

Manual operativo de protección de datos en El Salvador

Alfredo Chirino

Colección **Documentos de Trabajo nº 26**

Serie **Guías y Manuales**

Área **Institucionalidad Democrática**



Manual operativo de protección de datos en El Salvador

Alfredo Chirino

Documento de Trabajo nº 26

Serie: Guías y Manuales

Área: Institucionalidad Democrática



PROGRAMA FINANCIADO
POR LA UNIÓN EUROPEA

Edita:

Programa EUROSociAL
C/ Beatriz de Bobadilla, 18
28040 Madrid (España)
Tel.: +34 91 591 46 00
www.eurosocii-ii.eu

Con la colaboración:

Fundación Internacional y para Iberoamérica
de Administración y Políticas Públicas (FIIAPP)



Fundación CEDDET



Instituto de Acceso a la Información Pública



La presente publicación ha sido elaborada con la asistencia de la Unión Europea. El contenido de la misma es responsabilidad exclusiva de los autores y en ningún caso se debe considerar que refleja la opinión de la Unión Europea.

Edición no venal.

Realización gráfica:

Cyan, Proyectos Editoriales, S.A.

Madrid, febrero 2015



No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.

Índice

Prólogos.....	7
Presentación.....	13
Objetivos del manual	17
Estructura	19
Unidad uno.....	21
Objetivos.....	21
1. Derecho a la intimidad	21
2. Derecho a la privacidad.....	24
3. ¿Qué es un dato personal?.....	26
4. Protección de datos personales	29
Síntesis.....	32
Unidad dos	33
Objetivo.....	33
1. Antecedentes de las Leyes de Protección de Datos Personales	33
2. Antecedentes legislativos en materia de protección de datos	39
Síntesis	42
Unidad tres	45
Objetivos.....	45
1. La protección de datos personales en El Salvador.....	45
2. Principios	46
3. Medidas de seguridad	51
4. Tratamiento de datos personales.....	63
5. Obligaciones de los entes públicos.....	65
6. Instituto de Acceso a la Información Pública.....	67
7. Derechos del ciudadano y procedimiento para su ejercicio	69

8. Recursos	74
9. Infracciones	76
Síntesis.....	78
Glosario	81

Prólogo

Uno de los objetivos fundamentales de la Red Iberoamericana de Protección de Datos (RIPD) es, sin duda, la voluntad de extender por toda Iberoamérica una normativa que posibilite la aplicación del derecho a la protección de los datos de carácter personal. Todo ello en paralelo a la creación de unas autoridades que supervisen y controlen su cumplimiento efectivo por parte de los sujetos obligados.

A esta tarea se ha dedicado la RIPD durante estos casi doce años de funcionamiento, especialmente a través de sus talleres de capacitación y de formación, los seminarios temáticos y los Encuentros Iberoamericanos, cuya última edición —la XII— se ha celebrado durante el pasado mes de noviembre en la Ciudad de México.

Ello ha llevado a que la RIPD se haya consolidado como principal promotor del diálogo e impulsor de iniciativas y políticas en la región, que ha significado que más de 150 millones de ciudadanos latinoamericanos dispongan en la actualidad, junto al tradicional amparo de habeas data, de normas que permitan garantizar eficazmente el uso de su información personal y de autoridades especializadas con competencias para tutelar dichas garantías. Hasta el punto de que se puede afirmar, con toda rotundidad, que Iberoamérica es, hoy día, la región del mundo donde se está produciendo un mayor desarrollo del derecho.

En concreto, cuentan hoy día con ley y autoridad propia Argentina, Chile, Colombia, Costa Rica, España, México, Nicaragua (autoridad aún por constituirse), Perú, Portugal y Uruguay. A ello ha contribuido decisivamente la RIPD.

Sin embargo, reconociendo la ingente labor desarrollada hasta la fecha, aún queda mucho por hacer. Quedan amplias zonas de Iberoamérica donde todavía hay que seguir promoviendo procesos de desarrollo legislativo que completen el camino iniciado en 2003. En algunas, ya se han puesto en marcha iniciativas legislativas, como en los casos de Brasil, Chile y Honduras. En otras, en cambio, se necesita diseñar una estrategia que atienda de modo especial a las propias necesidades y características propias de cada país, y que hagan que a medio plazo se puedan empezar a ver resultados.

En una gran parte de estos países que aún carecen de ley y autoridad propia en materia de protección de datos personales, existe una referencia común, como es la existencia de una previa realidad jurídica, muy consolidada, asentada en la transparencia y el acceso a la información, lo que lleva a que la implantación y evolución de la protección de datos en estos países tenga que hacerse teniendo muy en cuenta esta realidad, mediante acciones que favorezcan el diálogo, tratando de dar a conocer a las Administraciones Públicas, al sector privado y a los ciudadanos de estos países la necesidad de contar con una legislación reguladora del derecho, no solo para favorecer los intercambios comerciales con otras zonas del mundo, como Europa, sino, también, para constatar que entre la protección de datos, la transparencia y el acceso a la información no existe incompatibilidad alguna entre ellos, sino que es un complemento necesario para reforzar las garantías de los ciudadanos de estos países.

Un ejemplo claro de lo que estamos hablando es Centroamérica. Esta zona de la región ha sido objeto de atención preferente de la RIPD durante los últimos años. Como antes se ha expuesto, ya se han producido algunos frutos significativos en esta estrategia, como es el caso de Costa Rica, que aprobó su ley en septiembre de 2011, y puso en marcha su propia agencia de forma inmediata, siendo en estos momentos la autoridad de referencia en la zona. Un caso especial es Nicaragua, cuya ley se aprobó en marzo de 2012, pero aún sin desarrollo alguno. El otro país centroamericano que está impulsando en estos momentos una iniciativa legislativa es Honduras, concretamente a través del anteproyecto de ley de protección de datos y habeas data propiciado por el Instituto de Acceso a la Información Pública.

Pues bien, a fin de impulsar con fuerza una estrategia de cooperación legislativa entre los distintos miembros de la RIPD de Centroamérica y El Caribe (Cuba y República Dominicana), se organizó el pasado mes de febrero, en el Centro de la Cooperación Española en La Antigua Guatemala, un taller de capacitación impartido por las autoridades de México, España y Uruguay. En el marco de este evento, tuvo lugar una reunión entre representantes de la OEA y de la RIPD para el desarrollo de los trabajos que está llevando a cabo esta organización internacional para la elaboración de un proyecto de ley Modelo de protección de datos personales.

Dentro del espacio centroamericano, El Salvador es objeto de una especial atención por parte de la RIPD. Por tal motivo, desde hace casi dos años se iniciaron los contactos con el Instituto de Acceso a la Información Pública, uno de cuyos comisionados ya participó en el XI Encuentro de Cartagena de Indias, en octubre de 2013. Fruto de esa colaboración, el IAIP solicitó su acreditación como Observador de la RIPD, que se ha hecho efectiva en el XII Encuentro de México, el pasado mes de noviembre.

Es en este contexto en el que hay que enmarcar la celebración del “Taller regional para la construcción del Manual de Acción en Protección de Datos Personales”, impulsado por el IAIP, con el inestimable apoyo de la FIIAPP y de CEDDET, en el marco del Programa

EUROsociAL. Este evento era necesario no solo para promover la deseable capacitación y formación de los empleados y directivos del IAIP en esta materia, sino también para que, a resultas del mismo, se generase una producción documental, como son los Lineamientos y el manual que ahora se presentan, cuya difusión y publicidad entre los diferentes ámbitos de la Administración salvadoreña contribuirá, sin duda, a incentivar el interés y el conocimiento por este derecho fundamental, presupuesto necesario para garantizar el éxito de futuras iniciativas legislativas en este ámbito.

Desde la Red estamos plenamente convencidos de la utilidad de estas iniciativas confiando que, en poco tiempo, den los frutos esperados, que no son otros que posibilitar que los ciudadanos de países, como El Salvador, puedan ser beneficiarios de un sistema normativo que les garantice eficazmente este derecho fundamental. Y en esa tarea, el Instituto de Acceso a la Información Pública tiene un papel protagonista, por lo que desde la RIPD queremos felicitar a su equipo directivo y a todos sus empleados por el encomiable trabajo que están realizando, ofreciéndole todo el apoyo necesario para que puedan seguir garantizando el pleno ejercicio de los derechos de acceso a la información y a la protección de los datos personales.

Jesús Rubí

Adjunto a la Dirección
Agencia Española de Protección de Datos

Prólogo

La promoción de la transparencia y, más concretamente, del acceso a la información al interior del poder público y demás sujetos que manejan fondos públicos debe evolucionar y fortalecerse de la mano del derecho a la protección de datos personales. Los derechos y garantías fundamentales no se vulneran únicamente por la generación de zonas grises o exentas de control, sino también por el inadecuado manejo y custodia de la información de los sujetos, concerniente a su esfera privada.

Los esfuerzos en materia de protección de datos personales en El Salvador aún son incipientes, aunque no se trata de un tema totalmente novedoso o inexplorado. El creciente interés en este derecho a la autodeterminación informativa se deriva del desarrollo acelerado de las tecnologías de la información y de las redes sociales, acompañado de un cambio cultural de empoderamiento de los sujetos que los ha llevado de sentirse “objetos” de derechos y obligaciones a reconocer su calidad de sujetos y eje central del ordenamiento jurídico. En otras palabras, las personas son cada vez más conscientes de su capacidad de exigir explicaciones e imponer límites a las acciones del poder público, incluyendo el reconocimiento de esferas de privacidad a las que solo puede accederse con su autorización y que merecen una protección reforzada. No es casualidad que el artículo 1 de la Constitución reconozca a la persona humana como el origen y el fin de la actividad del Estado, y establezca que está organizado para la concesión de la justicia, de la seguridad jurídica y del bien común.

En El Salvador, el derecho a la autodeterminación informativa se ha construido, fundamentalmente, por medio de la jurisprudencia constitucional¹ y, más recientemente, mediante la aprobación de la Ley de Acceso a la Información Pública (LAIP)². Esta norma representa una conquista en el campo de la protección de datos personales, pues brinda las primeras herramientas para promover la construcción de un sistema jurídico más sólido y definido.

Un régimen apropiado de protección de datos personales es una condición necesaria para la adecuada implementación de nuevas tecnologías que modernicen el Estado y, más concretamente, el quehacer de los entes públicos. La protección de la esfera de

1. Sentencias de la Sala de lo Constitucional de la Corte Suprema de Justicia de El Salvador, emitidas en los Amparos 118-2002, 58-2007, 934-2007, 142-2012 y en la Inconstitucionalidad 36-2004.

2. Decreto Legislativo n°. 534, publicado en el D.O. n°. 70, tomo n°. 391, publicado el 8 de abril de 2011.

privacidad también es un elemento fundamental en la implementación de herramientas de gobierno abierto y en la participación de los sujetos en el diseño, implementación y evaluación de políticas públicas, pues garantiza un uso legítimo de la información que identifique o permita identificar a su titular.

El tema de los datos personales es también un elemento fundamental en el entorno económico y social diferente de la actividad pública. Las nuevas formas de hacer negocios que incorporan las empresas multinacionales y las empresas estatales como sujetos económicos relevantes, así como la deslocalización de los negocios o la ubicación de las cadenas de suministro, producción y distribución en diversas jurisdicciones, demandan invertir esfuerzos en la protección de la información personal que circula en medios electrónicos y físicos, y promover iniciativas que reconozcan la importancia del tema y de su regulación adecuada. Prácticas de protección de datos que adopten estándares y principios reconocidos internacionalmente en la materia son un incentivo adicional para potenciales inversionistas y consumidores o usuarios.

En este contexto, y como parte de la atribución conferida al Instituto de Acceso a la Información Pública para dictar lineamientos para el manejo, mantenimiento, seguridad y protección de datos personales en posesión de las dependencias y entidades (artículo 58 letra “J” de la LAIP), con el apoyo de la cooperación internacional se han llevado a cabo esfuerzos y se ha trabajado de la mano con el consultor Alfredo Chirino Sánchez para la creación de la primera normativa en la materia, que ahora se presenta en la forma de “Lineamientos Generales de Protección de Datos Personales para Instituciones del Sector Público”.

Estos Lineamientos tienen por objeto brindar, tanto a los entes públicos como a los usuarios, herramientas básicas para el adecuado manejo, resguardo, transmisión, destino y obtención de datos personales; así como para el ejercicio, por parte de sus titulares, de los derechos de acceso, rectificación, supresión o eliminación.

Este documento no agota la regulación posible en la materia, pero brinda fundamentos esenciales para resaltar su relevancia en las actividades vinculadas con el poder público; y supone un esfuerzo concreto para la creación y consolidación de un sistema jurídico que reconozca y promueva el derecho de acceso a la información y el derecho a la autodeterminación informativa, como elementos fundamentales para el desarrollo de los sujetos dentro de la sociedad y para su involucramiento activo en la vida política y económica del país, participando de las decisiones del Estado y tomando decisiones informadas, con la certeza de que su esfera de privacidad o intimidad es protegida como garantía y derecho fundamental.

Carlos Ortega

Presidente-Comisionado

Instituto de Acceso a la Información Pública de El Salvador

Presentación

En la actualidad, la mayoría de las relaciones comerciales, transacciones gubernamentales y contratos y actos de comunicación que realizamos en la vida social requieren del intercambio de nuestra información personal. Desde que nacemos somos objeto de la recopilación de gran cantidad de datos, de igual manera en el trabajo, al obtener un seguro de salud, ante la necesidad de adquirir bienes y servicios, así como para realizar trámites ante entidades estatales y privadas, entre muchas otras actividades que realizamos cotidianamente. Para todo ello, requerimos proporcionar o intercambiar datos, que nos identifican y que se relacionan con nuestra vida privada.

El intercambio de este tipo de datos personales que circulan por distintos medios, ha sido potenciado por las así denominadas tecnologías de la comunicación e información, cuyo desarrollo vertiginoso ha permitido la recopilación, tratamiento, comparación y transmisión de millones de datos contenidos en las más variadas y poderosas bases de datos públicas y privadas que almacenan información sobre la vida privada de las personas.

El almacenamiento masivo de información concerniente a las personas, así como su comparación facilitada por estas tecnologías, permite que se creen perfiles de consumo, de uso de determinados servicios, de acceso a páginas Web, de interacción en redes sociales, entre otros. Todo esto provoca una mejor observación de las actividades de los ciudadanos y ciudadanas, lo que implica el riesgo que se construyan perfiles de estas actividades, y, por medio de ellos, definir un concepto o imagen de la persona, que eventualmente podría provocarle consecuencias negativas para su vida. Junto a ello, la circulación permanente de estos datos e informaciones personales hace que el ciudadano y ciudadana pierdan el control de la circulación de estos datos, lo que acarrearía, en muchos casos, que dichos datos pudieran ser utilizados para un fin distinto del que fueron recolectados originalmente, provocando injerencias ilegales en la vida privada, y, por ende una nueva amenaza para los derechos de las personas.

Estos riesgos, provocados por el uso intensivo de los datos e informaciones personales y los peligros que acarrearán para los derechos y libertades ciudadanos, han promovido nuevas formas de interpretación constitucional de la interacción de los seres humanos

con su entorno informativo y motivado la acción del legislador. Es así como se ha introducido en nuestro ordenamiento jurídico una serie de disposiciones para preservar el derecho de los ciudadanos para controlar este flujo de informaciones y la capacidad para auto determinarse en estos nuevos contextos, preservando, al mismo tiempo, su intimidad y privacidad, esenciales para el ejercicio pleno de sus derechos constitucionales. Esto se ha alcanzado con la introducción de previsiones sobre protección de datos en nuestra ley de acceso a la información pública.

El objetivo de estas normas no es obstaculizar el comercio electrónico, el uso de la tecnología o el acceso a la información pública, como tampoco evitar el desarrollo económico o social del país, por el contrario, se trata de conciliar el avance tecnológico con la protección y tutela de los derechos y libertades de las personas.

Luego de un esfuerzo muy intenso del Instituto de Acceso a la Información Pública, y de otras organizaciones del Estado y cooperantes, se emitieron los lineamientos generales para protección de datos personales. Estos lineamientos han permitido definir, organizar y establecer los mecanismos institucionales que le dan al Instituto de Acceso a la Información Pública la guía para cumplir su tarea de regular y fiscalizar las bases de datos personales a cargo del Sector Público. Lo anterior con el fin de verificar que dichos sistemas operan bajo estándares de calidad en materia de seguridad de la información, y asimismo, que se esté brindando adecuada retroalimentación a los ciudadanos, en especial sobre cómo están resguardando la información personal allí recopilada y tratada.

La Ley de Acceso a la Información Pública es, por así decirlo, el punto de encuentro de todas estas preocupaciones constitucionales dirigidas a preservar el derecho de los ciudadanos a acceder a la información de interés público, así como a obtener una protección adecuada de los datos personales en manos de entes y órganos del Estado. Esta ley es, sin dudar, un instrumento mediante el cual será posible apurar los esfuerzos de la administración pública por organizar un adecuado sistema de protección de datos personales, conforme a estándares internacionales.

Es en virtud de las disposiciones legales incluidas en este marco, que los entes públicos obligados deben procurar garantizar la confidencialidad de los datos personales que tienen sobre las personas que atienden, y por ello el tratamiento y gestión de este tipo de información debe ser, a partir de la promulgación de esta Ley, conforme a los mecanismos y disposiciones allí contemplados.

La normativa mencionada contiene definiciones conceptuales del derecho de protección de datos personales; se hace referencia a los sistemas, a la seguridad y tratamiento de los datos personales, así como a las obligaciones de las instituciones competentes en esta materia. De la misma manera, se detallan las atribuciones con que cuenta el IAIP para garantizar el cumplimiento de la LAIP por parte de los entes públicos, y se

establece el procedimiento al que deberán sujetarse tanto particulares como los sujetos obligados en el ejercicio de los derechos de los ciudadanos.

Por lo anterior, el Instituto de Acceso a la Información Pública, pone a su disposición el presente manual de protección de datos personales dirigido al sector público, con el fin de que se constituya en una alternativa de formación del personal a cargo del tratamiento de información personal. Se trata de un instrumento que le permitirá a los funcionarios estatales conocer la legislación vigente en sus diferentes aspectos, así como su puesta en práctica para garantizar los derechos de los usuarios.

Esperamos que el presente manual sea de utilidad al Sector Gubernamental para comprender la importancia que tiene el derecho a la protección de datos personales, como una condición para garantizar el derecho a la autodeterminación informativa de los ciudadanos, y que asimismo, se ejecuten los cambios necesarios para garantizar a la población la protección y el correcto tratamiento de sus datos personales.

Objetivos del manual

Explicar la importancia de la protección de los datos personales como una condición que contribuye a garantizar el derecho a la privacidad de las personas y a su autodeterminación como ciudadanos.

Describir los conceptos que sirven de fundamento a la Ley de Acceso a la Información Pública, en el área de protección de datos personales.

Estructura

La estructura del manual responde a toda la información que requiere el funcionario público para la comprensión de la temática expuesta.

Para facilitar su estudio, el manual está estructurado en tres unidades de aprendizaje, a saber:

- **La unidad uno, “Conceptos y definiciones básicas”:** explica los conceptos de derecho a la intimidad, derecho a la privacidad, datos personales y protección de datos personales.
- **La unidad dos, “Antecedentes de la protección de datos personales”:** define la institucionalización del derecho de protección de datos personales en El Salvador.
- **La unidad tres, “Aspectos relevantes de la Ley de Acceso a la Información pública de El Salvador”:** en lo que toca al tema de protección de datos personales. Explica con detalle todos los aspectos de la ley. Incluye 11 temas, a saber:
 - 1) La protección de datos personales.
 - 2) Definiciones.
 - 3) Principios.
 - 4) Sistemas de datos personales.
 - 5) Medidas de seguridad.
 - 6) Tratamiento de datos personales.
 - 7) Obligaciones de los entes públicos.
 - 8) Instituto de acceso a la información pública.
 - 9) Derechos de los ciudadanos y ciudadanas y procedimiento para su ejercicio.
 - 10) Recurso de revisión.
 - 11) Infracciones.

Así se dividen los temas en las unidades:

- **Título del tema,** que servirá como referencia para identificar la temática específica que se tratará.

- **Introducción**, que ayudará a integrar los conceptos por estudiar en el tema, entender la continuidad con respecto al anterior y preparar al servidor para los contenidos que seguirán.
- **Objetivos**, que mostrarán de manera puntualizada los aspectos por alcanzar cuando finalice el estudio del tema.
- **Desarrollo del tema**, donde se explicarán cada uno de los aspectos referidos al tema.
- **Síntesis**, que servirá como recapitulación de lo visto en el tema, con el fin de prepararlo para su paso al siguiente tema de estudio y ofrecerle una última base para la autoevaluación.
- **Referencias bibliográficas**, que en su conjunto ofrecen una pequeña colección de lecturas recomendadas para profundizar en el estudio de los temas relacionados con la protección de los datos personales.

Unidad uno

Comenzaremos el presente manual con el análisis de los conceptos que están directamente relacionados con las Leyes de Protección de Datos Personales y que constituyen un elemento fundamental para el entendimiento de las disposiciones que contienen, pero más allá de esto, dichos conceptos nos dan elementos para comprender por qué la facultad de decidir sobre el manejo y control de la información que nos concierne juega un papel fundamental en las democracias modernas.

En el tema que nos ocupa, el estudio de la Ley de Acceso a la Información Pública y sus Lineamientos, es importante unificar criterios sobre cada uno de los conceptos a que se hace referencia normativa, para clarificar de mejor manera, el abanico de obligaciones y derechos que nos ofrecen a los ciudadanos y a los servidores públicos.

Objetivos

Conocer y explicar en qué consiste el derecho a la protección de datos personales, a partir de la noción de dato personal.

Reflexionar sobre algunos conceptos directamente relacionados con la protección de datos personales que le conciernen e interesan al ciudadano a lo largo de toda su vida.

1. Derecho a la intimidad

La palabra intimidad proviene etimológicamente del latín *intus* que alude a un ámbito interior, recóndito y por lo mismo escondido y oculto. De aquí la frecuente alusión a la idea de exclusión y reserva que el derecho a la intimidad contiene en su contexto de significado.

Esta idea de exclusión puede comprenderse mejor cuando se conecta este significado de *intus* con la necesidad de los individuos de reservarse un espacio para desarrollar su

esfera personal, es decir, un ámbito donde puedan dedicarse a concretar su libertad y su derecho a ser quienes son, sin límites ni restricciones.

El poder desarrollar libremente nuestra personalidad es una necesidad imperiosa del ser humano, que encuentra este reconocimiento jurídico en el derecho a la intimidad. No se trata únicamente de poder ejercer en libertad nuestro ser, sino hacerlo libres de las intromisiones de otros, que pudieran limitar esta aspiración.

Lo anterior conduce a concluir que lo que ha de entenderse por “intimidad” tiene que ver con una esfera recóndita y reservada en la que se pueden hallar nuestras acciones más personales y la expresión de nuestro ser que no deseamos que llegue al conocimiento público¹.

Es claro entonces que el reconocimiento de la intimidad no solo es fundamental para que los ciudadanos puedan ejercer otros derechos derivados de su personalidad (tales como el derecho a la imagen, al honor objetivo, a la libre expresión), sino que es un límite importante para el Estado, para que tampoco las intromisiones institucionales pongan en peligro ese libre ejercicio de nuestra personalidad².

En una sociedad que ha hecho uso integral de los flujos de información, resulta esencial la tutela de la intimidad, esto no sólo como un resultado natural de los nuevos ámbitos en que los ciudadanos merecen protección jurídica, sino también porque los tradicionales derechos de la personalidad ahora desembocan en otras aspiraciones que podrían verse obstaculizadas por el influjo de la técnica y las posibilidades de observación que estas permiten.

En este documento se habla de protección de datos, así como también de las autoridades encargadas de dicha protección, y esta apelación podría llevar a una primera cuestión de gran validez como es la pregunta de cuál sería la conexión entre esta protección de los datos personales y el ámbito de intimidad de los seres humanos. La respuesta a esta interrogante tiene diversas implicaciones, pero quizá la

1. La jurisprudencia constitucional salvadoreña ha tenido ocasión de referirse a este hecho, al analizar el contenido de intimidad que podría derivarse de la revelación de los contenidos de un paquete postal. Ciertamente es que un paquete de este tipo no es la forma más acabada de intromisión en la intimidad, pero puede revelar aspectos de la vida privada de un ciudadano, y es por ello que el contenido de un envío postal debe quedar preservado del conocimiento de terceros no autorizados, conforme a las previsiones del Artículo 2, inciso 2, Constitución Nacional. Cfr. SALA DE LO CONSTITUCIONAL DE LA CORTE SUPREMA DE JUSTICIA, Sentencia de Habeas Corpus, con referencia No. 135-2005/32-2007 acumulado, de fecha 16 de mayo de 2008, Considerando IV.

2. La Sala de lo Constitucional de El Salvador se ha pronunciado sobre el delicado equilibrio entre los derechos al honor y a la intimidad, por un lado, y los derechos de acceso a la información y a la expresión, por el otro, indicando que estos derechos se encuentran recíprocamente limitados, por lo que la protección normativa de estas libertades debe garantizarse. Es por ello que la revisión sobre los eventuales conflictos entre estos derechos debe hacerse caso por caso, con el fin de observar cuál prevalecerá y en qué circunstancias. Cfr. Sala de lo Constitucional, Sentencia de Inconstitucionalidad, con referencia No. 91-2007, de 24 de septiembre de 2010. En la cual el peticionario Roberto Bukele, promueve proceso de inconstitucionalidad a fin de que se declare la inconstitucionalidad del art. 191 incs. 2° y 3° del Código Penal, por los supuestos vicios de contenido consistentes en violación a los Arts. 2, 3, 6 y 144 de la Constitución.

más importante de ella es que la protección de los datos personales es en realidad una protección de las personas frente a ese flujo de informaciones que ya no puede controlar por sus propios medios y que implica para ellas posibles restricciones, obstáculos o la inhibición del ejercicio de otros derechos y libertades que ostentan como ciudadanos en una sociedad que se tecnifica cada vez más³.

Más precisamente aún, protección de datos personales es la protección de la vida privada de las personas en una nueva era donde el influjo de la técnica y los vertiginosos cambios en el tejido social provocados por su influencia, aumentan los riesgos para la vida privada y para el desarrollo de la autodeterminación de las personas. Se trata de la protección de la persona en una sociedad que se automatiza a pasos agigantados, y centra su interés en el control de los datos e informaciones personales.

El ejercicio del derecho a la intimidad suele entenderse dogmáticamente como un derecho en dos fases. La primera de ellas, denominada muchas veces “pasiva”, es la que se refiere al derecho ser dejado solo o en paz. Se trataría de la fase más vinculada al reconocimiento básico del derecho a ejercer nuestra libertad de ser nosotros mismos. La segunda fase, también denominada “activa”, tiene que ver con el derecho a controlar el flujo de los datos personales, que es precisamente la que le da sentido al principio de autodeterminación.

Es común imaginar que la regulación jurídica de estas dos fases del derecho a la intimidad, no es fácil, y que hacerlo en una sociedad marcada profundamente por el signo tecnológico es todavía más difícil. Basta imaginar las mil maneras en que la información personal es procesada, transmitida y reconstruida para los más diversos efectos comerciales, de mercadotecnia e investigación penal, solo para citar sus usos más frecuentes. Todos estos usos abarcan diversos riesgos y peligros para la intimidad de las personas, y obligan a la consideración de regulaciones jurídicas precisas⁴.

Se trata de la construcción de un “ambiente informativo” en que los seres humanos, con dificultad, pueden mantenerse al tanto de los diversos usos de sus datos personales. Es un fenómeno moderno en donde el derecho mantiene cierto rezago, pero normativamente existen experiencias exitosas, que demuestran que es posible mantener

3. Al igual que en algunos otros países, el reconocimiento del derecho a la autodeterminación informativa, en su modalidad de protección judicial, fue reconocido en El Salvador en 2004. Fue la Sala de lo Constitucional, en un proceso de amparo constitucional contra una compañía dedicada a la comercialización de datos personales (proceso DICOM), donde se reconoció el así denominado derecho al habeas data. Este derecho se definió como una protección judicial del derecho de los ciudadanos a acceder a sus datos personales, a conocer la información que existe sobre él y solicitar las correcciones del caso cuando pudiere derivarse daños o perjuicios de esas inexactitudes. Cfr. Sentencia de Amparo 118 -2004 del día 2 de marzo de 2004, Considerando III.

4. La Sala de lo Constitucional de El Salvador consideró, con razón, que el derecho a la intimidad no es un derecho absoluto libre toda ingerencia privada o estatal. Es claro que la vida de convivencia requiere de la entrega de información de carácter personal, tanto para trámites y gestiones cotidianas en el mundo laboral y del comercio, así como también institucionales derivadas de la investigación fiscal o de los delitos. Tales intromisiones deben aceptarse, no obstante, el derecho a la autodeterminación informativa existiría para evitar el uso abusivo de estos datos personales. Sentencia de Amparo Referencia, 118-2002 de 02 de Marzo de 2004.

un equilibrio adecuado entre los nuevos desarrollos tecnológicos y los usos intensivos de información con los derechos de los ciudadanos a saber quién, cuándo, dónde y bajo qué circunstancias está teniendo acceso a sus informaciones de carácter personal.

2. Derecho a la privacidad

Junto al derecho a la intimidad, tal y como lo hemos observado anteriormente, y en una condición de derecho de exclusión a otros de un ámbito de desarrollo de nuestra personalidad, se ha venido hablando también de la “privacidad”, casi sin distinción, no obstante, hay algunas diferencias interesantes entre ambos conceptos. Por un lado, la privacy se desarrolla en la tradición inglesa y es producto del avance de los medios y de la difusión de información, como forma de tutela contra la injerencia arbitraria en la vida de los ciudadanos. Se considera que la base dogmática de construcción de este derecho es el artículo publicado en la Harvard Law Review por parte de dos juristas estadounidenses: Samuel Warren y Louis Brandeis. Este artículo científico de 1890 pone el énfasis en el poder invasivo de los medios de prensa y el grave riesgo que dicho poder implicaba para la vida privada. El resultado final de esta propuesta era desarrollar el derecho a ser dejado solo (right to be let alone) como garantía frente al abuso de los medios y la intromisión de los mismos en el ámbito de la vida privada⁵. De otra parte, el derecho a la intimidad tiene que ver con el fuero de lo más reservado, lo que ha quedado totalmente fuera del escrutinio público. Si se trata de intensidades, lo íntimo es todavía más exclusivo y reservado que lo privado. Datos de lo privado podrían llegar a conocimiento público, sin que tal acción acabe con el contenido esencial de ese derecho. Lo íntimo requiere una tutela que la preserve de tal invasión, de lo contrario su contenido podría ser destruido, pues se trata de una relación del sujeto consigo mismo, y cuyo acceso es una donación que hace el sujeto frente a relaciones de amor o amistad⁶.

El concepto de privacidad deriva de la palabra inglesa “privacy” que no tiene una traducción concreta al castellano, pero que alude a un cierto aislamiento de los ciudadanos, y a una expectativa de no ser arrastrados a la publicidad. Se trata, sin duda, de un concepto que tiene que ver con la idiosincrasia anglosajona, pero que ha sido conectada muchas veces también con el problema práctico de la protección de las personas frente al abuso de sus datos personales.

Se ha dicho, no sin razón, que uno de los riesgos más importantes de la vida moderna es que se configuren perfiles de nuestra personalidad conjuntando datos personales

5. Warren, Samuel y Brandeis, Louis, Right to Privacy, Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220. Disponible en: <http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf>.

6. González Gaitano, Norberto. El deber de respeto de la intimidad en la información periodística. En: Agejas, José Ángel. “Ética de la comunicación y de la información”. Editorial Ariel, Barcelona, 2002, p. 172.

desperdigados en diversos bancos de datos y en diversas fuentes públicas o privadas. Esta configuración de perfiles de nuestra personalidad, tanto como consumidores, ciudadanos activos, respetuosos de las leyes, que interactúan cotidianamente, realizando diversas actividades lícitas, podría constituir un riesgo importantísimo para nuestra vida íntima cuando dichos perfiles no responden a la realidad sino que son solo la sumatoria de datos personales que vamos dejando en ese quehacer cotidiano de intercambio de información.

Basta pensar en los diversos perfiles que se pueden realizar de nuestra personalidad si se conjuntan las informaciones que hemos difundido en redes sociales y diversos espacios de intercambio en la Internet. Estos retratos de nuestra personalidad pueden, perfectamente, no coincidir con nuestra verdadera imagen o con la que habíamos escogido compartir con nuestros conciudadanos. Hay aquí, por cierto, un derecho a mantener reservado un cierto ámbito de nuestra intimidad y, por supuesto, un derecho a que estos perfiles no se construyan sin que podamos decidir sobre su configuración.

Los datos con los que se configuran estos “perfiles ciudadanos” provienen de diversas fuentes. La sola interacción social de los ciudadanos puede producir rica información para establecer estos perfiles. Recientemente se ha discutido en la opinión pública mundial, por ejemplo, los “gráficos sociales” con los que los organismos de seguridad recopilan información sobre los ciudadanos, sobre sus contactos, su localización, códigos bancarios, información de la seguridad social, manifiestos de transporte, padrones electorales, registros de propiedad mueble e inmueble. Todos estos datos “desperdigados” son recopilados, tratados y conjuntados, de tal manera que se construyen patrones de conducta y de relaciones que permiten derivar conclusiones sobre las actividades, dedicaciones e ideología de las personas así observadas y clasificadas. Es evidente el riesgo que hay para la privacidad e intimidad de las personas afectadas por estas observaciones de los metadatos.

Estas intervenciones del Estado y de los organismos de seguridad son verdaderas intromisiones en el espacio íntimo de los ciudadanos, no suficientemente justificadas por los temores derivados, por ejemplo, del combate de la criminalidad organizada o del terrorismo, para sugerir dos de los justificantes más frecuentes. Ya ni las así denominadas informaciones sensibles quedan fuera de este frenesí del control. Los ciudadanos son etiquetados y perfilados con el objetivo de reducir el riesgo que pudieran significar, cuando ni siquiera se sospecha de un acto antijurídico de su parte.

Volviendo al tema de la “privacidad” y su diferenciación con la “intimidad” podemos concluir que ambos conceptos tienen mucho en común, se traslapan en sus contenidos y terminan garantizando un control del flujo de informaciones sobre uno mismo, evitando toda injerencia en hechos relativos al ámbito de exclusión que no haya sido consentida.

Por lo anterior, es posible comprender el valor esencial del concepto de “dato personal” y el papel que cumple en este análisis jurídico de la tutela de la intimidad y la privacidad de la persona en la sociedad tecnológica.

Una acepción muy frecuente del concepto de “dato personal” alude a aquellas informaciones que puedan vincularse a un individuo. Desde hace ya varias décadas se la conceptúa como toda información relativa a una persona identificada o identificable, entendiendo por esta última, aquella persona que pueda determinarse utilizando datos tales como el número de identificación, o sus características físicas, su posición socioeconómica, cultural o social, entre otros.

3. ¿Qué es un dato personal?

Los datos personales aluden, por ello, a toda información que es posible vincular con nuestra persona y que en virtud de tal vinculación nos identifica o permite nuestra identificación.

La Ley Orgánica de Protección de Datos Personales de España, por ejemplo, en su artículo 3. a), los define como *“cualquier información concerniente a personas físicas identificadas o identificables”*, definición que luego es completada por el artículo 5.1.f) del Reglamento a dicha ley, que indica que dato personal es *“cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables”*.

Los datos personales, pues, permiten identificar características de nuestra condición de ciudadanos. Todo aquello que aluda a nuestro origen, edad, lugar de residencia, o a nuestra trayectoria académica, laboral o profesional, podría servir para identificarnos sin lugar a dudas. Sin embargo, hay otros datos todavía más específicos, que podrían dar información sobre nuestra religión, ideología, escogencia sexual, entre otros aspectos. Estos datos son usualmente conocidos como datos sensibles.

Datos personales: toda información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física identificada o identificable.

Dentro de la Ley de acceso a la Información Pública y sus lineamientos, se establecen los principios, derechos, obligaciones y procedimientos que regulan la protección y tratamiento de los datos personales en posesión de los entes públicos. Podemos decir entonces lo siguiente:

Datos personales: toda información numérica, alfabética, gráfica acústica o de cualquier otro tipo concerniente a una persona física identificada o identificable.

Ejemplo de ello son el origen étnico o racial, características físicas, morales o emocionales, la vida afectiva y familiar, el domicilio y teléfono particular, correo electrónico no oficial, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas y filosóficas, estado de salud, preferencia sexual, la huella digital, el ADN y el número de seguridad social, y análogos.

En esta definición se incluye toda aquella información que se relaciona con una persona y que a través de ella se le puede reconocer como por ejemplo, el nombre, firma, huella, fotografías, imágenes de vídeo e incluso grabaciones sonoras.

Las definiciones de “dato personal” aluden, pues, a toda información disponible que pudiera caer dentro de su rango conceptual. De esta manera, se espera abarcar un gran número de datos que según su naturaleza pudieran entrar dentro de su contenido. Es usual que la determinación de estos datos en su contexto debe hacerse caso por caso, de tal manera que se pueda juzgar su vinculación a la persona.

Opiniones, expresiones del pensamiento, valoraciones, datos sobre situación socioeconómica o laboral, sobre nuestra salud o perfil genético así como sobre la vida privada o familiar, tienen cada uno su potencial de identificación y de posible incorrección, por lo que sin duda ha de contemplarse la posibilidad de rectificarlos cuando sean incorrectos, inexactos o falsos.

Estos datos pueden estar contenidos en un sinnúmero de formatos, pueden ser incluidos en colecciones de datos alfanuméricos, gráficos, fotográficos o sonoros, contenidos en documentos publicados en papel, formar parte del acervo informativo de un servidor ubicado fuera del país, en una cinta de grabación de audio o video o incluso en un CD o en un DVD.

Es por lo anterior, que se considera que no importa si los datos han sido incluidos en un banco de datos estructurado y lógicamente construido, los datos personales cuentan per se y el sistema de información que sirve para su procesamiento y organización no les agrega tal carácter.

Expedientes judiciales, clínicos o de procedimientos administrativos contienen datos personales, como los contienen también las páginas de Internet que usamos para comprar bienes y servicios, así como también existen datos personales recopilados en listados de bancos y financieras, listados de deudores y de electores.

Cuando cambiamos de cuenta de banco, pedimos un préstamo, gestionamos un nuevo puesto de trabajo, realizamos trámites en oficinas públicas, recogemos firmas para hacer presente nuestra opinión sobre un tema, y cuando nos hacemos exámenes clínicos para ver nuestro estado de salud estamos interactuando en el mundo de los datos personales, pues nos conciernen, nos definen de alguna manera, y permiten nuestra identificación.

El dato personal tiene una importancia señera en la identificación, en la determinación de las características que refieren a una persona o su comportamiento y adquieren relevancia por esa capacidad identificatoria pero también porque pueden influir en la forma en que podemos ser tratados o evaluados.

Se suele hacer referencia en la legislación comparada a la característica de los datos personales de referirse a una persona **identificada o identificable**, pues precisamente su capacidad de determinar a quien se refieren es su principal función. La característica de ser “identificables” deriva del potencial de referir a partir de los datos personales a una persona que aún no lo ha sido. Es por ello que la normativa suele prestar atención a ambas potencialidades.

La identificación de una persona a partir de sus datos personales sucede mediante la utilización de los así denominados **“identificadores”**, que lo son precisamente porque puedan conectarse directamente con una persona por su relación privilegiada y cercana con ella, como lo podrían ser, por ejemplo, la posición o cargo que se ocupa, los identificadores biométricos, el nombre, etc. Estos identificadores son los que precisamente podemos denominar “datos personales”.

También es posible identificar a una persona en específico estrechando el marco de las posibilidades de aquellos que podrían ostentar de manera genérica características que se comparten. Por ejemplo, compartimos con muchas personas la edad, el tipo de empleo, la propiedad de una determinada marca de vehículo o un determinado tipo de teléfono. Si quisiéramos concretar a quien se refieren en concreto estas características, podríamos cruzar estos datos genéricos con el nombre, el número de identificación único de identidad (cédula de identidad, número de pasaporte), las placas del vehículo, el número de teléfono, y así derivar a quién se refieren todos estos datos genéricos y específicos. Con esta comparación de datos podemos estrechar el grupo de las personas que eventualmente podrían ser identificadas y llegar precisamente a la persona que nos interesa.

En síntesis, podríamos concluir que una persona podría ser considerada “identificable” a partir de los medios tecnológicos disponibles para derivar razonablemente su identidad. Hoy en día estos medios son variados, y casi todos ellos están disponibles para los más diversos usos legítimos pero también para algunos no tan legítimos o incluso antijurídicos. El control de estos medios y la evitación del abuso es uno de los objetivos importantes de la protección de datos personales y de la legislación que ha venido desarrollándose al respecto.

Un dato se refiere a una persona si hace referencia a su identidad, características o comportamiento, o si esa información se utiliza para determinar o influir en la manera en que se le trata o se le evalúa dicha persona. La sola posibilidad de que podamos singularizar a aquella persona no lleva a concluir de manera directa que estemos

hablando de datos personales. Si la posibilidad de hacerlo no es realmente existente o es insignificante, podríamos calificar que la persona no es entonces “identificable” y, en tal caso, las características que están siendo manejadas como información no podrían calificarse de “datos personales”.

Es frecuente que las leyes de protección de datos personales hagan alusión al concepto de “**persona física**” y derivar de allí que la tutela jurídica que despliegan únicamente atiende a los seres humanos. Esto ha llevado a negar, en muchos casos, la protección de datos personales a las así denominadas “personas jurídicas”. Los datos de estas “personas jurídicas” ya obran en diversos registros (mercantiles, de bienes, de cooperativas, fundaciones, u otros). Es por esta razón que suelen negárseles el acceso a los derechos de acceso, rectificación, cancelación y oposición que ya existen para las personas físicas. Sin embargo, existen otros medios legales previstos en las normativas de los países, que tienen la virtualidad de proteger el honor, el buen nombre y la imagen de las personas jurídicas, bienes jurídicos indispensables para el buen funcionamiento y el cumplimiento de los fines de estas ficciones jurídicas

4. Protección de datos personales

Luego de lo analizado en las secciones anteriores, podemos concluir que el derecho a la protección de datos personales es un verdadero derecho que ofrece a los ciudadanos una serie de facultades para controlar el flujo de datos personales y controlar el uso que se hace de estos datos que le conciernen.

En la tradición jurídica latinoamericana, este derecho suele denominársele “*habeas data*”, y llegado a nuestra experiencia jurídica por la vía del desarrollo de una jurisprudencia constitucional proclive al reconocimiento de los derechos de acceso, rectificación, cancelación y oposición que ostentan las personas para revisar los datos que sobre ellas existen en bancos de datos públicos y privados. El “*habeas data*” a pesar de su característica procesal constitucional, ha contribuido a generar una sensibilidad importante sobre el tema de la protección de la vida privada en una sociedad profundamente marcada por el uso de las nuevas tecnologías de la comunicación y de la información, y de los riesgos que de ese uso se derivan. Las principales manifestaciones de su incidencia provienen del uso de datos financieros y bancarios y de los diversos problemas que se han generado con su abuso, que incluso le han negado a muchos ciudadanos un adecuado acceso al crédito. Sin embargo, hay otros aspectos involucrados que han aumentado el interés y el ámbito de cobertura del *habeas data* y ha extendido su uso también para garantizar el acceso a la información pública.

Lo cierto es que el derecho a la protección de datos personales, ya sea en su reconocimiento legislativo como tal o a través de su reconocimiento constitucional a través del proceso de *habeas data*, ha llegado para quedarse en la experiencia jurídica de nuestros

países, para reconocer que **los datos personales son aquellos datos relativos a los seres humanos vivos identificados o identificables**. Pero aun más que eso, se trata de un reconocimiento jurídico del derecho de acceder a la información que le concierne a esos seres humanos por estar referida a sus condiciones personales.

El origen de este reconocimiento, tal y como ha sucedido en otras latitudes, tiene su punto de partida en el reconocimiento de la protección de la intimidad y de la privacidad, pero cuyo horizonte de proyección resulta más amplio que el del derecho de la intimidad.

El derecho a la protección de datos pretende algo aún más esencial que el mero reconocimiento de la intimidad o la privacidad como derecho de exclusión, se trata pues de la garantía del derecho al control de los datos personales, tanto en cuanto a su uso y destino, como para prohibir su tráfico ilícito, su recogida por medios ilegítimos, y la potencial vulneración de diversos derechos conectados al respeto a la dignidad humana provocada por el uso o tratamiento ilícito de estos datos.

La intimidad, tal y como se ha observado, se concretaba a una mera exclusión de un ámbito o esfera privada. El derecho a la protección de datos, en una perspectiva diversa y más amplia, parte del derecho de los ciudadanos a consentir en la recogida y procesamiento de sus datos personales, garantizando que el uso, destino y transmisión de los mismos puede ser conocido por los afectados y decidir sobre estas circunstancias. Esto último, permite un control del tráfico ilícito y de la potencial vulneración de su dignidad como persona humana.

El derecho a la protección de datos personales reconoce, entonces, diversas prerrogativas de la persona en el tratamiento de dichos datos:

- a) Conocer de su inclusión en bancos de datos o registros.
- b) Acceder a toda información que sobre ella conste en los bancos de datos o registros.
- c) Actualizar o corregir, en su caso, la información que sobre ella conste en los bancos de datos o registros.
- d) Conocer el propósito o fines para los que se va a utilizar la información que conste sobre ella en los bancos de datos.
- e) Que se garantice la confidencialidad de determinada información obtenida legalmente para evitar su conocimiento por terceros.
- f) Que se garantice la supresión de información sobre la persona con datos sobre su filiación política o gremial, creencias religiosas, vida íntima y toda aquella que pudiera de un modo u otro producir discriminación.

Estas garantías prácticas permiten derivar la importancia de la protección de datos de carácter personal como elemento esencial del Estado de Derecho en una sociedad tecnológica, donde el control y manejo de los flujos de información tiene un papel tan

señero en el desarrollo de todas las actividades humanas. No es entonces por casualidad que se han venido desarrollando tutelas jurídicas de este derecho. El respeto de los derechos humanos y de las libertades fundamentales requiere de esta tutela y es por ello que las leyes de transparencia y acceso a la información pública, contemplan también como excepciones al derecho de acceso, el derecho a la vida privada y la intimidad de las personas, a menos que existan intereses colectivos superiores que justifiquen una intromisión en este derecho personalísimo.

El derecho a la protección de datos personales, está integrado por una serie de prerrogativas, principios y procedimientos para el tratamiento de información que concierne a personas físicas, no sólo por parte del Estado o los entes públicos, sino también, por parte de terceros o personas de derecho privado.

Este poder de control sobre los datos personales se manifiesta a través de los denominados derechos de acceso, actualización, rectificación, oposición o eliminación, a través de los cuales las personas tienen la facultad de:

- Conocer en todo momento quién dispone de sus datos y para qué están siendo utilizados.
- Solicitar rectificación de los datos en caso de que resulten incompletos o inexactos.
- Solicitar la cancelación de los mismos por no ajustarse a las disposiciones aplicables.
- Oponerse al uso de sus datos si es que los mismos fueron obtenidos sin su consentimiento.

Se ha dicho que el derecho a la protección de datos personales es un derecho “principalista” puesto que se desarrolla a partir de principios de garantía o tutela. Es así que en las normativas sobre la materia se incluyen una serie de principios rectores tales como: el de finalidad, calidad, consentimiento, deber de información, seguridad, confidencialidad, disponibilidad y temporalidad. El incumplimiento de estos principios, constituye una vulneración a la protección de datos personales y, lógicamente, tiene como consecuencia una sanción.

Los principios generales de protección de datos constituyen el contenido esencial del derecho a la protección de datos personales y configuran un sistema de tutela que garantiza un uso racional de los datos personales.

Completa estas garantías de tutela, la existencia de órganos garantes del derecho de protección de datos personales. Su surgimiento, desarrollo y trascendencia les ha dado un sitio de honor en la historia de la protección de datos, y hoy día son un estándar ineludible en la realización de este importante derecho en la sociedad de la información. Se trata de órganos dotados de independencia y autonomía para garantizar que los ciudadanos puedan gozar de una efectiva tutela jurídica de este derecho a la protección de sus datos personales, tanto en su interacción con órganos públicos pero

también con sujetos del derecho privado. Los órganos garantes son una parte esencial de esta tutela jurídica y su función es reconocida por todas partes, especialmente en Europa donde su papel orientador y de acompañamiento del desarrollo de las tecnologías, les ha impreso un importante papel en la función de prevención que también es trascendente en este campo.

Síntesis

La intimidad representa una esfera íntima, de exclusión, en la que la persona se refugia para que sus comportamientos, acciones y expresiones queden fuera de la esfera pública. Su garantía y reconocimiento sigue siendo trascendente en la vida moderna, y es un pilar esencial para toda sociedad democrática.

Ese papel esencial se entiende no sólo porque es una barrera para las intromisiones de otros en esa esfera íntima, sino también porque representa una barrera a las intromisiones del Estado, permitiendo, de esa manera, un libre desarrollo de la personalidad de los ciudadanos.

El reconocimiento jurídico del derecho a la intimidad suelen sintetizarse en fases o momentos de tutela. Se habla de una fase negativa, también denominada pasiva, en donde el ordenamiento jurídico reconocer el derecho del individuo a vivir en paz y en soledad. Junto a esta fase negativa, se reconoce también una fase positiva (activa), constituida por el principio de autodeterminación informativa o de poder de control sobre los datos personales.

La privacidad constituye un conjunto más amplio, más global de facetas de nuestra personalidad que, aisladamente consideradas, pueden carecer de un significado en sí mismo pero que, coherentemente enlazadas entre sí, arrojan un retrato de nuestra personalidad que tenemos derecho a mantener reservada.

Un dato personal, es toda información referida a un individuo que lo identifica o lo hace identificable. Dicha información puede ser numérica, alfabética, gráfica, acústica o de cualquier otro tipo y estar contenida en cualquier soporte.

El derecho a la protección de datos personales consiste en la facultad de los individuos de controlar la información que les concierne y está integrado por una serie de principios y prerrogativas.

Este derecho se compone de los llamados derechos ARCO: acceso, rectificación, cancelación y oposición. Para su tutela es necesaria la existencia de órganos autónomos ante los cuales puedan acudir aquellas personas que consideren que su derecho ha sido violentado.

Unidad dos

Una vez que estudiamos los conceptos básicos relacionados con la protección de datos personales, los cuales son fundamentales para la comprensión de las leyes en la materia, en este módulo abordaremos de manera general, el contexto mundial en el cual fueron creadas las primeras normas en protección de datos personales, así como la institucionalización de este derecho en nuestro país.

Asimismo, se presenta una breve reseña histórica que da cuenta de los hechos más significativos en el proceso de creación y aprobación de la Ley de Acceso a la Información Pública.

Objetivo

Conocer y explicar de dónde surge el derecho a la protección de datos personales teniendo una idea clara de las causas y el contexto en el que se dieron las primeras leyes en la materia.

1. Antecedentes de las Leyes de Protección de Datos Personales

El fenómeno de construcción de un ciudadano de “cristal”, uno de los temores más importantes existente al inicio del desarrollo normativo de la protección de datos personales, hacia finales de la década de los años sesenta del siglo pasado, es hoy tecnológicamente hablando, una realidad.

La tecnología disponible hoy permite una observación al mismo tiempo sutil e intensa de todos los movimientos, apetencias, gustos, costumbres, de los ciudadanos. El grado e intensidad de esta observación ha llevado incluso a acuñar el término de “sociedad panóptica” para describir el tipo de interacción con las informaciones personales que es posible gracias a las redes sociales, los servicios de valor agregado en la telefonía móvil, y el uso intensivo de la Internet.

El ciudadano se enfrenta a un espacio público invadido de cámaras de video, góndolas de supermercado dispuestas a dar información sobre los productos expuestos y a sugerir “mejores” posibilidades de compra. Estas observaciones *in situ* se complementan con servicios de minería de datos que complementan los perfiles de consumo y compra de los ciudadanos, y abren enormes posibilidades para incidir en las estrategias de mercadeo y oferta en los centros comerciales.

Estos modernos desarrollos han producido un desplazamiento del interés de la protección jurídica del Estado hacia los propios ciudadanos y sujetos del derecho privado, que hoy inciden de manera tan intensa en la esfera de intimidad de los ciudadanos y que están también apertrechados tecnológicamente para convertirse en actores importantes de nuevos escenarios de riesgo y peligro para las libertades.

Estos cambios en el ambiente de la información y de las tecnologías desplazó entonces el interés del legislador y promovió un cambio importante de las propuestas legislativas, las cuales hoy conducen, con mucha mayor intensidad, a una concentración en el acopio de datos personales, su intercambio, y la confección de perfiles de las personas por medio de las tecnologías de la comunicación de la información.

Sin embargo, esta situación problemática no era ni siquiera cercana a la que ocurría hacia finales de la década de los años sesenta del siglo XX, en que el gran líder en la recopilación de los datos personales era el Estado y no necesariamente los particulares, aun cuando grandes empresas privadas ya tenían para esa fecha grandes recopilaciones de datos sobre los ciudadanos, sobre todo las empresas de servicios públicos en países como los Estados Unidos y otros en Europa.

En esta época, quizá por las limitaciones de la técnica, y por la falta de capacidad de procesamiento de los computadores y la incipiente interconexión de los bancos de datos, llevó al legislador a pensar que era más conveniente poner un énfasis en el quehacer informativo del Estado, dejando a los particulares, al menos por varias décadas, sin una atención especial.

La legislación de este periodo histórico tendía a ser más formal, concentrada en la regulación de los bancos de datos públicos, y a garantizar la intervención de órganos de control que mediaran entre el Estado y los ciudadanos, cada vez más preocupados por las urgencias informativas en los más diversos campos del quehacer público.

Con el advenimiento de la así denominada “sociedad de la información”, el intercambio de los datos personales, se convertiría en la piedra de toque de una nueva comprensión del quehacer democrático. La democracia casi que adquiriría una nueva correlación de fuerzas: entre los ciudadanos que interactuaban en dicha sociedad de la información y los datos que sobre ellos empezaban a fluir por doquier, y donde casi era imposible asegurar un control sobre el mencionado flujo de informaciones.

Las informaciones en general, pero los datos personales en específico, empezaron a adquirir un valor de cambio, a considerarse una mercancía valiosa, y, por ende, a crear la necesidad de recopilarlos, acopiarlos y darles un uso intenso. El dato personal adquirió entonces un valor enorme para la sociedad en su conjunto; y para aquellos capaces de hacer uso de ellos.

Al mismo tiempo que estos desarrollos tienen lugar en los espacios públicos, en las interacciones cotidianas de los ciudadanos con el sector servicios, la “Red de Redes”, Internet, con su advenimiento en la década de los años noventa, abre la puerta a una mirada de servicios, a la facilitación de la comunicación y el intercambio de información, a crear nuevos nichos de mercado y a desarrollar potencialidades antes impensables, derribando las fronteras de espacio y tiempo.

La generalización del correo electrónico, primero, y de la consulta de servicios de información en las páginas dispuestas en la Internet, y los programas que facilitaban la así denominada “navegación”, como Netscape y Explorer, solo por citar los más importantes en aquella primera etapa, provocaron el flujo de una inusitada masa de datos que circularía casi sin límite por todo el globo terráqueo. Pronto, diversas herramientas informáticas permitirían rastrear dicha información, filtrarla, darle diversos contenidos, compararla de mil maneras, y provocar nuevas formas de interacción, de intercambio, pero también de riesgo y peligro para la intimidad y la privacidad de los ciudadanos.

No se puede entrar aquí a un análisis detallado de los cambios sociales sufridos por el influjo de las tecnologías, y del grado de desgaste de algunos derechos constitucionales que han tenido que reconceptualizarse a partir de estos progresos constantes y vertiginosos en el ambiente de la información, pero sí se puede hablar de una verdadera revolución del mundo de la vida que ha transformado la forma en que era posible comprender nuestra cultura, nuestras relaciones, y nuestra forma de entender la tecnología. En esencia, la vida de la sociedad moderna no puede entenderse ya sin el ingrediente omnipresente de las TIC’s.

De estos desarrollos en el ambiente de la información, el que quizá interesa de manera más preponderante para captar los cambios legislativos en la materia, lo es, el del intercambio de datos personales que ha sido facilitado por estas herramientas de comunicación. El acceso a los datos personales, a los detalles de vida y consumo de millones de seres humanos, se ha facilitado exponencialmente, y ha provocado que no solo la posibilidad de generar “ciudadanos de cristal” sea el riesgo permanente, pues dicha circunstancia ya llegó para quedarse, sino que la generación de perfiles de los ciudadanos, y de allí a la observación de sus escogencias, gustos, ideologías, preferencias y decisiones se constituya hoy en uno de los más importantes retos para resguardar las libertades públicas.

Los desarrollos que se anuncian en el corto y mediano plazo permiten pensar en el así denominado “*ubiquitous computing*”, el “*internet de las cosas*”, y el no menos ominoso

desarrollo de la computación “*en la nube*”, que ha llevado el procesamiento de datos a los ámbitos más inusitados pero también a extenderlo a todas y cada una de las actividades de los ciudadanos. Cada vez más, los instrumentos de nuestra vía cotidiana, vienen dispuestos con suficiente poder informático para comunicarse entre sí, incluso sin cables y realmente no es posible determinar en todos los casos, qué tipo de datos podrían estarse transmitiendo unos y otros y quiénes podrían estar interesados en intervenir en tan conspicua comunicación .

La tarea legislativa que debe desplegarse para dar una efectiva protección al derecho a la autodeterminación informativa no sólo es compleja, sino también llena de dificultades por la amplitud y diversidad de los servicios de información que dependen hoy, en diversas formas y en diversa intensidad, de un procesamiento de datos personales.

Luego de la Sentencia sobre la Ley de Censos del Tribunal Constitucional Federal Alemán de 1983, el antecedente más importante en dicho país sobre el desarrollo e importancia constitucional del derecho a la autodeterminación informativa, la doctrina no tardó en indicar que las áreas necesitadas de revisión y regulación abarcaban no sólo las tareas del *Bundespost* (Servicio de Correos Federal) sino también las relaciones jurídicas de información existentes en los Departamentos de Finanzas, las Autoridades encargadas de labores de Inteligencia y Seguridad (*Sicherheitsbehörden*), así como también los hospitales y centros de salud, solo para citar algunas áreas de urgente atención . Solo en el tema de seguridad era necesario introducir normas específicas para regular el intercambio de información entre el *Bundeskriminalamt* (Policía Federal) y las autoridades encargadas de fronteras (*Grenzschutzbehörden*), así como avanzar en un estándar legislativo que permitiera resolver arduos problemas con el tratamiento de la información realizado en el ámbito del proceso penal. No sólo el problema del tratamiento de datos sin la autorización del afectado, así como la generosa práctica administrativa de compartir datos o de generar bancos de datos con todas las informaciones imaginables, eran los fenómenos más trascendentales de aquellos días, también se trataba de obligar a las instituciones del Estado a sujetarse a una estricta separación entre intereses de investigación y las tareas que específicamente les había autorizado la ley, así como la obligación de sujetarse a los fines expresados por la ley para el tratamiento de los datos. El control institucional, resumido en la supervisión constante de los Comisionados de la Protección de Datos (*Datenschutzbeauftragten*), era otro elemento esencial del proceso de nivelación de la legislación a los requerimientos constitucionales establecidos por el Tribunal Constitucional Alemán. Pero también lo era lograr un adecuado desarrollo normativo en todas aquellas áreas que involucraran el procesamiento de datos personales, junto al desarrollo de Comisionados de la Protección de Datos en las propias instituciones públicas y privadas.

Hoy la protección de datos se encuentra viviendo un proceso muy interesante de reformas, algunas de ellas han permitido el desarrollo internacional de las disposiciones de tutela.

Por ejemplo, la Ley Federal de Protección de Datos de Alemania (*Bundesdatenschutzgesetz*, “*BDSG*”) ya ha incluido dentro de sus disposiciones algunos principios largamente acariciados por los expertos y los ciudadanos como el principio de evitación de datos (*Datenvermeidung*) y de ahorro de datos (*Datensparsamkeit*), que no son otra cosa que la aplicación en la práctica del principio de proporcionalidad en esta materia, concretamente del sub principio de necesidad.

La BDSG ha incluido también la llamada auditoría de protección de datos (*Datenaudit*), que no es más que una regulación complementaria a las ya establecidas de orden institucional y que persigue que haya auditorías llevadas a cabo por expertos particulares, quienes observen en los sistemas la efectiva realización de los principios vigentes en la materia. Todos estos cambios han sido bien recibidos por los Comisionados de la Protección de datos, quienes las observan como pasos decididos hacia una modernización del estándar de la protección de datos en Alemania y también en Europa, cuyos lemas de campaña son: “protección de datos por medio de la técnica”, y “mayor transparencia del procesamiento de datos”.

La Unión Europea ha avanzado hasta poner en vigencia una reglamentación sobre protección de datos, y lo mismo ha sucedido en la famosa “Carta de la Unión Europea” que ha reservado un lugar privilegiado para la autodeterminación informativa. Debe distinguirse esta reglamentación de la así denominada “Línea Directiva de la Unión Europea en materia de protección de datos”, la cual en realidad se refiere a temas que deben ser puestos en vigencia por los estados miembros de la Unión, así como por los órganos e instituciones de la Unión Europea.

La reglamentación a la que se ha hecho referencia tiene por objetivo proteger a las personas objeto de tratamiento de datos, por parte de órganos e instituciones de la Unión Europea. Contiene entre otras regulaciones, la prohibición para órganos e instituciones de la Unión Europea de enviar datos personales a países fuera del ámbito de vigencia de esta reglamentación que no tengan un estándar de protección similar al europeo.

Los datos sobre temas sensibles, como el origen o las convicciones religiosas de las personas, solo pueden ser tratados de manera automática en casos excepcionales.

También contempla regulaciones sobre el aseguramiento técnico de los datos, los cuales, desgraciadamente, deben contemplarse como superados, no obstante, la importancia de considerar este tema en la misma reglamentación.

Otros aspectos interesantes de esta normativa lo son: la inclusión de un Comisionado de la Protección de Datos, quien, entre otras funciones, le corresponde velar por el cumplimiento de la reglamentación a lo interno de la oficina a su cargo. Junto a este Comisionado, se ha decidido nombrar una autoridad de control constituida por el

Comisionado Europeo de la Protección de Datos, quien aconseja y controla a los órganos e instituciones de la Unión Europea en esta materia. Para cumplir con esta tarea se le conceden amplios poderes de acceso a todas las oficinas y centros de procesamiento, a todos los datos personales y a todas las informaciones generadas en el ámbito de la Unión. Contra las decisiones de este alto Comisionado solo se puede iniciar demanda ante el Tribunal Europeo.

Las personas afectadas por procesamientos de datos prohibidos en el ámbito de la Unión, tienen derecho a solicitar información, a obstruir datos y a solicitar y lograr el borrado de datos e informaciones que le afecten. También pueden acudir directamente ante el Comisionado Europeo.

Más importante que lo anterior, es que el ejercicio de los derechos que contempla la reglamentación no generan costos para el afectado, lo que indica que esta reglamentación es mucho más amigable con el ciudadano afectado que la misma Línea Directiva del Consejo de Europa, la cual indica que las normativas que se dicten bajo la mencionada Directiva no deben incluir costos que sean “exagerados” para el afectado.

Finalmente, la Carta de Derechos Fundamentales de la Unión Europea, que fuera anunciada el día 7 de diciembre de 2000 en Niza, contiene un artículo 8, el cual regula detalladamente aspectos relacionados con la protección de datos, siguiendo muy de cerca la normativa alemana, el texto reza:

- (1) “Toda persona tiene derecho a la tutela de sus datos personales.
- (2) Estos datos solo deben ser procesados de buena fe para el fin preestablecido con el consentimiento de la persona afectada o para cumplir con los fines establecidos con un adecuado fundamento legal. Toda persona tiene el derecho a recibir información sobre los datos referidos a su persona que hayan sido recogidos y a lograr su rectificación.
- (3) El cumplimiento de estas reglas será vigilada por un centro independiente.”

El artículo 42 de la Carta garantiza, adicionalmente, un derecho de acceso a los documentos del Parlamento Europeo, del Consejo y de la Comisión.

Aun cuando la Carta no tiene un efecto jurídico directo en la práctica, si es una fuente de interpretación para los órganos e instituciones de la Unión Europea, y objeto de aplicación jurídica y estudio por parte del Tribunal Europeo. En todo caso se nota el alto nivel que se le ha concedido al derecho de la protección de datos al nivel europeo, aspecto que terminará por trasladarse a los Estados miembros y a los países que vayan a tener una relación económica directa con la Unión Europea, como puede ser el caso de nuestro país.

Dados los cambios que se han venido produciendo, y la posibilidad de evaluar tres tipos de modelos regulatorios en el horizonte de proyección de esta materia, es que

resulta interesante analizarlos, con el fin de contextualizar la regulación de la protección de datos en El Salvador.

La regulación en la materia encuentra eco en diversos instrumentos internacionales que aportan a este tema como es el de derechos humanos, así como regulaciones formuladas por bloques económicos como la Unión Europea, la Organización para la Cooperación y el Desarrollo Económico, y del Foro de Cooperación Económica Asia Pacífico, así como la resolución que en esta materia elaboró la Organización de las Naciones Unidas. Ultimamente también la Organización de Estados Americanos ha impulsado los trabajos conducentes a elaborar una “ley modelo” en materia de protección de datos personales. Como parte de esta actividad, la OEA ha promovido la elaboración de un estudio preliminar sobre la protección de datos. Este documento, presentado formalmente a la Comisión de Asuntos Jurídicos y Políticos del Consejo Permanente de la OEA en el año 2011, contiene un conjunto de principios y recomendaciones en la materia⁷.

El tema forma parte oficial de la actividad jurídica de la Asamblea General de la OEA, lo que ha llevado a la elaboración de un documento con principios de privacidad y protección de datos personales en las Américas, que fue presentado en el año 2012. Todo ello manifiesta el interés del Organismo Regional por promover la temática y generar actividad legislativa en los países miembros.

Adicionalmente, se han hecho algunos llamamientos, como el de la Cumbre Mundial de la Sociedad de la Información, dirigidos a solicitar a todos los países que garanticen el respeto a la privacidad y a la protección de información y datos personales, ya sea mediante la adopción de legislaciones, la aplicación de marcos de colaboración, mejores prácticas y medidas tecnológicas y de autorregulación por parte de empresas y usuarios

2. Antecedentes legislativos en materia de protección de datos

Es así que la regulación de protección de datos que ha intentado El Salvador, encuentra antecedentes en Europa, desde la década de los años setenta, con las primeras leyes de protección de datos, como la Data Lag Sueca y la misma Ley de Protección de Datos Personales del Estado Federado de Hesse, también de los años setenta. Antecedentes en los Estados Unidos pueden encontrarse también con la ya famosa Privacy Act de 1974.

Como ya se ha planteado en el acápite anterior, estas normativas surgen a partir de la preocupación por los desarrollos tecnológicos, aun incipientes, en el procesamiento y

7. Cfr. http://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp

almacenamiento de información, y por la inquietud que estos desarrollos provocaban en los ciudadanos, primordialmente frente a las necesidades crecientes de información del Estado.

Modelos más modernos han tendido a ofrecer un esquema regulatorio libre que es optativo para sus empresas, fomentando de esa manera una reactivación de los intercambios comerciales. Se trata del famoso “safe harbor” planteado en la normativa estadounidense.

Sin embargo, las propuestas de carácter supranacional son las que han provocado los cambios más importantes. Baste recordar la Recomendación de la OCDE de 23 de septiembre de 1980 sobre flujo internacional de datos, o las sucesivas Recomendaciones del Parlamento y del Consejo de Europa, que alentaron a los Estados europeos en su desarrollo legislativo. De igual manera, los principios o directrices de protección de datos tempranamente aprobados por las Naciones Unidas, han planteado muy importantes cambios en diversos continentes.

Paulatinamente, la protección de datos como derecho autónomo fue ganando terreno en la concepción general. En el ámbito del Consejo de Europa, se aprobó el Convenio No. 108, del 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, cuyo objetivo (artículo 1º) es el de “garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona” (“protección de datos”).

El concepto de vida privada en relación con la protección de datos personales ha sido objeto de interpretación extensiva. En este sentido, el Tribunal Europeo de Derechos Humanos, entiende que también incluye las relaciones personales y las comerciales, citando, precisamente la Convención 108.

Efectivamente, no sólo la intimidad o la vida privada están en juego cuando se trata de protección de datos personales. El principio de calidad de los datos, con sus consecuencias de derecho a la exactitud, actualización, rectificación y supresión, no siempre está directamente vinculado a la privacidad, sino, también cuando se trata de proteger el derecho a la no discriminación o la igualdad de trato en las decisiones individuales automatizadas.

Las variaciones en la legislación europea, más importantes, esperarían a la Directiva del año 1995. Esta Directiva no llegaría a nacer a la vida jurídica sin un debate muy intenso de sus contenidos y principios. Muchos países de la Unión Europea pensaron que sus estándares nacionales eran suficientes y no era necesario transponer una

directiva nueva que, a la postre, obligara a más intensas variaciones de la práctica de la protección de los datos personales.

Pese a todas las reservas, en 1995 se aprueba la Directiva 95/46/CE, del 24 de octubre sobre protección de datos personales, cuyo objeto y finalidad no se articula sobre la limitación en la actividad informática para asegurar la tutela de los derechos personales, sino sobre la libre circulación de los datos en Estados de acuerdo con la necesaria protección de las personas. Se trata, sin duda, de un difícil equilibrio entre el principio de libre circulación de las informaciones y la protección de la autodeterminación informativa en un mundo comercial que necesitaba, y necesita, cada vez más, de un flujo intenso de datos personales. Este equilibrio, se entiende, no debía evitar un obstáculo al progreso y al desarrollo económico pero tampoco una exposición innecesaria a los ciudadanos a enfrentar vejaciones a sus derechos en la sociedad tecnológica.

La Directiva de 1995 daría paso después a diversas normas sectoriales, un desarrollo que no se ha detenido desde entonces, y donde ha habido cambios legislativos muy importantes. Un ejemplo de estos cambios podemos percibirlo en la Directiva 97/66/CE del 15 de diciembre sobre protección de datos personales y de la intimidad en el sector de las telecomunicaciones, o el Reglamento 45/2001 del 18 de diciembre, para la protección de las personas respecto al tratamiento de datos por instituciones y organismos comunitarios.

Es por lo anterior, que puede decirse que la Directiva de 1995 se constituye en un elemento esencial que caracteriza el desarrollo posterior de la protección de datos en Europa, con importantes repercusiones en la estandarización de límites a la recogida y utilización de datos personales, pero sobre todo en dirección al uso extendido de órganos nacionales independientes encargados de la protección de datos personales. Podemos decir, que este es el antecedente reciente, más importante, para implantar como un estándar internacional la constitución de organismos de protección.

Tema 3. Breve Reseña de la inclusión de temas de protección de datos personales en la Ley de Acceso a la Información Pública de El Salvador.

El propósito de esta reseña es dar un vistazo general a los principios de protección de datos personales que se incluyen en la Ley de Acceso a la Información Pública de El Salvador, mediante el Decreto 534 del 30 de marzo del 2011. Esto último, con el objetivo de ofrecer un panorama de los estándares de protección del derecho a la autodeterminación informativa planteados por el legislador salvadoreño.

Desde la Sentencia DICOM de 2004, existe en El Salvador un interés científico por el tema del *habeas data*, no sólo por haber establecido un precedente jurisprudencial de un amparo especial en materia de acceso a datos personales, sino por la necesidad de mantener ese avance mediante una ley de *habeas data*.

Sin embargo, el camino hacia una garantía normativa del *habeas data* no termina precisamente con un reconocimiento de todas las necesidades de tutela involucradas, muy especialmente de aquellas que son de naturaleza preventiva. En efecto, el *habeas data* no alcanza a cumplir una garantía preventiva, pues su ejercicio se produce, recién, cuando el ciudadano ya ha sentido la lesión en su derecho a la autodeterminación informativa.

Es por lo anterior, que la propuesta de una ley específica en materia de protección de datos personales, conforme a los estándares internacionales, resulta tan importante. Este hecho fue ratificado por la sentencia de Inconstitucionalidad del dos de septiembre de dos mil cinco, en ella la Sala estableció la inexistencia de una inconstitucionalidad por omisión al no haberse emitido una ley que regulase la autodeterminación informativa y sus principios protectores.

Frente a la ausencia de un desarrollo legislativo, se presenta también la necesidad de una autoridad encargada de garantizar las condiciones preventivas que el derecho a la autodeterminación informativa contribuye a desarrollar. En efecto, la garantía institucional abarca la creación de un órgano de tutela, que además de asumir la tarea de llevar un control de bases y bancos de datos personales, pueda también dictar políticas preventivas en la materia, además de atender solicitudes de acceso por parte de los ciudadanos.

Es así que antes de la Ley de Acceso a la Información Pública de El Salvador, los precedentes constitucionales se satisfacían con el desarrollo del amparo de *habeas data*, y no exigían, directamente otros aspectos derivados del derecho de la protección de datos personales. Quizá la necesidad específica de una protección a través de principios reguladores, vendría planteada por las urgencias derivadas de los movimientos legislativos internacionales, y de la actividad de organizaciones regionales y mundiales, tal y como se expuso anteriormente.

Con todo, la promulgación de la Ley de Acceso a la Información Pública, y la concentración de normas en pocos artículos, ha permitido desarrollar al Instituto de Acceso a la Información Pública una serie de lineamientos que pueden ser la base de una regulación normativa integral y sectorial en materia de protección de datos personales.

La garantía del *habeas data*, mientras tanto, puede seguir jugando un papel importante de protección complementaria, conforme el legislador avanza a un estándar más amplio de consideración de los principios de protección de datos personales.

Síntesis

El derecho a la protección de datos personales surge ante la evolución tecnológica por el riesgo que representaba la amenaza a los derechos fundamentales, sobre todo a la intimidad y a la privacidad, el manejo indiscriminado de información personal.

Frente a esta gran problemática generada en materia de protección a la privacidad con la evolución de las tecnologías de la información, diversos organismos y países, desde hace algunas décadas, han emitido regulaciones en materia de protección a la intimidad y privacidad.

Se han creado diversos instrumentos internacionales que aportan a este tema como es el de derechos humanos, así como regulaciones formuladas por bloques económicos como la Unión Europea, la Organización para la Cooperación y el Desarrollo Económico, y del Foro de Cooperación Económica Asia Pacífico, así como la resolución que en esta materia elaboró la Organización de las Naciones Unidas y los documentos producidos en el marco de la Organización de Estados Americanos.

La Ley de Acceso a la Información Pública de El Salvador contiene la base normativa para un desarrollo posterior tanto de normativa sectorial en protección de datos personales, así como una ley orgánica que contenga los aspectos más esenciales de dicha tutela, junto con una ampliación de las competencias de control asignadas preliminarmente al Instituto de Acceso a la Información Pública.

Unidad tres

En este módulo haremos un recorrido sobre los aspectos establecidos en la Ley de Acceso a la Información Pública, tales como definiciones de los términos utilizados y objetivos de la Ley, así como disposiciones generales en lo que se refiere a la protección de datos personales.

Objetivos

- Conocer los aspectos fundamentales que establecen la Ley de Acceso a la Información Pública y los Lineamientos.
- Comprender los objetivos que persigue la Ley.
- Familiarizarse con los términos más importantes utilizados en ambas normas.

1. La protección de datos personales en El Salvador

En la Ley de Acceso a la Información Pública de El Salvador no encontramos una definición de “protección de datos personales”, sin embargo, se aproxima a una definición cuando refiere que se trataría de un derecho de la persona, directamente o a través de su representante, a saber si se están procesando sus datos personales; a conseguir una reproducción inteligible de ellos sin demora; a obtener las rectificaciones o supresiones que correspondan cuando los registros sean injustificados o inexactos y a conocer los destinatarios cuando esta información sea transmitida, permitiéndole conocer las razones que motivaron su petición. Esto está claramente establecido en el Art. 31 de la Ley⁸.

Asimismo, se tomó en consideración la importancia de que las personas tengan a su alcance mecanismos para conocer la información que de ellas obra en los archivos de

8. Art. 31.- Toda persona, directamente o a través de su representante, tendrá derecho a saber si se están procesando sus datos personales; a conseguir una reproducción inteligible de ella sin demora; a obtener las rectificaciones o supresiones que correspondan cuando los registros sean injustificados o inexactos y a conocer los destinatarios cuando esta información sea transmitida, permitiéndole conocer las razones que motivaron su petición, en los términos de esta ley. El acceso a los datos personales es exclusivo de su titular o su representante.

cualquier ente público, y así poder ejercer los derechos de acceso, rectificación, oposición y eliminación de sus datos personales.

Tanto la Ley como los Lineamientos que la desarrollan, contienen un apartado de definiciones que ayudan a comprender y aplicar las normas, mismos que están en el artículo 4 de los Lineamientos.

Algo importante a tener en consideración, es que la interpretación de la Ley y los Lineamientos debe ser conforme a la Constitución, y a los distintos instrumentos internacionales suscritos por El Salvador en materia de derechos humanos, así como la interpretación que sobre los mismos hayan realizado los órganos internacionales respectivos.

2. Principios

El derecho a la protección de datos es un derecho “principalista”, esto es, se desarrolla a partir de principios, que no sólo articulan su regulación, sino que su observancia permite ligar el tratamiento de datos en todas sus fases: desde la recogida de los datos, hasta su procesamiento y transmisión. Es por ello, que los principios sintetizan las aspiraciones normativas y su vulneración se constituye en el elemento fundamental para considerar una infracción a la normativa de tutela.

Es por lo anterior, que conocer y aplicar los principios de protección de datos es un requisito indispensable para todo aquél que quiera realizar una adecuada tutela de la persona y sus derechos en el tratamiento informativo. Esto es especialmente cierto en el ámbito de la acción de los entes públicos, donde la asunción de las medidas necesarias para realizar estos principios son la garantía fundamental que el estándar de protección de datos personales que fija la ley ha sido obtenido.

Principios de Protección de Datos (artículos 7 a 11 de los Lineamientos):

Licitud: el principio de licitud sujeta, en primer lugar, la recogida de datos personales a medios lícitos, esto es, que no han de obtenerse con infracción legal. De la misma manera, los sistemas de datos personales, esto es, la instauración de sistemas automatizados de procesamiento de información personal deberá respetar las atribuciones legales o reglamentarias en vigencia. Cada entidad pública que realice procesamiento de datos personales, en consecuencia, deberá sujetarse a las atribuciones, permisos, limitaciones y regulaciones específicas o sectoriales que se refieran a la materia o temática desarrollada por dicho ente.

Se considera que es compatible con tales fines lícitos, el tratamiento de datos personales que responda a fines históricos, estadísticos o científicos, siempre y cuando se salvaguarden las garantías derivadas de la protección de datos personales.

Calidad de los datos: el tratamiento de datos personales deberá ser exacto, adecuado, actual, pertinente y no excesivo, respecto de las atribuciones legales de la dependencia o entidad que los posea.

La exigencia de calidad tiene que ver directamente con la naturaleza del tratamiento de datos personales, toda vez que siempre habrá que revisarse que los datos tratados y recopilados son los necesarios para cumplir con el fin público. Lo anterior implica, por supuesto, que no son excesivos o que se hayan recopilado a destajo para cumplir otras funciones no expresamente señaladas en el fin legal para el cual fueron recopilados.

El principio de calidad compromete, asimismo, a una constante auditoría de los datos tratados y almacenados en reservorios de información para que sean siempre exactos y actuales. Aquellos que ya no cumplen el fin legal o que han dejado de ser necesarios para tal fin, deberán ser eliminados por el encargado o responsable de la base de datos.

El principio de calidad de los datos, entonces, está directamente relacionado con el así denominado “derecho al olvido”, esto es a la eliminación, luego de un plazo razonable, de aquellas informaciones y datos que pudieran afectar a su titular, más allá del plazo previsto para su utilización para el fin legal. En algún caso, dichos datos podrán ser conservados más allá del plazo legal, pero en tal supuesto se estipula la obligación de anonimización de los datos, con el objetivo de que ya no sean ligados directamente a su titular.

Este principio de calidad establece un deber de constatación de la pertinencia de los datos que se requieren para la prestación de servicios públicos. Deberá tenerse especial cuidado, entonces, que para proveer una ayuda para estudio, por ejemplo, que se pida información sobre alguna minusvalía o enfermedad del titular, pues tal información no es relevante para decidir sobre tal ayuda.

Exactitud: este principio está profundamente unido al principio de calidad. Los datos que sean tratados han de ser exactos, es decir, no incompletos ni imprecisos con respecto a los fines para los que se justificó su recopilación. Si los datos no son exactos y precisos deberán de ser suprimidos o rectificados.

Es deber del encargado o responsable del banco de datos hacer un análisis de los registros para observar si la información contenida tiene algún grado de inexactitud. Si es así, deberá procurar completar los datos, sustituirlos o eliminarlos, todo esto de oficio.

De igual manera, el responsable del tratamiento de los datos personales deberá procurar el consentimiento informado de los afectados, pues los datos que hayan sido recogidos sin un consentimiento informado del titular o afectado, no podrían conservarse.

Otro aspecto que debe cuidarse a la hora del tratamiento de datos personales es que los mismos deben ser tratados únicamente para los fines que motivaron su recogida. Cualquier desviación del fin legal llevaría a que el tratamiento sea ilícito y con ello a la vulneración de varios principios de protección de datos, entre ellos, al de consentimiento informado. Esto último porque una desviación del fin, hemos de suponerlo, no quedaría abarcado por el consentimiento dado de previo por el titular.

El procesamiento de datos para fines distintos al establecido legalmente llevaría a la obligación de cancelar dichos datos, salvo que sean usados para fines históricos, estadísticos o científicos, como ya se había explicado anteriormente.

Acceso y corrección: la garantía de protección de datos se satisface, muchas veces, asegurando el derecho de los ciudadanos a acceder a sus datos, revisarlos y proceder a las correcciones de aquellas informaciones inexactas, imprecisas o falsas. Es por ello que la garantía de acceso es una de las más importantes para el ciudadano y la parte más visible del ejercicio de este derecho. Es así, entonces, que los encargados o responsables del procesamiento de datos deben almacenarlos de tal manera que garanticen el ejercicio de estos derechos de acceso y corrección en el marco de las reglamentaciones y de los lineamientos que han sido establecidos por el Instituto de Acceso a la Información.

También debe garantizarse que en aquellos casos de aparente contradicción entre el derecho del ciudadano a solicitar la cancelación de los datos y la obligación legal de conservar dichos datos, se proceda a bloquear los datos personales, suspendiendo su tratamiento. En tal supuesto, solo tendrán acceso a esos datos personales, las autoridades competentes dentro del marco de la obligación legal de la que se trate.

En virtud de lo anterior, los datos que resulten cancelados podrían entrar en una de dos constelaciones posibles:

- *Datos Bloqueados.* Los datos sólo están disponibles para la tramitación de posibles responsabilidades derivadas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades.
- *Eliminación de los datos.* Significa la destrucción o desaparición física de los datos personales bloqueados una vez cumplido el plazo.

Información: se deberá hacer del conocimiento del Titular de los datos, al momento de recabarlos y de forma escrita, el fundamento y motivo de ello, así como los propósitos para los cuales se tratarán dichos datos

Seguridad: se deberán adoptar las medidas necesarias para garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado.

Custodia y cuidado de la información: los datos personales serán debidamente custodiados y los Responsables, Encargados y Usuarios deberán garantizar el manejo cuidadoso en su tratamiento.

Consentimiento para la transmisión: toda transmisión de datos personales deberá contar con el consentimiento del Titular de los datos, mismo que deberá otorgarse en forma libre, expresa e informada, salvo lo dispuesto en el Lineamiento Vigésimo segundo.

Del consentimiento informado: cuando se soliciten datos de carácter personal será necesario informar de previo a las personas titulares o a sus representantes, de modo expreso, preciso e inequívoco:

- a) De la existencia de una base de datos de carácter personal.
- b) De los fines que se persiguen con la recolección de estos datos.
- c) De los destinatarios de la información, así como de quiénes podrán consultarla.
- d) Del carácter obligatorio o facultativo de sus respuestas a las preguntas que se le formulen durante la recolección de los datos.
- e) Del tratamiento que se dará a los datos solicitados.
- f) De las consecuencias de la negativa a suministrar los datos.
- g) De la posibilidad de ejercer los derechos que le asisten.
- h) De la identidad y dirección del responsable de la base de datos

Quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo.

No será necesario el consentimiento expreso cuando:

- a) Exista orden fundamentada, dictada por autoridad judicial competente o acuerdo adoptado por una comisión especial de investigación de la Asamblea Legislativa en el ejercicio de su cargo.
- b) Se trate de datos personales de acceso irrestricto, obtenidos de fuentes de acceso público general.
- c) Los datos deban ser entregados por disposición constitucional o legal⁹.

9. Art. 34.- Los entes obligados deberán proporcionar o divulgar datos personales, sin el consentimiento del titular, en los siguientes casos:

- a) Cuando fuere necesario por razones estadísticas, científicas o de interés general, siempre que no se identifique a la persona a quien se refieran.
- b) Cuando se transmitan entre entes obligados, siempre y cuando los datos se destinen al ejercicio de sus facultades.
- c) Cuando se trate de la investigación de delitos e infracciones administrativas, en cuyo caso se seguirán los procedimientos previstos en las leyes pertinentes.
- d) Cuando exista orden judicial.

Estos supuestos están contemplados en el artículo 34 de la Ley de Acceso a la Información Pública. En la legislación comparada, además, se prohíbe el acopio de datos sin el consentimiento informado de la persona, o bien, adquiridos por medios fraudulentos, desleales o ilícitos.

La obtención del consentimiento deberá ser:

- a) Libre: no debe mediar error, mala fe, violencia física o psicológica o dolo, que puedan afectar la manifestación de voluntad del titular;
- b) Específico: referido a una o varias finalidades determinadas y definidas que justifiquen el tratamiento;
- c) Informado: que el titular tenga conocimiento previo al tratamiento, a qué serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento. Asimismo, de saber quién es el responsable que interviene en el tratamiento de sus datos personales, y su lugar o medio de contacto;
- d) Expreso: debe ser escrito e inequívoco, de forma tal que pueda demostrarse de manera indubitable su otorgamiento.
- e) Individualizado: debe existir mínimo un otorgamiento del consentimiento por parte de cada titular de los datos personales.

En este sentido, el consentimiento debe ser obtenido libre de coacción y basado en información veraz y clara, asimismo, debe ser comprobable. La doctrina señala que este principio es el eje fundamental a partir del cual se construye el derecho a la protección de datos personales y que conlleva la idea de la *autodeterminación informativa*. En suma, el consentimiento implica que todo tratamiento de datos requiere de nuestra autorización previa.

Para todo lo anterior, existe un deber de confidencialidad, que consiste en garantizar que sólo las personas autorizadas accedan a los datos personales para su tratamiento con la obligación de observar el deber de secreto.

El deber de confidencialidad subsiste aun después de finalizado el tratamiento de los datos y, también, después de terminada la relación laboral entre el ente público y las personas que realizaban el tratamiento de datos personales.

Este principio conlleva que, si el ente público contrata servicios que requieran el tratamiento de datos personales, éste deberá asegurarse de que, en los instrumentos jurídicos que correspondan a esa contratación, se estipule la obligación de garantizar la seguridad y confidencialidad de los sistemas de datos personales, así como la prohibición de

e) Cuando contraten o recurran a terceros para la prestación de un servicio que demande el tratamiento de datos personales. Los terceros no podrán utilizar los datos personales con propósitos distintos a aquellos para los cuales se les hubieren proporcionado y tendrán las responsabilidades legales que genere su actuación.

utilizarlos con propósitos distintos a los establecidos en el contrato, mismo que deberá contemplar penas convencionales en caso de incumplimiento.

Ejemplo de cláusula de confidencialidad: Las partes asumen la obligación de guardar secreto profesional sobre cuanta información pudieran recibir, gestionar y articular con relación a los datos personales y a no comunicarlos a terceros, salvo excepciones legales, así como a destruirlos, cancelarlos o devolverlos en el momento de la finalización de la relación contractual entre ambas partes, así como a aplicar las medidas de seguridad necesarias

Principio de seguridad, este consiste en garantizar que únicamente el responsable del sistema de datos personales o en su caso las personas debidamente autorizadas puedan llevar a cabo el tratamiento de los datos personales mediante procedimientos establecidos para este efecto.

3. Medidas de seguridad

El responsable deberá adoptar las medidas de índole técnica y organizativa que sean necesarias a fin de garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los datos de carácter personal y así evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Para ello, los lineamientos prevén la existencia de un documento de seguridad, cuya característica es la de ser un aspecto interno de la organización que sintetiza las políticas de seguridad, al recoger todas las medidas, normas, procedimientos, reglas y estándares técnicos para preservar la integridad del tratamiento de datos personales.

Desde el punto de vista jurídico, el cumplimiento de las medidas técnicas y organizativas dispuestas en el documento de seguridad, tiene como finalidad garantizar el derecho de protección de datos de carácter personal de los sistemas que almacena y trata el ente público para el cumplimiento de sus atribuciones legales.

El **documento de seguridad** debe contener como mínimo:

- El ámbito de aplicación.
- Las medidas, normas, procedimientos de actuación, reglas y estándares utilizados.
- Las funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal.
- La estructura de los sistemas de datos personales que contengan datos de carácter personal y la descripción de los sistemas de información que los tratan.
- El procedimiento de notificación, gestión y respuesta ante incidencias.
- Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

- Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.
- Los principios universales en materia de protección de datos establecen que el documento de seguridad deberá mantenerse actualizado y ser revisado siempre que se produzcan cambios relevantes en los sistemas de información o en el tratamiento de datos de la empresa o entidad.

a) Sistemas de datos

Los datos deben almacenarse en un sistema o conjunto organizado de información, de forma tal que se permita, en todo momento, el ejercicio de los derechos de acceso, rectificación y eliminación.

Es por lo anterior, que los sistemas de datos personales deben organizarse de tal manera que el acceso a los datos personales sea ágil y confiable.

Gracias a una organización técnica adecuada, es posible que las solicitudes de acceso a la información planteadas por los ciudadanos sean atendidas prontamente.

En el sector público, deberán los órganos y entes establecer políticas de seguridad que permitan esta agilidad en el trámite y en el procesamiento de información, con el objetivo que los ciudadanos puedan sentirse confiados en la gestión de datos que se realiza en las instituciones del Estado. Esto es muy importante de cara a la profundización de una cultura de acceso a la información pero, al mismo tiempo, de confianza de los ciudadanos en lo que se refiere a la entrega de sus datos personales para trámites propios de su relación con los órganos y entes gubernamentales.

Una política de transparencia y de protección de datos debería, entonces, tomar en cuenta los siguientes aspectos:

- a) La finalidad del sistema de datos personales y los usos previstos para el mismo.
- b) Las personas o grupos de personas sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
- c) El procedimiento de recolección de los datos de carácter personal.
- d) La estructura básica del sistema de datos personales y la descripción de los tipos de datos incluidos en el mismo.
- e) De la cesión de las que pueden ser objeto los datos.
- f) Las instancias responsables del tratamiento del sistema de datos personales.
- g) La unidad administrativa ante la que podrán ejercitarse los derechos de acceso, rectificación o eliminación.
- h) El nivel de protección exigible.

Las disposiciones que se dicten para la supresión de sistemas de datos personales, deben indicar el destino que vaya a darse a los datos contenidos en los mismos o, en su caso, las medidas previstas para su destrucción. Al respecto corresponde tener en cuenta que debe documentarse el tipo de datos que están siendo destruidos, sus titulares y quien es la persona encargada de hacerlo, así como quien supervisa la destrucción.

En este caso, podrán excluirse aquellos datos que, previa disociación, sean tratados para finalidades estadísticas o históricas.

El proceso de disociación de los datos puede ser tanto automático o manual y consiste en evitar la relación del dato con la persona a quien refiere. Esta disociación permite utilizar datos personales con fines científicos o históricos, sin provocar con ello lesiones al derecho a la autodeterminación informativa. Los Lineamientos contienen esta posibilidad en su Artículo 23.

b) Registro del sistema de datos

Es importante que los sistemas de datos personales en posesión de los entes públicos, se inscriban en el registro que al efecto habilite el IAIP, ya que esto permitirá a los interesados, conocer los sistemas de datos personales que obran en las distintas dependencias locales, y les facilitará, también, el ejercicio de sus derechos.

La información que debe contener el registro es similar a la del acuerdo de creación de un sistema de datos personales. Un sistema de datos personales es un conjunto organizado de archivos, registros, ficheros, bases o bancos de datos personales en poder de los órganos o entes públicos. Al respecto, no importa la forma en que hayan sido almacenados dichos datos, como tampoco interesa la forma específica en que hayan sido tratados, organizados o creados.

El acuerdo de creación de uno de estos sistemas deberá contener, entre otras referencias, una indicación de la finalidad del sistema de datos, el origen de los datos, el procedimiento de recopilación, la estructura básica del sistema de datos, y una indicación de los encargados de garantizar el acceso a los datos. Los Lineamientos regulan con mayor detalle, los campos que deben contener tanto el acuerdo de creación como los del registro:

- I. Denominación del sistema de datos personales, indicando normativa aplicable, así como la descripción de la finalidad y usos previstos.
- II. Nombre del sistema.
- III. El origen de los datos, indicando el colectivo de personas sobre las que se pretende obtener datos de carácter personal, o que resulten obligados a suministrarlos; su procedencia (propio interesado, representante, ente público, etc.), así como el

- procedimiento de obtención de los mismos (formulario, Internet, transmisión electrónica, etc.).
- IV. Nombre y cargo del responsable del sistema.
 - V. La estructura básica del sistema, con descripción detallada de datos identificativos y, en su caso, de los especialmente protegidos, así como las restantes categorías de datos de carácter personal; modo de tratamiento utilizado en su organización (manual o automatizado). En su caso, señalar los datos de carácter obligatorio y facultativo.
 - VI. Identificación del sistema, finalidades y usos previstos, así como el soporte en el que se encuentra.
 - VII. Las cesiones de datos que se tengan previstas, indicando, en su caso, los destinatarios o categorías de destinatarios.
 - VIII. La categoría de los datos personales contenidos en el sistema, forma de recolección y actualización de los mismos.
 - IX. La identificación de la unidad administrativa a la que corresponde el sistema de datos personales, así como del cargo del responsable.
 - X. Unidad administrativa en la que se encuentra el sistema.
 - XI. Domicilio oficial y dirección electrónica de la Oficina de Información Pública.
 - XII. Destino y personas físicas o morales a las que puedan ser transmitidos.
 - XIII. Indicación del nivel de seguridad que resulte aplicable: básico, medio o alto.
 - XIV. Modo de interrelacionar la información contenida en el sistema y el plazo de conservación de los datos.
 - XV. Teléfono y correo electrónico del responsable.
 - XVI. Normativa aplicable al sistema.
 - XVII. Indicación del nivel de seguridad aplicable: básico, medio o alto.

Un principio fundamental que se regula en el capítulo en estudio, es la obligación de cumplir con el denominado “**deber de información**” o “derecho de información al interesado”, el cual constituye el fundamento previo necesario para el correcto funcionamiento de un esquema jurídico de protección de datos, ya que sería difícil que se puedan ejercer derechos tales como el de acceso o de oposición al tratamiento de sus datos, si previamente no se conoce en qué sistema y bajo qué parámetros serán tratados los datos personales.

Los entes públicos, en concordancia con una política de protección de datos, deben tener claro que deben informar a las personas afectadas por un proceso de recopilación de informaciones, de manera expresa e inequívoca, sobre diversos extremos de este proceso. En primer lugar, debe darse referencia al ciudadano que sus datos se integrarán en un sistema de datos personales, que sus datos serán tratados para una específica finalidad relacionada con el trámite o procedimiento en el que el ciudadano interesado esté involucrado, así como lo que podría suceder con sus datos una vez recopilados.

Se suele tomar en cuenta en políticas existentes en la materia en otros países, entre otros, los siguientes extremos:

- 1) De la existencia de un sistema de datos personales, del tratamiento de datos personales, de la finalidad de la obtención de éstos y de los destinatarios de la información.
- 2) Del carácter obligatorio o facultativo de responder a las preguntas que les sean planteadas.
- 3) De las consecuencias de la obtención de los datos personales, de la negativa a suministrarlos o de la inexactitud de los mismos.
- 4) De la posibilidad para que estos datos sean difundidos, en cuyo caso deberá constar el consentimiento expreso del interesado, salvo cuando se trate de datos personales que por disposición de una Ley sean considerados públicos.
- 5) De la posibilidad de ejercitar los derechos de acceso, rectificación y eliminación y oposición.
- 6) Del nombre del responsable del sistema de datos personales y en su caso de los destinatarios.

En los casos en que los datos no fueron obtenidos directamente del interesado, el ente público debe hacer de su conocimiento los aspectos que conforman el deber de información dentro de un plazo prudencial, que suele fijarse en tres meses.

En este sentido, no hay obligación de hacerlo, si el interesado fue informado con anterioridad que:

- 1) Sus datos están incorporados en un sistema.
- 2) Del tratamiento.
- 3) La finalidad y destinatarios de la información.
- 4) De una posible difusión, en la que habrá que otorgar su consentimiento expreso, salvo que por ley sean considerados públicos.
- 5) De la posibilidad de ejercer los derechos ARCO contemplados en la legislación y en los lineamientos.

Entonces las excepciones al deber de informar son:

- 1) Que se haya informado al interesado con anterioridad.
- 2) Que así lo prevea expresamente una Ley.
- 3) Cuando los datos provengan de fuentes accesibles al público en general.
- 4) Cuando resulte imposible o exija un esfuerzo desproporcionado realizar tal comunicación, siempre atendiendo al número de interesados y antigüedad de los datos. En este caso deberán de tomarse cuidados especiales en virtud de la magnitud del sistema de datos personales. En el caso de sistemas muy grandes deberían proveerse medios de comunicación vía WEB a los afectados.

c) Medidas de seguridad. Datos sensibles

Otro aspecto importante a tomar en cuenta dentro de las medidas de seguridad del sistema de datos, es lo relativo a los **datos especialmente protegidos**, conocidos como datos sensibles. Este es un principio muy importante que establece que nadie está obligado a proporcionar datos como:

- 1) Origen étnico o racial.
- 2) Características morales o emocionales.
- 3) Ideología y opiniones políticas.
- 4) Creencias.
- 5) Convicciones religiosas.
- 6) Ideas filosóficas.
- 7) Preferencia sexual.

En este sentido, está prohibida la creación de sistemas de datos personales que tengan la finalidad exclusiva de almacenar este tipo de datos personales, con la excepción de que solo pueden ser tratados cuando:

- 1) Medien razones de interés general.
- 2) Así lo disponga una ley.
- 3) Lo consienta expresamente el interesado.
- 4) Con fines estadísticos o históricos, esto siempre y cuando se hubiera realizado previamente el procedimiento de disociación.

El procedimiento de disociación no es necesario en caso de estudios científicos o de salud pública.

Los **datos sensibles** están referidos a características de las personas que por su naturaleza provocarían una profunda lesión al ámbito de intimidad si son difundidos. Pertenecen a esta condición todos aquellos datos que tienen que ver con la salud, las creencias y prácticas religiosas o filosóficas, costumbres sexuales, entre otras. Se entiende que en el caso de los datos sensibles, estos solo podrían ser difundidos por la propia persona, ejerciendo para ello las condiciones propias del derecho a la intimidad, que como se estudió más atrás, tienen que ver con una donación específica de esa parte tan recóndita de su personalidad en un ámbito de confianza.

Es evidente que los datos sensibles podrían provocar rechazo y discriminación de la persona referida por ellos, basta pensar, por ejemplo, en ciertas condiciones de salud, padecimientos específicos o incluso las propias creencias religiosas o ideologías políticas, que en ciertas condiciones colocarían a la persona afectada ante riesgos de gravedad para su condición de ciudadano.

La vulnerabilidad que estos datos provocan exige un especial nivel de protección. Debido a que la Ley de Acceso a la Información Pública no es muy detallada al respecto, debe procurarse establecer políticas claras en relación a estos datos sensibles. No debe olvidarse que toda posibilidad de referir a las personas por estas características de su ámbito de intimidad los colocan ante riesgos inusitados de discriminación que se oponen directamente a toda la lógica del derecho a la autodeterminación informativa.

d) Datos de carácter personal obtenidos para fines policiales

Uno de los temas más delicados a los que se enfrenta una política de protección de datos tiene que ver con la eventual construcción de sistemas de datos personales para la investigación penal, tanto de carácter preventivo como también represivo. Voces que pretenden disminuir la importancia de este derecho y comprometer los esfuerzos que se realizan por doquier por garantizarlo, no dejan de decir que el derecho de la protección de datos personales es un obstáculo para una investigación penal eficiente. Esto último, por supuesto, no es cierto y es un argumento débil que desgraciadamente tiene algo de influencia en círculos políticos. Lo cierto es que el derecho de la protección de datos personales no limita que se recaben datos con fines de investigaciones penales, también de investigaciones administrativas, siempre y cuando se tomen ciertos recaudos y, en especial, se cuente con una autorización judicial de la recogida y tratamiento de los datos personales de interés.

La situación en el derecho comparado es muy variable, siendo la situación en Europa quizá más avanzada y más detallada al respecto, en virtud, principalmente de los esfuerzos supranacionales en dicho continente por garantizar el derecho a la autodeterminación informativa en el ámbito de la investigación penal.

En América Latina, en concreto en Centroamérica, el reconocimiento de limitaciones a la investigación penal derivadas del reconocimiento del derecho a la autodeterminación informativa no se han alcanzado como hubiera sido esperable y deseable se alcanzara. Esto último pudo haberse debido, por una parte, a la inadvertencia del legislador de la situación normativa en los Códigos Procesales Penales, que no contienen todavía un capítulo sobre la incidencia de la autodeterminación informativa en el ámbito de la investigación penal, pero también a que aun no termina de fraguarse la base para una discusión constitucional sobre las prohibiciones probatorias derivadas del derecho a la autodeterminación informativa en el campo penal.

En El Salvador, concretamente en el Art. 34 de la Ley de Acceso a la Información Pública, se contempla una excepción al principio del consentimiento del ciudadano interesado cuando el proceso de recabar datos se realiza con el objetivo de respaldar una investigación penal o administrativa. Otras referencias a la forma y contenido de las intervenciones en materia sancionatoria, tanto penal como administrativa, deberán

esperar un desarrollo mayor en una legislación sectorial que podría venir en un futuro no muy lejano.

En la doctrina comparada, especialmente alemana, se sugiere que estas intervenciones del poder penal en el ámbito de los datos personales deben ser legitimadas y justificadas a partir de una interpretación, caso por caso, de los extremos derivados del principio de proporcionalidad. Esto es, debe valorarse en cada caso que la intervención sea no sólo necesaria e idónea para cumplir el fin legal, sino también soportable, a nivel individual, para la persona afectada. Investigaciones penales de amplio espectro, sin ni siquiera un umbral de sospecha de comisión de un hecho delictivo, quedarían prohibidas por la violación que implicarían al principio de proporcionalidad.

Una discusión de estos temas aun debe plantearse en El Salvador, no obstante, la situación de la discusión científica es proclive a hacer a algunos aportes normativos que podrían alcanzarse sin grave afectación de los fines de la investigación penal y administrativa.

En algunos países, se incluyen limitaciones para el almacenamiento de datos con fines policiales y de evidente carácter preventivo. Una de las razones para ello es, por supuesto, que deben eliminarse una vez que dejaron de ser útiles para cumplir con esas funciones preventivas y eliminar el riesgo de que se puedan confundir las finalidades preventivas y represivas en una sola plataforma informativa. Esto último podría suceder si se construye una plataforma informativa con fines policiales que no establece separaciones de los datos recabados con fines preventivos de aquellos obtenidos con fines represivos.

La idea original que late en el trasfondo de estas disposiciones existentes en el derecho comparado, tiene que ver con el derecho al olvido, que no es más que una pretensión de gran valor para la democracia que es, en esencia, permitir al ciudadano reinventarse, reconstruirse y reinsertarse socialmente, una vez que la sanción penal ha tenido su acción, así como también cuando no haya interés en afectarle más allá de la investigación penal en la que tuvo que verse involucrado.

La normativa comparada suele sujetar la recopilación con fines policiales a limitaciones tales como que los datos recogidos sólo pueden ser aquellos estrictamente necesarios para la investigación concreta, con autorización judicial, y valoración de requisitos de proporcionalidad de la medida.

Junto a estas previsiones, se suele tomar en cuenta la prohibición de acceso a estos datos con fines policiales para objetivos distintos a los que originalmente permitieron su recogida y tratamiento, salvo que ello pudiera comprometer la defensa del Estado o la seguridad pública.

Los entes públicos están obligados a adoptar medidas de seguridad tan sólo por el hecho de contar con sistemas de datos personales y realizar tratamientos de datos, tanto de particulares, como de servidores públicos.

e) Medidas de seguridad. Características

Los entes públicos están obligados a adoptar medidas de seguridad tan sólo por el hecho de contar con sistemas de datos personales y realizar tratamientos de datos, tanto de particulares, como de servidores públicos.

Es por ello que el Artículo 12 de los Lineamientos contempla la obligación de establecer medidas de seguridad adecuadas y suficientes que eviten la alteración, pérdida, transmisión y acceso no autorizado a los datos personales.

Las medidas de seguridad, se entiende, son estándares mínimos impuestos por el ente u órgano público, que han de ser respetados para garantizar la integridad, exactitud y calidad de los datos.

Los Lineamientos no entran al detalle de establecer niveles en los criterios de seguridad que deben ser asumidos y puestos en práctica. Esto que ha sido propio de la legislación en la materia en otras latitudes, en El Salvador, deberá esperar a que se hagan avances decisivos en la incorporación de una política de protección de datos en los órganos del derecho público.

Esta derivación de políticas de seguridad en niveles, que van desde el más bajo, el intermedio y los más altos son de carácter acumulativo, y se integran con el objetivo de hacer un círculo de tutela que le permita al ciudadano y a las autoridades administrativas involucradas confiar en el procesamiento de datos que se realiza cotidianamente.

Es probable que habrá obligaciones de seguridad que se irán incorporando en el quehacer público salvadoreño, y estas obligaciones tendrán que ver con recaudos técnicos para la conservación de los datos, pero también para garantizar la calidad de los datos que eventualmente se compartirán con otros organismos públicos. Entre ellos pueden citarse, por ejemplo, disposiciones sobre controles de acceso, gestión de soportes técnicos de hardware y software, copias de respaldo y registro de incidencias, auditorías y controles periódicos.

Con todo, se puede sugerir que los órganos y entes públicos preparen documentos de seguridad, esto es, manuales de procedimientos de seguridad, que sirvan como instrumentos orientadores para los ciudadanos sobre los cuidados que se han tomado para la conservación de sus datos personales. Se entiende que serán requisitos

que procurarán garantizar la protección, confidencialidad, integridad y disponibilidad de los datos contenidos en dichos sistemas.

Puede sugerirse, además, que las medidas de seguridad y los manuales sobre ella, se construyan tomando en cuenta el tipo de datos que se conservarán en los diversos sistemas de datos. Esto último es muy variable y depende de cada administración pública.

La responsabilidad de la elaboración del documento de seguridad, recae en el responsable del sistema de datos personales.

En otros países se ha notado una tendencia a solicitar que las medidas de seguridad se vayan remozando en plazos precisos, usualmente de un año, conforme se produzcan cambios tecnológicos que pudieran repercutir en la integridad y calidad de los datos concernidos. Aquí tienen un papel importante medidas de carácter técnico como los registros de incidencias. Estos últimos llevan un acompañamiento cotidiano de los movimientos, cambios e interacciones con los bancos o sistemas de datos personales, y así poder rastrear quién, cuándo y por qué ha tenido acceso con dichos datos y en qué consistió la intervención.

Para poder llevar adelante un sistema funcional de incidencias, debe haber un sistema de identificación de quién tuvo acceso a los datos personales. Para ello se utilizan herramientas de hardware y software tales como la encriptación, uso de claves y firmas digitales, que sin duda ofrecen diversos niveles de certeza y de calidad en estas materias.

Se suele considerar importante también que las normas de seguridad tomen en cuenta el organigrama de la institución, así como los manuales de puestos, con el objetivo de dejar estas tareas de seguridad a funcionarios en específico, de tal manera que pueda realizarse un control también del cumplimiento de las tareas, sujetando su incumplimiento a responsabilidades administrativas pero también penales.

Uno de los aspectos esenciales en estos niveles de seguridad básicos es, sin duda, el de las copias de seguridad y recuperación. No contar con respaldos ante ataques informáticos o daños al sistema provocados por actos agresivos y de sabotaje, puede llevar al traste con la integridad del sistema pero también con el ejercicio de los derechos ciudadanos de acceso y control de los datos personales. Por ello, una medida de seguridad muy valiosa es garantizar protocolos de recuperación de los datos, de tal forma que haya garantía que ante una incidencia pueda recuperarse, reconstruirse y llegar al estado original de los mismos, antes del accidente o acto vandálico.

En ese contexto creciente de seguridad, y ahora en un nivel medio, sería deseable que el órgano o ente público provea consideraciones sobre el responsable de seguridad,

es decir, que defina a quien corresponde tomar las medidas, darles seguimiento y mantener sus estándares de calidad de manera periódica.

En otros países, se suele tomar en cuenta que la designación del responsable recae en una única persona, quien a su vez revisa las condiciones de seguridad de todos los sistemas de datos disponibles. No se trata que sea necesariamente un especialista en TIC's, podría ser también una persona que pueda llevar un control de las medidas organizativas cuando estas han sido ya dispuestas por el órgano público de una manera intensa.

Un área en espera de desarrollo en Centroamérica, en general, y en El Salvador, en concreto, es la figura de la auditoría de protección de datos personales. Se trata de un especialista que pueda verificar el cumplimiento de las disposiciones normativas en la materia, y establecer las condiciones en que el tratamiento de datos personales está teniendo lugar, incluyendo todas y cada una de sus fases (recogida, almacenamiento, tratamiento y transmisión).

En el derecho comparado coexisten sistemas de varias naturalezas: auditorías internas del ente y auditorías externas verificadas por órganos privados técnicos. Estos dos sistemas que pueden, por supuesto, coexistir, han demostrado su utilidad para intensificar el nivel de protección preventivo del derecho a la autodeterminación informativa.

Los informes de resultados proveídos por estas auditorías, provoca cambios importantes en las políticas de seguridad, subraya aquellos elementos necesarios de tomar en cuenta, y procura la mejora de aquellas políticas e instrumentos que tienen su punto de partida en el contexto de las políticas de seguridad interna que hayan sido asumidas.

En el derecho comparado se suele sugerir que los informes de auditoría sean entregados al órgano de control de la protección de datos. En El Salvador, cuya labor en esa materia ha sido encomendada al IAIP, debería de haber un análisis de estas auditorías en un plazo razonable (usualmente de 20 días) con el objetivo de tomar medidas institucionales que obliguen al órgano y haya acompañamiento de las transformaciones sugeridas.

Además de los niveles básicos e intermedios de seguridad, se sugieren niveles altos, que pueden venir acompasadamente una vez se hayan alcanzado los niveles previos. Resaltan, entre ellos, las así denominadas "pruebas con datos reales", que pretende garantizar que las pruebas sobre obtención de copias de seguridad y de recuperación de los datos no se realicen con datos reales, salvo que se asegure los niveles de seguridad y que esta prueba no dañará los datos personales conservados.

Nivel de seguridad alto. Además de las medidas del nivel básico y medio, *se conocen aquellas denominadas de nivel alto. Estas medidas tienen que ver con la manipulación y*

aseguramiento de los soportes de datos. Lo que se pretende, en síntesis, es que la información manipulada no sea inteligible, por si hubiera interés en conocerla, o manipulada, afectando la integridad y calidad de los datos.

En el derecho comparado se suelen incluir entre las medidas de seguridad de alto nivel aquellas que tienen que ver con la utilización intensiva de claves de acceso, encriptación y otros medios técnicos de aseguramiento.

Registro de acceso. Implica que el acceso a los sistemas de datos personales, está limitado exclusivamente al personal autorizado. En el caso en que los sistemas puedan ser utilizados por múltiples autorizados deben existir mecanismos que permitan identificar sus accesos.

Los mecanismos de registro de accesos suelen estar bajo el control de responsables del tratamiento de datos. Se entiende que su función es recopilar una detallada bitácora de quien accedió, en qué circunstancias, fecha y hora, qué parte del sistema y si el específico acceso fue autorizado o no. Como medida adicional, se suele sugerir mantener estos datos de acceso por un periodo mínimo de dos años, con el fin de cubrir contingencias que solo podrían ser descubiertas en un plazo razonable entre las auditorías periódicas del sistema.

Todas las aplicaciones o programas internos que traten con datos de carácter personal, deben configurarse para que registren y almacenen los datos de todas aquellas personas que acceden o intentan acceder a la aplicación.

Esta medida de seguridad se ve aumentada en el nivel alto para los sistemas automatizados respecto del registro de accesos: identificación, hora, fichero, tipo de acceso, autorizado o denegado. No es necesario este registro si el responsable del sistema es una persona física y es el único que accede al mismo.

Telecomunicaciones. No hay duda que una de las áreas más sensibles en la seguridad de un sistema de datos personales lo constituye la fase de la transmisión esos datos, tanto a nivel nacional como internacional.

La transmisión de datos tiene lugar en diversos contextos geográficos y tecnológicos, donde destacan, por ejemplo, las transmisiones mediante cable, conexión inalámbrica, y ultimamente microondas. Estas transmisiones de datos personales, no importa su medio, deben producirse de manera cifrada, de esta forma no podrían ser inteligibles o manipulables ni en el lugar de origen ni en el origen de llegada.

Los entes públicos realizan tratamiento de datos personales necesarios para el ejercicio de sus atribuciones, derivado de este tratamiento, deben atender una serie de obligaciones que reflejan la observancia de los principios básicos de la protección de datos, entre ellas:

- Informar al interesado con carácter previo al tratamiento de los datos de carácter personal.
- Recabar sólo datos imprescindibles para ejercer sus atribuciones.
- Facilitar a las personas el ejercicio de los derechos de los titulares.

4. Tratamiento de datos personales

La base de regulación de datos personales planteado en El Salvador requerirá el consentimiento del interesado.

El consentimiento del interesado implica, la manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual éste consiente el tratamiento de sus datos personales. Sin embargo, las regulaciones normativas, como ya ha sido posible ser analizado supra, contienen una serie de excepciones a este principio, en las cuales **no se requiere** del consentimiento para el tratamiento de datos personales. Destacan, entre ellas, cuando se esté en presencia del ejercicio de las atribuciones legales atribuidas a los entes públicos. Es el caso de la recaudación de impuestos o la recogida de datos con el fin de tomar decisiones en el campo de salud.

Existen procesamientos de datos naturales, como los que se dan en el contexto de las relaciones laborales: el trabajador, sujeto a un horario y al cumplimiento de una serie de instrucciones por parte de su patrono, somete datos de carácter personal para el control de dicha relación laboral, como sería el caso de tener una tarjeta de control horario, un sistema de control digital de asistencia y similares, con los cuales deja un rastro de su actividad laboral en el contexto de las tareas encomendadas. En estos casos, el consentimiento no resulta necesario, y es, de alguna manera, autorizado el procesamiento de datos y, en especial, su recogida, por la naturaleza de dicha relación. Es posible encontrar ejemplos similares en las relaciones negociales, en el cumplimiento de contratos públicos de construcción, por ejemplo, o en las mismas relaciones de los entes y órganos públicos con los ciudadanos. En estos casos, y siempre que haya cumplimiento de esas condiciones legales de funcionamiento, podría exceptuarse el consentimiento de la persona afectada.

Ejemplos del campo de salud y sanitario son también comprensibles. En ocasiones, el estado de salud del paciente no permite recabar su consentimiento para un tratamiento de datos (perfiles genéticos, elaboración de exámenes a profundidad de algún padecimiento, datos sobre grupos sanguíneos y sus diversas variables), por lo que en tales casos se suele no exigir que haya un consentimiento previo para tal tratamiento de datos. Lo anterior no exceptúa, por supuesto, que haya sigilo profesional del personal médico involucrado en los exámenes y en la recopilación de los datos derivados de tales intervenciones.

Siempre en el campo de la salud, pero ahora en materia de salud pública, medidas de urgencia para detener un brote o epidemia, llevaría al Estado a tomar decisiones para recoger información y someter a la población a pruebas obligatorias, donde el consentimiento debe exceptuarse.

Pueden imaginarse otros ámbitos de lo público donde el consentimiento no entra en consideración directa. Tal es el caso, por ejemplo, en materia electoral, donde los padrones electorales, la inclusión en listas de partidos y electores, podrían no considerar el consentimiento expreso de los ciudadanos.

En general, puede decirse que ninguno de estos tratamientos de datos sin consentimiento puede realizarse sin hacerse una consideración de los extremos del principio de proporcionalidad: necesidad, idoneidad y soportabilidad individual (prohibición de exceso) en el análisis de cada caso concreto.

Otros supuestos de interés serían los siguientes:

- Cuando hay transmisión de datos entre organismos gubernamentales para su tratamiento posterior con fines estadísticos, históricos o científicos.
- La cesión de datos personales de un ente público a un tercero prestador de un servicio. Ejemplos de ello pueden encontrarse en gran variedad, pero es especialmente plástico el de las compañías aseguradoras las cuales, vía contrato, pueden someter a tratamiento sin consentimiento previo, información de los empleados públicos que quieren hacer uso de su póliza de gastos médicos. Esto último, cuando dicho tratamiento de datos esté amparado en la finalidad legítima establecida en el contrato, y en el ámbito de las estipulaciones contractuales.
- Cuando media una orden judicial, si una autoridad jurisdiccional requiere acceso a ciertos datos para el desarrollo de su labor, no se considera que se vulnere este principio de consentimiento.
- Cuando los datos figuren en registros públicos en general y el tratamiento sea necesario, siempre que no se vulneren sus derechos y libertades. En la definición de fuente de acceso público contenida en los lineamientos, se dice que tienen este carácter: los registros públicos, los diarios, gacetas y boletines gubernamentales, así como otros medios oficiales de difusión. Por lo tanto, la consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, sin más exigencia que, en su caso, el pago de una contraprestación, para acceder a determinado medio de información.

En cuanto al consentimiento, éste puede ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. Lo anterior mediante solicitud presentada ante el órgano público que corresponda, a través de los formatos que para tal efecto emita el Instituto de Acceso a la Información Pública.

Los interesados deben especificar la finalidad para la cual se revoca el consentimiento para tratar sus datos personales, de acuerdo a ciertos datos mínimos como nombre del órgano público al que se dirige la revocatoria, nombre del ciudadano, datos de localización y notificación, indicación de los datos personales sobre los cuales se hace ejercicio de la revocatoria del consentimiento, así como la modalidad de acceso a sus datos personales, que puede ser por consulta directa, copia simple o certificada.

El órgano o ente público deberá proceder conforme a la expresión de voluntad del ciudadano y proveer a que se cumpla en un plazo razonable.

En caso de que sea procedente la solicitud de revocación del consentimiento, el responsable debe cesar en el tratamiento de los datos, sin perjuicio de la obligación de bloquear los datos. Esta decisión, por supuesto, depende de la naturaleza de los datos, las razones expresadas por el ciudadano y las circunstancias en que hace ejercicio de sus facultades legales.

El interesado podrá revocar su consentimiento mediante solicitud presentada ante la Oficina pertinente, a través de los formatos que para tal efecto emita el Instituto.

En el supuesto de que los datos hubieren sido cedidos previamente, el responsable, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios. También se prevé que ante la improcedencia de la revocación del consentimiento, el interesado podrá ejercer su derecho de cancelación. Esto es muy frecuente que se regule en las disposiciones legales sobre cesión de datos, y El Salvador deberá esperar, quizá, a una regulación más específica de carácter sectorial.

Por otra parte, en los supuestos de utilización o cesión de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de derechos de las personas, el Instituto podrá revisar las condiciones en que se ha realizado la cesión de datos.

En otros ordenamientos jurídicos, si el requerimiento fuera desatendido, mediante resolución fundada y motivada, se puede bloquear tales sistemas, de conformidad con el procedimiento que al efecto se establece. Tal supuesto no ha sido considerado ni en la Ley ni en los Lineamientos que han sido establecidos para la regulación de la materia de protección de datos personales en El Salvador, pero conviene pensarse de cara a una regulación integral de la materia en el país.

5. Obligaciones de los entes públicos

La primera obligación a cumplir por parte de los entes públicos recae sobre el titular del mismo, ya que es quien debe designar al **responsable de los sistemas de datos**

personales. La Ley y los Lineamientos definen al Responsable de los Sistemas de Datos Personales como:

La persona física que decida sobre su protección y tratamiento, así como el contenido y finalidad de los sistemas El servidor público de la unidad administrativa a la que se encuentre adscrito el sistema de datos personales, designado por el titular del ente público, que decide sobre el tratamiento de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

El responsable del sistema de datos personales tiene, entre sus obligaciones, la de adoptar las medidas necesarias para evitar una vulneración en cualquiera de los principios de protección de datos y debe asegurarse que toda persona que intervenga en el tratamiento de datos del sistema bajo su responsabilidad los conozca y respete.

En tanto que el **usuario** es aquella persona física o moral externa al ente público, que le presta servicios para tratar datos personales o que implica el tratamiento de los mismos.

En estos casos, el responsable deberá asegurarse que el tratamiento de datos personales esté regulado en un contrato por escrito o en alguna otra forma que permita acreditar su celebración y contenido.

En este contrato debe estipularse que el usuario:

- Únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.
- No aplicará o utilizará los datos con una finalidad distinta a la que figura en el contrato.
- No comunicará los datos a otras personas.
- Adoptará las medidas de seguridad que se deban implementar para su tratamiento.
- Concluida la relación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable.

Por otra parte, en los **Lineamientos** se inserta la figura de **encargado** que se define como:

Los órganos de control de la protección de datos han sido creados con el objetivo de asegurar el cumplimiento de la legislación en la materia. En El Salvador, esta competencia ha sido asumida legalmente por el Instituto de Acceso a la Información Pública, pero sin los requerimientos normativos que acompañan las atribuciones de otros órganos similares en países de nuestro margen cultural, como México, Argentina, Uruguay o Costa Rica. Por ello la revisión

del estándar de protección de datos personales tendrá ciertas limitaciones, y una de las más importantes, es que el Instituto dependerá de las tareas que un encargado en cada oficina y órgano público pueda realizar.

El IAIP tiene competencias de comprobación, de inspección y de fiscalización, por lo que el desempeño, evolución y estandarización de los niveles de protección en los sistemas de datos personales del sector público puede alcanzarse de una manera razonable, con la esperanza que el estándar pueda elevarse conforme reglas sectoriales sean debidamente aprobadas por el legislador salvadoreño.

Las leyes que existen sobre la materia a nivel internacional normalmente atribuyen a las autoridades de control ciertas facultades tales como ordenar medidas cautelares, conferir o negar autorización para tratar determinada categoría de datos, así como ordenar la implementación de medidas de seguridad específicas y, en algunos casos, están dotadas de amplias facultades sancionadoras. Estas condiciones son algo deseable y que conviene pensar en ellas para una reforma normativa.

6. Instituto de Acceso a la Información Pública

En la República de El Salvador, el Instituto de Acceso a la Información Pública, es el encargado de dirigir y vigilar el cumplimiento de la Ley de Acceso a la Información Pública y los Lineamientos Generales de Protección a Datos Personales para el Sector Público, así como de las normas que de ella deriven.

Dicho Instituto es un órgano autónomo creado por la Ley de cita y cuenta con personalidad jurídica y patrimonio propios, autonomía presupuestaria de operación y de decisión en materia de transparencia y acceso a la información pública. El Instituto de Acceso a la Información Pública es, al mismo tiempo, la autoridad encargada de garantizar la protección y el correcto tratamiento de datos personales con la atribución de establecer, en el ámbito de su competencia, políticas y lineamientos de observancia general para el manejo, tratamiento, seguridad y protección de los datos personales que estén en posesión de los entes públicos, así como expedir aquellas normas que resulten necesarias para su cumplimiento.

Fruto del ejercicio de esa atribución es la emisión, por parte del Instituto, de los Lineamientos Generales para la Protección de Datos Personales en el Sector Público, de acuerdo a las atribuciones legales conferidas por la Ley en mención.

El Artículo 35 de los Lineamientos sobre Protección de Datos contiene las siguientes tareas que ha de cumplir el IAIP en sus funciones de órgano de control de la protección de datos personales en El Salvador:

- a) Reglamentar la Ley de Acceso a la Información Pública, específicamente lo que refiere a las acciones de protección de datos personales, procedimientos de inscripción, registro, denuncias y sanciones con su categorización según la gravedad de la falta, en un plazo de seis meses a partir de la entrada en vigor de los presentes lineamientos.
- b) Elaborar un manual de protección de datos dirigido al Sector Público, en un plazo máximo de un mes a partir de la entrada en vigor de los presentes lineamientos.
- c) Elaborar e iniciar un plan de capacitación sobre datos personales dirigida al Sector Público con el fin de implementar los presentes lineamientos y el manual de protección de datos, en un plazo máximo de un mes a partir de la publicación de este último.
- d) Elaborar las recomendaciones sobre las medidas de seguridad que se mencionan en los presentes Lineamientos, a más tardar en un plazo de un mes a partir de su entrada en vigor.

En el ejercicio de sus atribuciones, el Instituto deberá emplear procedimientos automatizados, de acuerdo con las mejores herramientas tecnológicas a su alcance.

Las dependencias y entidades deberán permitir a los servidores públicos del Instituto o a terceros previamente designados por éste, el acceso a los lugares en los que se encuentran y operan los sistemas de datos personales, así como poner a su disposición la documentación técnica y administrativa de los mismos, a fin de supervisar que se cumpla con la Ley y los Lineamientos.

En los siguientes párrafos, se presenta una breve sistematización de las atribuciones del Instituto en materia de protección de datos personales:

- 1) **Difusión, asistencia y promoción.** El IAIP es responsable de la difusión de las disposiciones legales y reglamentarias aplicables al tratamiento de datos personales. Además de brindar asistencia tanto a los titulares de datos como a los responsables de los sistemas que los contienen. A esta tarea, se suma la de realizar acciones de promoción en la materia, por ejemplo, mediante el desarrollo de eventos que fomenten la profesionalización de los servidores públicos sobre la protección de datos personales.
- 2) **Registro.** Es responsable de llevar un registro de los sistemas de datos personales en posesión de los entes públicos, quienes deben notificar al Instituto la creación, modificación o supresión de sistemas de datos personales.
- 3) **Facultades normativas.** Tiene facultades normativas, ya sea de orden general, que se concreta en disposiciones de orientación como los “Lineamientos”, o bien particular, mediante la emisión de dictámenes y pronunciamientos específicos.
- 4) **Facultad revisora.** Es la instancia ante la cual los particulares pueden presentar un recurso de apelación si consideran que la respuesta a su solicitud de un derecho les agravia. Las resoluciones que emita serán definitivas, inatacables y obligatorias.

7. Derechos del ciudadano y procedimiento para su ejercicio

Un aspecto fundamental de los sistemas jurídicos en materia de protección de datos lo constituye el establecimiento de los derechos de los ciudadanos:

- A.** Acceso.
- R.** Rectificación.
- C.** Corrección y Eliminación.
- O.** Oposición

La posibilidad de ejercer estos derechos es lo que dota a la persona de una verdadera facultad de disposición sobre sus propios datos personales, ya que mediante ellos:

- Puede conocer qué datos tienen los entes públicos.
- Rectificarlos en caso de errores.
- Cancelarlos si dejaron de ser necesarios.
- Oponerse a su tratamiento si es que fueron obtenidos sin su consentimiento.

La Ley establece la posibilidad de ejercer los derechos a toda persona, y precisa que se trata de derechos independientes, por lo que el ejercicio de alguno no es condicionante ni impedimento para ejercer otro.

Por tanto, cualquier persona puede ejercitar los derechos de acceso, rectificación, oposición y eliminación sobre datos de carácter personal que le conciernan tratados por los entes públicos.

Un requisito indispensable para el ejercicio de estos derechos es la identificación del interesado o, en su caso, la de su representante legal. Mediante los derechos mencionados, toda persona tiene derecho a que se le informe gratuitamente del origen de sus datos y a saber a qué otras personas o entidades, sean de derecho público o privado, han sido comunicados.

Este derecho se complementa con el de rectificar la información incorrecta o no actualizada, con el derecho a solicitar que se destruyan aquellos datos que sean inexactos o incompletos, o aquéllos que no cumplan el principio de adecuación con la finalidad para la que fueron recabados.

A continuación describiremos cada uno de estos derechos:

- **Derecho de Acceso.** Permite solicitar y obtener información de los datos personales sometidos a tratamiento, la finalidad, su origen, así como las comunicaciones realizadas o previstas.

Asimismo, permite obtener datos concretos, así como los datos incluidos en un determinado sistema o la totalidad de los datos sometidos a tratamiento en los sistemas de datos personales en posesión de un ente público.

- **Derecho de Rectificación.** Otorga la facultad de solicitar que se modifiquen los datos que resulten inexactos o incompletos con respecto a la finalidad para la cual fueron obtenidos. Los datos deben ser considerados exactos cuando:
 - 1) Corresponden a la situación actual.
 - 2) Reflejen hechos constatados en un procedimiento administrativo o judicial.
- **Derecho de Eliminación.** Procede cuando los datos son inadecuados o excesivos:
 - 1) *Inadecuados* cuando no guardan relación con el ámbito de aplicación y finalidad por la cual fueron recabados, o bien, si dejaron de ser necesarios con respecto a dicha finalidad.
 - 2) *Excesivos*, si los datos obtenidos son más de los estrictamente necesarios en relación a dicha finalidad.

La cancelación también procede cuando el tratamiento de nuestros datos personales no se ajuste a lo dispuesto en la Ley o en los Lineamientos.

Aquí cabe recordar el principio de calidad que determina que, los datos personales recabados deben ser ciertos, adecuados, pertinentes y no excesivos con relación al ámbito y finalidad para los que fueron obtenidos.

La cancelación no implica la desaparición física del dato de modo tal que no permita su recuperación posterior, sino que existe un paso intermedio en el que se bloquea el dato y sólo permanece accesible para algunos y en determinadas circunstancias, como es el caso de autoridades públicas y jurisdiccionales para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante los plazos de prescripción aplicables.

Pensemos, por ejemplo, en la responsabilidad administrativa, la cual tiene plazos de prescripción para imponer sanciones que van desde los tres hasta los cinco años, por lo que los datos relacionados con este tema tienen que conservarse hasta que ese tiempo transcurra.

En caso de que se realice cualquier rectificación o cancelación sobre unos datos que previamente fueron cedidos, el responsable tendrá que notificar al cesionario dicha actuación para que éste a su vez efectúe las operaciones correspondientes sobre los datos cedidos.

- **Derecho de Oposición.** Mediane el derecho de oposición, el interesado también puede pedir que no se lleve a cabo o que cese el tratamiento de sus datos de carácter

personal. Las razones pueden ser por falta de consentimiento en el tratamiento, desviación del fin o por la obtención ilegal de los datos que están siendo tratados de cualquier forma.

Los derechos mencionados no son absolutos, por lo que el responsable del sistema de datos personales podrá denegarlos cuando exista una causa legal o justificada para ello.

En este sentido, no procede la rectificación si se trata de datos que:

- Reflejen hechos que formen parte de un procedimiento administrativo o un proceso judicial.
- Resulta imposible o exija esfuerzos desproporcionados, como podría ser el caso de una solicitud para que se corrijan datos de un expediente laboral de 1980 que ya no se encuentre en los archivos del ente público.

Puede denegarse la cancelación cuando:

- Exista un deber de conservación de los datos.
- Pudiera afectar derechos o intereses legítimos de otras personas, como lo es el propio Estado. En este sentido, se puede negar la cancelación de datos por motivos de seguridad pública.

En cuanto al procedimiento de ejercicio de derechos, la aplicación cotidiana de cualquier instrumento jurídico requiere del establecimiento de un procedimiento preciso y claro que facilite la concreción, en el terreno de lo práctico, de los preceptos y fundamentos que tutela.

Actualmente, los mecanismos para la actuación en materia de protección de datos personales se concentran a unas pocas normas de la Ley de Acceso a la Información Pública, que se complementan con los “Lineamientos” recientemente aprobados por el IAIP. Con este marco normativo, y el eventual crecimiento de decisiones en la materia, que informarán, a no dudarlo, el quehacer administrativo nacional en la materia, puede decirse se tiene un marco básico que podría contribuir a impulsar los primeros pasos en la realización de la aspiración de tutela de los datos personales en El Salvador.

En este sentido, el procedimiento para el ejercicio de los derechos establecido en la Ley y los Lineamientos es aun incipiente, pero señala los mecanismos iniciales para dar cumplimiento a esta necesidad.

Instancia ante la que se presenta la solicitud

Todos los entes públicos, los entes obligados según el Artículo 7 de la Ley de Acceso a la Información Pública, así como los concesionarios, estos últimos como ejecutores de

función pública, deben contar con una oficina encargada, entre otras funciones, de recibir las solicitudes para el ejercicio de derechos.

Medios de acceso

Recordemos que estos derechos sólo los puede ejercer el titular de los datos (interesado), o en su caso, su representante legal, como sería el caso del padre en relación con sus hijos menores de edad, o los tutores y las personas sujetas a su tutela. Existen diversos medios para la presentación de una solicitud:

- 1) Por escrito material, o enviado por correo ordinario, certificado o mensajería.
- 2) Verbal, de manera oral y directa, la cual será capturada por el responsable en el formato respectivo
- 3) Correo electrónico a la dirección de correo electrónico.

Requisitos

A fin de que el Ente comprenda la forma adecuada, en cualquiera de los medios de acceso disponibles, es necesario que en la solicitud se proporcionen los siguientes datos:

- 1) Ente público a quien se dirige la solicitud.
- 2) Nombre completo y, en su caso, el de su representante legal.
- 3) Descripción clara y precisa de los datos personales respecto de los que se busca ejercer algún derecho.
- 4) Cualquier otro elemento que facilite su localización.
- 5) El domicilio, u otro medio para recibir notificaciones

Además de estos requisitos, existen algunos otros que son específicos del derecho que se vaya a ejercer:

- **Derecho de acceso:** indicar la modalidad en la que prefiere se otorgue el acceso que puede ser consulta directa, copias simples o certificadas.
- **Derecho de rectificación:** señalar el dato erróneo y la corrección que deba realizarse, acompañado de la documentación que lo avale.
- **Derecho de eliminación:** indicar las razones por las cuales se considera que el tratamiento de los datos no se apegan a las disposiciones normativas.

Si sucede que la solicitud no es clara o no cumple con todos los requisitos que ya se han mencionado, el responsable puede, después de recibida la solicitud, pedir que se corrijan las deficiencias que detectó. De lo contrario, no se dará trámite a la solicitud, pues se tendrá por no presentada. Cabe precisar que este requerimiento interrumpe el plazo para dar respuesta.

Tiempos y tipo de respuesta

Una vez que el responsable recibe la solicitud mediante cualquiera de los medios previstos, se realiza un proceso interno de análisis para determinar la aceptación o rechazo de la misma. El ente público cuenta con un plazo de diez días hábiles para responderla, contados a partir de la fecha de la solicitud, según lo regula el artículo 36 del de la Ley de Acceso a la Información Pública.,

La respuesta a la solicitud puede ser:

- *Procedente*, esto es decir, el ente estará dando una respuesta positiva a la petición del ciudadano, y deberá hacerlo de su conocimiento a través del medio indicado para recibir notificaciones. La determinación se hará efectiva dentro de los siguientes diez días.
- *No procedente*, significa que se ha negado la petición realizada y la respuesta debe especificar las razones y las normas jurídicas aplicables que determinaron la negativa.

Esta respuesta debe estar suscrita y firmada por el responsable del ente público que corresponda. Hay un plazo de 30 días en el Artículo 36, para las hipótesis contenidas en el literal d), cuando la solicitud sea admitida y se indiquen, con ello, las modificaciones, o bien, de manera motivada, por qué no se procedió a las reformas solicitadas por el ciudadano.

En caso de que los datos personales sobre los cuales se está solicitando ejercer un derecho no se localicen en los sistemas del ente, se elaborará un acta, misma que se dará a conocer dentro del plazo de respuesta. En esta acta, se dará cuenta de los sistemas en que fueron buscados los datos personales del ciudadano y deberá estar firmada por un representante del órgano interno de control y del responsable del sistema de datos personales.

Acreditación de identidad para recibir la respuesta: Es importante que independientemente del medio a través del cual se reciba la solicitud, es necesario que el ciudadano acredite su identidad o, en su caso, la personalidad, identidad y facultades de su representante legal, esto debe hacerse en el momento que se presente a la oficina pertinente para obtener la respuesta sobre la solicitud de tus datos personales.

Para acreditar la identidad o la de su representante legal, se debe de presentar cualquier documento oficial en original como:

- Credencial para votar.
- Pasaporte vigente.
- Cédula profesional.

Del pago de derechos:

La Ley establece que el trámite de la solicitud es gratuito, lo cual constituye un principio comúnmente adoptado en las leyes sobre la materia. Sin embargo, se prevé que el solicitante debe cubrir los costos de reproducción de los datos solicitados.

Estos derechos se cobrarán previo a la entrega de la información y se calcularán atendiendo a los costos de los materiales, del envío y, en su caso, de la certificación de documentos.

8. Recursos

Un recurso administrativo es un medio de defensa con el que cuenta un ciudadano en contra de los actos de autoridad que considere ilegales y que le causen un agravio específico; se interpone ante el mismo órgano de autoridad, su superior jerárquico o la instancia que determine la Ley, para que ese acto sea revocado (es decir, dejado sin efectos) o bien modificado. Cabe señalar que el órgano que resuelve el recurso también puede confirmar el acto que se impugna o recurre.

La Institución responsable del sistema de datos personales tiene la obligación de informar al ciudadano en la respuesta a su solicitud, sobre el derecho que tiene a presentar un recurso de apelación ante el Instituto de Acceso a la Información Pública, así como el modo y plazo que tiene para hacerlo.

Ahora bien, si el recurso de apelación se presenta por falta de respuesta del Ente Público, el plazo para presentarlo se cuenta a partir del momento en que concluye el período que tenía el Ente para dar contestación a la solicitud, en este caso, basta que el solicitante acompañe el documento que pruebe la fecha en que presentó la solicitud.

El recurso de revisión debe cumplir los requisitos establecidos por el Artículo 84 de la LAIP, esto es, indicación de:

- a) La dependencia o entidad ante la cual se presentó la solicitud.
- b) El nombre del recurrente y el lugar o medio para recibir notificaciones, fax o correo electrónico.
- c) La fecha en que se notificó al recurrente.
- d) El acto recurrido y los puntos petitorios.

Si se da el caso de que el recurrente no cumple con alguno de los requisitos mencionados, el Instituto, en un plazo no mayor de tres días hábiles (Artículo 86 LAIP), lo prevendrá para que en un período de tres días hábiles corrija las irregularidades encontradas.

Procedimiento

Una vez presentado el recurso, el Instituto tiene 15 días hábiles para emitir una resolución a través del siguiente procedimiento:

- 1) El IAIP revisa y emite el acuerdo de correspondiente (puede ser de admisión, prevención o desechamiento) dentro de los 3 días hábiles siguientes.
- 2) En caso de no cumplir con alguno de los requisitos establecidos, el IAIP puede solicitarte que se corrijan las deficiencias en un lapso máximo de 3 días hábiles (prevención).
- 3) Admitido el recurso o denuncia, el Instituto lo someterá a uno de sus comisionados el caso de manera rotativa. El comisionado designado deberá, dentro de los quince días hábiles siguientes a la admisión del recurso o denuncia, dar trámite a la solicitud, formar el expediente, recabar pruebas y elaborar un proyecto de resolución que someterá al pleno del Instituto. Este comisionado no participará en las decisiones del pleno referentes al caso.
- 4) Admitido el recurso, esto será comunicado al interesado y al ente obligado, el que deberá rendir informe dentro de un plazo de siete días hábiles a partir de la notificación. En caso de denuncia o si en el escrito de interposición del recurso se hiciera denuncia de una infracción por parte de un servidor público, éste también será notificado inmediatamente y podrá justificar su actuación y alegar su defensa en el mismo plazo de siete días hábiles.
- 5) Las partes podrán ofrecer pruebas hasta el día de la celebración de la audiencia oral. Serán admitidos los medios de prueba reconocidos en el derecho común, en lo que fueren aplicables, incluyendo los medios científicos idóneos. Las pruebas aportadas en el proceso serán apreciadas según las reglas de la sana crítica.
- 6) El Instituto celebrará una audiencia oral con las partes en la cual conocerá la prueba y el comisionado designado presentará el proyecto de resolución.
- 7) Cuando haya causa justificada, el pleno del Instituto podrá ampliar, por una vez y hasta por un período de diez días hábiles el plazo para celebrar la audiencia. La resolución motivada en la que se determine nueva fecha para la audiencia será notificada a las partes inmediatamente.

Tipos de resolución

El Instituto puede resolver los recursos en estos sentidos:

- a. Desestimar el recurso por improcedente o sobreseerlo.
- b. Confirmar la decisión impugnada del Oficial de Información.
- c. Confirmar la inexistencia de la información pública solicitada.
- d. Revocar o modificar las decisiones del Oficial de Información y ordenar a la dependencia o entidad que permita al particular el acceso a la información solicitada o a los datos personales, que reclasifique la información, o bien, que modifique tales datos.

- e. Establecer sanciones o requerir el trámite de imposición de las mismas a las autoridades respectivas.

Las resoluciones del Instituto pueden ser cuestionadas por los particulares ante la Sala de lo Contencioso Administrativo de la Corte Suprema de Justicia.

La Sala de lo Contencioso Administrativo tendrá acceso a la información confidencial cuando la considere indispensable para resolver el asunto sometido a su conocimiento. Dicha información deberá ser mantenida con ese carácter y no será agregada en el expediente judicial.

9. Infracciones

Las infracciones constituyen mecanismos coercitivos para exigir el cumplimiento de las leyes.

Infracción

Se entiende por infracción la transgresión, quebrantamiento, violación, incumplimiento de ley, reglamento, convenio, tratado, contrato u orden. Los artículos 76 y siguientes de la Ley de Acceso a la Información Pública establece una serie de infracciones que serían aplicables tanto a las violaciones al derecho de acceso a la información, como también al tema de protección de datos personales. Algunas de las infracciones contra los derechos ARCO estarían consideradas en las infracciones muy graves, como lo es la alteración de información, entregar o difundir información reservada, o cuando mantenga la información bajo su custodia de manera desactualizada. Ciertamente es que estos supuestos podrían hacer referencia más directa a los derechos de acceso a la información pública, pero pueden ser aplicados también a los derechos de protección de datos personales.

Son infracciones muy graves:

- a) Sustraer, destruir, ocultar, inutilizar o alterar, total o parcialmente, información que se encuentre bajo su custodia o a la que tengan acceso o conocimiento con motivo de su empleo, cargo o comisión.
- b) Entregar o difundir información reservada o confidencial.
- c) No proporcionar la información cuya entrega haya sido ordenada por el Instituto.
- d) El incumplimiento por parte del funcionario competente de nombrar a los Oficiales de Información.
- e) Negarse a entregar la información solicitada, sin la debida justificación.
- f) Tener la información bajo su custodia de manera desactualizada, desordenada, en violación ostensible a las medidas archivísticas establecidas en esta ley y por el Instituto.

Son infracciones graves

- a) Actuar con negligencia en la sustanciación de las solicitudes de acceso a la información o en la difusión de la información a que están obligados conforme a esta ley.
- b) Denegar información no clasificada como reservada o que no sea confidencial.
- c) No proporcionar la información cuya entrega haya sido ordenada por un Oficial de Información.
- d) Proporcionar parcialmente o de manera ininteligible la información cuya entrega haya sido ordenada por el Instituto.
- e) Invocar como reservada información que no cumple con las características señaladas en esta ley. La responsabilidad solo existirá cuando haya una resolución previa respecto del criterio de clasificación de esa información.
- f) Proporcionar parcialmente o de manera ininteligible la información cuya entrega haya sido ordenada por el Oficial de Información.

Son infracciones leves:

- a) Pedir justificación para la entrega de información.
- b) Elevar los costos de reproducción de la información sin justificación alguna.
- c) No proporcionar la información en el plazo fijado por esta ley.

Sanciones

Por la comisión de las infracciones señaladas en el artículo anterior, se impondrán al funcionario público con facultad para tomar decisiones dentro de las atribuciones de su cargo las siguientes sanciones:

- a) Por la comisión de infracciones muy graves, se impondrá al infractor una multa de veinte a cuarenta salarios mínimos mensuales para el sector comercio y servicios. La comisión de dos o más infracciones muy graves en el plazo de trescientos sesenta y cinco días, dará lugar, en función de los criterios de graduación del artículo siguiente, a la suspensión de funciones por el término de treinta días calendario ordenada por la autoridad superior correspondiente, salvo si la conducta es causal de destitución de acuerdo con el régimen del servicio aplicable.
- b) Por la comisión de infracciones graves, se impondrá al infractor una multa de diez a dieciocho salarios mínimos mensuales para el sector comercio y servicios.
- c) Por la comisión de infracciones leves, se impondrá al infractor una multa cuyo importe será de uno hasta ocho salarios mínimos mensuales para el sector comercio y servicios.

Todas las sanciones impuestas serán publicadas en los medios electrónicos del Instituto e incorporadas como anexos del informe anual.

La cuantía de las multas que se impongan, dentro de los límites indicados, se graduará teniendo en cuenta lo siguiente:

- a) La existencia de intencionalidad o de reiteración en el hecho.
- b) La reincidencia, por comisión de infracciones de la misma naturaleza, sancionadas mediante resolución firme.
- c) La naturaleza y cuantía de los perjuicios causados por el infractor.
- d) La extensión del período durante el que se haya venido cometiendo la infracción.

La aplicación de las sanciones se entenderá sin perjuicio de las responsabilidades penales, civiles, administrativas o de otra índole en que incurra el responsable.

Síntesis

La protección de datos personales es un derecho que consiste en ofrecer a los individuos los medios jurídicos necesarios para controlar el uso de la información personal que les concierne.

La Ley de Acceso a la Información Pública, a efecto de garantizar la debida protección de los mismos, además de establecer los derechos, incluye una serie de principios rectores en el tratamiento de este tipo de datos, como son el de finalidad, calidad, consentimiento, deber de información, seguridad y confidencialidad.

Asimismo, la Ley establece la obligación, por parte de los entes públicos, de que los datos organizados en sus archivos, registros, ficheros, bases o bancos de datos personales —denominados en los Lineamientos como sistemas de datos personales— deban contar con medidas y tipos de seguridad, en atención a la sensibilidad de los datos contenidos en cada sistema.

De igual forma, los entes públicos deben realizar el tratamiento de los datos estrictamente necesarios para el ejercicio de sus atribuciones, atendiendo a una serie de obligaciones, que reflejan la observancia de los principios básicos de la protección de datos, como lo son:

- 1) Informar al interesado con carácter previo al tratamiento de datos.
- 2) Recabar sólo los datos imprescindibles para el ejercicio de sus atribuciones.
- 3) Facilitar a las personas el ejercicio de los derechos de Acceso, Rectificación y Eliminación.

En este sentido, todas aquellas personas que de alguna forma se relacionen con el tratamiento de los datos personales y, en particular el responsable del sistema, deben cumplir con ciertas obligaciones, entre las que se encuentran: guardar confidencialidad

de los datos que manejan en el ejercicio de sus funciones; presentar un informe anual sobre el cumplimiento de la Ley; actualizar los datos personales de oficio; establecer criterios específicos sobre medidas de seguridad, así como elaborar un plan de capacitación y resolver sobre el ejercicio de derechos.

Ahora bien, los titulares de los datos personales, cuentan con el derecho de recurrir ante el Instituto de Acceso a la Información Pública –órgano garante del derecho de acceso a la información pública, y de la protección de los datos personales, cuando se consideren agraviados por la respuesta que haya recaído a su solicitud para ejercer cualquiera de los derechos o ante la omisión de la misma, lo anterior a través de un recurso de apelación.

El procedimiento para el ejercicio de los derechos se hará de conformidad con lo dispuesto en la Ley y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

La Ley contiene un capítulo relativo a las infracciones que, derivadas del incumplimiento a estas disposiciones, las cuales serán aplicadas por el Órgano Interno de Control correspondiente y atenderán a las sanciones establecidas en la Ley.

Glosario

Autenticación: comprobación de la identidad de aquella persona autorizada para el tratamiento de datos personales.

Bloqueo: identificación y conservación de datos personales con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo, legal o contractual, de prescripción de estas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido este, se procederá a su cancelación del sistema a que correspondan.

Cesionario: persona física o moral, pública o privada, a la que un ente público realice una cesión de datos personales.

Cesión de datos personales: toda obtención de datos resultante de la consulta de un archivo, registro, base o banco de datos, una publicación de los datos contenidos en él, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta a la interesada, así como la transferencia o comunicación de datos realizada entre entes públicos.

Cifrado de datos: el cifrado se puede entender como el hecho de guardar algo valioso dentro de una caja fuerte cerrada con llave. Los datos confidenciales se cifran con un algoritmo de cifrado y una clave que los hace ilegibles si no se conoce dicha clave. Las claves de cifrado de datos se determinan en el momento de realizar la conexión entre los equipos. El uso del cifrado de datos puede iniciarse en su equipo o en el servidor al que se conecta.

Consentimiento: autorización o permiso para que se haga algo.

Copia de respaldo: COPIA de los datos de un archivo informático en un soporte que posibilite su recuperación.

Datos disociados: aquellos que no permiten la identificación de un afectado o interesado.

Datos personales: la información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable. Tal y como son, de manera enunciativa y no limitativa: el origen étnico o racial, características físicas, morales o emocionales, la vida afectiva y familiar, el domicilio y teléfono particular, correo electrónico no oficial, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas y filosóficas, estado de salud, preferencia sexual, la huella digital, el ADN y el número de seguridad social, y análogos.

Documento de seguridad: instrumento que establece las medidas y procedimientos administrativos, físicos y técnicos de seguridad aplicables a los sistemas de datos personales necesarios para garantizar la protección, confidencialidad, integridad y disponibilidad de los datos contenidos en dichos sistemas.

Documentos: los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas, o bien cualquier otro registro en posesión de los entes públicos sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier soporte, análogos escrito, impreso, sonoro, visual, electrónico, informático u holográfico.

Eliminación: supresión de determinados datos de un sistema de datos personales previo bloqueo de los mismos.

Encargado: servidor público que en ejercicio de sus atribuciones, realiza tratamiento de datos personales de forma cotidiana.

Enlace: servidor público que funge como vínculo entre el ente público y el Instituto para atender los asuntos relativos a la Ley de Protección de Datos Personales.

Fuente de acceso público: aquella consulta que puede ser realizada por cualquier persona, no impedida por una norma limitativa, sin más exigencia que, en su caso, el pago que genere el acceso a un determinado medio de información. Tendrán el carácter de fuentes de acceso público los registros públicos, los diarios, gacetas y boletines gubernamentales, así como otros medios oficiales de difusión.

Incidencia: cualquier anomalía que afecte o pudiera afectar la seguridad de los datos personales.

Inequívoco: que no admite duda o equivocación.

Inmovilización: medida cautelar que consiste en la interrupción temporal en el uso de un sistema de datos personales ordenada por el Instituto en los supuestos de tratamiento ilícito de datos de carácter personal.

Interesado: persona física titular de los datos personales que sean objeto del tratamiento al que se refiere la presente ley.

Oficina de Información Pública: la unidad administrativa receptora de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales en posesión de los entes públicos, a cuya tutela estará el trámite de las mismas, conforme a lo establecido en esta ley y en los Lineamientos que al efecto expida el Instituto.

Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a una persona física identificada o identificable.

Responsable: el servidor público de la unidad administrativa a la que se encuentre adscrito el sistema de datos personales, designado por el titular del ente público, que decide sobre el tratamiento de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

Responsable de seguridad: persona a la que el responsable del sistema de datos personales asigna formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Revocar: dejar sin efecto una concesión, mandato o resolución.

Sistema de datos personales: conjunto organizado de datos personales que estén en posesión de los entes públicos, contenidos en archivos, registros, ficheros, bases o bancos de datos, que permita el acceso a datos con arreglo a criterios determinados, cualquiera que fuere la modalidad de su creación, almacenamiento, organización o acceso.

Soporte electrónico: son los medios de almacenamiento inteligibles solo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs y DVDs), discos magnetoópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil.

Soporte físico: son los medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados “a mano” o “a máquina”, fotografías, placas radiológicas, carpetas, expedientes, demás análogos.

Transmisión de datos: cualquier traslado, comunicación, envío, entrega o divulgación de los datos.

Tratamiento de datos personales: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos automatizados o físicos, aplicados a los sistemas de datos personales, relacionados con la obtención, registro, organización, conservación, elaboración, utilización, cesión, difusión, interconexión o cualquier otra forma que permita obtener información de los mismos y facilite al interesado el acceso, rectificación, cancelación u oposición de sus datos.

Usuario: aquel autorizado por el ente público para prestarle servicios para el tratamiento de datos personales.

Vulneración: transgresión, quebranto, violación de una ley o precepto.

Consortio Liderado por



Socios Coordinadores



Participan más de 80 Socios Operativos y Entidades Colaboradoras de Europa y América Latina

EUROsocial es un programa de cooperación regional de la Unión Europea con América Latina para la promoción de la cohesión social, mediante el apoyo a políticas públicas nacionales, y el fortalecimiento de las instituciones que las llevan a cabo. EUROsocial pretende promover un diálogo euro-latinoamericano de políticas públicas en torno a la cohesión social. Su objetivo es contribuir a procesos de reforma e implementación en diez áreas clave de políticas, en ciertas temáticas, seleccionadas por su potencial impacto sobre la cohesión social. El instrumento del que se dota es el de la cooperación institucional o aprendizaje entre pares: el intercambio de experiencias y la asesoría técnica entre instituciones públicas de Europa y de América Latina.

