la altura de las normas internacionales.

## 6.2. ANTEPROYECTO DE LEY DE PROTECCION DE DATOS PERSONALES EN BOLIVIA

**LEY Nº…….. DE …….. DE …… DE 2021**

**Capítulo I**

**Disposiciones Generales**

**ARTICULO 1. (Objeto).**

La presente ley tiene por objeto la protección de los datos personales establecidos en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información.

**ARTICULO 2. (Finalidad de la Ley).**

La finalidad de la ley es contribuir en la concreción del derecho que tiene toda persona a la protección de sus datos personales establecidos en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados y para garantizar el derecho al honor y a la privacidad de las personas.

**ARTICULO 3. (Ámbito de aplicación).**

La presente ley es de orden público y de aplicación en lo pertinente en todo el territorio nacional.

Será de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero, realizado por las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

**ARTICULO 4. (Definiciones).**

A los fines de la presente ley se entiende por:

1. Datos personales: Cuando se habla de datos personales, nos estamos refiriendo a datos que contienen información sobre o relativos a una persona. De esta manera, un dato personal es igual a la información sobre una persona. Algunos ejemplos bastantes conocidos son el nombre, la dirección, el teléfono, el correo electrónico y hasta el historial médico y los antecedentes penales. Estos datos nos dan información sobre una persona en particular. Actualmente no sólo son datos personales las informaciones que identifican a una persona directamente sino también aquellas que la hacen identificable tras un análisis posterior; ejemplo de esto son las imágenes de las cámaras de video vigilancia o la ubicación GPS.

   Toda esta información es clave y revela detalles íntimos sobre la vida personal y familiar.
2. Datos sensibles: son aquellos que preferimos mantener en reserva y que pueden causar daños graves si son difundidos o mal utilizados; ejemplos de estos datos sensibles son los concernientes a la salud, la genética, la religión, las preferencias políticas, y hasta aquellos que denotan ingresos económicos o preferencias sexuales.
3. Archivo, registro, base o banco de datos: Se designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.
4. Tratamiento de datos: Es toda actividad que se realiza con los datos personales, y comprende desde su recopilación y almacenamiento hasta actividades más complejas como un análisis con inteligencia artificial.

   Dicho tratamiento puede ser manual (como el que se hace en papel) o automatizado que es aquel que emplea software para analizar información a gran escala.

5. Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.
6. Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.
7. Datos anonimizados o disociados: Estos son datos que en principio permiten identificar a personas pero que gracias a mecanismos de anonimización o disociación terminan teniendo poca o nula relación con la persona que antes identificaban.
8. Los metadatos: Estos son los llamados “datos sobre los datos”, puesto que son datos que se obtienen al analizar otros conjuntos de datos; esto incluye, por ejemplo, algunos datos de navegación en internet e información sobre comunicaciones entre personas (a qué hora se mandó un SMS, en qué ubicación GPS se tomó una foto, etc)
9. Titular de los datos: Referida a toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.
10. Usuario de datos: Es toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

## Capítulo II

## Principios generales relativos a la protección de datos

**ARTICULO 5. (Archivos de datos – Licitud).**

La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia.

Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.

**ARTICULO 6. (Calidad de los datos).**

1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.

3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.

5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.

6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

**ARTICULO 7. (Consentimiento).**

1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información

2. No será necesario el consentimiento cuando:

a) Los datos se obtengan de fuentes de acceso público irrestricto;

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

**ARTICULO 8. (Información).**

Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

**ARTICULO 9. (Categoría de datos).**

Ninguna persona puede ser obligada a proporcionar datos sensibles.

Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

**ARTICULO 10. (Seguridad de los datos).**

1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.
2. Está prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

**ARTICULO 11. (Deber de confidencialidad).**

1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos; tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.

2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

**ARTICULO 12. (Cesión).**

Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.

**ARTICULO 13. (Transferencia internacional).**

Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.

## Capítulo III

## Derechos de los titulares de datos

**ARTICULO 14. (Derecho de Información).**

Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables.

**ARTICULO 15. (Derecho de acceso).**

El titular de los datos, previa acreditación de su identidad, tiene derecho a conocer de primera mano si un ente privado o de gobierno tiene o trata nuestros datos; este derecho incluye el de obtener una copia de ese archivo.

**ARTICULO 16. (Derecho de rectificación).**

El titular tiene derecho a corregir y actualizar los datos personales que estén almacenados en bases de datos; por ejemplo, podríamos querer actualizar nuestro estado civil o el registro de deudas que figura en servicios de información crediticia.

**ARTICULO 17. (Derecho a revocar el consentimiento o cancelación).**

Toda persona puede retirar dicho consentimiento cuando el tratamiento de los datos sea excesivo, no pertinente, inadecuado, entre otros; ello significa que el responsable del tratamiento deberá dejar de tratar los datos personales del titular.

**ARTICULO 18. (Derecho de supresión).**

Toda persona luego de terminado el uso de un servicio, tiene el derecho de solicitar que el responsable elimine todos los datos personales que lo conciernen.

**ARTICULO 19. (Derecho al olvido).**

Toda persona puede pedir que se disocie de los buscadores en internet aquella información personal que ya no sea relevante.

**ARTICULO 20. (Derecho a la oposición).**

El titular tiene el derecho a oponerse a la recolección o tratamiento de su información personal ante ciertos casos puntuales, que cada legislación determina en función de objetivos de política pública; estos son los casos en los que se puede oponer previamente al tratamiento de sus datos con fines de marketing o si se hace para la toma automatizada de decisiones que nos conciernen.

**ARTICULO 21. (Derecho a la portabilidad).**

El titular de los datos tiene el derecho de poder movilizar sus datos personales de una base de datos a otra; ello puede implicar solicitar al responsable del tratamiento una copia o el original de toda nuestra información en un formato compatible que permita trasladarla a otro proveedor de servicios.

**ARTICULO 22. (Derecho a la explicación).**

Toda persona tiene el derecho de permitir obtener explicaciones sobre las decisiones que se realizan mediante el tratamiento automatizado de su información personal; es el caso de las decisiones que se toman mediante sistemas de inteligencia artificial o algoritmos.

## Capítulo IV

## Usuarios y responsables de archivos, registros y bancos de datos

**ARTICULO 23. (Registro de archivos de datos).**

Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control.

**ARTICULO 24. (Archivos, registros o bancos de datos privados).**

Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme a criterios previamente establecidos.

**ARTICULO 25. (Archivos, registros o bancos de datos con fines de publicidad).**

En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.

**ARTICULO 26. (Prestación de servicios de información crediticia).**

En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

## Capítulo V

## Control

**ARTICULO 27. (Órgano de Control).**

1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley.

a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza;

b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley;

c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos;

d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley;

e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados;

f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia;

g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley;

h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley.

2. El órgano de control gozará de autonomía funcional.

3. El órgano de control será dirigido y administrado por un Director designado para el efecto.

## Capítulo VI

## Sanciones

**ARTICULO 28. (Sanciones administrativas).**

Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan.

**ARTICULO 29. (Sanciones penales).**

Incorpórese el artículo 363 Bis. (MANIPULACIÓN INFORMÁTICA). del Código Penal:

El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno (1) a cinco (5) años y con multa de sesenta (60) a doscientos (200) días.

Incorpórese el artículo 363 Ter. (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS). El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un (1) año o multa hasta doscientos (200) días.

## Capítulo VII

## Autoridad nacional de protección de datos personales

**Artículo 30. (Órgano competente y régimen jurídico)**

El Ministerio de Justicia y transparencia institucional, es la Autoridad Nacional de Protección de Datos Personales.

La Autoridad Nacional de Protección de Datos Personales se rige por lo dispuesto en esta Ley, en su reglamento y en los artículos pertinentes del Reglamento de Organización y Funciones del Ministerio de Justicia.

Corresponde a la Autoridad Nacional de Protección de Datos Personales realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la presente Ley y de su reglamento.

La Autoridad Nacional de Protección de Datos Personales debe presentar periódicamente un informe sobre sus actividades al Ministro de Justicia.

**Artículo 31. (Funciones de la Autoridad Nacional de Protección de Datos Personales)**

La Autoridad Nacional de Protección de Datos Personales ejerce las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras siguientes:

1. Representar al país ante las instancias internacionales en materia de protección de datos personales.
2. Cooperar con las autoridades extranjeras de protección de datos personales para el cumplimiento de sus competencias y generar mecanismos de cooperación bilateral y multilateral para asistirse entre sí y prestarse debido auxilio mutuo cuando se requiera.
3. Administrar y mantener actualizado el Registro Nacional de Protección de Datos Personales.
4. Publicitar, a través del portal institucional, la relación actualizada de bancos de datos

personales de administración pública y privada.

5. Promover campañas de difusión y promoción sobre la protección de datos personales.

6. Promover y fortalecer una cultura de protección de los datos personales de los niños y de los adolescentes.

7. Coordinar la inclusión de información sobre la importancia de la vida privada y de la protección de datos personales en los planes de estudios de todos los niveles educativos y fomentar, asimismo, la capacitación de los docentes en estos temas.

8. Supervisar el cumplimiento de las exigencias previstas en esta Ley, para el flujo transfronterizo de datos personales.

9. Emitir autorizaciones, cuando corresponda, conforme al reglamento de esta Ley.

10. Emitir las directivas que correspondan para la mejor aplicación de lo previsto en esta Ley y en su reglamento, especialmente en materia de seguridad de los bancos de datos personales, así como supervisar su cumplimiento, en coordinación con los sectores involucrados.

11. Promover el uso de mecanismos de autorregulación como instrumento complementario de protección de datos personales.

12. Conocer, instruir y resolver las reclamaciones formuladas por los titulares de datos personales por la vulneración de los derechos que les conciernen y dictar las medidas cautelares o correctivas que establezca el reglamento.

13. Velar por el cumplimiento de la legislación vinculada con la protección de datos personales y por el respeto de sus principios rectores.

14. En el marco de un procedimiento administrativo en curso, solicitado por la parte afectada, obtener de los titulares de los bancos de datos personales la información que estime necesaria

para el cumplimiento de las normas sobre protección de datos personales y el desempeño de sus funciones.

15. Supervisar la sujeción del tratamiento de los datos personales que efectúen el titular y el encargado del banco de datos personales a las disposiciones técnicas que ella emita y, en caso de contravención, disponer las acciones que correspondan conforme a ley.

16. Iniciar fiscalizaciones de oficio o por denuncia de parte por presuntos actos contrarios a lo establecido en la presente Ley y en su reglamento y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento.

17. Las demás funciones que le asignen esta Ley y su reglamento.

## Capítulo VIII

## Acción de protección de los datos personales

**ARTICULO 32. (Procedencia).**

La acción de protección de los datos personales o de hábeas data considerado como un derecho fundamental cuya finalidad primordial es preservar el derecho a la autodeterminación informativa, garantía procesal constitucional para tutelares derechos fundamentales ligados a la intimidad y privacidad.

Con la aplicación de los siguientes principios:

1° Principio de información oficial de la existencia de ficheros públicos o privados

2° Principio de la necesidad del consentimiento libre, expreso e informado

3° Principio de la veracidad de los datos

4° Principio de acceso, actualización, rectificación, confidencialidad y cancelación de datos.

5° Principio de responsabilidad

6° Principio de la protección reforzada de datos sensibles

7° Principio de secreto

8° Principio de seguridad

9° Principio de oposición

10° Principio de control

11° Principio de celeridad

12° Principio de gratuidad

13° Principio al olvido

**ARTICULO 33.** El Poder Ejecutivo Nacional deberá reglamentar la presente ley y establecer el organismo de control dentro de los ciento ochenta días de su promulgación.

**ARTICULO 34. (Disposiciones transitorias).**

Los archivos, registros, bases o bancos de datos destinados a proporcionar informes, existentes al momento de la sanción de la presente ley, deberán inscribirse en el registro que se habilite y adecuarse a lo que dispone el presente régimen dentro del plazo que al efecto establezca la reglamentación.

**ARTICULO 35.** Los bancos de datos prestadores de servicios de información crediticia deberán suprimir, o en su caso, omitir asentar, todo dato referido al incumplimiento o mora en el pago de una obligación, si ésta hubiere sido cancelada al momento de la entrada en vigencia de la presente ley.

**ARTICULO 36.** Comuníquese al Poder Ejecutivo.

ES DADA EN LA SALA DE SESIONES DEL CONGRESO DEL ESTADO PLURINACIONAL DE BOLIVIA, A LOS …….. DIAS DEL MES DE …….. DEL AÑO DOS MIL…….

— REGISTRADO BAJO EL N° …….. —

# CAPÍTULO VII

# CONCLUSIONES Y RECOMENDACIONES

## 7.1. CONCLUSIONES

- De acuerdo al estudio y análisis efectuado en la presente investigación, el derecho a la privacidad o vida privada es un derecho humano reconocido en los principales instrumentos internacionales, implica la exclusión de los demás, la abstención de entrometimientos por parte de otros. Este concepto del derecho a la vida privada ha ido evolucionando con los avances tecnológicos y surge un nuevo derecho fundamental el cual es la autodeterminación informativa, el control de los propios datos por parte de su titular.

- El derecho a la protección de los datos personales a simple vista parecería que queremos proteger el dato; sin embargo, va más allá. No se está hablando de proteger el dato, sino a la persona que está detrás del dato, es decir a la persona a la cual ese dato identifica o hace identificable. Por lo tanto, a fin de generar esa protección se le brindan herramientas para que controle la información que está relacionada a su persona.

- En estos tiempos existen grandes cambios y transformaciones tecnológicas que hacen necesarias establecer medidas de protección y regulación que brinden seguridad y certidumbre jurídica a los datos de carácter personal. Información que se encuentra en bases de datos o bancos de datos privados o públicos.

- Los casos de abuso de la información personal de los usuarios de internet no pasan de ser hechos noticiosos en países donde no existe una ley de datos personales, como es

el caso de Bolivia. La inexistencia de un marco normativo hace que no se puede ir más allá y cuestionar esos hechos ante las instituciones pertinentes, quedando usuarios y usuarias sin acceso a protecciones y reparaciones básicas por abuso de su información personal.

- Existen ciertos avances legislativos, leyes y normas sectoriales pero es necesaria una legislación integral que sancione incluso la violación a este derecho fundamental. En este sentido es crucial que en Bolivia se legisle al respecto cuanto antes, como ya ha ocurrido en otros países de Europa y América.

- Es de suma importancia la difusión de información por internet y su aceptación por parte de los usuarios, pero esta publicación que tiene base en la creación de sistemas informáticos internos, debe hallarse de manera obligatoria muy bien protegida, permitiendo de esta manera una garantía para los titulares de los datos personales que en esos sistemas internos pudieran haber sido registrados.

- El Habeas Data o Acción de Protección de Privacidad y/o Protección de Datos Personales, es un derecho fundamental cuya utilidad es para que no se comparta la información íntima y para que esta información pueda corregirse, actualizarse o modificarse en todo momento, esta acción puede efectuar solamente el titular.

- De acuerdo a la necesidad actual de nuestro país se plantea una propuesta de ley de regulación y protección de datos personales en el marco del desarrollo tecnológico actual, esta propuesta expresa y da a conocer artículos referentes a los principios jurídicos, formas de control y sistemas de protección de los datos personales.

## 7.2. RECOMENDACIONES

- Además de contar con una ley sobre datos personales, los Estados también deben crear una autoridad con capacidad de hacer cumplir la norma legal. Se recomienda que esta autoridad sea independiente en todo sentido, para que pueda realizar investigaciones, fiscalizaciones y pueda sancionar a cualquier entidad sea esta pública o privada. Asimismo, esta autoridad debe contar con mecanismos robustos de control que le permitan actuar sin retraso.

- Se debe destacar la importancia de contar con una autoridad de protección de datos adecuada; se puede ver en Chile y Brasil, países donde existe legislación pero no se cuenta con una autoridad independiente, haciendo que la ley y sus disposiciones se queden tan solo en el papel.

- Se hace indispensable modernizar los elementos jurídicos con que contamos para proteger a la persona en su esfera de intimidad. Los elementos tecnológicos de uso común hoy en día no pudieron ser imaginados, por lo que la necesidad de protección a las garantías de intimidad, autonomía de las personas y privacidad en sus comunicaciones y manejo de datos personales, requiere un nuevo enfoque.

- Con el uso de internet y con esta tecnología la difusión de información, es crucial el adecuado reconocimiento legal de una protección de nuestros datos personales minuciosa y a profundidad, utilizados o registrados en sistemas informáticos.

- Se recomienda actualizar la normativa de protección de la información de manera permanente acorde a los cambios tecnológicos, a través de una instancia determinada e independiente definida en la ley de protección de datos personales.

- Es fundamental la participación de todos los interesados en diálogo abierto y democrático sobre la norma de protección de datos para Bolivia. La sociedad civil, el sector privado, el sector académico, la comunidad técnica y el gobierno tienen mucho para aportar al debate. Y una ley efectiva deberá contar con la legitimidad y apoyo de todos los sectores para su eficiente creación e implementación. Asimismo, para establecer futuras actualizaciones o modificaciones.

## BIBLIOGRAFÍA


- Aguilar, M.A. (2018). La Ley de Protección de Datos en Colombia: sus inicios y examen de sus principales postulados. https:// repository.ucatolica.edu.co/bitstream/10983/23060/1/La%20Ley%20De%20Protecci%C3%B3n%20D.
- Arroyo, V. (2019). Guía básica sobre datos personales para Bolivia. www.accessnow.org/cms/assets/uploads/2019/03/Guia-Basica-Proteccion-de-Datos-Bolivia.pdf
- Arroyo, V. (2019). Guía para una ley de protección de datos personales en Bolivia. https:/www.accessnow.org
- ASAMBLEA NACIONAL REPÚBLICA DE PANAMÁ. (2019). Sobre protección de datospersonales.https://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/2010/2019/2019_645_3008.pdf
- Athento. (2017). ¿Por qué Canadá es un país seguro para mis datos?. soporte.athento.com/hc/es/articles/115004366045--Por-qu%C3%A9-Canad%C3%A1-es-un-pa%C3
- Botero, B.A. (2003). La metodología documental en la investigación jurídica: alcances y perspectivas. thttps://dialnet.unirioja.es
- Cazurro, V. (2020). Antecedentes y fundamentos del derecho a la protección de datos. www.marcialpons.es/libros/antecedentes-y-fundamentos-del-derecho-a-la-proteccion-de-datos/9788
- COPLUTIC. (2017). Plan de Implementación de Gobierno Electrónico. https://repositorio.uasb.edu.bo:8080/bitstream/54000/1280/1/COPLUTIC-Gobierno%20electr%C3%B3n
- Cortes, S. (2019). Protección de datos: sus orígenes y la privacidad desde el diseño. https:// mujeresenelsectorpublico.com/proteccion-de-datos-sus-origenes-y-la-privacidad-desde-el-diseno
- Decreto Supremo Nº 3525. (2018). https://www.lexivox.org/norms/BO-DS-N3525.html.
- Delgado, I. (2020). Protección de datos personales Bolivia. https://www.protecciónddedatos. bolivia.bo
- Diaz, K., Escudero, S. (2019). Manual de Protección de Datos Personales. https:// www.defensoria.gob.pe/wp-content/uploads/2019/11/Manual-de-Protecci%C3%B3n-de-Datos-Pe
- Durán, M. (2018). Normativa sobre protección de datos personales en Bolivia. https://medium.com/@mrduranch/normativa-sobre-datos-personales-en-bolivia-ece7a61f50b0
- Durán, W. (2006). Contenido y Alcances del Habeas Data en Bolivia. www.corteidh.or.cr/tablas/R08047-12.pdf
- Escobar, G. (2004). Los Derechos Fundamentales y las Telecomunicaciones. https://ebuah.uah.es/xmlui/bitstream/handle/10017/454/Los%20derechos%20fundamentales%20y%20la
- FUNDEMAS. (2014). Qué son los derechos humanos?. https;//fundemas.org/index.php?option=com_content&view=article&id=387&Itemid=80. El Salvador, C.A.
- Gamez, R. (2021). Qué es el Common Law. https://traduccionjuridica.es/que-es-el-common-law

- Herranz, A. (2018). GDPR/RGPD: qué es y cómo va a cambiar internet la nueva ley de protección de datos. https://www.xataka.com/legislacion-y-derechos/gdpr-rgpd-que-es-y-como-va-a-cambiar-internet-la-nueva-ley
- Huerta, P. P. (2017). La génesis del derecho fundamental a la protección de datos personales. (Tesis Doctoral) Universidad Complutense de Madrid, Madrid. Recuperado de https://eprints.ucm.es/43050//1/T38862.pdfA
- Leon, C.C., Quiroz, E., Foronda, A. (2018). Protección de Datos Personales y Derechos Digitales.http://library.fes.de
- López, J. (2014). Antecedentes internacionales en materia de privacidad y protección de datos personales. https://publicaciones.eafit.edu.co/index.php/ejil/article/view/2849/2626
- Mayorga, J.T.C.,Garcia,J.M. (2019). Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos. https://dialnet.unirioja.es
- Mazzoli, R. (2021). Ley de Protección de Datos Personales (PDPA) de Argentina. https:// docs.microsoft.com/es-es/compliance/regulatory/offering-pdpa-argentina
- Medinaceli, K. (2016). El Tratamiento de los Datos Sanitarios en la Historia Clínica Electrónica: Caso Boliviano. https://www.aepd.es/sites/default/files/2019-10/tratamiento-de-datos-sanitarios.pdf
- Melian, V.J (2003). Métodos de la Ciencia Jurídica. https://accedacris.ulpgc.es
- Milenio, Diario, S.A. (2014). Derecho Humano a la Protección de Datos Personales. (https:// www.milenio.com/opinion/varios-autores/derechos-humanos/derecho-humano-a-la-proteccion-de
- Ministerio de Asuntos Exteriores. (2016). Derechos Humanos en el Mundo. www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/DerechosHumanos/Paginas/Derec
- Nisa, A. J. (2020). Origen Jurídico Histórico de la Protección de Datos. https:// elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la
- Nisa,J. (2020). Origen jurídico histórico de la protección de datos: evolución de las diferentes teorías jurídicas que la han protegido. https://elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la-protegido
- Nogueira, H. (2007). El derecho a la propia imagen como derecho fundamental implícito, fundamentación y caracterización. www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122007000200011
- Ortiz, O. (2020). Protección de datos personales en Chile. https://www2.deloitte.com/content/dam/Deloitte/cl/Documents/legal/2020/cl-protecci%C3%B3n-datos-pers
- Perez del Castillo, R., Quiroz, E. (2019). Guia básica sobre datos personales para Bolivia. https://www.accessnow.org.
- Perez, R. M. (2011). La regulación para el acceso a datos en los registros públicos y privados en Bolivia. 2011. https://repositorio.umsa.bo/xmlui/handle/123456789/14189
- Rojas, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales.https://novumjus.ucatolica.edu.co/article/download/652/670
- Saltor, C. E. (2013). La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina. (Memoria grado Doctor).

Universidad Complutense de Madrid. Madrid-España. Recuperado de https://eprints.ucm.es

- Sanchez, Gabriel., Rojas, I. (2018). Leyes de protección de datos personales en el mundo y la protección de datos biométricos – parte I. https://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo.
- Soto, C. C., Espinosa, C. A., Ducuara, C. (2018). Protección de datos personales en los servicios de internet. Universidad Católica, Colombia. Recuperado de https://repository.ucatolica.edu.co
- Sumup. (2021). Privacidad y protección de datos ¡Qué es la privacidad y protección de datos? .https://debitoor.es/glosario/privacidad-y-proteccion-de-datos-personales
- UNIVERSITAT POLITÉCNICA DE VALENCIA (2016, enero 28 ). Historia de la Protección de Datos Personales. www.youtube.com/watch?v=S7uXyCyOwyw
- Villabella. A.C.M. (2015). Los Métodos en la Investigación Jurídica. https://archivos.juridicas.unam.mx.
- Villalta, A. E. (2017). La privacidad y la protección de datos personales. www.oas.org/es/sla/cji/docs/informes_culminados_recientemente_Proteccion_Datos_Personale.
- Zaballos, E. (2013) La protección de datos personales en España: evolución normativa y criterios de aplicación. (Memoria-grado Doctor). Universidad Complutense de Madrid, Madrid España. Recuperado de https://eprints.ucm.es/22849.Madrid, España

# ANEXOS

# ENCUESTA SOBRE PROTECCIÓN DE DATOS PERSONALES

**Finalidad:** Obtener información acerca del conocimiento que tiene la población sobre la importancia de la protección que deben recibir sus datos personales. Dicha información será consolidada e incluida en el Trabajo dirigido "**BASES JURIDICAS FUNDAMENTALES PARA PLANTEAR UNA FUTURA LEY ESPECÍFICA DE PROTECCIÓN DE DATOS PERSONALES EN NUESTRO PAÍS"** aporte para la **UMSA – Carrera de Derecho.**

Sírvase responder de forma anónima, las siguientes preguntas:

1. Edad: _____

2. ¿Cuál(es) son dato(s) personal(es)?

| | | | | | |
|---|---|---|---|---|---|
| Nombre | ☐ | Origen racial o étnico | ☐ | Huella digital | ☐ |
| Numero CI | ☐ | Religión | ☐ | Firma | ☐ |
| Domicilio | ☐ | Dirección electrónica | ☐ | Estado civil | ☐ |
| Afiliación política | ☐ | Fotos | ☐ | Videos | ☐ |

3. ¿Considera que la protección de sus datos personales constituye un derecho fundamental?

Sí ☐ No ☐

4. ¿Conoce de alguna ley que proteja sus datos personales?

Si ☐ No ☐

5. Sabe usted que sus datos personales que proporciona a los diferentes registros públicos y privados tienen que estar protegidos conforme a su identidad personal, intimidad, privacidad, honor, imagen?

Si ☐ No ☐

6. Conoce en qué consisten los derechos (Información, Acceso, rectificación, cancelación, supresión, olvido y oposición) aplicable a sus datos personales?

Si ☐ No ☐

7. ¿Alguna empresa o entidad le ha pedido consentimiento para el uso de sus datos personales? (ejemplo: empresas de telefonía, seguros, bancos )

Sí ☐ No ☐

8. ¿Conoce usted alguna institución encargada de fiscalizar el acceso a datos personales y si estos tienen un control y sanción para aquellos que atenten contra su honor, privacidad, imagen, intimidad y puedan ser denunciados y sancionados ante autoridad competente?

Sí ☐ No ☐ ¿Cuál?

9. Sabe usted cuando debe presentar el recurso de acción de protección de privacidad, o conocido también como el habeas data?

Sí ☐ No ☐

10. ¿Considera usted importante y necesario que sus datos personales deben ser protegidos, en el sistema informático y la tecnología actual?

Sí ☐ No ☐