Establecimiento de políticas armonizadas en el mercado de las Tecnologías de la Información y la Comunicación en los países ACP

Privacidad y protección de datos:

Modelos de directrices para políticas y textos legislativos

HIPCAR

Armonización de políticas, legislación y procedimientos reglamentarios de las TIC en el Caribe

Establecimiento de políticas armonizadas en el mercado de las Tecnologías de la Información y la Comunicación en los países ACP

Privacidad y protección de datos:

Modelos de directrices para políticas y textos legislativos

HIPCAR

Armonización de políticas, legislación y procedimientos reglamentarios de las TIC en el Caribe

Descargo de responsabilidad

Este documento ha sido elaborado con el apoyo financiero de la Unión Europea. Los puntos de vista expuestos en el mismo no reflejan necesariamente los de la Unión Europea.

Las denominaciones empleadas y la presentación del material, incluidos los mapas, no representan en absoluto opinión alguna de la UIT en relación con la situación jurídica de cualquier país, territorio, ciudad o zona geográfica, o en relación con las fronteras o límites de los mismos. Las menciones a empresas concretas o a ciertos productos no significan que la UIT los recomiende o respalde frente a otros de similar naturaleza que no se mencionan. Este informe no ha pasado por una revisión editorial.

Por favor, tenga en cuenta la protección del medioambiente antes de imprimir este informe.

Prólogo

Las tecnologías de la información y la comunicación (TIC) están configurando el proceso de mundialización. Al reconocer su potencial para acelerar la integración económica de la región del Caribe y acrecentar así su prosperidad y transformación social, el Mercado y la Economía Comunes de la Comunidad del Caribe (CARICOM) ha elaborado una estrategia de TIC centrada en una conectividad y un desarrollo fortalecidos.

La liberalización del sector de las telecomunicaciones es uno de los elementos fundamentales de dicha estrategia. La coordinación de toda la región resulta esencial para que las políticas, legislaciones y prácticas resultantes del proceso de liberalización de cada país no difieran hasta el punto de convertirse en un obstáculo para el desarrollo de un mercado regional.

El proyecto "Mejora de la competitividad en el Caribe mediante la armonización de las políticas, la legislación y los procedimientos reglamentarios de las TIC" (HIPCAR) ha tratado de superar este posible obstáculo reuniendo y acompañando a los 15 países caribeños en el Grupo de Estados de África, el Caribe y el Pacífico (ACP), a medida que formulan y adoptan políticas, legislaciones y marcos reglamentarios de TIC armonizados. Ejecutado por la Unión Internacional de Telecomunicaciones, el proyecto se ha llevado a cabo en estrecha colaboración con la Unión de Telecomunicaciones del Caribe (CTU), que preside el Comité de Dirección de HIPCAR. El Comité de Dirección, compuesto por representantes de la Secretaría de APC y la Dirección General de Desarrollo y Cooperación - EuropeAid (DEVCO, Comisión Europea) se encarga de la ejecución general del proyecto.

Este proyecto se enmarca en el programa de Tecnologías de la Información y la Comunicación de la ACP (@CP-ICT) y está financiado con cargo al 9º Fondo de Desarrollo Europeo (EDF), que es el principal instrumento de ayuda europeo para la cooperación y el desarrollo en los Estados de ACP, y está cofinanciado por la UIT. El proyecto @CP-ICT tiene por objeto ayudar a los gobiernos e institución de ACP a armonizar sus políticas en materia de TIC en el sector mediante la prestación de asesoramiento de alta calidad comparable a escala mundial pero, a su vez, relevante en el ámbito local, así como mediante la formación y la capacitación correspondiente.

Todos los proyectos que reúnen a múltiples partes interesadas se enfrentan al doble desafío de crear una sensación de propiedad compartida y de velar por la obtención de resultados óptimos para todas las partes. HIPCAR ha prestado una atención especial a esta cuestión desde el principio del proyecto en diciembre de 2008. Tras acordarse unas prioridades compartidas, las partes interesadas crearon grupos de trabajo para abordarlas. Después, se definieron las necesidades específicas de la región y, del mismo modo, prácticas regionales con posibilidades de éxito, que posteriormente se compararon a las prácticas y normativas establecidas en otros lugares.

Estas evaluaciones detalladas, que reflejan las peculiaridades propias de los países, sirvieron de base para las políticas y los textos legislativos modelo que ofrecen la perspectiva de un panorama legislativo del que toda la región puede mostrarse orgullosa. Es seguro que el proyecto se convertirá en un ejemplo para otras regiones a la hora de tratar de aprovechar el potencial catalizador de las TIC para acelerar la integración económica y el desarrollo económico y social.

Quisiera aprovechar esta oportunidad para dar las gracias a la Comisión Europea y a la Secretaría de ACP por su contribución financiera. También quisiera dar las gracias a la Secretaría de la Comunidad del Caribe (CARICOM) y la Unión de Telecomunicaciones del Caribe (CTU) por su contribución a estos trabajos. Sin la voluntad política de parte de los países beneficiaros, se habría logrado muy poco. Por ese motivo, deseo manifestar mi más profundo agradecimiento a todos los gobiernos de ACP por su voluntad política que ha permitido que este proyecto sea un rotundo éxito.

Brahima Sanou
Director de la BDT

Agradecimientos

El presente documento es el resultado de las actividades regionales llevadas a cabo en el marco del proyecto HIPCAR, "Mejorar la competitividad en el Caribe a través de la armonización de las políticas, la legislación y los procedimientos reglamentarios relativos a las TIC", lanzado oficialmente en la isla de Granada en diciembre de 2008.

En respuesta a los retos y las oportunidades que las tecnologías de la información y las comunicaciones (TIC) ofrecen para el desarrollo político, social, económico y medioambiental, la Unión Internacional de Telecomunicaciones (UIT) y la Comisión Europea (CE) han aunado esfuerzos y han firmado un acuerdo con el objetivo de proporcionar "apoyo para el establecimiento de políticas armonizadas en el mercado de las TIC en los países ACP (África, el Caribe y el Pacífico)", como parte del Programa "Tecnologías de la información y las comunicaciones en los países ACP (@CP-ICT)" en el marco del Noveno Fondo Europeo de Desarrollo (FED) , es decir, el proyecto UIT-CE-ACP.

Este proyecto global UIT-CE-ACP se ejecuta a través de tres subproyectos adaptados a las necesidades específicas de cada región: el Caribe (HIPCAR), África subsahariana (HIPSSA) y los países insulares del Pacífico (ICB4PAC).

El Comité de Dirección del HIPCAR, presidido por la Unión de Telecomunicaciones del Caribe (CTU), proporcionó orientación y apoyo a un equipo de consultores, entre ellos la Sra. Karen Stephen-Dalton y el Sr. Kwesi Prescod. El proyecto del documento fue examinado, debatido y aprobado por amplio consenso por los participantes en dos talleres de consulta del Grupo de Trabajo del HIPCAR sobre la sociedad de la información, celebrados respectivamente en Santa Lucía, del 8 al 12 de marzo de 2010, y en Saint Kitts y Nevis, del 19 al 22 de julio de 2010 (véanse los anexos). Las notas explicativas sobre el modelo de textos legislativos contenidas en este documento fueron redactadas por el Sr. Prescod para abordar, entre otras cosas, las cuestiones planteadas en el segundo taller.

La UIT desea expresar su especial agradecimiento a los delegados de los ministerios caribeños responsables de las TIC, así como de las telecomunicaciones, que participaron en los talleres, así como a los representantes de los Ministerios de justicia y asuntos jurídicos y otros organismos públicos, organismos reguladores, instituciones académicas, la sociedad civil, operadores y organizaciones regionales, por su arduo trabajo y dedicación consagrados a la elaboración del contenido de este informe. Esta participación de amplia base del sector público, en representación de diferentes sectores, permitió que el proyecto pudiera disponer de una gama intersectorial de puntos de vista e intereses. Asimismo, la UIT desea agradecer las contribuciones de la Secretaría de la Comunidad del Caribe (CARICOM) y de la Unión de Telecomunicaciones del Caribe (CTU).

Un documento como éste, que refleja las necesidades y condiciones generales en la región del Caribe, así como las mejores prácticas a nivel internacional, no habría podido elaborarse sin la participación activa de todas esas partes interesadas.

Las actividades han sido realizadas por la Sra. Kerstin Ludwig, encargada de la coordinación de las actividades en el Caribe (Coordinadora de Proyectos de HIPCAR), y el Sr. Sandro Bazzanella, encargado de la gestión de todo el proyecto que abarca el África Subsahariana, el Caribe y el Pacífico (Director de Proyecto UIT-CE-ACP) con el apoyo global de la Sra. Nicole Morain, Asistente de Proyecto de HIPCAR, y de la Sra. Silvia Villar, Asistente de Proyecto UIT-CE-ACP. La labor se llevó a cabo bajo la dirección general del Sr. Cosmas Zavazava, Jefe del Departamento de Apoyo a los Proyectos y Gestión del Conocimiento (PKM). El documento también se benefició de los comentarios de la División de Aplicaciones de las TIC y Ciberseguridad (CYB) de la Oficina de Desarrollo de las Telecomunicaciones (BDT) de la UIT. El Sr. Philip Cross, Representante de Zona de la UIT para el Caribe, también prestó su apoyo. El equipo del Servicio de Composición de Documentos de la UIT se encargó de su publicación.

Índice

Página

Introducción

1.1 Proyecto HIPCAR – Objetivos y beneficiarios

La Unión Internacional de Telecomunicaciones (UIT) y la Comisión Europea (CE), en estrecha colaboración con la Secretaría de la Comunidad del Caribe (CARICOM) y la Unión de Telecomunicaciones del Caribe (CTU), presentaron oficialmente el proyecto HIPCAR[1] en diciembre de 2008 en el Caribe. El proyecto HIPCAR forma parte de un proyecto global UIT-CE-ACP, que también abarca a los países del África subsahariana y el Pacífico.

El objetivo del HIPCAR es prestar ayuda a los países CARICOM/ACP/CARIFORUM[2] en el Caribe para armonizar sus políticas, legislación y procedimientos reglamentarios relativos a las tecnologías de la información y las comunicaciones (TIC) con el fin de facilitar la integración del mercado, impulsar las inversiones en mejores capacidades y servicios de las TIC, y ampliar la protección de los intereses de los consumidores en toda la región. En definitiva, el objetivo del proyecto es mejorar, mediante las TIC, la competitividad y el desarrollo socioeconómico y cultural en la región del Caribe.

De conformidad con el Artículo 67 del Tratado de Chaguaramas revisado, el HIPCAR puede considerarse parte integrante de los esfuerzos de la región para el desarrollo de un mercado y economía únicos de la Comunidad del Caribe (CARICOM) a través de la liberalización progresiva del sector de servicios de las TIC. El proyecto también brinda su apoyo al programa de conectividad para la CARICOM y los compromisos asumidos respecto de la región en la Cumbre Mundial de la Sociedad de la Información (CMSI), al Acuerdo General sobre el Comercio de Servicios, de la Organización Mundial del Comercio (AGCS-OMC) y los Objetivos de Desarrollo del Milenio (ODM). Asimismo, apunta directamente a promover la competitividad y un mejor acceso a los servicios, en el contexto de los compromisos contraídos en diversos tratados, como por ejemplo el Acuerdo de Asociación Económica de los Estados del CARIFORUM con la Unión Europea (UE-CARIFORUM).

Los países beneficiarios del proyecto HIPCAR son Antigua y Barbuda, las Bahamas, Barbados, Belice, la Commonweath de Dominica, la República Dominicana, Granada, Guyana, Haití, Jamaica, Saint Kitts y Nevis, Santa Lucía, San Vicente y las Granadinas, Suriname, y Trinidad y Tobago.

1.2 Comité de Dirección del proyecto y Grupos de Trabajo

El proyecto HIPCAR ha establecido un Comité de Dirección encargado de proporcionar la necesaria orientación y supervisión. El Comité está integrado por representantes de la Secretaría de la Comunidad del Caribe (CARICOM), la Unión Internacional de Telecomunicaciones del Caribe (CTU), la Autoridad de Telecomunicaciones del Caribe Oriental (ECTEL), la Asociación de Organizaciones Nacionales de

[1] El nombre completo del proyecto HIPCAR es ''Mejorar la competitividad en el Caribe a través de la armonización de las políticas, la legislación y los procedimientos reglamentarios relativos a las TIC''. HIPCAR forma parte de un proyecto global UIT-CE-ACP que se lleva a cabo con una financiación de la Unión Europea fijada en 8 millones de euros y un complemento de 500 000 USD aportados por la Unión Internacional de Telecomunicaciones (UIT). La ejecución está a cargo de la UIT, en colaboración con la Unión de Telecomunicaciones del Caribe (CTU) y con la participación de otras organizaciones de la región.
(véase www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html).

[2] El CARIFORUM es una organización regional de 15 países independientes en la región del Caribe (Antigua y Barbuda, las Bahamas, Barbados, Belice, Dominica, la República Dominicana, Granada, Guyana, Haití, Jamaica, Saint Kitts y Nevis, Santa Lucía, San Vicente y las Granadinas, Suriname, y Trinidad y Tobago). Todos estos Estados son signatarios de los Convenios ACP-CE.

Telecomunicaciones del Caribe (CANTO), la Comunidad Virtual de las TIC del Caribe (CIVIC) y la Unión Internacional de Telecomunicaciones (UIT).

Con el fin de garantizar la contribución de los interesados y la pertinencia para cada país, se establecieron también los Grupos de Trabajo HIPCAR, cuyos integrantes fueron designados por los gobiernos de los países y que incluyen especialistas de los organismos de TIC, representantes de organismos judiciales y de otras instituciones públicas, órganos nacionales de regulación, centros nacionales de coordinación de las TIC y personas responsables de la elaboración de la legislación nacional. Los Grupos de Trabajo también incluyen a representantes de organismos regionales relevantes (Secretaría de la CARICOM, CTU, ECTEL y CANTO) y observadores de otras entidades regionales interesadas (por ejemplo, la sociedad civil, el sector privado, los operadores, las instituciones académicas, etc.).

Los Grupos de Trabajo se han encargado de los dos ámbitos de trabajo siguientes:

1. *Políticas y marco legislativo de las TIC en relación con los temas de la sociedad de la información,* que abarca seis subtemas: comercio electrónico (transacciones y prueba), privacidad y protección de datos, interceptación legal de comunicaciones, ciberdelincuencia y acceso a la información pública (libertad de información).
2. *Políticas y marco legislativo de las TIC en relación con las telecomunicaciones,* que abarca tres subtemas: acceso/servicio universal, interconexión y concesión de licencias en un entorno convergente.

Los informes de los Grupos de Trabajo publicados en esta serie de documentos se estructuran en torno a estos dos ámbitos de trabajo principales.

1.3 Contenido y ejecución del proyecto

Las actividades del proyecto se iniciaron con una mesa redonda de presentación del mismo, organizada en la isla de Granada los días 15 y 16 de diciembre de 2008. Hasta la fecha, todos los países beneficiarios del HIPCAR (con excepción de Haití) han participado activamente en las reuniones del HIPCAR, junto con las organizaciones asociadas al proyecto, reguladores, operadores, instituciones académicas y la sociedad civil, que además del evento de presentación del proyecto en Granada, incluyen talleres regionales en Trinidad y Tobago, Santa Lucía, Saint Kitts y Nevis, Suriname y Barbados.

Las actividades principales del proyecto han estado dirigidas por equipos de expertos regionales e internacionales que han colaborado con los miembros de los Grupos de Trabajo, con un enfoque centrado en los ámbitos antes mencionados.

Durante la *Fase I* (ya finalizada), el proyecto HIPCAR:

1. ha analizado las legislaciones existentes en los países beneficiarios para compararlas con las mejores prácticas a nivel internacional y situarlas en el contexto de la armonización en la región; y
2. ha diseñado un modelo de directrices para políticas y un modelo de textos legislativos en los ámbitos señalados, como punto de partida para formular políticas nacionales y legislaciones o reglamentaciones nacionales sobre las TIC.

Se pretende que estas propuestas sean validadas o respaldadas por la CARICOM/CTU y por las autoridades de los países de la región, como base para la siguiente fase del proyecto.

La *Fase II* del proyecto HIPCAR tiene por objeto asistir a los países beneficiarios para que transpongan los modelos indicados en políticas y legislaciones nacionales sobre las TIC, adaptadas a sus necesidades, circunstancias y prioridades específicas. Con miras a la consecución de este objetivo, el HIPCAR dispone de fondos para responder a las peticiones de asistencia técnica de dichos países, incluso para la creación de capacidad.

1.4 Reseña general de los seis modelos de directrices para políticas y textos legislativos del HIPCAR que abordan cuestiones de la sociedad de la información

Todos los países del mundo, entre ellos los del Caribe, buscan formas de establecer marcos jurídicos para abordar las necesidades de la sociedad de la información, con miras a aprovechar la creciente ubicuidad de Internet como canal de prestación de servicios, y garantizar un entorno seguro y una capacidad de tratamiento de datos de los sistemas de información que contribuya a mejorar la eficiencia y eficacia de las actividades.

La sociedad de la información se basa en la premisa del acceso a la información y los servicios, así como la utilización de sistemas automatizados de tratamiento de la información que mejoren la prestación de servicios a los mercados y las personas en cualquier parte del mundo. La sociedad de la información en general, y el acceso a las tecnologías de la información y las comunicaciones (TIC) en particular, ofrecen oportunidades únicas, tanto a los usuarios particulares como a las empresas. Dado que los imperativos básicos del comercio no han cambiado, la transmisión inmediata de información comercial genera oportunidades para mejorar las relaciones de negocios. Esta facilidad de intercambio de información comercial introduce nuevos paradigmas: en primer lugar, cada vez que se utiliza la información para apoyar las transacciones relacionadas con bienes físicos y servicios tradicionales, y en segundo lugar, cuando esa propia información es el producto principal objeto de transacción.

La disponibilidad de las TIC y de nuevos servicios basados en redes ofrece una serie de ventajas para la sociedad en general, y especialmente para los países en desarrollo. Algunas aplicaciones de las TIC, que introducen los medios electrónicos en ámbitos como la administración, el comercio, la educación, la salud y el medio ambiente, se consideran factores propicios del desarrollo, ya que ofrecen un canal eficiente para prestar una amplia gama de servicios básicos en zonas rurales y distantes. Esas aplicaciones de las TIC pueden facilitar el logro de los Objetivos de Desarrollo del Milenio, reducir la pobreza y mejorar el estado de la salud y el medio ambiente en los países en desarrollo. El libre acceso a la información puede además servir de sustento a los procesos democráticos, ya que el flujo de información escapa al control de las autoridades estatales (como ha sucedido, por ejemplo, en Europa oriental). Si se dan el enfoque, el contexto y los procesos de ejecución adecuados, las inversiones en aplicaciones y herramientas de las TIC pueden contribuir a mejorar considerablemente la productividad y la calidad.

Sin embargo, este proceso de transformación también presenta problemas, en la medida en que el marco jurídico actual no atiende necesariamente a las necesidades específicas que surgen en un entorno tecnológico en constante evolución. Cuando la información se usa para apoyar el comercio de bienes y servicios tradicionales, es preciso clarificar de qué manera afecta a los supuestos comerciales tradicionales; y cuando la información es el propio producto objeto de comercio, es necesario proteger al creador o propietario de ese producto. En ambos casos, se debe justificar cómo se detectan, se persiguen y se suprimen las conductas indebidas, teniendo en cuenta que en realidad se trata de transacciones transfronterizas, basadas en productos intangibles.

Los seis modelos de marcos interrelacionados

El HIPCAR ha elaborado seis modelos interrelacionados que sientan un marco jurídico exhaustivo para abordar la evolución constante del entorno de las sociedades de la información, al ofrecer orientación y apoyo para establecer una legislación armonizada en los países beneficiarios del proyecto.

En primer lugar, se ha elaborado un marco jurídico para proteger el derecho de los usuarios en un entorno en evolución y, de este modo, granjearse, entre otros aspectos, la confianza de consumidores e inversores en la certidumbre jurídica y la protección de la privacidad. Se han preparado modelos de textos legislativos del HIPCAR que abordan aspectos relacionados con los ámbitos de **acceso a la información pública (libertad de información)**, con miras a fomentar una cultura adecuada de transparencia en las cuestiones de reglamentación, en provecho de todos los interesados; y **privacidad y protección de datos**, con miras a garantizar la intimidad y la protección de la información personal de los particulares. Este último marco se centra en las prácticas de confidencialidad adecuadas, en los sectores público y privado.

En segundo lugar, se ha elaborado otro modelo de texto legislativo sobre las **transacciones en el comercio electrónico**, que incluye la firma electrónica, con el objeto de facilitar la armonización de las leyes en lo que respecta a la validez jurídica de las prácticas de formación de los contratos y las previsiones en caso de incumplimiento. Este marco se orienta a equiparar los documentos y contratos impresos y los electrónicos, así como a sentar las bases para el comercio en el ciberespacio. El marco para las transacciones en el comercio electrónico está acompañado de un texto legislativo relativo a la **prueba por medios electrónicos**, destinado a reglamentar los medios de prueba jurídicos en los procedimientos civiles y penales.

Para garantizar que los órganos de cumplimiento de la ley puedan investigar las violaciones graves del carácter confidencial, integridad y disponibilidad de las TIC y de los datos, se prepararon modelos de textos legislativos para armonizar la legislación en materia penal y de procedimiento penal. El texto legislativo sobre la **ciberdelincuencia** define los delitos, los instrumentos de investigación y la responsabilidad penal de los principales agentes. Otro texto legislativo trata sobre la **interceptación de comunicaciones electrónicas** y establece un marco apropiado que prohíbe interceptar de forma ilegal esas comunicaciones, y define un estrecho margen de situaciones en que los órganos encargados de hacer cumplir la ley pueden hacerlo, siempre que se den determinadas condiciones claramente definidas.

Elaboración de los modelos de textos legislativos

Los modelos de textos legislativos se elaboraron teniendo en cuenta los principales elementos de las tendencias internacionales, así como las tradiciones jurídicas y las mejores prácticas de la región. El proceso se inició para obtener marcos jurídicos que puedan satisfacer de forma óptima las realidades y necesidades de los países beneficiarios del HIPCAR en la región, para los cuales y por los cuales se establecieron esos modelos. Por consiguiente, el proceso supuso una importante interacción con partes interesadas en cada etapa de su elaboración.

El primer paso en este complejo proceso fue evaluar los marcos legales existentes en la región, mediante un examen de las leyes relativas a todos los ámbitos pertinentes. Además de la legislación en vigor, también se examinaron, cuando se consideró oportuno, los proyectos de ley ya preparados, pero todavía en proceso de promulgación. En un segundo paso, se identificaron las mejores prácticas internacionales (por ejemplo de las Naciones Unidas, la OCDE, la Unión Europea, la Commonwealth, la CNUDMI y la CARICOM), así como las legislaciones nacionales más avanzadas (por ejemplo, del Reino Unido, Australia, Malta y el Brasil, entre otras). Estas prácticas se utilizaron como base de referencia.

Se procedió a complejos análisis jurídicos en cada uno de los seis ámbitos, a los fines de comparar la legislación vigente en la región con la base de referencia mencionada. Este análisis de derecho comparado produjo una imagen del nivel de adelanto en los principales ámbitos de política dentro de la región. Las conclusiones fueron instructivas y mostraron que los marcos relativos a las transacciones electrónicas, la ciberdelincuencia (o "utilización abusiva de la informática") y el acceso a la información pública (libertad de información) estaban más avanzados que los relativos al resto de temas.

Sobre la base de los resultados de este análisis comparado de las legislaciones, los agentes regionales establecieron los componentes fundamentales de políticas de referencia que, una vez aprobadas por las partes interesadas, sentaron las bases para continuar la deliberación sobre políticas y la elaboración de los textos legislativos. Dichos componentes fundamentales confirmaron algunas tendencias y temas comunes encontrados en la jurisprudencia internacional, pero a la vez sirvieron para definir algunas consideraciones particulares que deberían incluirse, en el contexto de una región formada por un conjunto de pequeños Estados insulares soberanos en desarrollo. Por ejemplo, una de las principales consideraciones específicas que afectó a las deliberaciones, en esta y otras etapas del proceso, fue la cuestión de la capacidad institucional para asumir una administración adecuada de estos nuevos sistemas.

Los componentes fundamentales se utilizaron a continuación para elaborar modelos de textos legislativos adaptados, que se ajustaran al mismo tiempo a las normas internacionales y a las necesidades de los países beneficiarios del HIPCAR. Seguidamente, los interesados evaluaron nuevamente cada modelo de

texto, desde el punto de vista de la viabilidad y aplicabilidad inmediata a diferentes contextos regionales. Este grupo de interesados – formado por legisladores y expertos en política de la región – preparó textos que reflejaban de la mejor manera posible la convergencia de las normas internacionales con las consideraciones locales. La amplia participación de representantes de casi todos los 15 países beneficiarios del HIPCAR, entre ellos reguladores, operadores, organizaciones regionales, la sociedad civil e instituciones académicas, garantizó la compatibilidad de los textos legislativos con las diferentes normas jurídicas de la región. No obstante, también se contempló la posibilidad de que cada Estado beneficiario pudiera tener sus preferencias particulares con respecto a la aplicación de determinadas disposiciones. Por tanto, los modelos de textos también ofrecen diferentes opciones dentro del carácter general de un marco armonizado. Tal enfoque apunta a facilitar la aceptación generalizada de los documentos y aumentar la posibilidad de aplicarlos oportunamente en las jurisdicciones de todos los países beneficiarios.

Interacción y superposición de la cobertura de los modelos de textos

Por la propia índole de las cuestiones objeto de examen, hay elementos comunes que se recogen en los seis marcos.

En primer lugar, se deben considerar los marcos que contemplan el uso de medios electrónicos en la comunicación y en la actividad comercial, en cuestiones como las **transacciones en el comercio electrónico, la prueba por medios electrónicos, la ciberdelincuencia y la interceptación de las comunicaciones**. Estos cuatro marcos abordan aspectos relacionados con el tratamiento de los mensajes transmitidos a través de redes de comunicaciones, el establecimiento de pruebas apropiadas para determinar la validez de los registros o documentos, y la incorporación generalizada de sistemas orientados a tratar de forma equivalente los documentos impresos y electrónicos en los procesos de protección contra comportamientos indebidos, atención al consumidor y procedimientos de solución de controversias.

En este sentido, entre todos estos marcos hay varias definiciones comunes que se deberán tener en cuenta, cuando se considere necesario, para evaluar los diversos alcances de su aplicabilidad. Algunos conceptos comunes son: "red de comunicaciones electrónicas" – que se debe alinear con la definición de las leyes de telecomunicaciones vigentes de la jurisdicción; "documento electrónico" o "registro electrónico" – que deben reflejar una interpretación amplia, a fin de incluir el material sonoro y de vídeo; y "firma electrónica", "firma electrónica avanzada", "certificados", "certificados de acreditación", "proveedores de servicios de certificación" y "autoridades de certificación", conceptos todos que se relacionan con la aplicación de técnicas de cifrado para validar de forma electrónica la autenticidad y con el reconocimiento del sector tecnológico y económico que se ha desarrollado alrededor de la prestación de esos servicios.

En este contexto, el marco dedicado a las **transacciones en el comercio electrónico** establece, entre otras cosas, los principios básicos de reconocimiento y atribución necesarios para la eficacia de los otros marcos. Se centra en definir los principios fundamentales que se han de emplear para determinar si los casos son de naturaleza civil o mercantil. Este marco también es esencial para definir una estructura de mercado adecuada y una estrategia realista para la supervisión del sector, en aras del interés del público y la confianza del consumidor. Las decisiones que se adopten en las cuestiones relativas a este sistema administrativo tendrán un efecto ulterior en la forma de utilizar la firma electrónica con fines de prueba en el procedimiento, y la manera de atribuir adecuadamente las responsabilidades y obligaciones definidas en la ley.

Esa presunción de equivalencia permite que los otros marcos puedan abordar adecuadamente los aspectos básicos relacionados con el tratamiento adecuado de las transferencias de información por medios electrónicos. El marco de la **ciberdelincuencia**, por ejemplo, define los delitos relacionados con la interceptación y la alteración de la comunicación, así como el fraude informático. El marco sobre **la prueba en el comercio electrónico** sienta las bases para presentar la prueba por medios electrónicos como una nueva categoría de prueba.

Un importante elemento común de las **transacciones electrónicas** y la **ciberdelincuencia** es la determinación de las responsabilidades y compromisos que asumen los proveedores de servicios cuando dichos servicios se utilizan para un proceder malintencionado con empleo de medios electrónicos. Se ha prestado especial atención a obrar con coherencia a la hora de determinar las partes destinatarias de las secciones pertinentes y atribuir adecuadamente las obligaciones y su cumplimiento.

En el caso de los marcos orientados a mejorar la supervisión reglamentaria y la confianza del usuario, los modelos de textos elaborados por el HIPCAR tratan con los extremos opuestos de una misma cuestión: mientras que el modelo dedicado al **acceso a la información pública** procura promover la divulgación de la información pública, con excepciones concretas, el modelo de **privacidad y protección de datos** fomenta la protección de un subconjunto de información que se considera no abarcado por el modelo anterior. Es importante destacar que estos dos marcos se orientan a fomentar la mejora en la gestión de documentos y las prácticas de mantenimiento de registros dentro del sector público y, en el caso del último marco, también algunos aspectos del sector privado. Sin embargo, es de destacar que, a diferencia de los otros cuatro modelos de textos, estos marcos no se aplican exclusivamente a los medios electrónicos ni pretenden crear un marco en el que las consideraciones sobre un nuevo medio se superpongan a los procedimientos existentes. Para garantizar la coherencia en este sentido, los marcos se orientan a regular la gestión adecuada de los recursos de información, tanto en formato electrónico como no electrónico.

Entre estos dos marcos legislativos existen algunos factores de superposición estructural y logística, entre ellos, la definición de conceptos clave como "autoridad pública" (personas a quienes se aplicarían los marcos), "información", "datos" y "documento", así como su relación mutua. Otra forma importante de superposición se refiere a la supervisión adecuada de estos marcos. Ambos requieren el establecimiento de órganos de supervisión suficientemente independientes de influencias externas, para garantizar al público la ecuanimidad de sus decisiones. Estos organismos independientes también deberían tener la capacidad de imponer multas y/o sanciones contra las partes que ejecuten actividades dirigidas a frustrar los objetivos de alguno de estos marcos.

Conclusión

Los seis modelos de textos legislativos del HIPCAR ofrecen a los países beneficiarios del proyecto un marco global para abordar la mayoría de aspectos pertinentes sobre la reglamentación de las cuestiones relativas a la sociedad de la información. En su redacción se reflejan tanto las normas internacionales más actuales como las necesidades de los pequeños Estados insulares en desarrollo del Caribe en general y, más específicamente, de los países beneficiarios del proyecto HIPCAR. La amplia participación de las partes interesadas de los países beneficiarios en todas las fases de elaboración de los modelos de textos legislativos garantiza que este modelo se apruebe de manera fácil y oportuna. Aunque el enfoque se ha centrado en las necesidades de los países de la región del Caribe, algunos países de otras regiones del mundo ya han determinado que esos modelos de textos legislativos también pueden servir como posibles directrices.

Dada la índole específica e interrelacionada de los modelos de textos del HIPCAR, para los países beneficiarios del proyecto será más ventajoso elaborar e introducir una legislación basada en esos modelos de forma coordinada. Por ejemplo, los modelos relativos al comercio electrónico (transacciones y prueba) funcionarán más eficazmente si los marcos sobre ciberdelincuencia e interceptación de las comunicaciones se elaboran y aprueban simultáneamente, ya que están estrechamente relacionados y son interdependientes para abordar los problemas relacionados con un desarrollo reglamentario sólido. Del mismo modo, los marcos sobre acceso a la información pública y privacidad y protección de datos contienen esas sinergias entre lo que se refiere al entorno administrativo y los requisitos en materia de aptitudes básicas, por lo que su aprobación simultánea necesariamente ha de reforzar ambos marcos en el momento de su aplicación.

De este modo, se creará una oportunidad óptima de utilizar el marco establecido para la región de forma integral.

1.5 El presente informe

El presente informe trata sobre privacidad y protección de datos, uno de los ámbitos abordados por el Grupo de Trabajo sobre políticas y marco legislativo de las TIC en relación con los temas de la sociedad de la información. Incluye un modelo de directrices para políticas y un modelo de texto legislativo con notas explicativas que los países del Caribe tal vez deseen utilizar para la formulación o actualización de sus propias políticas y legislaciones nacionales en esta materia.

Antes de redactar este documento, el equipo de expertos del HIPCAR, en estrecha colaboración con los miembros del mencionado Grupo de Trabajo, preparó y revisó una evaluación de la legislación vigente sobre cuestiones de la sociedad de la información en los 15 países beneficiarios del proyecto. La evaluación se centró en seis ámbitos: transacciones en el comercio electrónico, prueba por medios electrónicos en el comercio electrónico, privacidad y protección de datos, interceptación de las comunicaciones, ciberdelincuencia y acceso a la información pública (libertad de información). Esta evaluación tuvo en cuenta las mejores prácticas a nivel internacional y regional.

Esta evaluación regional, publicada por separado como un documento complementario al informe actual[3], abarcaba un análisis comparado de la legislación vigente sobre la prueba por medios electrónicos en el comercio electrónico en los países beneficiarios del HIPCAR, y la identificación de las posibles deficiencias en este sentido, como base para preparar los modelos de directrices para políticas y de texto legislativo que se presentan. Al recoger las mejores prácticas y normas nacionales, regionales e internacionales, velando siempre por la compatibilidad con las tradiciones jurídicas en el Caribe, los modelos de documentos contenidos en este informe están orientados a satisfacer y responder a las necesidades específicas de la región.

El modelo de texto legislativo sobre privacidad y protección de datos se elaboró en tres fases: 1) redacción de un informe de evaluación, 2) preparación del modelo de directrices para políticas; y 3) redacción de un modelo de texto legislativo. Los consultores del HIPCAR prepararon el informe de evaluación en dos etapas. La Sra. Karen Stephen-Dalton se encargó de la primera, y el Sr. Kwesi Prescod se ocupó de la segunda. Posteriormente, los participantes en dos talleres de consulta del Grupo de Trabajo del HIPCAR sobre la sociedad de la información, celebrados en Santa Lucía, del 8 al 12 de marzo de 2010, y en Saint Kitts y Nevis, del 19 al 22 de julio de 2010 (véanse los anexos) examinaron, debatieron y aprobaron por amplio consenso el proyecto del documento. Las notas explicativas sobre el modelo de texto legislativo contenidas en este documento fueron redactadas por el Sr. Prescod con el objetivo de abordar, entre otras cosas, las cuestiones planteadas en el segundo taller. Este documento contiene por lo tanto los datos y la información conocidos en julio de 2010.

Después de este proceso, los documentos se ultimaron y distribuyeron a todos los interesados para su consideración por los gobiernos de los países beneficiarios del HIPCAR.

1.6 La importancia de políticas y legislación efectivas sobre privacidad y protección de datos

La privacidad ha sido identificada como un derecho humano, según se desprende de diversas disposiciones de la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos, así como la Convención Americana de Derechos Humanos y el Convenio Europeo de Derechos Humanos. Este derecho a la privacidad protege la vida privada del individuo contra la injerencia arbitraria, ilegal o abusiva, y por extensión los datos personales del individuo y la transmisión de esa información.

[3] Véase HIPCAR Privacy and Data Protection: Assessment Report, disponible en www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

Introducción

El debate actual sobre los marcos de la privacidad y la protección de datos no tendría sentido si no se aludiera a la ubicuidad de las tecnologías de la información y las comunicaciones y a las posibilidades que ofrecen para el análisis, tratamiento e intercambio de información. En la medida en que las empresas tratan de utilizar nuevos canales para mejorar su posición competitiva en el mercado nacional o global, para que la revolución electrónica basada en Internet se adopte y prospere, es fundamental lograr la confianza del usuario en el sentido de que la información que facilita durante la realización de una transacción no será utilizada por terceros sin su conocimiento. De esta manera, la aplicación de los marcos de la privacidad y protección de datos apoya los objetivos de las leyes sobre comercio electrónico, al ofrecer un marco integral que consolida el tan necesario sentido de integridad con el marco reglamentario más amplio y refuerza su capacidad de proteger al cliente.

Las leyes sobre privacidad y protección de datos se basan en la premisa de que la persona debe ejercer un cierto control sobre la manera en que se usa, trata o divulga la información personal que facilita al gobierno o las empresas. Este control se afirma desde el mismo momento en que se recopila la información, cuando la parte que la recibe debe dar a conocer claramente el uso que pretende darle y comprometerse a no hacer un uso distinto al manifestado. El otro factor importante que propicia el control de la persona es la obligación de quien recopila la información de darle la oportunidad de examinar toda la información que ha almacenado sobre ella. A pesar de ello, en los casos en que resulta difícil obtener el consentimiento de la persona para acceder a esta información, deben preverse excepciones a la norma general de restricción del uso de la información personal, mediante la aplicación de unas directrices específicas y diferentes en el ámbito de los servicios médicos y la seguridad nacional.

Así pues, las políticas y marcos y legislativos relativos al tratamiento de la privacidad y protección de datos se orientan a abordar sólo la gestión de la información privada y personal. De este modo, esos marcos funcionan de acuerdo con las reglas relativas al acceso a la información pública no sensible que posee el gobierno, ya que dichos marcos no suelen ocuparse de la gestión de información personal, salvo por las exenciones generales de las disposiciones contenidas en esas leyes.

Si bien la supervisión por parte del gobierno merece una consideración especial, los marcos sobre privacidad y protección de datos no deben limitarse al sector público, sino abarcar todas las partes que, dentro del conjunto de sus actividades, recopilan, almacenan y analizan información personal de sus clientes. Las leyes sobre privacidad y protección de datos son fundamentales para favorecer el establecimiento de sistemas de gobierno electrónico orientados a mejorar la eficiencia en la prestación de bienes y servicios públicos, y para la competitividad del sector comercial.

Los organismos gubernamentales y otras entidades que intervienen en la prestación de servicios públicos han usado tradicionalmente, en el desempeño de sus funciones, información personal de sus clientes. No obstante, la evolución hacia una mayor transparencia y equidad en la gestión de los asuntos públicos ha traído consigo una serie de preocupaciones sobre cómo se deberá utilizar esa información. Estas preocupaciones abarcan desde cómo limitar la influencia de los prejuicios por motivos de raza, religión, etnia, género u orientación sexual en la asignación de los recursos, bienes o servicios públicos que no están directamente relacionados con esas características, hasta qué sistemas emplear para proteger la información almacenada del acceso no autorizado por parte de terceros. Así pues, del mismo modo que se ha contemplado la obligación de establecer marcos para reducir al mínimo la consideración de las características particulares en la evaluación del acceso a los recursos públicos (a menos que dichas características sean, en la ley, el factor discrecional determinante en el proceso de evaluación), se debe también contemplar la protección contra la divulgación o el acceso no autorizado a información personal mediante la aplicación garantizada de unos niveles mínimos y adecuados de seguridad.

Desde la perspectiva del sector privado, los clientes exigen cada vez más garantías de que ningún tercero usará indebidamente la información personal obtenida durante la realización de una transacción comercial particular. Esta garantía debe limitar la venta u otros medios de divulgación de información personal a terceros sin el conocimiento y la aprobación tácita de la persona.

Introducción

Las leyes de privacidad y protección de datos también deben reconocer que el comercio electrónico es un fenómeno emergente, y que las transferencias de información transfronterizas se han incrementado. Las empresas que aprovechan las tecnologías de la información y las comunicaciones tienden a buscar oportunidades para racionalizar su inversión a fin de reducir costes y aumentar la eficiencia. En muchos casos estas estrategias incluyen la acumulación en un solo lugar de la información recopilada en el curso de las actividades. En el caso de las compañías multinacionales, este impulso se traduce por lo general en la acumulación de información comercial procedente de varios países en un solo lugar que puede no estar situado en ninguna de las jurisdicciones de las cuales se obtuvo la información. En este caso, si las normas relativas a la protección de datos personales en ese país no son tan estrictas como las del país donde la empresa recopiló la información, se puede comprometer la privacidad de las personas en las jurisdicciones que son la sede principal de las actividades. Este aspecto es tan importante que la protección recíproca de la información personal se ha convertido actualmente en un componente fundamental de los acuerdos comerciales entre naciones y/o de las restricciones reglamentarias impuestas a las empresas multinacionales. La aplicación de las reglas de privacidad y protección de datos proporciona en ese caso a los países la oportunidad de acceso, participación y beneficio en nuevos ámbitos de la actividad económica en el comercio internacional para la prestación de servicios en lugares apartados y distantes.

Por último, ha surgido recientemente un debate sobre las oportunidades económicas asociadas con el control, uso y análisis de la información recopilada por las empresas que añaden contenidos en Internet o de mercadotecnia. Esto ha llevado a la discusión sobre la "cadena de valor en la información personal" y al reconocimiento del potencial económico asociado a los diferentes agentes que intervienen en esta cadena. En el centro de este marco de referencia para la nueva economía de la información se sitúa el reconocimiento de los derechos del individuo a ejercer control sobre el uso concreto que se dará a la información personal. Dado que la revolución económica de Internet está cobrando impulso, la aplicación y cumplimiento de las normas sobre privacidad y protección de datos de una jurisdicción, y por tanto su credibilidad, han de convertirse en una ventaja competitiva clave para que esa jurisdicción se convierta en un foco de inversión dentro de este floreciente sector de actividad económica, que en gran medida implica la gestión de información personal.

Por lo tanto, la aplicación de políticas, leyes y sistemas eficaces que garanticen la privacidad y protección de datos puede proporcionar importantes y variados beneficios a cualquier país, lo que repercutirá positivamente en la gobernabilidad y la democracia, y preparará al país, y a las empresas con sede en el mismo, para aprovechar las nuevas oportunidades que les ofrece la era de la información. La aplicación de esas políticas, leyes y sistemas debe reflejar los marcos administrativos que limitan la posibilidad de injerencias indebidas por parte del poder ejecutivo del Estado o de las empresas comerciales para reforzar la importancia de la privacidad y protección de datos dentro de las normas y principios del buen gobierno.

Sección I:
Modelo de directrices para políticas – Privacidad y protección de datos

A continuación se presenta el modelo de directrices para políticas que un país puede considerar en relación con la privacidad y protección de datos.

1. LOS PAÍSES DE LA CARICOM/DEL CARIFORUM SE PONDRÁN COMO OBJETIVO INTRODUCIR MARCOS JURÍDICOS E INSTITUCIONALES CLAROS PARA GARANTIZAR LA PROTECCIÓN DE LA INFORMACIÓN PERSONAL Y PRIVADA

- Existe un mandato jurídico claro en derecho que apoya el establecimiento de un régimen para garantizar la protección de la información personal y/o privada.
- El régimen de protección de datos no debería ser específico para una tecnología, por lo que debería ser igualmente pertinente para las versiones impresas que para los entornos propiciados por las TIC.
- La ley o el mandato jurídico debería indicar claramente que la Ley obliga al Estado.
- La ley o el mandato jurídico debería garantizar que la obligación de proteger la privacidad se aplica tanto al sector público como al privado.
- La ley o el mandato jurídico identificará claramente un organismo designado para la aplicación del marco jurídico sobre privacidad y protección de datos.
- La ley o el mandato jurídico establecerá claramente la independencia del organismo designado.
- La ley o el mandato jurídico establecerá claramente que la información personal debe recopilarse y tratarse con el consentimiento del titular de esa información.
- La ley o el mandato jurídico especificará claramente las circunstancias en que puede recopilarse y tratarse información personal sin recabar el consentimiento del titular de esa información o notificarle esa circunstancia.
- La ley o el mandato jurídico debería identificar una categoría de información personal como "información sensible", que necesitaría una supervisión y control más estrictos.

2. LOS PAÍSES DE LA CARICOM/DEL CARIFORUM SE ASEGURARÁN DE QUE LOS PRINCIPIOS FUNDAMENTALES SOBRE PROTECCIÓN DE DATOS ESTÁN CLARAMENTE DEFINIDOS EN LAS LEYES PERTINENTES

- Los principios fundamentales del marco jurídico de la protección de datos están claramente definidos en las leyes.
- Entre los principios fundamentales de la protección de datos deberá haber disposiciones que garanticen que en el momento de la recolección la persona interesada está informada del fin/uso que se dará a esos datos, y manifiesta de forma clara su consentimiento al respecto.
- Entre los principios fundamentales de la protección de datos deberá haber disposiciones sobre la responsabilidad de la persona y/o entidad que recopila y/o trata la información personal respecto de la seguridad, precisión y uso adecuados de esa información.
- Entre los principios fundamentales de la protección de datos deberá haber disposiciones para infundir confianza en el público, al permitir que la persona a quien corresponden los datos pueda examinar la información sobre ella que conserva cualquier persona o entidad, y asegurarse de su precisión.
- Entre los principios fundamentales de la protección de datos deberá haber disposiciones que prohíban la transferencia transfronteriza de datos personales a aquellas jurisdicciones que no ofrezcan garantías similares a las de la jurisdicción de origen en materia de privacidad y protección de datos.

3. LOS PAÍSES DE LA CARICOM/DEL CARIFORUM SE PONDRÁN COMO OBJETIVO ESTABLECER LOS MARCOS ADECUADOS QUE PROPORCIONEN A LAS INSTITUCIONES LAS ATRIBUCIONES ADECUADAS PARA FACILITAR SU TAREA DE SUPERVISIÓN

- La ley o el mandato jurídico estipulará claramente que habrá disposiciones que permitan identificar claramente a los que recopilaron, utilizaron y se ocuparon del tratamiento de la información personal, lo que puede incluir la notificación a la agencia designada para la supervisión, o el registro ante este organismo.
- El organismo designado para garantizar el cumplimiento de la ley o el mandato jurídico deberá ser una persona jurídica con atribuciones para poseer o disponer de bienes y capacidad de celebrar contratos, y que pueda desempeñar sus funciones con independencia.
- El jefe de este organismo será nombrado de manera que se garantice la independencia e imparcialidad en el desempeño de sus funciones.
- El jefe de este organismo deberá gozar de unas condiciones de empleo que incluyan cláusulas de estabilidad y condiciones de renovación de contrato, contempladas en la ley o el mandato jurídico, que sean suficientes para limitar las posibilidades de incentivo o coacción.
- La ley o el mandato jurídico concederá al jefe de este organismo las atribuciones de investigación necesarias para facilitar la ejecución de las funciones contempladas en el marco de la protección de datos.
- La ley o el mandato jurídico concederá al jefe de este organismo la facultad de delegar cierta autoridad en entidades reconocidas para facilitar la ejecución de sus funciones.
- El organismo designado podrá llevar a cabo auditorías o investigaciones sobre las operaciones realizadas por personas a las que sea aplicable el marco, ya sea por propia iniciativa o en respuesta a reclamaciones de los ciudadanos. El reglamento determinará quién debe asumir los costes derivados de esas auditorías o investigaciones.
- Las personas a quienes se aplica la ley deberán cooperar con el mencionado organismo en el ejercicio de sus funciones, bajo pena de sanciones civiles y/o penales.
- Este organismo podrá solicitar la presentación de ciertos documentos para facilitar sus investigaciones, y las personas pertinentes tendrán la obligación de presentarlos. Si se justifica, el organismo podrá obtener una orden judicial para lograrlo.
- En la ley o el mandato jurídico se podrá contemplar ofrecer protección al organismo designado en lo que respecta a la responsabilidad derivada de los actos realizados de buena fe en el ejercicio de su función.
- Este organismo presentará anualmente un informe al Parlamento/Consejo Legislativo sobre las actividades realizadas durante el año anterior.
- La ley o el mandato jurídico especificará un plazo para la entrada en funcionamiento de este organismo, tras la aprobación de la Ley.

4. LOS PAÍSES DE LA CARICOM/DEL CARIFORUM ESBOZARÁN LOS REQUISITOS Y OBLIGACIONES CONCRETOS RELATIVOS A LA RECOPILACIÓN DE INFORMACIÓN PERSONAL

- La ley o el mandato jurídico insistirá en que las autoridades públicas sólo recabarán aquella información personal que esté expresamente autorizada por una ley escrita.
- La ley o el mandato jurídico dispondrá que se notifique expresamente al titular de los datos la finalidad para la cual se recopilan y la pertinencia de la información recopilada a esos efectos.
- La ley o el mandato jurídico dispondrá que el titular de los datos deberá dar su consentimiento explícito para la recopilación de información.
- La ley o el mandato jurídico contempla la recopilación de los datos personales solamente de la persona concreta, sujeto a determinadas excepciones relacionadas con la seguridad nacional o la gestión de la salud pública.
- La ley o el mandato jurídico establecerá excepciones claras, precisas y limitadas, de modo que el titular de los datos reciba una protección adecuada contra la recopilación innecesaria de datos.
- En la ley o reglamentaciones asociadas se expondrán las consideraciones específicas para garantizar que haya adecuados pesos y contrapesos para el acceso y uso de la información personal en relación con las excepciones señaladas en las leyes generales sobre privacidad y protección de datos.
- La ley o el mandato jurídico establecerá que, en el momento de la recopilación, se debería informar al titular de los datos sobre quién tendrá los datos en su poder, el período que tiene previsto conservarlos y la forma en que serán eliminados cuando venza ese plazo, salvo en circunstancias basadas en la gestión de la salud pública y la seguridad nacional.
- La ley o el mandato jurídico limitará la recopilación de información personal sensible, excepto en ciertos casos y para objetivos determinados. Esas excepciones pueden basarse en:
  - Elaboración de estadísticas;
  - Gestión de la salud pública;
  - Requisitos para hacer cumplir la ley;
  - Requisitos de un estado de derecho;
  - Requisitos de una orden judicial.
- La ley o el mandato jurídico establecerá sanciones civiles y penales por el incumplimiento de las disposiciones definidas relativas a la recopilación de información personal. Dichas sanciones podrán imponerse a la parte que recaba la información, o a cualquier funcionario o director, si se demuestra que ha incumplido intencionalmente los términos de la ley o el mandato jurídico.

5. LOS PAÍSES DE LA CARICOM/DEL CARIFORUM ESBOZARÁN LOS REQUISITOS Y OBLIGACIONES CONCRETOS RELATIVOS AL TRATAMIENTO DE INFORMACIÓN PERSONAL

- La ley o el mandato jurídico impondrá a la parte que recopila información un uso o tratamiento de esa información limitados a fines específicos y consentidos por el titular de los datos en el momento y lugar de la recopilación.
- La ley o el mandato jurídico limitará la retención de la información recopilada al período necesario para los fines especificados.
- La ley o el mandato jurídico obligará a la parte que utiliza la información ("la parte que trata los datos") a velar por que esa información se registre y trate con precisión.
- La ley o el mandato jurídico obligará a la parte que trata los datos a proteger la información almacenada mediante la adopción de métodos apropiados que garanticen una seguridad adecuada.
- La ley o el mandato jurídico exigirá que la parte que trata los datos solicite el examen y la aprobación del organismo designado antes de iniciar determinados tipos de tratamiento.
- La ley o el mandato jurídico establecerá que un titular de los datos podrá tener acceso, previa solicitud, a la información personal sobre él que conserve la parte que trata los datos.
- La ley o el mandato jurídico reconocerá al jefe de la parte que trata los datos la facultad de rechazar una solicitud de acceso a la información almacenada sobre una persona interesada si:
  - la difusión de la información puede poner en peligro el anonimato de otra persona;
  - por su índole, la solicitud es irritante y redunda en un perjuicio excesivo sobre la operatividad de la parte que trata los datos.
- La ley o mandato jurídico otorgará al organismo designado la posibilidad de recurrir la decisión en este sentido del jefe de la parte que trata los datos.
- La ley o el mandato jurídico prohibirá el tratamiento de información personal sensible excepto en ciertos casos y para objetivos determinados. Esas excepciones pueden basarse en:
  - Elaboración de estadísticas;
  - Gestión de la salud pública;
  - Requisitos para hacer cumplir la ley;
  - Requisitos de un estado de derecho;
  - Requisitos de una orden judicial.
- La ley o el mandato jurídico establecerá sanciones civiles y penales por el incumplimiento de las disposiciones definidas relativas al tratamiento de información personal. Dichas sanciones podrán imponerse a la parte que trata los datos o a cualquier funcionario o director si se demuestra que ha incumplido los términos de la ley o el mandato jurídico.

6. LOS PAÍSES DE LA CARICOM/DEL CARIFORUM ESBOZARÁN LOS REQUISITOS Y OBLIGACIONES CONCRETOS RELATIVOS A LA DIVULGACIÓN DE INFORMACIÓN PERSONAL

- La ley o el mandato jurídico obligará a la parte que recopila, trata y utiliza información personal a no divulgar esa información personal sin el consentimiento previo del titular de los datos.
- La ley o el mandato jurídico dispondrá la exención de la obligación de contar con el consentimiento del titular cuando los datos sean requeridos por una norma de derecho o estén relacionados con los intereses de la seguridad nacional, la administración de justicia y la gestión de la salud pública.
- La ley o el mandato jurídico prohibirá la transferencia transfronteriza de información personal a las jurisdicciones que carecen de leyes y sistemas similares de protección de datos personales. Para esos casos, la ley dispondrá sólo la transferencia de aquella información que no ponga en peligro la protección de la información personal del titular de los datos.
- La ley o el mandato jurídico establecerá, sin perjuicio de cualquier restricción de las normas, que la transferencia de información personal pueda hacerse sólo con el consentimiento expreso del titular de los datos para transferir información a dicha jurisdicción, tras haber sido informado de los riesgos asociados.
- La ley o el mandato jurídico dispondrá la divulgación de información personal en respuesta a una solicitud del titular de los datos. Cuando dicha divulgación pueda dar lugar a su vez a que se divulgue otra información reservada, la ley o el mandato jurídico determinará las directrices apropiadas que debe seguir el jefe de la parte que trata la información.
- La ley o el mandato jurídico establecerá sanciones civiles y penales por el incumplimiento de las disposiciones relativas a la divulgación de información personal. Dichas sanciones podrán imponerse a la parte que trata los datos o a cualquier funcionario o director si se demuestra que ha incumplido los términos de la ley o el mandato jurídico.

Sección II:
Modelo de texto legislativo –
Privacidad y protección de datos

A continuación se presenta un modelo de texto legislativo que un país puede considerar en la elaboración de la legislación nacional relativa a la privacidad y protección de datos. Este texto modelo se basa en el modelo de directrices para políticas descrito anteriormente.

Disposición de los artículos

PARTE I – OBSERVACIONES PRELIMINARES

Título abreviado e inicio

1. Esta Ley podrá citarse como Ley de privacidad y protección de datos, y entrará en vigor [xxx después de la publicación en el *Boletín Oficial]*.

Objetivo

2. El objetivo de esta Ley es proporcionar un marco jurídico habilitante en apoyo del establecimiento de una cultura y práctica de la protección de la privacidad a través de:

   a. La definición de los principios generales que deben regir el tratamiento de la información personal de un individuo;

   b. La definición de las directrices (incluidas las referidas a sistemas y tecnología) que deben seguir las personas que gestionen información personal; y

   c. El establecimiento de un marco administrativo que garantice una supervisión transparente y la resolución imparcial de conflictos, de modo que se fortalezca la protección de la información personal por parte tanto del sector público como privado.

Definiciones

3. (1) En esta Ley, las siguientes palabras y frases tendrán el significado que se les asigna a continuación:

   a. Por "datos" o "información" se entenderá todo registro, documento, correspondencia, memorándum, libro, plano, mapa, dibujo, obra pictórica o gráfica, fotografía, película, microfilm, grabación sonora, grabación de video, registro legible por máquina y cualquier otro material documental, independientemente de su forma o características físicas, y toda copia de los mismos.

   b. Por "Comisionado de datos" se entenderá el comisionado de datos designado en virtud de la Parte VII, Artículo 49 de esta Ley.

   c. Por "entidad responsable de los datos" se entenderá una persona (ya sea sola o conjuntamente o en común con otras personas) que determina para qué fines los datos personales son o serán recopilados, tratados o divulgados, y de qué manera.

   d. Por "titular de los datos" se entenderá el individuo a quien se refieren los datos personales.

   e. Por "Ministro" se entenderá el Ministro al que se ha asignado la responsabilidad de la [información/administración pública].

   f. Por "institución de atención de salud" se entenderá las instituciones registradas como servicios para la prestación de asistencia sanitaria de conformidad con la [ley pertinente de asistencia sanitaria] y que incluye hospitales, centros de salud, clínicas [y consultorios médicos].

   g. Por "profesional de atención de salud" se entenderá un profesional inscrito para ejercer la medicina, de acuerdo con la [ley pertinente de atención de salud pública].

h. Por "información personal" se entenderá la información sobre una persona identificable que se registra en alguna forma, lo que incluye:

   i. información relativa a la nacionalidad, domicilio, edad o estado civil de la persona;

   ii. información sobre el origen racial o étnico de la persona;

   iii. información sobre opiniones políticas o afiliaciones de la persona;

   iv. información sobre creencias religiosas u otras creencias de naturaleza similar de la persona;

   v. información relativa a la salud o condición física o mental de la persona;

   vi. información relacionada con los indicadores biométricos de la persona;

   vii. información relacionada con la orientación sexual o la vida sexual de la persona;

   viii. información relacionada con los antecedentes penales o financieros de la persona;

   ix. información relativa a la educación o antecedentes laborales de la persona;

   x. todo número de identificación, símbolo o particularidad diseñada para identificar a la persona;

   xi. los puntos de vista y opiniones de otro sobre la persona.

i. El concepto "autoridades públicas" incluye:

   i. un Parlamento o una comisión de una Cámara del Parlamento;

   ii. el Consejo de Ministros constituido en virtud de la Constitución;

   iii. un Ministerio o un departamento o una división de un Ministerio,

   iv. una autoridad local;

   v. una sociedad u organismo público establecido por ley;

   vi. un organismo colegiado o un órgano constituido con fines públicos que es propiedad del Estado o está sujeto a su control;

   vii. cualquier otro organismo designado por el Ministro mediante una reglamentación elaborada en virtud de esta Ley, para que ejerza como autoridad pública a los efectos de esta *Ley.*

j. Por "tratamiento", "tratados", en relación a los datos, se entenderá la obtención, registro o almacenamiento de datos, o cualquier operación o conjunto de operaciones realizadas sobre datos, lo que incluye:

   i. la organización, adaptación o modificación de los datos;

   ii. la búsqueda, consulta o uso de los datos; o

   iii. la alineación, combinación, bloqueo, borrado o destrucción de los datos.

k. Por "sistema de archivo pertinente" se entenderá todo conjunto de informaciones relativas a personas en la medida en que, aunque no estén tratadas mediante equipos que funcionan automáticamente en respuesta a instrucciones establecidas para tal fin, el conjunto está estructurado, bien mediante referencias a personas o a criterios relativos a personas, de tal manera que permite un fácil acceso a la información específica relativa a una persona en particular.

(2) Cuando el Estado miembro considere que se justifica definir un conjunto particular de datos personales, puede hacerlo de la siguiente manera:

a. Por "información personal sensible" se entenderá la información sobre una persona que se refiera a:

i. su origen racial o étnico;

ii. sus opiniones políticas;

iii. sus creencias religiosas u otras creencias de naturaleza similar;

iv. su salud o condición física o mental;

v. su orientación sexual o su vida sexual; o

vi. sus antecedentes penales o financieros;

Obligación para el Estado

4. El Estado deberá acatar obligatoriamente esta Ley.

Aplicabilidad de la Ley

5. Esta Ley se aplicará al responsable de los datos respecto de toda información, si:

a. se ha establecido un responsable (uno con sede o sucursal habitual, o una persona jurídica constituida) en [nombre del Estado miembro] y los datos se tratan en el marco de las actividades de dicho establecimiento;

b. no se ha establecido un responsable en [nombre del Estado miembro], pero hace uso del equipo en [nombre del Estado miembro] para el tratamiento de los datos con fines diferentes al tránsito a través de [nombre del Estado miembro].

Límites en la aplicabilidad de la Ley

6. Esta Ley no:

a. limitará el acceso a la información disponible por ley a una parte en un procedimiento;

b. limitará las atribuciones de un juzgado o tribunal para obligar a un testigo a dar testimonio u obligar a la presentación de un documento u otra prueba;

c. se aplicará a las notas preparadas por o para una persona que preside un juzgado o tribunal de [país] si dichas notas se han preparado para el uso personal de esa persona en relación con el procedimiento.

Principios generales de privacidad

7. De conformidad con esta Ley, toda persona que trate con datos personales en el ejercicio de una actividad deberá observar los principios generales siguientes:

a. Los datos personales se tratarán de forma equitativa y lícita, y, en concreto, no serán sometidos a tratamiento a menos que se cumplan las condiciones particulares.

b. Los datos personales se obtendrán sólo para uno o más fines específicos y legítimos, y no se tratarán en una manera incompatible con esos fines.

c. Los datos personales deberán ser adecuados, pertinentes y no excesivos en relación con los propósitos para los que se tratan.

d. Los datos personales deberán ser precisos y, cuando sea necesario, mantenerse actualizados.

e. Los datos personales tratados para cualquier fin o fines no se conservarán por más tiempo del necesario para dichos fines.

f. Los datos personales se tratarán de acuerdo con los derechos de los titulares de los datos en virtud de la presente Ley.

g. Se tomarán las medidas técnicas e institucionales apropiadas para prevenir el tratamiento ilícito de datos personales y la pérdida o destrucción accidental o deterioro de tales datos.

h. Los datos personales no se transferirán a un país o territorio fuera de [*nombre de la jurisdicción*] a menos que ese país o territorio garantice a los titulares de los datos un nivel adecuado de protección de los derechos y libertades en relación con el tratamiento de datos personales.

PARTE II – OBLIGACIONES DE LAS ENTIDADES RESPONSABLES DE LOS DATOS

Limitaciones en la recopilación y tratamiento de información personal

8. (1) Ninguna persona podrá recopilar o tratar datos personales si no figura inscrita como entidad responsable de los datos en el registro mantenido por el Comisionado.

(2) La entidad responsable de los datos no podrá recopilar información personal a menos que:

a. la recopilación de esa información se considere justa y necesaria como parte de un acuerdo entre la entidad responsable de los datos y el titular de los datos;

b. la recopilación esté expresamente autorizada por o en virtud de una ley escrita.

Información personal que se recopila directamente

9. (1) Cuando la entidad responsable de los datos necesite información personal de una persona, se encargará de recabar esa información directamente de la persona con su consentimiento expreso.

(2) El titular de los datos, a menos que otra ley disponga otra cosa, tendrá derecho a oponerse en cualquier momento a que la entidad responsable de los datos trate de los datos, por razones imperiosas y legítimas.

(3) A pesar del párrafo 1, se podrá recopilar información personal de una fuente que no sea la persona cuando:

a. la persona, el Comisionado u otra ley escrita autoricen otro método de recopilación;

b. la información se recopile con el fin de:

i. determinar la idoneidad para recibir un honor o concesión, como por ejemplo un título honorífico, beca, premio o ayuda financiera;

ii. realizar trámites ante un juzgado o tribunal judicial o cuasi judicial;

iii. cobrar una deuda o multa o realizar un pago; o

iv. hacer cumplir la ley.

Información de la finalidad al titular de los datos

10. En el momento de recopilar los datos personales, o antes, la entidad responsable de los datos deberá asegurarse de que el titular de los datos está informado de:

a. la finalidad para la que se recopilan;

b. los destinatarios previstos;

c. si la respuesta a las preguntas es voluntaria u obligatoria, así como las posibles consecuencias de la negativa a responder;

d. si procede, la autoridad jurídica para recopilarla; y

e. el cargo, dirección comercial, número de teléfono y otros datos de contacto de un funcionario de la entidad responsable de los datos que pueda responder a las preguntas del titular de los datos sobre dicha recopilación.

Conservación de la información personal

11. La entidad responsable de los datos sólo conservará la información personal que haya utilizado para una finalidad administrativa durante el período que establezca la reglamentación correspondiente, con el fin de garantizar que el titular de los datos tenga una oportunidad razonable de acceder a esa información.

Eliminación de la información personal

12. La entidad responsable de los datos deberá eliminar toda la información personal bajo su control o custodia de conformidad con la reglamentación aprobada por el Ministro en virtud de esta Ley.

Precisión de la información personal

13. La entidad responsable de los datos deberá hacer todos los esfuerzos razonables para garantizar que la información personal de un titular de los datos que esté bajo su custodia sea precisa y completa.

Protección de la información personal

14. (1) La entidad responsable de los datos deberá proteger la información personal bajo su custodia o control tomando medidas razonables de seguridad técnica e institucional frente a riesgos como el acceso, recopilación, uso, alteración o divulgación no autorizados, o la eliminación accidental.

(2) En caso de que otra persona trate la información personal en nombre de la entidad responsable de los datos, ésta deberá asegurarse de que esa persona:

a. está en condiciones de adoptar las medidas de seguridad necesarias;

b. adopta efectivamente las medidas identificadas por la entidad responsable de los datos.

Tratamiento de la información personal en consonancia con la finalidad

15. (1) La información personal bajo custodia o control de la entidad responsable de los datos sólo podrá ser tratada para la finalidad para la cual se recopiló, o bien para un uso compatible con dicha finalidad, a menos que el titular de los datos autorice un uso distinto.

(2) El tratamiento de la información personal será coherente con los fines para los que se obtuvo si el tratamiento tiene una relación razonable y directa con la finalidad, y si dicha finalidad está de acuerdo con los criterios señalados en el párrafo 3.

(3) Los datos personales sólo podrán tratarse:

a. si el titular de los datos ha dado su consentimiento de forma inequívoca; o

b. si lo hace un profesional de atención de salud en cumplimiento de sus funciones en una institución para el cuidado de la salud; o

c. cuando el titular de los datos ya los haya hecho públicos;

d. con fines de investigación o estadísticos, de conformidad con el Artículo 17;

e. para hacer cumplir la ley y velar por la seguridad nacional, o

f. a los efectos de determinar el acceso a los servicios sociales;

g. si dicho tratamiento es necesario para la ejecución de un contrato en que el titular de los datos sea parte o para tomar medidas, a petición del titular de los datos, antes de celebrar un contrato;

h. si dicho tratamiento es necesario para el cumplimiento de una obligación legal a la que está sujeta la entidad responsable de los datos; o

i. si dicho tratamiento es necesario para salvaguardar intereses vitales del titular de los datos; o

j. si dicho tratamiento es necesario para el desempeño de una actividad de interés público o en el ejercicio de la autoridad pública conferida a la entidad responsable de los datos o a un tercero a quien revelan los datos; o

k. si dicho tratamiento es necesario para un propósito que concierne al interés legítimo de la entidad responsable de los datos o de un tercero a quien se facilitan los datos personales, excepto cuando dicho interés queda anulado por el interés de proteger el derecho a la intimidad del titular de los datos.

(4) Cuando la jurisdicción considere necesario distinguir entre "información personal" e "información personal sensible", podrá limitar aún más la recopilación y tratamiento de dicha información, con las excepciones relacionadas con los párrafos b) a f) *supra*.

Divulgación de la información personal

16. Salvo lo dispuesto en cualquier otra ley escrita, la información personal sujeta al control de la entidad responsable de los datos sólo puede ser divulgada:

a. para la finalidad para la cual se recopiló, o bien para un uso compatible con dicha finalidad;

b. para cualquier finalidad que esté de acuerdo con una ley escrita, o con una orden que autorice la divulgación, emitida en virtud de dicha ley escrita;

c. con la finalidad de cumplir con una citación o mandamiento u orden dictados por un tribunal, persona u organismo con competencia para obligar a la presentación de la información, o bien para cumplir con las normas del tribunal relativas a la presentación de información;

d. al Fiscal General de [nombre de la jurisdicción] para su uso en los procedimientos jurídicos en que participe el Estado;

e. a un organismo de investigación indicado por orden ministerial, tras una solicitud por escrito del propio organismo, con la finalidad de investigar el cumplimiento de una ley escrita o iniciar una investigación legal, siempre que dicha solicitud especifique el propósito y describa la información que debe suministrarse;

f. por un organismo encargado del cumplimiento de la ley en [nombre de la jurisdicción] a otro organismo similar dentro de [nombre de la jurisdicción] con la finalidad de hacer cumplir una ley escrita;

g. a un organismo encargado del cumplimiento de la ley en un país extranjero en virtud de un acuerdo por escrito, un tratado o la autoridad del Gobierno de [nombre de la jurisdicción];

h. si el jefe de la entidad responsable de los datos está de acuerdo en que se da una situación apremiante que afecta a la salud o seguridad de una persona, y si, sujeto al Artículo 23 d), se envía aviso de la divulgación a la última dirección conocida del titular de los datos;

i. para poder contactar con los parientes o amigos más próximos de una persona herida, enferma o fallecida;

j. para recaudar el dinero que el titular de los datos debe al Gobierno de [nombre de la jurisdicción] o al responsable de los datos;

k. para fines estadísticos cuando la divulgación cumple con los requisitos del Artículo 17; o

l. con fines de archivo cuando la divulgación cumple con los requisitos del Artículo 18.

Divulgación para fines de investigación o estadísticas

17. La entidad responsable de los datos puede proceder a la divulgación de la información personal bajo su custodia o control con fines de investigación, incluyendo una investigación estadística, sólo si:

a. el objetivo de la investigación no se puede alcanzar razonablemente si no se suministra la información de una manera que permita la identificación de un individuo;

b. la información se divulga a condición de que no se use con el propósito de ponerse en contacto con una persona para participar en una investigación;

c. ninguna vinculación registrada es perjudicial para el titular de los datos y los beneficios que se derivan de cualquier vinculación de registros redundan claramente en el interés público;

d. el jefe de la entidad responsable de los datos interesada ha aprobado condiciones relativas a:

i. seguridad y confidencialidad;

ii. la eliminación o destrucción de los elementos de identificación individual lo antes posible;

iii. la prohibición de todo uso o divulgación posterior de esa información presentada de una manera que permita una identificación individual sin autorización expresa de la entidad responsable de los datos; y

e. la persona a quien se da a conocer la información ha firmado un acuerdo para cumplir con las condiciones aprobadas, la presente Ley y cualquiera de las políticas y procedimientos de la entidad responsable de los datos relativas a la confidencialidad de la información personal.

Divulgación para fines de archivo

18. Los Archivos Nacionales del Gobierno de [nombre de la jurisdicción] o los archivos de la entidad responsable de los datos pueden divulgar, o hacer que se divulgue, información personal que esté bajo su custodia o control con fines históricos o de archivo, si:

a. la divulgación no supone una invasión poco razonable de la vida privada personal o profesional;

b. la divulgación tiene como finalidad la investigación histórica y está en consonancia con el Artículo 18;

c. la información se refiere a alguien que ha fallecido hace [...] o más años;

d. la información está en un registro que tiene [...] o más años de existencia.

Restricciones en la transferencia a la jurisdicción de un tercero

19. (1) Sin perjuicio de lo dispuesto a continuación, la transferencia de datos personales objeto de tratamiento a la jurisdicción de un tercero sólo puede llevarse a cabo en virtud de las disposiciones de esta Ley y siempre que dicha jurisdicción garantice niveles de protección equiparables.

(2) El nivel adecuado de protección de la jurisdicción de un tercero será evaluado a la luz de todas las circunstancias que rodean la operación de transferencia de datos o un conjunto de operaciones de transferencia de datos; se tendrá en cuenta en particular la naturaleza de los datos, la finalidad y la duración de la operación u operaciones de tratamiento propuestas, el país de origen y el país de destino, las normas de derecho, tanto generales como sectoriales, vigentes en el país del tercero y las normas profesionales y medidas de seguridad que se aplican en ese país.

(3) El Comisionado de datos deberá determinar si el país de un tercero garantiza un nivel adecuado de protección. Tras tomar la 27ecision, el Comisionado de datos dará a conocer:

a. la autoridad pública pertinente responsible de la protección de datos en la otra jurisdicción;

b. su determinación de los niveles de protección equiparables que ofrece; y

c. en caso de que determine que los niveles de protección no son compatibles, los aspectos de la información personal [y de la información personal sensible] que no quedarían adecuadamente protegidos.

(4) Cuando, a pesar de no existir unos niveles de protección equiparables, el Comisionado de datos determina que puede haber algún tipo de transferencia por la cual la violación de los derechos del titular de los datos se mantenga dentro de los límites contemplados en esta Ley, el Comisionado podrá autorizar dicha transferencia si:

a. el titular de los datos da su consentimiento a la transferencia de la información a la jurisdicción de un tercero; y

b. se delimitan convenientemente por escrito los aspectos de la información que el Comisionado de datos estime oportunos.

(5) [Cuando exista un acuerdo en vigor para el tratamiento de datos o información en la jurisdicción de un tercero, el Comisionado de datos puede conceder un período razonable de transición para permitir que la entidad responsable de los datos traslade el tratamiento a otra jurisdicción, si fuera necesario.]

(6) Salvo por lo establecido en los párrafos 4 y 5, está prohibida la transferencia de datos personales a la jurisdicción de un tercero que no garantice una protección adecuada.

Códigos de conducta

20. El Comisionado de datos entablará consultas con la industria para promover la aplicación de los principios generales de privacidad a través de la elaboración de códigos de conducta, para lo cual:

a. proporcionará orientación sobre la preparación de códigos de conducta;

b. proporcionará orientación sobre los mecanismos de resolución adecuados;

c. fomentará la educación en los principios generales de privacidad;

d. trabajará con los organismos públicos y privados para promover el conocimiento de los códigos de conducta entre los consumidores; y

e. adoptará cualquier otra acción que considere pertinente.

Códigos de conducta de cumplimiento obligatorio

21. (1) Cuando, en opinión del Comisionado de datos, el interés público justifique la formulación de códigos de conducta de cumplimiento obligatorio en relación con la aplicación de los principios generales de privacidad a una industria, sector económico o actividad en concreto, el Comisionado de datos podrá, mediante orden, solicitar la preparación de un código de conducta y establecer un plazo para su elaboración.

(2) Sujeto al párrafo 1, cuando exista un órgano gubernamental competente regulador de una industria, sector económico o actividad, el Comisionado de datos podrá pedirle que supervise el proceso de elaboración del código de conducta para esa industria, sector económico o actividad.

PARTE III – DERECHOS DEL TITULAR DE LOS DATOS

Derecho de acceso a la propia información personal

22. (1) Toda persona que sea ciudadano o residente de [nombre de la jurisdicción] tiene derecho a acceder, previa petición y una vez realizado el pago de la tasa correspondiente, a:

a. la información personal acerca de esa persona que figura en un sistema de archivo correspondiente que está bajo la custodia y control de la entidad responsable de los datos;

b. cualquier otra información personal acerca de esa persona que esté bajo la custodia o el control de la entidad responsable de los datos y con respecto a la cual la persona pueda proporcionar información lo suficientemente específica como para que la entidad responsable de los datos pueda encontrarla en condiciones razonables.

(2) La solicitud de acceso a la información personal se deberá formular a la entidad responsable de los datos que tiene el control del sistema de archivo o de la información, según sea el caso, mediante el formulario aprobado por el Comisionado de datos.

Facultad de la entidad responsable de los datos para denegar el acceso

23. (1) La entidad responsable de los datos podrá negarse a divulgar información personal a la persona a quien se refiere dicha información cuando:

a. la entrega constituiría una injerencia injustificada en la vida privada de otro individuo;

b. se trate de un registro penitenciario que, si se divulga, podría previsiblemente revelar información suministrada de forma confidencial;

c. se trate de información sujeta al secreto profesional u obtenida en el curso de una investigación o procedimiento judicial;

d. se trate de información médica o sanitaria y el jefe de la entidad responsable de los datos tenga razones para pensar que el acceso a la información podría dañar la salud o seguridad de una persona;

e. se trate de opiniones o material de valoración compilado con el único fin de determinar la idoneidad o condiciones de una persona para aspirar a un empleo, a la adjudicación de contratos públicos y otros beneficios, si la divulgación pudiera revelar la identidad de la fuente que suministró la información, en circunstancias en que sería razonable que dicha identidad permaneciera oculta.

(2) El jefe de la entidad responsable de los datos puede desestimar las peticiones de una persona para acceder a su información personal cuando considere que dicho acceso constituiría una injerencia considerable en las operaciones de la entidad responsable de los datos, por ser solicitudes repetitivas y sistemáticas o de índole superflua o irritante.

Separación de la información exenta

24. (1) La entidad responsable de los datos deberá hacer todo lo posible para separar la información que no pueda divulgarse, de conformidad con el Artículo 24, de la que puede estar disponible para la persona que solicita el acceso a su información personal, y poner a disposición la información no exenta de divulgación.

(2) El jefe de la entidad responsable de los datos puede negarse a revelar la existencia de información cuando el reconocimiento de dicha existencia revelaría aspectos críticos acerca de la exención de esa información.

Delegación de los derechos del titular de los datos

25. Cualquier derecho o facultad conferido a una persona por la presente Ley podrá ser ejercido:

a. por su representante personal, cuando la persona haya fallecido, si el ejercicio del derecho o facultad está relacionado con la administración de los bienes;

b. por el abogado de la persona, en virtud de un poder de representación jurídica;

c. por el tutor o representante legal de la persona; o

d. cuando la persona tenga menos de 18 años, por la persona que tenga su custodia legal.

Plazos para responder a la solicitud

26. (1) Cuando se formula una solicitud de acceso a la información personal de conformidad con el Artículo 23, el jefe de la entidad responsable de los datos deberá, dentro de los [...] días posteriores a la recepción de la solicitud:

a. permitir el acceso, en todo o en parte, y dar la información a la persona que presentó la solicitud; o

b. negar el acceso, en todo o en parte, y responder por escrito a la persona que presentó la solicitud, para indicarle:

i. que la información no existe; o

ii. que hay una disposición específica de la Ley que justifica de forma razonable la denegación del acceso a la información, en caso de que ésta exista; y

iii. la información que la persona pueda necesitar para ejercer su derecho a recurrir esta decisión ante el Comisionado de datos.

(2) Cuando se conceda el acceso a la información, en todo o en parte, el jefe de la entidad responsable de los datos deberá garantizar que la información está disponible de forma íntegra, incluso, cuando sea razonable, de una forma accesible para una persona con una discapacidad sensorial.

Corrección de errores en la información personal almacenada

27. (1) Cuando una persona considere que hay un error o una omisión en sus datos personales, podrá pedir que se corrija al jefe de la entidad responsable de los datos que tenga esa información bajo su custodia o control.

(2) Si tras la solicitud mencionada en el párrafo 1 no se introduce ninguna corrección, el jefe de la entidad responsable de los datos deberá anotar en la información que la corrección se solicitó, pero no se introdujo, y notificar tal circunstancia a la persona que presentó la solicitud.

(3) Al introducir una corrección o anotación en la información personal a que se refiere este Artículo, el jefe de la entidad responsable de los datos deberá notificarlo a toda otra entidad responsable de los datos o a cualquier tercero al que se hubiera comunicado esa información durante el año anterior a la presentación de la solicitud de corrección.

(4) Una vez notificada la corrección o anotación de la información personal en virtud del párrafo 3, la entidad responsable de los datos deberá incorporar esa corrección o anotación en todos los registros de esa información que estén bajo su custodia o control.

PARTE IV – OBLIGACIONES ESPECÍFICAS DE LAS AUTORIDADES PÚBLICAS

Evaluaciones del impacto sobre la privacidad

28. (1) Cada Ministerio deberá preparar una evaluación del impacto sobre la privacidad, en la forma prescrita por el Comisionado de datos, de cualquier acto legislativo, sistema, proyecto, programa o actividad propuestos.

(2) Una vez preparada esa evaluación del impacto sobre la privacidad, cada Ministerio la presentará al Comisionado de datos para su aprobación.

(3) Cuando se presente una evaluación de este tipo, de conformidad con el párrafo 2, el Comisionado de datos la valorará de acuerdo con los principios generales de privacidad y, si lo considera necesario, sugerirá al Ministerio enmiendas para garantizar su cumplimiento.

(4) Cuando el Comisionado de datos formule una recomendación en virtud del párrafo 3, el Ministerio introducirá las modificaciones necesarias al acto legislativo, sistema, proyecto, programa o actividad propuestos.

(5) Cada Ministerio tomará todas las medidas razonables de acuerdo con su evaluación del impacto sobre la privacidad para evitar intrusiones innecesarias en la intimidad personal durante los procesos de diseño, ejecución o aplicación de actos legislativos, sistemas, proyectos, programas o actividades.

Sistemas de archivo de la información personal

29. El jefe de una entidad pública registrada como responsable de información personal tomará las disposiciones para que se incluyan en los sistemas de archivo todos los datos de ese tipo que estén bajo su control o custodia que:

a. hayan sido tratados, estén siendo tratados o estén disponibles para su uso con una finalidad administrativa; o

b. estén organizados o destinados a ser localizados mediante el nombre de una persona o un número, símbolo u otro elemento de identificación asignado a una persona.

Exención de los archivos nacionales

30. Sin perjuicio de lo establecido en el Artículo 31, la información personal bajo custodia o control de los archivos del Gobierno de [nombre de la jurisdicción] que ha sido transferida a los mismos por una autoridad pública con fines históricos o de archivo no se incluirán en los bancos de datos personales.

Representante sobre datos personales

31. (1) La entidad responsable de los datos deberá notificar al Comisionado de datos el nombramiento o cesación en el cargo de un representante sobre datos personales.

(2) El representante sobre datos personales actuará de forma independiente con la misión de garantizar que la entidad responsable de los datos trata los datos personales de manera lícita y correcta, y de acuerdo con las buenas prácticas; en caso de que detecte una irregularidad en este sentido, deberá ponerla en conocimiento de la entidad responsable de los datos.

(3) Si el representante sobre datos personales tiene motivos para sospechar que la entidad responsable de los datos ha contravenido las disposiciones aplicables para el tratamiento de los datos personales y ésta no lleva a cabo una rectificación tan pronto como sea posible después de que se le ha señalado la infracción, deberá dar cuenta de esta situación al Comisionado de datos.

Autorización para compartir información

32. Cuando una autoridad pública tenga la intención de comunicar información a otras autoridades públicas, sólo podrá hacerlo en virtud de un acuerdo en la forma que prescriba, y por lo tanto apruebe, el Comisionado de datos.

Informe del Comisionado sobre bancos de informa-ción personal

33. El Comisionado de datos publicará periódicamente, y al menos una vez al año, un índice de la información personal en posesión de las autoridades públicas, que incluirá un resumen de:

a. los sistemas de archivo de información personal que están bajo custodia o control de cada autoridad pública;

b. los acuerdos de intercambio de información celebrados por una autoridad pública con otra autoridad pública u otra persona;

c. las actividades de correlación de datos aprobadas por el Comisionado de datos;

d. la información de contacto del funcionario a quien se deben enviar las peticiones relativas a información personal contenida en el banco de datos;

e. una relación de los fines para los cuales se obtuvo o compiló la información personal que figura en el banco de datos y una relación de los diferentes usos coherentes con esos fines que se da a la información utilizada o divulgada;

f. una declaración de las normas y prácticas de conservación y eliminación aplicables a la información personal almacenada en el banco de datos; y

g. las evaluaciones del impacto sobre la privacidad preparadas por un Ministerio.

PARTE V – EXENCIONES ESPECIALES

Fines domésticos

34. Una persona estará exenta de las disposiciones de las Partes 3, 4 y 5 cuando trate datos para fines que atañen sólo a asuntos personales, familiares o domésticos, o con fines recreativos.

Seguridad nacional, delincuencia y tributación

35. (1) El Ministro podrá, mediante orden publicada en el Boletín Oficial, en interés de la seguridad nacional, eximir a la entidad responsable de los datos del cumplimiento de alguna disposición de esta Ley.

(2) Una entidad responsable de los datos que también sea una autoridad pública estará exenta del cumplimiento de las disposiciones de [las Partes II y III] si el tratamiento de los datos es necesario para:

a. prevenir o descubrir delitos;

b. arrestar o enjuiciar delincuentes; o

c. calcular o recaudar un impuesto, derecho o gravamen de naturaleza similar.

Exenciones en la aplicabilidad a las actividades reguladoras

36. (1) Los datos personales tratados para los fines de dar cumplimiento a determinadas funciones, en virtud de las actividades reguladoras requeridas por una ley escrita, estarán exentos de las Partes II y III de esta Ley en la medida en que la aplicación de las disposiciones contenidas en ellas pueda probablemente perjudicar el buen desempeño de dichas funciones.

(2) El párrafo 1 se aplicará a cualquier función relevante diseñada para:

a. proteger a los ciudadanos contra:

i. las pérdidas económicas debidas a comportamiento deshonesto, falta profesional u otra conducta indebida grave, o a falta de idoneidad o incompetencia de las personas dedicadas a la prestación de servicios de banca, seguros, inversiones u otros servicios financieros, o a la gestión de personas jurídicas,

ii. las pérdidas económicas debidas a la conducta de personas insolventes, rehabilitadas o no, o

iii. el comportamiento deshonesto, falta profesional u otra conducta indebida grave, o falta de idoneidad o incompetencia, de las personas autorizadas para ejercer una profesión o actividad.

b. proteger a las instituciones de beneficencia de la mala conducta indebida o mala gestión en su administración (ya sea por parte de los administradores u otras personas),

c. proteger los bienes de las instituciones de beneficencia de pérdidas o uso indebido,

d. recuperar bienes de las instituciones de beneficencia,

e. garantizar la salud, seguridad y bienestar de las personas que trabajan, o

f. proteger a otras personas, distintas de las que trabajan, contra los riesgos para la salud o la seguridad que surjan de la actividad de las personas que trabajan, o tengan conexión con ella.

Excepciones en la aplicabilidad al periodismo, la literatura y el arte

37. (1) Cuando deba tratarse información personal en un caso particular en que:

a. el tratamiento se lleva a cabo con miras a la publicación por una persona de material periodístico, literario o artístico;

b. la entidad responsable de los datos considera de forma razonable, y teniendo especialmente en cuenta la importancia del interés público en la libertad de expresión, que su publicación redundaría en el interés público; o

c. la entidad responsable de los datos considera de forma razonable que, teniendo plenamente en cuenta las circunstancias, el cumplimiento de las disposiciones pertinentes de la Parte II es incompatible con los fines periodísticos, literarios o artísticos que se persiguen,

la información personal estará exenta de las Partes II y III de esta Ley.

(2) A los fines del párrafo 1, el Comisionado de datos puede establecer códigos de conducta de acuerdo con los Artículos 21 y 22, los cuales pueden modificar en su caso las disposiciones de las Partes II y III a fin de lograr un equilibrio apropiado de los objetivos de esta Ley y el derecho a la libertad de expresión imperante.

PARTE VI – REVISIÓN Y RECURSOS

Derecho de un solicitante a recurrir la decisión de la entidad responsable de los datos

38. Una persona que ha presentado una solicitud de acceso a su información personal de conformidad con el Artículo 22 o que haya solicitado la corrección de datos personales de conformidad con el Artículo 27 puede recurrir cualquier decisión del jefe de la entidad responsable de los datos ante el Comisionado de datos.

Plazo para la presentación del recurso

39. Un recurso ante el Comisionado de datos en virtud del Artículo 39 se deberá presentar dentro de las [...] semanas posteriores a la fecha en que se recibió notificación de la decisión recurrida, mediante la presentación de un escrito de apelación ante el Comisionado de datos.

Facultad del Comisionado de desestimar un recurso

40. El Comisionado de datos puede desestimar un recurso si el escrito de apelación no expone una base razonable que demuestre la existencia de la información personal a que se refiere el escrito.

Facultad del Comisionado de transmitir el escrito de apelación al responsable de los datos

41. Una vez recibido el escrito de apelación, el Comisionado de datos informará del mismo al jefe de la entidad responsable de los datos de que se trata, y a cualquier otra persona interesada.

Facultad del Comisionado de datos de designar un mediador

42. El Comisionado de datos puede designar un mediador para que investigue las circunstancias del recurso y trate de llegar a un arreglo en el asunto que ha dado lugar a ese recurso.

Facultad del Comisionado de llevar a cabo una investigación

43. (1) El Comisionado de datos puede llevar a cabo una investigación para revisar la decisión del jefe de la entidad responsable de los datos si el Comisionado:

a. no autorizó que un mediador llevara a cabo una investigación en virtud del Artículo 43, o

b. autorizó que un mediador llevara a cabo una investigación en virtud del Artículo 43, pero no se llegó a un arreglo.

(2) Si el Comisionado de datos lleva a cabo una investigación en virtud de este artículo puede, sobre la base de las conclusiones de esa investigación:

a. confirmar la decisión del jefe de la entidad responsable de los datos, u

b. ordenar al jefe de la entidad responsable de los datos que facilite la información personal o introduzca las correcciones solicitadas.

Reuniones en privado

44. La investigación realizada por el Comisionado de datos o un mediador y las reuniones celebradas por un mediador con las partes en el recurso pueden llevarse a cabo en privado.

Representación en la investigación

45. La persona que recurre la decisión por la que se le deniega el acceso a su información personal, el jefe de la entidad responsable de los datos y cualquier otra parte interesada, pueden estar representados por un abogado o agente.

Carga de la prueba asignada a la entidad responsable de los datos

46. Cuando la entidad responsable de los datos deniegue el acceso a información personal, la carga de la prueba de que la información queda dentro de una de las exenciones especificadas en la Ley se basará en un equilibrio de probabilidades y recaerá sobre la entidad responsable de los datos.

Recurso ante los tribunales

47. Cualquiera de las partes puede recurrir la decisión del Comisionado de datos ante los tribunales, de conformidad con el Artículo 80 de esta Ley.

PARTE VII – INFRACCIONES Y EJECUCIÓN DEL CUMPLIMIENTO

Creación de la Oficina del Comisionado de datos

48. (1) Con sujeción al párrafo 2 *infra*, el [Jefe de Estado], previa consulta con el Primer Ministro y el líder de la oposición, nombrará un Comisionado de datos.

(2) Una persona no reúne las condiciones para ocupar el cargo de Comisionado de datos si:

a. es Ministro, Secretario Parlamentario, o miembro de la Asamblea Legislativa; o

b. es juez o magistrado; o

c. es funcionario público; o

d. es miembro de una autoridad local; o

e. tiene intereses económicos o de otro tipo en cualquier empresa o actividad que pueda afectar el desempeño de sus funciones como Comisionado; o

f. es insolvente no rehabilitada; o

g. ha sido condenada por un delito de fraude.

(3) El Comisionado de datos contratará el personal que sea necesario, que estará sujeto a su control administrativo.

(4) El Comisionado de datos no podrá ocupar ningún otro cargo retribuido, ni público ni privado, ni desempeñar ninguna otra ocupación por la que perciba una remuneración.

(5) El [Jefe de Estado], previa consulta con [el Primer Ministro y el líder de la oposición], nombrará a una persona que reúna las condiciones para aspirar al cargo de Comisionado provisional si:

a. el Comisionado de datos renuncia o si su cargo queda vacante por cualquier otro motivo;

b. el Comisionado de datos no puede, por cualquier motivo, ejercer las funciones propias de su cargo;

c. el Comisionado de datos considera necesario no desempeñar con carácter temporal ninguna de sus funciones por alguna circunstancia que, de ser magistrado del Tribunal Superior, habría hecho que se abstuviera;

y cualquier persona así nombrada cesará en el cargo de Comisionado provisional cuando se nombre un Comisionado para ocupar la vacante o, en su caso, cuando el Comisionado de datos que no podía ejercer las funciones de su cargo reanude su actividad o, en caso de una finalidad limitada en el tiempo, cuando el Comisionado provisional haya llevado a cabo la tarea que se le encomendó.

(6) Sólo se procederá al nombramiento de un Comisionado provisional con una finalidad limitada en el tiempo, conforme a lo dispuesto en los párrafos 3 b) y c), en virtud de un certificado firmado por el Comisionado de datos en que indique que, a su juicio, es necesario el nombramiento de un Comisionado provisional para el desarrollo normal de las actividades del Comisionado de datos en el marco de la aplicación de esta Ley.

Personalidad jurídica y representación del Comisionado de datos

49. (1) El Comisionado de datos tendrá una personalidad jurídica diferenciada y, con sujeción a las disposiciones de esta Ley, deberá tener capacidad para celebrar contratos; adquirir, mantener y utilizar cualquier tipo de bienes en el ejercicio de sus funciones; demandar y ser demandado; y actuar y participar en todas las operaciones que se deriven del ejercicio o desempeño de sus funciones en virtud de esta Ley, o que las favorezcan.

(2) Cualquier documento que se presente como un instrumento creado o emitido por el Comisionado de datos y firmado por él se admitirá como prueba y, hasta que se demuestre lo contrario, se considerará un instrumento creado o emitido por el Comisionado de datos.

Duración del mandato

50. (1) El Comisionado de datos ocupará el cargo por un período no superior a cinco años y podrá ser reelegido al expirar su mandato.

(2) Sin perjuicio de lo dispuesto en el párrafo 3 *infra*, el Comisionado de datos dejará vacante su cargo:

a. al vencimiento del período para el cual fue designado;

b. si deja de reunir las condiciones en virtud del Artículo 48, párrafo 2; o

c. si es nombrado para otro cargo retribuido o se dedica a otra ocupación por la que perciba una remuneración;

(3) El Jefe de Estado, previa consulta con [el Primer Ministro y el líder de la oposición] sólo podrá dejar cesante de su cargo al Comisionado de datos por incapacidad para ejercer las funciones propias de su cargo, ya sea por enfermedad física o mental sobrevenida, o por otra causa, o por una falta profesional.

Remuneración del Comisionado de datos y del personal

51. El Comisionado de datos y su personal percibirán una remuneración y asignaciones para gastos, con cargo al Fondo Consolidado.

Protección del Comisionado de datos

52. No se podrá emprender ninguna acción u otro procedimiento por daños y perjuicios contra el Comisionado de datos por actos realizados de buena fe en el ejercicio de sus funciones o de las atribuciones y facultades que le confiere esta Ley.

Delegación de atribuciones

53. El Comisionado de datos podrá delegar cualquiera de las atribuciones de investigación y ejecución que le confiere la presente Ley a un funcionario autorizado y a un agente de policía designado a tal efecto por el propio Comisionado.

Independencia en el ejercicio de sus funciones

54. El Comisionado de datos actuará, en el ejercicio de sus funciones en virtud de esta Ley, con total independencia, y no estará sujeto a la dirección o control de ninguna otra persona o autoridad.

Funciones del Comisionado de datos

55. El Comisionado de datos:

a. garantizará el cumplimiento de esta Ley y las reglamentaciones;

b. creará y mantendrá un registro de las entidades responsables de los datos;

c. controlará todas las actividades de tratamiento de datos y, ya sea de oficio o a petición del titular de los datos, verificará si dichas actividades se llevan a cabo de acuerdo con las disposiciones de esta Ley o las reglamentaciones;

d. dará instrucciones a la entidad responsable de los datos para que tome las medidas necesarias para garantizar que el tratamiento de los datos está en consonancia con esta Ley o las reglamentaciones; e

e. investigará las quejas y reclamaciones de los titulares de los datos, o de las asociaciones que los representen, sobre violaciones de esta Ley o las reglamentaciones, y adoptará las medidas correctivas que considere necesarias o que puedan estar previstas en virtud de esta Ley, e informará del resultado a los titulares de los datos o las asociaciones;

f. emitirá las instrucciones o declaraciones públicas que se le requieran a los efectos de esta Ley;

g. adoptará las medidas que sean necesarias para dar a conocer las disposiciones de esta Ley al público en general;

h. promoverá, mediante la educación y la publicidad, la comprensión y aceptación de los principios para la protección de datos y los objetivos de esos principios;

i. asesorará al Gobierno sobre cualquier medida legislativa que se desee adoptar en relación con la privacidad y protección de datos;

j. por propia iniciativa, o previa solicitud, informará al Ministro cuando lo considere necesario sobre cualquier asunto que afecte a la privacidad de un titular de los datos, lo que incluirá recomendaciones relativas a la necesidad o conveniencia de adoptar medidas legislativas, administrativas o de otro tipo para conceder o mejorar la protección de la privacidad del titular de los datos;

k. colaborará con las autoridades de supervisión de otros países, en la medida que se considere necesario para facilitar el desempeño de sus funciones, en particular mediante el intercambio de información útil, en cumplimiento de los convenios en que [nombre del Estado miembro] sea parte o de cualquier otra obligación internacional de [nombre del Estado miembro];

l. en general, vigilará el cumplimiento de las disposiciones de esta Ley por parte de los organismos gubernamentales y no gubernamentales;

m. preparará y emitirá o aprobará, en consulta con las partes interesadas de la industria, los correspondientes códigos de conducta o directrices para la orientar a las personas e instituciones comerciales que tratan datos personales;

n. investigará y hará un seguimiento de la evolución en el tratamiento de datos y en las tecnologías de la información para asegurar que se reduzcan al mínimo los efectos adversos de esos cambios en la privacidad de los titulares de los datos, e incluirá los resultados de esas investigaciones y ese seguimiento, en su caso, en el informe anual que debe elaborar de conformidad con el Artículo 72;

o. prestará asesoramiento, con o sin previa solicitud, a un Ministro u otra autoridad pública en todos los asuntos relativos a la puesta en práctica de esta Ley, e informará al Ministro, según sea necesario, sobre la conveniencia de que [nombre del Estado miembro] manifieste su aceptación a los instrumentos internacionales sobre la privacidad de los titulares de datos;

p. llevará a cabo cualquier acción subsidiaria o que favorezca el cumplimiento de alguna de las funciones anteriores; y

q. ejercerá y desempeñará otras funciones que le sean conferidas o impuestas en virtud de esta ley u otro acto legislativo.

Confidencialidad y juramento

56. (1) El Comisionado de datos y los funcionarios autorizados deberán prestar juramento ante el Jefe de Estado, tal como se desprende del apéndice.

(2) La persona que sea o haya sido Comisionado de datos, o un funcionario del personal o un agente del Comisionado de datos, no deberá utilizar ni divulgar, ya sea directa o indirectamente, ningún dato obtenido a raíz del ejercicio de su autoridad o durante el desempeño de su función en virtud de esta Ley, salvo:

a. si es conforme con esta ley u otro acto legislativo; o

b. si está autorizado por orden de un tribunal.

(3) La persona que, sin excusa legítima, contravenga el párrafo 2, cometerá un delito y será sancionada con una multa de hasta [...] dólares o una pena de prisión no superior a [...], o con ambas.

Atribuciones del Comisionado

57. El Comisionado de datos tendrá, en el cumplimiento de sus funciones, atribuciones para realizar todos los actos que le parezcan necesarios, ventajosos o convenientes para la realización de dichas funciones, o en relación con las mismas.

Atribuciones del Comisionado para obtener información

58. (1) El Comisionado de datos podrá, mediante un aviso por escrito, solicitar a una persona que le proporcione, también por escrito y en el plazo especificado en el aviso:

a. acceso a sus datos personales;

b. información y documentación relativas al tratamiento de datos personales;

c. información relacionada con la seguridad en el tratamiento de datos personales; y

d. cualquier otra información en relación con los asuntos especificados en el aviso que sea necesaria o conveniente para el desempeño de sus funciones y el ejercicio de sus atribuciones y obligaciones en virtud de esta Ley.

(2) Cuando la información solicitada por el Comisionado de datos se encuentre almacenada en un ordenador, disco, casete, microfilm o cualquier otro medio, o conservada en un dispositivo o sistema mecánico o electrónico, la persona a la que se dirige el aviso presentará la información, o dará acceso a la misma, en un formato que la haga transferible, inteligible y recuperable.

(3) Una ley en vigor en [nombre del Estado miembro] o una norma de derecho que prohíba o restrinja la divulgación de información no impedirá que una persona ponga a disposición del Comisionado de datos cualquier información que sea necesaria o conveniente para el desempeño de sus funciones.

(4) El párrafo 3 no se aplicará a la información que, en opinión del Ministro responsable de la seguridad nacional, se conserva, o en algún momento se conservó, con el propósito de salvaguardar la seguridad de [nombre del Estado miembro] ni a la información de carácter reservado en los procedimientos en un tribunal.

Contenido del aviso

59. El aviso mencionado en el Artículo 58 deberá indicar:

a. que la persona a quien va dirigida tiene derecho a presentar un recurso, en virtud del Artículo 81, contra la solicitud especificada en el aviso dentro de los 30 días posteriores a su recepción; y

b. el plazo para cumplir con la solicitud especificada en el aviso, que no podrá expirar antes de los 30 días referidos en el párrafo a) *supra*.

Omisión o negativa a cumplir con el aviso

60. (1) Una persona no podrá, sin causa justificada, omitir o negarse a cumplir una solicitud especificada en un aviso.

(2) Una persona no podrá, en cumplimiento de un aviso de solicitud de información, proporcionar al Comisionado de datos información a sabiendas de que es falsa o engañosa en un aspecto material.

(3) Una persona que infrinja lo dispuesto en los párrafos 1 o 2 cometerá un delito y será sancionada [en juicio sumario] con una multa de hasta [...] dólares o una pena de prisión no superior a [...] meses, o con ambas.

(4) Una persona acusada de un delito en virtud de los párrafos 1 o 2 podrá defenderse demostrando que actuó con la debida diligencia para cumplir con el aviso de solicitud de información.

Información insuficiente conforme al aviso

61. Si el Comisionado de datos no puede, de conformidad con una solicitud formulada en virtud del Artículo 58, párrafo 1, obtener información suficiente que demuestre que el tratamiento de datos personales es lícito, podrá prohibir a la entidad responsable de los datos que proceda a tratar datos personales de cualquier forma que no sea su almacenamiento.

Quejas al Comisionado y atribuciones de investigación

62. (1) El Comisionado de datos puede, a partir de la queja del titular de los datos o de oficio, investigar, u ordenar que se investigue, si una entidad responsable de los datos ha infringido, está infringiendo o podría infringir alguna disposición de esta Ley o de la reglamentación en relación con un titular de los datos.

(2) Cuando se presenta una queja ante el Comisionado de datos en virtud del párrafo 1, éste:

a. investigará la queja, u ordenará que un funcionario autorizado la investigue, a menos que considere que es superflua o irritante; y

b. tan pronto como sea razonablemente posible, notificará por escrito su decisión sobre la queja al titular de los datos interesado, quién podrá, si se siente agraviado por la decisión del Comisionado de datos, recurrir ante un tribunal en virtud del Artículo 81.

(3) Ninguna disposición de esta Ley impide que el Comisionado de datos reciba e investigue las quejas presentadas por una persona que haya sido autorizada por escrito por el titular de los datos interesado a actuar en su nombre, y toda referencia al titular de los datos que figure en otro artículo de esta Ley abarca a esta persona autorizada.

Formulario de queja

63. (1) Toda queja de conformidad con esta Ley se deberá presentar al Comisionado de datos por escrito, a menos que éste autorice otra cosa.

(2) El Comisionado de datos facilitará una asistencia razonable, cuando las circunstancias lo hagan necesario, para que cualquier persona que desee presentar una queja pueda hacerlo por escrito.

Aviso de investigación

64. Antes de iniciar una investigación sobre una queja presentada de conformidad con esta Ley, el Comisionado de datos, cuando se trate de una autoridad pública, notificará al Secretario permanente, o en cualquier otro caso, al Director general, su intención de iniciar la investigación, e incluirá en la notificación el fundamento de la queja.

Facultad de entrada, allanamiento e incautación

65. (1) Sujeto al párrafo 2 *infra*, un funcionario autorizado acompañado por un agente de policía puede, en cualquier momento, entrar en locales, realizar un allanamiento, inspeccionar, examinar, hacer funcionar y probar todos los equipos que se encuentren y se utilicen o estén destinados a ser utilizados para el tratamiento de datos personales, e inspeccionar e incautarse de todos los documentos, equipos y cualquier otro material encontrado.

(2) Un funcionario autorizado no podrá entrar en ningún local con la intención de allanarlo e incautarse de documentos a menos que esté acompañado por un agente de policía y muestre al propietario u ocupante del local una orden emitida por un [magistrado o autoridad competente (según la jurisdicción)].

Asuntos exentos de inspección e incautación

66. (1) Las facultades de inspección e incautación conferidas por una orden judicial no podrán ejercerse respecto de los datos de carácter personal que en virtud de la Parte V están exentos de algunas de las disposiciones de esta Ley.

(2) Las facultades de inspección e incautación conferidas por una orden judicial no pueden ejercerse en relación con:

a. la comunicación entre un asesor jurídico profesional y su cliente en el marco de la prestación de asesoramiento jurídico al cliente sobre sus obligaciones, responsabilidades o derechos en virtud de esta Ley; o

b. la comunicación entre un asesor jurídico profesional y su cliente, o entre este asesor o su cliente y cualquier otra persona, en el marco o como parte de los procedimientos en virtud de la presente Ley o que deriven de ella.

Atribuciones del Comisionado para emitir un aviso de ejecución

67. Cuando el Comisionado de datos considera que la entidad responsable de los datos ha infringido o está infringiendo una disposición de esta Ley, podrá, con sujeción al Artículo 69, enviar un aviso de ejecución a la persona responsable de los datos, a fin de que adopte las medidas que se especifican en el aviso de ejecución, en el plazo que se estipule en ese aviso para cumplir con la disposición de que se trata.

Aviso de ejecución

68. (1) El aviso de ejecución se hará por escrito y:

a. especificará la disposición de esta Ley que, en opinión del Comisionado de datos, ha infringido o está infringiendo la entidad responsable de los datos, y las razones que le han llevado a formarse esa opinión; y

b. especificará las medidas que el Comisionado de datos exige que adopte la entidad responsable de los datos;

c. informará al responsable de los datos, con sujeción al párrafo 2, de su derecho a presentar recurso en virtud del Artículo 81, y del plazo para interponer dicho recurso.

(2) Un aviso de ejecución podrá, sin perjuicio de las especificaciones generales enunciadas en el párrafo 1, exigir que la entidad responsable de los datos:

a. rectifique o suprima cualquiera de los datos en cuestión; o

b. complete los datos personales con la declaración que apruebe el Comisionado de datos en relación con los asuntos de los que tratan, así como aquellos datos personales que sean inexactos o no estén actualizados.

(3) El plazo fijado en un aviso de ejecución para el cumplimiento de una solicitud especificada en ese aviso no podrá expirar antes que el plazo para presentar recurso, tal como se indica en el Artículo [81].

(4) Una vez haya cumplido con la solicitud en virtud del párrafo 2 *supra*, la entidad responsable de los datos, tan pronto como sea posible y en cualquier caso no más tarde de 30 días después de dicho cumplimiento, notificará:

a. al titular de los datos en cuestión;

b. si el Comisionado de datos considera que razonablemente es posible hacerlo, a toda persona a la que se divulgaron los datos inmediatamente antes del cumplimiento de la solicitud de rectificación, supresión o declaración complementaria, si el cumplimiento de esa solicitud modifica sustancialmente los datos en cuestión.

(5) El Comisionado de datos podrá cancelar un aviso de ejecución; si lo hace, deberá notificarlo por escrito, como corresponde, a la persona a la que iba dirigido.

Incumplimiento del aviso de ejecución como delito

69. (1) Una persona no podrá, sin causa justificada, omitir o negarse a cumplir con una solicitud especificada en un aviso de ejecución.

(2) La persona que infrinja lo dispuesto en el párrafo 1 cometerá un delito y será sancionada en juicio sumario con una multa de hasta [...] dólares o una pena de prisión no superior a [...] meses, o con ambas.

Confidencialidad de las investigaciones

70. (1) Todas las investigaciones de una queja presentada de conformidad con esta Ley tendrán carácter privado.

(2) En el curso de la investigación de una queja iniciada por el Comisionado de datos en virtud de esta Ley, la persona que presentó la queja, el jefe de la entidad responsable del tratamiento o cualquier parte interesada tendrá la oportunidad de presentar sus argumentos al Comisionado de datos, pero ninguna parte tendrá derecho a estar presente durante la exposición de argumentos realizada ante el Comisionado de datos, ni tener acceso a esos argumentos o formular comentarios al respecto.

Remisión de asuntos a la policía

71. Al término de una investigación realizada en virtud de esta Ley, el Comisionado de datos podrá, cuando la investigación revele que se ha cometido un delito contemplado en esta Ley o en la reglamentación, remitir el asunto a la policía para que adopte las medidas pertinentes.

Informe anual

72. El Comisionado de datos deberá presentar un informe anual de las actividades de su oficina en el Parlamento dentro de los [...] meses siguientes a la finalización de cada ejercicio financiero.

PARTE VIII – INFRACCIONES Y EJECUCIÓN DEL CUMPLIMIENTO

Persona que actúa como responsable de los datos sin autorización

73. (1) La persona que recopile, trate o divulgue información personal sin haberse inscrito previamente en el registro del Comisionado de datos, o al margen de un acuerdo para actuar en nombre de una entidad responsable de los datos registrada, cometerá un delito según lo previsto en esta Ley y será sancionada en juicio sumario con una multa de hasta [...] o a una pena de prisión de [...].

(2) Cuando una jurisdicción considere necesario establecer una distinción para la "información personal sensible", las sanciones podrán ser más severas que las descritas en el párrafo 1 en caso de recopilación, tratamiento o divulgación inadecuados de dicha información.

Incumplimiento de la restricción de transferir datos a jurisdicciones de terceros

74. (1) La persona registrada como responsable de los datos en virtud de esta Ley que no cumpla con alguna de las disposiciones del Artículo 19 cometerá un delito con arreglo a esta Ley y será sancionada:

a. en juicio sumario, con multa de hasta [...] o pena de prisión por un período de [...]; y

b. en sentencia condenatoria, con multa de hasta [...] o pena de prisión por un período de hasta [...].

Obstrucción de la labor de un funcionario autorizado

75. (1) Ninguna persona podrá, en relación con el ejercicio de las atribuciones conferidas por los Artículos 66 y 67:

a. obstruir o impedir el ejercicio de las atribuciones conferidas a un funcionario autorizado;

b. negarse a proporcionar la asistencia o información solicitada por el funcionario autorizado;

c. negarse a permitir que un funcionario autorizado entre en un local en el ejercicio de sus funciones;

d. facilitar a un funcionario autorizado una información a sabiendas de que es falsa o engañosa en un aspecto material.

(2) La persona que infrinja lo dispuesto en el párrafo 1 cometerá un delito y será sancionada en juicio sumario con una multa de hasta [...] dólares, una pena de prisión no superior a [...] meses, o con ambas.

Declaraciones falsas presentadas por los solicitantes

76. (1) La persona que formule una solicitud de acceso o de corrección de datos personales con argumentos falsos cometerá un delito contemplado en esta Ley y será sancionada en juicio sumario con multa de hasta [...] o pena de prisión por un período de [...];

(2) La persona que intencionadamente formule una declaración falsa para engañar o tratar de inducir a error al Comisionado de datos en el ejercicio de sus funciones en virtud de esta Ley, cometerá un delito contemplado en esta Ley y será sancionada en juicio sumario con multa de hasta [...] o pena de prisión por un período de [...].

Violación del carácter confidencial

77. La persona que viole la obligación de confidencialidad establecida en el Artículo 57 cometerá un delito contemplado en esta Ley y será sancionada en juicio sumario con multa de hasta [...] o pena de prisión por un período de [...].

PARTE IX – ASUNTOS VARIOS

Protección de los denunciantes

78. Un empleador, sea o no una autoridad pública, no podrá despedir, suspender, degradar, sancionar, acosar, poner de otro modo en situación de desventaja o negar una prestación a un empleado por el hecho de que:

a. dicho empleado, actuando de buena fe y sobre la base de una convicción razonable:

i. haya notificado al Comisionado de datos que el empleador o cualquier otra persona ha infringido o está a punto de infringir esta Ley;

ii. haya hecho, o haya declarado su intención de hacer, todo lo necesario para evitar que una persona infrinja esta Ley; o

iii. se haya negado a hacer, o haya declarado su intención de negarse a hacer, algo que infrinja esta Ley; o

b. el empleador crea que el empleado va a hacer cualquiera de las cosas descritas en el párrafo a).

Tasas

79. (1) El Ministro podrá, a raíz de las consultas entabladas con la autoridad designada, prescribir, mediante la reglamentación correspondiente:

a. la tasa que deberá cobrar una entidad responsable de los datos, o cada categoría de las entidades responsables de los datos, para atender la presentación de una solicitud de un interesado para acceder a su información personal;

b. la manera en que se calculará la tasa que deberá pagarse en virtud de esta Ley, y el importe máximo.

Reglamentaciones

80. (1) El Ministro podrá, en consulta con el Comisionado de datos, elaborar reglamentaciones para dar efecto a los propósitos de esta Ley y prescribir todo lo que esta Ley requiera o autorice a prescribir.

(2) Sin perjuicio del enunciado general del párrafo 1, las reglamentaciones elaboradas en virtud de este artículo podrán:

a. prescribir las tasas que deberá pagar la entidad responsable de los datos;

b. proporcionar directrices de procedimiento para recurrir la decisión de una entidad responsable de los datos;

c. prescribir todo lo que sea necesario prescribir en virtud de esta Ley; y

d. dar efecto a las disposiciones de esta Ley.

(3) Las reglamentaciones elaboradas en virtud de este artículo estarán sujetas a la resolución afirmativa del Parlamento.

Función de los tribunales

81. (1) Con sujeción al párrafo 2, se podrá presentar un recurso ante un tribunal contra:

a. una solicitud especificada en un aviso de solicitud de información o en un aviso de ejecución;

b. una decisión del Comisionado de datos en relación con una queja; o

c. una decisión del Comisionado de datos en relación con el desempeño de sus deberes y atribuciones en virtud de la presente Ley.

(2) El recurso se deberá interponer dentro de los [...] días a partir de la entrega al interesado de la notificación pertinente, o, cuando sea el caso, de la recepción por parte de dicha persona de la pertinente notificación de rechazo o decisión.

(3) El tribunal tendrá jurisdicción para oír y dictar sentencia, a petición del Comisionado de datos, en los casos que supongan una violación de las disposiciones de esta Ley y para emitir las órdenes adecuadas a ese respecto.

Sección III:
Notas explicativas del modelo de texto legislativo sobre privacidad y protección de datos

INTRODUCCIÓN

1. Este modelo de texto legislativo sobre privacidad y protección de datos forma parte de un conjunto de modelos de textos legislativos destinados a facilitar el desarrollo de la "sociedad de la información" en virtud de un proyecto de alcance regional que abarca los países de la CARICOM y la República Dominicana.
2. La sociedad de la información se basa en la utilización de sistemas automatizados de tratamiento de datos que permiten mejorar la prestación de servicios a los mercados y a las personas en cualquier parte del mundo. Dada la gran capacidad de tratamiento de estos sistemas de información, este nuevo paradigma ha traído también un aumento exponencial de las oportunidades de uso abusivo de la información recopilada acerca de una persona en el curso de una transacción. Para alentar al público a usar estos sistemas es necesario establecer entornos que infundan confianza al usuario y le den la tranquilidad de que la información obtenida de él no se utilizará para fines no autorizados, y que si ello sucede, se aplicarán las acciones que correspondan.
3. El marco jurídico sobre privacidad y protección de datos es uno de los principales aspectos de ese sistema más amplio de creación de confianza.
4. El modelo de texto legislativo sobre privacidad y protección de datos se basa en los componentes básicos para políticas elaborados en las primeras fases del proyecto HIPCAR[4]. Estos componentes básicos revisaron las mejores prácticas internacionales en relación con los objetivos, las principales herramientas comunes y los precedentes, e identificaron las posiciones políticas y los principales sistemas que se deben consagrar dentro de los marcos legislativos en toda la región[5]. El modelo de texto legislativo trata de codificar las directrices para políticas en un instrumento legislativo que procure un equilibrio entre el impulso por la claridad de intención, estructura y función, y la necesidad de abstracción necesaria para facilitar su adaptación y encaje, según sea necesario, dentro del marco legislativo de cada Estado beneficiario del HIPCAR.

---

4 Ed.: El título completo del proyecto HIPCAR es "Mejorar la competitividad en el Caribe a través de la armonización de las políticas, la legislación y los procedimientos reglamentarios relativos a las TIC". Este proyecto de tres años de duración se inició en septiembre de 2008, en el contexto de un proyecto global que abarca a los países ACP y que cuenta con financiación de la Unión Europea (UE) y la Unión Internacional de Telecomunicaciones (UIT). La UIT se encarga de su ejecución en colaboración con la Secretaría de la Comunidad del Caribe (CARICOM) y la Unión de Telecomunicaciones del Caribe (CTU).

5 Ed.: Véase también el Capítulo 1.5 de este documento en que se explica la metodología. Los miembros de los Grupos de Trabajo incluyen representantes del Ministerio y de los organismos reguladores designados por sus gobiernos nacionales, organismos regionales y observadores, como los operadores y otras partes interesadas. El mandato de los Grupos de Trabajo está disponible en www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/docs/ToR%20HIPCAR%20WGs.pdf .

5. Este modelo de texto legislativo sobre privacidad y protección de datos se compone de nueve partes y 81 artículos.

- **La Parte I** trata de consideraciones preliminares, como el título abreviado y la interpretación de determinados términos, y aborda las preocupaciones sobre el ámbito de aplicación del modelo de texto, y además define los principios generales de privacidad que consagra este modelo de texto.
- **La Parte II** trata del establecimiento de una obligación general de las autoridades públicas y los organismos privados que pueden ser considerados responsables de los datos para que asuman su responsabilidad particular en lo que respecta a la gestión de la información personal que está en su poder.
- **La Parte III** crea el derecho general de las personas o titulares de los datos a acceder a la información personal sobre ellos que está en poder de organismos públicos y privados, y velar por su exactitud, y establece los mecanismos y procedimientos para facilitar el otorgamiento de dicho acceso.
- **La Parte IV** identifica las obligaciones específicas de las autoridades públicas en virtud del modelo de texto. Estas obligaciones se orientan a las circunstancias de funcionamiento particulares de los organismos públicos.
- **La Parte V** trata de las condiciones especiales en que la entidad responsable de los datos no está obligada a obtener el consentimiento previo del titular de los datos para su divulgación.
- **La Parte VI** trata de los procedimientos a través de los cuales el titular de los datos puede solicitar una revisión de la decisión de una entidad responsable de los datos por la que se deniega el acceso a los mismos, y cuando sea necesario, interponer un recurso contra esta decisión ante un órgano de supervisión independiente.
- **La Parte VII** establece el marco general y las atribuciones del organismo designado como autoridad de supervisión para velar por la privacidad y protección de datos, y además crea un foro para los recursos interpuestos de conformidad con las disposiciones de la Parte VI.
- **La Parte VIII** esboza las infracciones particulares contra las disposiciones del modelo de texto y las sanciones asociadas con tales infracciones.
- **La Parte IX** aborda asuntos diversos, incluida la clarificación del papel de los tribunales y el establecimiento de un enfoque de regulación conjunta en la aplicación del marco de supervisión, y fija las atribuciones para elaborar reglamentaciones de conformidad con el modelo de texto.

PANORAMA GENERAL DE LAS CLÁUSULAS

PARTE I – OBSERVACIONES PRELIMINARES

6. **La Parte 1 del modelo de texto legislativo (Ley),** se compone de siete artículos. Estos primeros artículos ofrecen observaciones preliminares, como el título abreviado y las disposiciones de inicio de la Ley[6], así como el objetivo general de la misma, lo que ofrece el contexto para la interpretación de los artículos presentados a continuación.

[6] Ed.: El autor de las notas explicativas utiliza la noción "Ley" principalmente para referirse al modelo de texto legislativo (Ley) sobre privacidad y protección de datos.

Sección III

Artículo 3: Interpretaciones y definiciones

7. El Artículo 3 se ocupa de la interpretación de términos específicos de la Ley[7]. Son de interés las interpretaciones de términos como los que se describen a continuación.

8. "Datos" e "información" (términos que se presentan como equivalentes) ponen de relieve una interpretación amplia de las formas, los formatos y las tecnologías (electrónicas o de otro tipo) aplicables en que se pueden presentar o almacenar los datos. Esto es imprescindible ya que, a pesar de la justificación predominante asociada con la ubicuidad de las tecnologías de la información y las comunicaciones (TIC), la definición prevé la aplicación de la Ley y su propósito en entornos que no utilizan sistemas de TIC[8].

9. La definición de "entidad responsable de los datos" está formulada de manera que abarque de forma suficientemente la expresión "personas", para incluir partes del sector tanto público como del privado. Es de destacar que la definición no da a entender que todos los organismos del sector público o privado son entidades responsables de los datos, y limita la aplicabilidad de la Ley a las personas que tienen necesidades legítimas de manejar información personal en el curso de sus actividades sustantivas[9].

10. A pesar de que los componentes básicos para políticas y algunos precedentes internacionales indican la necesidad de distinguir entre "información personal" e "información personal sensible" se consideró en general que las disposiciones pertinentes eran en gran medida equivalentes para abordar ambos tipos de información. Así pues, el modelo de texto legislativo establece que la definición de este último tipo queda abarcada por la del primero. La información personal sensible se incluyó en gran medida en los marcos para la protección de datos como otra forma de abordar los problemas de discriminación sexual, racial o de otros tipos groseros de discriminación. Por lo general, esto se logra limitando aún más el tratamiento aplicable de esas características (género, orientación sexual, opiniones políticas, origen étnico o raza) más allá de la limitación general prevista de todos modos en el marco legislativo, así como aumentando las sanciones para las infracciones relacionadas con este subconjunto de información en comparación con las aplicables a la información "no sensible". No obstante, parece haber un consenso general en el sentido de que el ámbito de la protección de datos no es el mejor para conseguir este propósito. A pesar de ello, en todo el modelo de texto legislativo se ofrece orientación sobre los ámbitos que podrían necesitar una distinción más acentuada, si la jurisdicción decide distinguir entre la información personal y la información personal sensible[10].

11. "Profesional de atención de salud" e "institución de atención de salud " son términos que necesitan una definición apropiada, ya aparecen constantemente con respecto a la no aplicabilidad de la ley en relación con el consentimiento del titular para la recopilación, tratamiento y divulgación de datos personales. Esta exención, como todas las que se refieren al cumplimiento de la ley, se basa en garantizar que el marco de protección de datos no obstaculice el funcionamiento normal de los servicios. Por lo general, en la prestación de servicios de atención de salud, debido a la propia índole de la profesión, no parece razonable esperar que el médico que atiende principalmente al paciente sea capaz de identificar a todas las partes con las que compartirá la información médica en la determinación de un diagnóstico,

---

7 Componente básico 1.1 para políticas: "Hay un mandato jurídico claro en el derecho que apoya el establecimiento de un régimen que garantice la protección de la información personal y/o privada".

8 Componente básico 1.2 para políticas: "El régimen de protección de datos no debería ser específico para una tecnología, por lo que debería ser igualmente pertinente para las versiones impresas que para los entornos propiciados por las TIC".

9 Componente básico 1.4 para políticas: "La ley o el mandato jurídico debería garantizar que la obligación de proteger la privacidad se aplica tanto al sector público como al privado".

10 Componente básico 1.9 para políticas: "La ley o el mandato jurídico debería identificar una categoría de información personal como 'información sensible', que necesitaría una supervisión y un control más estrictos."

o sobre todo, en situaciones de emergencia en que el titular de los datos puede estar incapacitado. Por lo tanto, es necesario establecer una exención general del marco de protección de los datos para las personas que trabajan en estos entornos específicos, ya que este sector debería abordarse específicamente con legislaciones más directamente adaptadas. Es de destacar que algunas funciones administrativas que no están directamente relacionadas con la prestación de servicios de salud quedarían incluidas en esta misma exención.

Artículo 4: La Ley obliga al Estado

12. El Artículo 4 establece que la Ley obliga al Estado. Esta disposición es necesaria debido a que las leyes de interpretación de los Estados miembros mencionan la bien establecida norma de interpretación utilizada en el caso del ***Fiscal General c. Hancock [1940] 1 KB 427***, según la cual un acto legislativo no obliga ni afecta al derecho del Estado a menos que dicha obligación se establezca expresamente en la ley[11].

Artículo 5: Límites jurisdiccionales de la Ley

13. Reconociendo el carácter multinacional de ciertas empresas comerciales, y el entorno globalizado de comercio facilitado por el uso de las TIC, el Artículo 5 intenta aportar claridad sobre los límites jurisdiccionales de la ley en lo que respecta a los responsables de los datos que puedan estar establecidos en una jurisdicción concreta (donde la aplicabilidad es segura) y los otros que no están establecidos o residen en esa jurisdicción, pero que utilizan los recursos que se encuentran en ella. Este artículo es particularmente importante en el contexto de las disposiciones del Artículo 22.

Artículo 6: Límites en la aplicabilidad de la Ley

14. Posteriormente, el Artículo 6 limita la aplicabilidad de la Ley en lo que respecta a limitar la información disponible por ley para los tribunales y juzgados.

Artículo 7: Reseña general de los principios de privacidad

15. Esta Parte también describe, en el Artículo 7, los principios de privacidad que la Ley trata de consagrar en la ejecución de empresas del sector público y privado[12]. Estos principios, basados en los precedentes de la OCDE y la UE, incluyen:

Principio de rendición de cuentas

Una entidad responsable de los datos debe rendir cuentas del cumplimiento de las medidas necesarias para dar efecto a los principios mencionados *supra*.

Principio de limitación en la recopilación

Debe haber límites a la recopilación de datos personales, y todo dato se debe obtener por medios lícitos y justos y, cuando sea apropiado, con el conocimiento o consentimiento del titular de los datos[13].

---

11 Componente básico 1.3 para políticas: "La ley o el mandato jurídico debería establecer claramente que la ley obliga al Estado".

12 Componente básico 2.1 para políticas "Los principios fundamentales del marco jurídico de la protección de datos están claramente definidos [en las Leyes]".

13 Componente básico 1.7 para políticas: "La ley o el mandato jurídico establece claramente que la información personal debería recopilarse y tratarse con el consentimiento del titular de esa información".

Principio de calidad de los datos

Los datos personales deben ser pertinentes a los fines para los que se van a utilizar, y, en la medida necesaria para esos fines, deben ser precisos, completos y actualizados.

Principio de especificación de la finalidad

Se deben especificar los fines para los que se recopilan datos personales, a más tardar en el momento de su recopilación, y el posterior uso de los mismos debe estar limitado al cumplimiento de los fines, o de otros que no sean incompatibles con los fines para los que se recopilaron, y que se hayan especificado cada vez en caso de un cambio de finalidad[14].

Principio de limitación del uso

Los datos personales no deben divulgarse, ponerse a disposición o utilizarse de otro modo para fines distintos a los especificados de conformidad con el principio de especificación de la finalidad, excepto:

a) con el consentimiento del titular de los datos; o

b) por la autoridad de la ley.

Principio de las medidas de seguridad

Los datos personales deben estar protegidos con medidas de seguridad razonables contra riesgos como la pérdida o acceso no autorizado, destrucción, uso, modificación o divulgación de esa información.

Principio de apertura

Debe haber una política general de apertura ante los nuevos avances, prácticas y políticas en el ámbito de los datos personales. Los medios para establecer la existencia y naturaleza de los datos personales, y los principales objetivos de su uso, así como también la identidad y residencia habitual de la entidad responsable de los datos deben estar fácilmente disponibles.

Principio de participación de la persona

Una persona debería tener derecho a:

a) obtener de la entidad responsable de los datos, o de quien corresponda, la confirmación de que dicha entidad tiene o no en su poder datos relativos a la persona interesada;

b) que se le comuniquen los datos relativos a ella:

- en un plazo razonable;
- con un coste, si lo hubiere, que no sea excesivo;
- de una manera razonable; y
- en un formato que sea fácilmente accesible para ella;

c) que se le comuniquen, si una solicitud hecha conforme a los párrafos a) y b) se le deniega, los motivos que justifican esa negativa, de manera que pueda impugnar esa decisión;

[14] Componente básico 2.2 para políticas: "Entre los principios fundamentales de la protección de datos debe haber disposiciones que garanticen que en el momento de la recopilación la persona interesada está informada del fin/uso que se dará a esos datos, y manifiesta de forma clara su consentimiento al respecto".

d) impugnar los datos relativos a ella y, si la impugnación prospera, pedir que se borren, rectifiquen, completen o modifiquen[15].

PARTE II – OBLIGACIONES GENERALES DE LA ENTIDAD RESPONSABLE DE LOS DATOS

16. **La Parte 2 de la Ley modelo** describe las normas a que deben ajustarse todas las entidades responsables de los datos en la aplicación de los principios de privacidad descritos en la Parte 1.

Artículo 8: Registro de entidades responsables de los datos

17. El Artículo 8 prevé la inscripción de las entidades responsables de los datos y el mantenimiento de un registro por parte del Comisionado de datos. En esta disposición se podría facilitar otra alternativa para quien prefiera un proceso de notificación menos obstructivo[16]. En cualquier caso, esto permitirá el cumplimiento del ***principios de rendición de cuentas y apertura de la OCDE,*** que exige que haya una política general de apertura frente a nuevos avances, prácticas y políticas en el ámbito de los datos personales y de los recursos destinados a establecer la existencia y naturaleza de los datos personales y los principales objetivos de su uso, así como la identidad y residencia habitual de la entidad responsable de los datos, que debería ser fácilmente accesible. Asimismo, el Artículo 8, párrafo 2, garantiza el cumplimiento del ***principio de limitación en la recopilación de información de la OCDE,*** que establece que se deben poner límites a la recopilación de datos personales, que dichos datos deben ser obtenidos por medios legítimos y justos y, en su caso, con el conocimiento o consentimiento del interesado[17,18]. Es necesario reiterar que la persona debe conocer la finalidad de la recopilación, uso y divulgación de los datos, y hacerle saber que puede dar o denegar su consentimiento. Por lo general se requiere el consentimiento expreso (comunicado verbalmente o por escrito), pero en circunstancias limitadas puede ser implícito. El consentimiento también debe ser voluntario, debe estar relacionado con la información de que se trata, y no se puede obtener mediante engaño o coacción. La persona también puede retirar o limitar el consentimiento que ya ha dado en todos los casos en que se requiera el consentimiento (implícito o explícito).

Artículo 9: Limitación en la recopilación de información personal

18. Estas últimas obligaciones asociadas con este principio están incluidas en el Artículo 9, junto con la estipulación de que, cuando sea posible, la información siempre se deberá obtener directamente de la persona interesada. De conformidad con este artículo, las entidades responsables de los datos deben garantizar que conocen el propósito para el cual recogen los datos personales y los nombres de las personas que serán destinatarias de esos datos. Sin perjuicio de estos derechos generales, el Artículo 9, párrafo 2, describe las circunstancias

15 Componente básico 2.3 para políticas: "Entre los principios fundamentales de la protección de datos debe haber disposiciones sobre la responsabilidad de la persona y/o entidad que recopila y/o trata la información personal respecto de la seguridad, precisión y uso adecuados de esa información".

16 Componente básico 3.1 para políticas: "La ley o mandato jurídico estipulará que habrá disposiciones que permitan identificar claramente a los que recopilaron, utilizaron y se ocuparon del tratamiento de la información personal, lo que puede incluir la notificación a la persona designada, o el registro ante esta persona".

17 Componente básico 4.1 para políticas: "La ley o mandato jurídico insistirá en que las autoridades públicas solo recabarán aquella información personal que esté expresamente autorizada por la ley".

18 Componente básico 4.3 para políticas: "La ley o mandato jurídico dispondrá que el titular de los datos deberá dar su consentimiento explícito para la recopilación de información".

particulares en que puede no ser posible para el organismo encargado de recopilar la información personal obtenerla directamente del titular de los datos[19].

Artículo 10: Especificación de la finalidad de la recopilación de información

19. El Artículo 10 establece un marco para asegurar el cumplimiento con el ***principio de especificación de la finalidad de la OCDE,*** según el cual se deben especificar los fines para los que se recogen datos personales, a más tardar en el momento de la recopilación de los datos. Así pues, el titular de los datos puede determinar si da o no su consentimiento para la recopilación de la información que sea necesaria para cumplir con esa finalidad. Además, el responsable de los datos está obligado a destruir los datos personales cuando ya no sean necesarios. Para hacerlo, las entidades responsables de los datos deben aplicar prácticas adecuadas de gestión de registros, que incluyan métodos de almacenamiento y eliminación seguros.

Artículo 11: Limitación en la retención de información personal

20. El Artículo 11 establece por lo tanto las limitaciones en la retención de dicha información, permitida sólo durante el tiempo necesario para cumplir con la finalidad para la que se recopiló, así como otras obligaciones (conforme al Artículo 13 de esta Ley y otros) relacionadas con el derecho del titular de los datos a acceder a la información.

Artículo 12: Eliminación adecuada de los datos personales

21. En cumplimiento de esta definición de los aspectos relativos a la retención de datos, el Artículo 12 ofrece una definición de la eliminación adecuada de la información de acuerdo con las mejores prácticas en gestión de registros. En previsión de la necesidad de realizar consultas y tener flexibilidad para fijar el período adecuado para eliminar los datos, en conjunto con las partes interesadas en general (incluso, en el caso de los registros públicos, los archivos nacionales de la jurisdicción), la determinación final de este período se ha dejado a la reglamentación de la aplicación de esta Ley.

Artículo 13: Precisión de la información personal

22. El Artículo 13 de esta Ley modelo prevé el cumplimiento del ***principio de calidad de datos de la OCDE.*** Este artículo, junto con el Artículo 28 de la Parte III, ofrece un marco en el que las entidades responsables de los datos asumen la responsabilidad de la exactitud de la información retenida o destinada a ser tratada.

Artículo 14: Protección de la información personal

23. El Artículo 14 de la Ley modelo prevé el cumplimiento del ***principio de medidas de seguridad de la OCDE*** que establece la existencia de medidas de seguridad razonables contra riesgos tales como:

    a) la pérdida o

    b) el acceso no autorizado,
        i. destrucción,

[19] Componente básico 1.8 para políticas: "La ley o mandato jurídico especifica claramente las circunstancias en que puede recopilarse y tratarse información personal sin recabar el consentimiento del titular de esa información o notificarle esa circunstancia".

ii. uso,
iii. modificación o
iv. divulgación

de los datos. Las medidas de seguridad deben ser apropiadas en función del carácter delicado de la información personal. Por tanto, la disposición no trata de imponer al responsable de los datos un tipo especial de medidas de seguridad. Una supervisión adecuada del seguimiento de las directrices y códigos y, en el caso de las autoridades públicas, de evaluaciones de riesgos aprobadas, facilitarán la flexibilidad que necesita la entidad designada.

Artículo 15: Limitación de uso de la información personal

24. El Artículo 15 prevé el cumplimiento del ***principio de limitación de uso de la OCDE,*** que establece que los datos personales no deben tratarse para fines distintos a los especificados de acuerdo con el ***principio de especificación de la finalidad,*** antes mencionado, ya que en general será necesario el consentimiento del titular para la recopilación, uso y divulgación[20]. Cabe señalar que aunque la redacción prevé que la entidad responsable de los datos obtenga la autorización del titular de la información con posterioridad a su recopilación, no se debe fomentar esta práctica. La entidad responsable está obligada a proporcionar al titular acceso y control sobre sus datos de carácter personal, sin injerencia en el intercambio de información lícito y adecuado que se requiere para facilitar y apoyar el comercio electrónico. A pesar de este principio general, hay casos en que la información recopilada tendrá que ser tratada para fines distintos, o comunicada a otras partes especificadas, en interés público. Para asegurarse de que no se socava sustancialmente la disposición, la Ley define en la **Parte V** las exenciones al ***principio*** general de ***limitación de uso***.

25. Cabe señalar que el párrafo 4 prevé la posibilidad de un trato diferente para la "información personal sensible". Se pueden obtener ejemplos de cómo aplicarlo a partir de las jurisdicciones de la UE, donde las entidades responsables de los datos tienen explícitamente prohibido tratar la información personal sensible, con determinadas excepciones[21], mientras que sí pueden tratar la información personal una vez establecida la finalidad para la que se recopiló originalmente, de acuerdo con lo dispuesto en el Artículo 15. En consecuencia, es lógico concluir, de acuerdo con el ***principio de limitación de la recopilación*** y salvo en los casos identificados como exenciones, que no se debe recopilar información personal sensible. Entre las excepciones notables a esta restricción de tratamiento (y recopilación), aunque más limitadas que las referidas a la información personal, pueden mencionarse:

a) el uso por un profesional de atención de salud, en las circunstancias particulares del desempeño de sus funciones médicas y relacionadas con la salud en una institución de atención de salud;

b) el uso por personal encargado del cumplimiento de la ley y de la seguridad, en el marco de su competencia expresa de prevención, represión y detección de delitos, o de otros asuntos que afecten a la seguridad nacional;

c) el uso para determinar si una persona reúne las condiciones para acceder a un servicio social específico, para lo cual esa información es necesaria.

26. Los Artículos 16, 17 y 18 describen cuándo se puede divulgar información personal sin el consentimiento previo del titular de la misma. Estas situaciones se enumeran a continuación.

---

20 Componente básico 5.1 para políticas: "La ley o mandato jurídico impone a la parte que recopila información un uso o tratamiento de esa información limitado a fines específicos y consentidos por el titular de los datos en el momento y lugar de la recopilación".

21 Componente básico 5.9 para políticas: "La ley o mandato jurídico prohíbe el tratamiento de información personal sensible excepto en ciertos casos y para objetivos determinados".

Artículo 16: Divulgación de información personal de acuerdo con la finalidad de la recopilación

27. El Artículo 16 contempla la divulgación de información personal para fines coherentes a los que el titular dio su consentimiento en el momento de la recopilación de los datos, sin perjuicio de la información recopilada de conformidad con una ley escrita, las medidas adoptadas para el cumplimiento de la ley, los procedimientos jurídicos o el beneficio de la salud pública[22].

Artículo 17: Divulgación de información personal para investigaciones o estadísticas

28. El Artículo 17 contempla la divulgación de información personal con fines de investigaciones y análisis estadísticos, siempre que la entidad responsable de los datos se asegure de que se observan los requisitos de seguridad y que el receptor tiene la intención de cumplir con lo dispuesto en la Ley.

Artículo 18: Divulgación de información personal con fines de archivo

29. El Artículo 18 contempla la divulgación de información personal con fines de archivo cuando la información cumple determinados criterios o cuando ha pasado cierto tiempo del fallecimiento del titular de los datos. Esta cláusula dispensa esencialmente del cumplimiento de las obligaciones de esta Ley modelo a toda la información personal relacionada con una persona fallecida, pero de importancia a nivel nacional o cultural, que se haya entregado a las instituciones y entidades dedicadas al archivo. Sin una cláusula como ésta, la Ley impediría el funcionamiento de entidades como los archivos nacionales, que tienen gran importancia para la preservación de la cultura y la historia nacionales.

Artículo 19: Limitación en la transferencia de información personal entre jurisdicciones

30. En lo que respecta particularmente al almacenamiento de información personal, el Artículo 19 de esta parte limita la actividad de las entidades responsables de los datos a la jurisdicción en que se aplique esta Ley o a una jurisdicción que posea unas leyes de protección de la privacidad equiparables. En el segundo caso, la entidad responsable de los datos está obligada a recabar primero la aprobación del:

    a) Comisionado de datos; y del

    b) titular de los datos

    para efectuar la transferencia. Esa entidad deberá facilitar a las personas interesadas la identidad del administrador de las leyes de protección de la privacidad en la otra jurisdicción[23]. El párrafo 5 incluye una disposición transitoria, en la que reconoce la existencia de empresas transregionales que pueden haber organizado su actividad en torno a centros de datos situados dentro de la región, y reconoce también que no es razonable esperar que una disposición como

---

22 Componente básico 6.2 para políticas: "La ley o mandato jurídico prevé la exención de la obligación de contar con el consentimiento del titular cuando los datos son requeridos por una norma de derecho o están relacionados con los intereses de la seguridad nacional, la administración de justicia y la gestión de la salud pública".

23 Componente básico 6.3 para políticas: "La ley o mandato jurídico prohíbe la transferencia transfronteriza de información personal a las jurisdicciones que carecen de leyes y sistemas de protección personal y de datos semejantes. Para esos casos, la ley contempla solo la transferencia de la información que no ponga en peligro la protección de la información personal del titular de los datos".
Componente básico 6.4 para políticas: "La ley o el mandato jurídico establece, sin perjuicio de cualquier restricción de las normas, que la transferencia de información personal puede hacerse solo con el consentimiento expreso del titular de los datos para transferir información a dicha jurisdicción, tras haber notificado a este de los riesgos asociados".

el Artículo 19 se aplique de forma simultánea en toda la región. De esta manera, antes de que se imponga una sanción, el Comisionado de datos puede prescribir un período razonable para que los centros de datos migren a jurisdicciones que ofrezcan la debida protección.

31. Los Artículos 20 y 21 de la presente parte disponen que el Comisionado de datos podrá aplicar un enfoque de regulación conjunta cuando lo estime conveniente, a fin de equilibrar mejor los imperativos de reglamentación de su función, al mismo tiempo que se reducen al mínimo los efectos y el coste en la industria.

Artículo 20: Establecimiento de los códigos de conducta

32. El Artículo 20 prevé la elaboración de códigos de conducta específicos para diferentes sectores. Estos códigos, ya sean de cumplimiento voluntario u obligatorio, se consideran fundamentales para fomentar la adhesión del sector privado a los principios generales de privacidad descritos en la Parte 1. Además, el párrafo 2 establece que el Comisionado de datos podrá solicitar a los reguladores de los sectores o las industrias, donde éstos se hayan establecido, que desarrollen estos códigos de conducta.

Artículo 21: Códigos de conducta de cumplimiento obligatorio

33. Esta Parte establece que cuando los códigos de conducta se consideren de cumplimiento obligatorio, el Ministro podrá establecer estos códigos como reglamentaciones, sujetas a la resolución afirmativa del Parlamento.

PARTE III – DERECHOS DE LOS TITULARES DE LOS DATOS

34. La **Parte III de la Ley modelo** trata de los derechos del titular de los datos con respecto al acceso a la información personal que está en manos de un responsable de los datos. El ***principio de participación de la persona de la OCDE*** prevé que una persona tendrá derecho a pedir a la entidad responsable de los datos que le confirme si tiene o no datos que le conciernen; a acceder a esa información y a tener la oportunidad de impugnar esos datos; y, si la impugnación prospera, a que se borren, rectifiquen, completen o modifiquen los datos.

Artículo 22: Derecho de acceso a la propia información personal

35. La legislación y la jurisprudencia establecen generalmente que una persona debe tener pleno acceso a sus propios registros personales, con muy limitadas excepciones, y es conveniente que la legislación sobre la privacidad mantenga este derecho, que se contempla de forma general en las disposiciones del Artículo 22[24]. Sin embargo, hay detalles específicos que requieren mayor consideración. El derecho de acceso a los datos personales no es absoluto, ya que puede haber algunas excepciones.

Artículo 23: Facultad de la entidad responsable de los datos de denegar el acceso

36. El Artículo 23 establece el marco en virtud del cual una entidad responsable de datos podrá denegar el acceso a una persona que lo solicite, al tiempo que garantiza que si se deniega el acceso a un documento o a parte del mismo, la entidad responsable de datos deberá justificar esa negativa. Estas excepciones incluyen, por ejemplo, los casos en que se deniega una

[24] Componente básico 6.5 para políticas: "La ley o el mandato jurídico prevé la divulgación de información personal en respuesta a una solicitud del titular de los datos. Cuando dicha divulgación pueda dar lugar a su vez a que se divulgue otra información reservada, la ley o el mandato jurídico determinará las directrices apropiadas que debe seguir el jefe de la parte que trata la información".

solicitud de acceso con el fin de proteger al solicitante o a otra persona[25], o debido a consideraciones de protección de la información ya arraigadas, como el caso de la información sujeta al secreto profesional (por ejemplo, la que se desprende de la relación abogado-cliente), o cuando la información se recopiló en el curso de una investigación o primordialmente para ser utilizada en un procedimiento jurídico.

37. Además, si bien es de esperar que la gran mayoría de personas solicitarán el acceso a su información de manera responsable, también es de prever que alguna lo haga exclusivamente para obstruir el normal funcionamiento de la entidad responsable de los datos. Por ejemplo, un titular de datos podría presentar solicitudes de información semanales, a pesar de que la información ya se le haya suministrado y no haya habido ninguna actualización. En estos casos, puede ser apropiado permitir a la entidad responsable de los datos que deniegue la solicitud. Como sucede en la mayoría de los casos en que se deniega un derecho, la entidad responsable de los datos deberá justificar su negativa. El Artículo 23, párrafo 2, prevé esta posibilidad y proporciona a la entidad responsable de los datos los fundamentos para denegar el acceso.

Artículo 24: Separación de la información exenta

38. El Artículo 24 trata de proporcionar orientación a la entidad responsable de los datos sobre el procedimiento apropiado cuando la respuesta a una solicitud de acceso pueda dar lugar a la divulgación de información personal de otro individuo. Siempre que sea posible, se propone que la información que pueda ser objeto de divulgación no deseada se separe antes de hacer pública la información solicitada.

39. El párrafo 2 aclara que la obligación de la entidad responsable de los datos de proteger la información personal puede abarcar incluso el no reconocimiento de la existencia de determinada información.

Artículo 25: Delegación de los derechos del titular de los datos a un tercero

40. El Artículo 25 prevé la delegación de los derechos particulares de un titular de datos a un tercero. El principal derecho delegado en el contexto de esta Ley sería el de dar su consentimiento para la recopilación, el tratamiento o la divulgación de información personal. En este artículo se establece que puede dar dicho consentimiento tanto el titular de los datos como su sustituto en la toma de decisiones. En los casos en que es necesario que un tercer sustituto actúe en nombre de una persona, por ejemplo, cuando el titular de los datos es menor de edad, o debido a un problema de salud, o cuando el sujeto no puede dar su consentimiento (por ejemplo, cuando está fuera del Estado), o cuando la persona ha fallecido, la legislación establecerá, de conformidad con las leyes relativas a la responsabilidad parental, una jerarquía de las personas a las que se podrá pedir que tomen decisiones con respecto a la información del interesado.

Artículo 26: Plazos para responder a la solicitud

41. El Artículo 26 establece unos objetivos amplios para el desempeño de las funciones de las entidades responsables de los datos en relación a las respuestas a las solicitudes de los titulares de datos. Entre otras cosas, un punto de referencia para este desempeño será alentar a las entidades responsables de los datos a que establezcan y dispongan de un proceso para gestionar la recepción de, y la respuesta a, dichas solicitudes. Este proceso puede prever la definición de procedimientos normalizados que deberán seguir los interesados cuando soliciten una copia de sus datos personales. Esto puede incluir un formulario, un plazo para la presentación de la solicitud y una tasa (si corresponde).

[25] Componente básico 6.5 para políticas, *sic.*

Artículo 27: Corrección de errores en la información personal almacenada

42. De conformidad con el principio de la OCDE, otro derecho que la legislación sobre privacidad debe poner a disposición de los titulares de datos es el de solicitar una corrección de la información. Ello se hace en el Artículo 27. Tales casos pueden darse cuando el interesado desea introducir una corrección relativa a errores materiales (por ejemplo, fecha de nacimiento incorrecta). Si bien en esos casos las normas profesionales o institucionales no siempre permiten cambiar un registro, el marco prevé la posibilidad de que la entidad responsable de los datos realice una anotación en el registro para señalar que se ha verificado la información personal y esbozar la información correcta. La entidad responsable de los datos también puede incluir una declaración en que manifieste que no está de acuerdo con la persona respecto a la discrepancia de la información contenida en el expediente.

PARTE IV – OBLIGACIONES ESPECÍFICAS DE LAS AUTORIDADES PÚBLICAS

43. **La Parte IV de la Ley modelo** describe las reglas particulares a que deben ajustarse los jefes de autoridades públicas para observar los principios de privacidad descritos en la Parte I, en conjunto con las directrices generales descritas en la Parte II. Estas obligaciones particulares están orientadas a asegurar que en la Ley se establezcan sistemas de control adecuados para facilitar el seguimiento de la aplicación de los principios de privacidad.

Artículo 28: Evaluaciones del impacto sobre la privacidad

44. El Artículo 28 de esta parte recoge ejemplos notables de tales sistemas, como la obligación de las autoridades públicas de realizar evaluaciones del impacto sobre la privacidad de las operaciones de tratamiento de datos en curso o previstas, de acuerdo con las directrices del Comisionado de datos. Estas evaluaciones de impacto pueden sentar la base de un enfoque de regulación conjunta entre los poderes públicos y el Comisionado de datos que ponga en práctica un enfoque *ex ante* de la autorización de las funciones de tratamiento de datos. Aunque esto puede causar algunos retrasos administrativos en el establecimiento del nuevo sistema de tratamiento, redundará en un beneficio global para la flexibilidad y capacidad de respuesta de la autoridad pública, en comparación con la aplicación de un enfoque *ex post* o *ad hoc* de esa autorización.

Artículo 29: Sistemas de archivo de información personal

45. El Artículo 29 proporciona un requisito funcional de las autoridades públicas que, de nuevo, está estructurado para ayudar a la labor del Comisionado de datos en la observancia de las obligaciones de la Ley. El requisito legal de establecer sistemas de archivo de la información personal en que primordialmente se almacene y se gestione toda la información individual en poder de la autoridad pública facilita la eficacia de cualquier otro mecanismo que se pueda poner en práctica. A pesar de este requisito general, se debe reconocer que los archivos nacionales pueden gestionar información personal que por su propia índole debe archivarse.

Artículo 30: Exención de los archivos nacionales de las disposiciones del Artículo 29

46. El Artículo 30 prevé que los archivos nacionales están especialmente exentos de las disposiciones del Artículo 29, ya que esta información, autorizada para consulta pública a través de los archivos nacionales, por lo general no entra en el ámbito de cobertura previsto por los sistemas de archivo de información personal.

Artículo 31: Establecimiento de enlaces dentro de la entidad responsable de los datos

47. En consonancia con el enfoque general de establecer requisitos funcionales particulares de las autoridades públicas para supervisar efectivamente la protección de la privacidad, el Artículo 31 establece que las autoridades públicas señalarán funcionarios que actúen como enlace dentro de sus organizaciones para facilitar la evaluación interna de los sistemas y funciones en el cumplimiento de la Ley de protección de datos. De esta manera, es de esperar que mejore considerablemente el funcionamiento de ese sector, en la medida en que las autoridades públicas procederán de forma activa a estructurar sus sistemas y procesos para garantizar el cumplimiento de los principios de privacidad y de las disposiciones de la Ley de protección de la privacidad, así como a mejorar los canales de comunicación con la Oficina del Comisionado de datos. Aunque esta disposición parezca apropiada para las operaciones de una autoridad pública, puede no serlo para algunas empresas privadas, por lo que se considera una obligación específica del sector público.

Artículo 32: Autorización previa para los acuerdos de intercambio de información

48. A continuación, el Artículo 32 contempla el intercambio de información entre los ministerios de acuerdo con las directrices establecidas por el Comisionado de datos, o aprobadas por éste. Este intercambio es fundamental para la prestación de servicios de gobierno electrónico.

Artículo 33: Publicación de un informe del Comisionado de datos sobre los sistemas de archivo de la información

49. El Artículo 33 impone al Comisionado de datos la publicación de informes sobre el estado de los diversos mecanismos e instrumentos establecidos en la presente parte para supervisar la gestión de la información personal recopilada por las autoridades públicas. De esta manera se facilitará la difusión oportuna al público de la información en poder de una autoridad pública determinada, pues permitirá su visibilidad a las personas que utilicen las disposiciones de la Parte III para ejercer sus derechos de acceso a la información sobre ellas.

PARTE V – EXENCIONES ESPECIALES

50. La **Parte V de la Ley modelo** establece las disposiciones generales que permiten al Ministro ordenar por decreto que se introduzcan modificaciones en la aplicabilidad de las disposiciones de la Parte II a grupos identificados de las entidades responsables de los datos para fines y circunstancias específicos. Estas cláusulas se elaboraron en gran medida tomando como modelo las promulgadas en el Reino Unido y Malta, basadas a su vez en las Directivas pertinentes de la Comisión Europea.

Artículo 34: Uso personal o familiar

51. El Artículo 34 deja claro que una persona puede utilizar la información personal cuando lo haga para asuntos personales o familiares.

Artículo 35: Seguridad nacional, delincuencia y tributación

52. El Artículo 35 prevé exenciones específicas de las Partes II, III y IV de la Ley, de conformidad con las mejores prácticas internacionales. Las exenciones están bien articuladas en base a precedentes de tratamiento de datos personales y sobre la libre circulación de estos datos, que se podrá restringir con vistas a salvaguardar:

a) la seguridad nacional, la defensa; la seguridad pública;

d) la prevención, investigación, detección y enjuiciamiento de delitos penales o de infracciones de la deontología para las profesiones reglamentadas;

c) un importante interés económico o financiero de una jurisdicción, incluidos los asuntos monetarios, presupuestarios y tributarios;

Artículo 36: Exención de asuntos regulatorios

53. El Artículo 36 establece exenciones en los casos de las funciones de vigilancia, inspección o regulación relacionadas, incluso ocasionalmente, con el ejercicio de la autoridad pública, la protección del titular de los datos o de los derechos y libertades de otras personas.

Artículo 37: Exenciones relativas al periodismo y las artes

54. El Artículo 37 prevé la exención de la aplicabilidad a las actividades relacionadas con el ejercicio de la libertad de expresión, como la preparación de obras periodísticas, literarias y artísticas. Esta cláusula se basa en otras similares promulgadas en los marcos de protección de datos en Europa. Se han establecido marcos generales que protegen de forma suficiente contra la difamación, con el fin proporcionar algún tipo de protección al titular de los datos, sin restringir indebidamente la actividad. Además, el artículo contempla que el Comisionado de datos podrá establecer códigos sectoriales que faciliten el adecuado equilibrio entre los objetivos de la Ley y el derecho prevalente de la libertad de expresión.

PARTE VI – EXAMEN DE LOS RECURSOS CONTRA LAS DECISIONES DE LAS ENTIDADES RESPONSABLES DEL TRATAMIENTO DE LOS DATOS RELATIVAS AL ACCESO

55. La **Parte VI de la Ley modelo** ofrece al titular de datos la posibilidad de recurrir y/o solicitar la revisión, ante el Comisionado de datos, de una decisión de una entidad responsable de datos[26]. Este artículo es fundamental, ya que, mediante un recurso ante una autoridad independiente, ofrece a la persona los medios para obligar a una entidad responsable de datos a darle un trato equitativo.

Artículo 38: Derecho del titular de los datos a recurrir una decisión

56. El Artículo 38 establece el derecho general de una persona que no está satisfecha con la respuesta dada a una solicitud hecha de conformidad con los Artículos 22 (derecho de acceso a la propia información personal) y 27 (derecho a solicitar una corrección de la información personal) a interponer recurso. Este artículo estipula la interposición del recurso contra la decisión correspondiente ante el Comisionado de datos, que tiene atribuciones para resolver el litigio.

[26] Componente básico 5.8 para políticas: "La ley o mandato jurídico otorga al organismo designado la posibilidad de recurrir la decisión en este sentido del jefe de la parte que trata los datos".

Artículo 39: Plazo para la presentación del recurso del titular de los datos

57. Los Artículos 39 a 41 establecen el proceso genérico por el cual el Comisionado de datos acepta un recurso. El Artículo 39 se refiere al plazo máximo para interponer el recurso a partir del momento de la decisión en cuestión, para garantizar un rápido inicio del proceso.

Artículo 40: Facultad del Comisionado de datos de desestimar un recurso

58. El Artículo 40 establece la facultad del Comisionado de datos de desestimar un recurso antes de notificarlo al jefe de la entidad responsable de los datos si, en su opinión, no hay fundamento sustancial para la presentación del recurso.

Artículo 41: Obligación del Comisionado de datos de informar a la entidad responsable de los datos

59. De acuerdo con el procedimiento habitual, el Artículo 41 encarga al Comisionado de datos que envíe un aviso al jefe de la entidad responsable de los datos sobre un recurso pendiente en relación con una decisión tomada por dicha entidad.

60. Los Artículos 42 a 46 estipulan el mecanismo general a través del cual el Comisionado de datos puede utilizar técnicas alternativas de solución de conflictos para resolver el recurso.

Artículo 42: Facultad del Comisionado de nombrar un mediador o actuar como árbitro

61. En virtud del Artículo 42, el Comisionado podrá nombrar a un mediador para la solución de controversias, y en última instancia, para actuar como árbitro en nombre del propio Comisionado.

Artículo 43: Deber del Comisionado de realizar una investigación

62. En particular, el Artículo 43 establece que el Comisionado de datos lleve a cabo una investigación en respuesta a un recurso, cuando la decisión que pronuncie en virtud de dicha investigación sea vinculante para las partes.

63. Los Artículos 44 a 46 establecen las condiciones operacionales y de procedimiento que se requieren para iniciar dicha investigación.

Artículo 44: Facultad del Comisionado para mantener en secreto las investigaciones

64. El Artículo 44 establece la facultad del Comisionado de datos de mantener en secreto dichas investigaciones.

Artículo 45: Representación de las partes en una investigación

65. El Artículo 45 establece que cualquiera de las partes puede estar representada por un abogado u otro agente que actúe en su nombre en una investigación.

Artículo 46: Carga de la prueba en una investigación

66. El Artículo 46 enuncia las premisas jurídicas para la procedencia de la investigación, y sitúa la carga de la prueba en la entidad responsable de los datos, pues considera que es la parte que dispone de más recursos.

Artículo 47: Recurso de la decisión de una investigación ante los tribunales

67. El Artículo 47 establece que los tribunales serán un foro de apelación para cualquier decisión adoptada en el curso de la investigación.

PARTE VII – ESTABLECIMIENTO, FUNCIONES Y ATRIBUCIONES DEL COMISIONADO DE DATOS, EN CALIDAD DE AUTORIDAD DE SUPERVISIÓN

68. La **Parte VII de la Ley modelo** establece la Oficina del Comisionado de datos. Éste es un elemento fundamental para un marco legislativo eficaz sobre privacidad. La exigencia de un control independiente es indispensable para supervisar el cumplimiento de la Ley por parte de las entidades responsables de los datos, tanto en el sector público como en el privado. Cabe señalar que, si bien esta parte está redactada como si el jefe de este organismo fuera una persona (por lo que se habla de "Comisionado de datos"), es igual de válida si este organismo está dirigido por un grupo de personas (por ejemplo, "Comisión de datos", "Tribunal de datos" o similar). Las jurisdicciones tienen plena libertad para elegir la forma que tomará este órgano de supervisión. Lo importante es que el órgano sea independiente del poder ejecutivo, y tenga suficiente autonomía frente a determinados intereses del sector privado que quedarían abarcados por esta Ley por la índole de la actividad empresarial realizada.

Artículo 48: Creación de la Oficina del Comisionado de datos

69. En vista del alcance de esta función, y para garantizar que la supervisión de la privacidad no esté influida por la percepción parcial de un grupo de entidades responsables de datos, el Artículo 48 contiene disposiciones sobre el nombramiento y cesación de un Comisionado de protección de datos independiente, siguiendo criterios y formas similares a los requisitos exigidos para un miembro de una comisión parlamentaria o un defensor del pueblo[27], y estipulando que el Comisionado sólo podrá ser cesado por causa justificada.

70. En caso de ausencia del Comisionado de datos, el artículo también prevé el nombramiento de un Comisionado provisional hasta que se designe al nuevo titular.

71. Alternativamente, la legislación podrá incluir disposiciones para el nombramiento de un Comisionado de datos adjunto, que actuará en nombre del Comisionado en caso de necesidad. Además, el artículo garantiza que el Comisionado no percibirá ninguna otra remuneración ni asumirá otras obligaciones o modalidades de lealtad expresas que pudieran generar una percepción de parcialidad[28]. Este aspecto de la cláusula podrá ser modificado de acuerdo con el modelo de gobierno propuesto y las circunstancias logísticas de cada jurisdicción. En este modelo de texto se propone que la función tradicional del Ejecutivo, de regulación del mercado, se aplique también, en este caso, al sector público. Sin embargo, puesto que un grupo de entidades responsables de datos puede estar formado por empresas públicas o casi públicas, y el poder ejecutivo conserva cierto grado de supervisión administrativa sobre las mismas, el marco de gobernanza general prevé:

---

27 Componente básico 3.3 para políticas: "El jefe de este organismo será nombrado de manera que se garantice la independencia e imparcialidad de sus funciones".

28 Componente básico 3.4 para políticas: "El jefe de este organismo deberá gozar de unas condiciones de empleo que incluyan disposiciones de estabilidad y condiciones de renovación de contrato, contempladas en la ley o el mandato jurídico, que sean suficientes para limitar las posibilidades de incentivo o coacción".

a) La presentación de informes al Ministro pertinente sobre el estado de protección de la privacidad por parte del sector privado;

b) La presentación de informes al Parlamento sobre el estado de protección de la privacidad por parte de las autoridades públicas.

72. Este artículo también establece, en el párrafo 3, que el Comisionado de datos podrá contratar personal para cumplir con las funciones de la Oficina. Por último, este artículo define un plazo máximo tras la proclamación de la Ley para la designación del Comisionado de datos.[29]

Artículo 49: Personalidad jurídica diferenciada del Comisionado de datos

73. En cualquier caso, el Artículo 49 prevé que se atribuya al Comisionado una personalidad jurídica diferenciada que le permita celebrar contratos; adquirir, mantener y utilizar cualquier tipo de propiedad para los propósitos de sus funciones; demandar y ser demandado; y actuar y participar en todas las operaciones que se deriven del ejercicio o desempeño de sus funciones en virtud de esta Ley, o lo favorezcan[30].

Artículo 50: Definición de la duración del mandato

74. Además, como mecanismo para mantener la integridad e imparcialidad de la oficina, el Artículo 50 establece que el mandato del Comisionado tendrá una duración máxima. Tomando como base las mejores prácticas, este período debe ser superior al ciclo electoral[31].

Artículo 51: Remuneración del Comisionado de datos y del personal

75. Además, con el fin de preservar la independencia e imparcialidad del Comisionado, el Artículo 51 prevé que la remuneración del Comisionado y su personal se determine a través de un medio independiente, para que no se perciba que el titular de la Oficina se debe a alguna administración. El texto utilizado en este artículo apunta en la dirección de dar a cada jurisdicción la flexibilidad necesaria para determinar el mecanismo más adecuado con miras a esta independencia. A modo de ejemplo, algunas jurisdicciones establecerán que los salarios de estos funcionarios sean fijados por una comisión independiente, o si no, mediante una reglamentación. La cláusula propuesta no pretende imponer un mecanismo como el apropiado, pero apunta que, una vez determinado dicho mecanismo, la asignación fiscal se determine de forma transparente dentro del ciclo anual presupuestario del gobierno, en una partida separada del resto.

Artículo 52: Protección del Comisionado de datos

76. Además, con el fin de preservar la independencia y la imparcialidad del Comisionado de datos, el Artículo 52 establece su protección frente a la responsabilidad derivada de un acto cometido u omitido de buena fe, en el ejercicio o supuesto ejercicio de sus funciones. Esta protección no debería ampliarse a los casos de daños personales. Además, en el marco legislativo se prevé una indemnización al Comisionado de datos por las costas en que incurra para su defensa[32].

---

29 Componente básico 3.12 para políticas: "La ley o mandato jurídico especificará un plazo para la entrada en funcionamiento de este organismo tras la aprobación de la ley".

30 Componente básico 3.2 para políticas: "El organismo designado para garantizar el cumplimiento de la ley o mandato jurídico deberá ser una persona jurídica con atribuciones para poseer o disponer de bienes y capacidad de celebrar contratos, y que pueda desempeñar sus funciones con independencia".

31 Componente básico 3.4 para políticas, *sic.*

32 Componente básico 3.10 para políticas: "En la ley o mandato jurídico se podrá contemplar ofrecer protección al organismo designado en lo que respecta a la responsabilidad derivada de los actos realizados de buena fe en el ejercicio de su función".

Artículo 53: Delegación de atribuciones del Comisionado de datos

77. El Artículo 53 faculta al Comisionado, a un nivel práctico operacional e institucional, a delegar algunas de las atribuciones de investigación y ejecución que le confiere esta Ley, a un funcionario autorizado, designado a tal efecto por el propio Comisionado[33].

Artículo 54: Independencia del Comisionado de datos

78. El Artículo 54 insiste en que el Comisionado debe actuar con independencia en el ejercicio de sus funciones conforme a la Ley, y no estar sujeto a la dirección o control de otra persona o autoridad[34].

Artículo 55: Funciones del Comisionado de datos

79. Como se indica en el Artículo 55, las principales funciones de este organismo de supervisión, que es una oficina administrativa dirigida por el Comisionado de datos, consistirán en garantizar el cumplimiento de la legislación sobre privacidad, a través de las siguientes actividades:

- seguimiento de la aplicación de la legislación y realización de evaluaciones;
- iniciación de investigaciones sobre el respeto a la privacidad;
- solución de las quejas relativas a la privacidad, y mediación en esos procesos;
- organización de exámenes y supervisión de las evaluaciones de impacto relativas a la privacidad;
- realización de investigaciones sobre asuntos relacionados con la legislación relativa a la privacidad;
- creación de programas de educación pública;
- promoción de las mejores prácticas en materia de privacidad; y
- prestación de asesoramiento y formulación de comentarios a las entidades responsables de los datos.

Artículo 56: Juramento de respeto de la confidencialidad

80. El Artículo 56 exige que las personas que, en el ejercicio de sus funciones en virtud de la presente Ley, tengan acceso a información que se pueda considerar privada o personal, presten juramento de no divulgar los datos obtenidos como resultado del ejercicio de una atribución o en el cumplimiento de una función prevista por la ley, salvo que la Ley de privacidad, otro acto legislativo o una autoridad judicial dispongan otra cosa.

Artículo 57: Atribuciones generales del Comisionado de datos

81. El Artículo 57 presenta al Comisionado como una entidad semejante a un regulador a los efectos de sus funciones; esto le supone las facultades necesarias para realizar todos los actos que considere indispensables, ventajosos o convenientes para la ejecución de esas funciones, o en conexión con ellas, incluida la facultad para investigar las operaciones de una entidad

[33] Componente básico 3.6 para políticas: "La ley o el mandato jurídico concederá al jefe de este organismo la facultad de delegar cierta autoridad en entidades reconocidas para facilitar la ejecución de sus funciones".

[34] Componente básico 1.6 para políticas: "La ley o mandato jurídico establece claramente la independencia del organismo designado".

responsable de datos[35], en respuesta a una queja o de oficio; para obtener información sobre documentación, tratamiento y seguridad de los datos; y, entre otras cosas, para solicitar que una persona le proporcione, por escrito y en el plazo especificado, acceso a datos personales, o cualquier otra información concreta en relación con las prácticas del responsable de los datos en materia de gestión de la información[36].

82. Los Artículos 58 a 61 establecen un mecanismo mediante el cual el Comisionado de datos puede pedir información en cumplimiento de una investigación o el aviso de solicitud de información, y refuerzan la obligación de responder a esa solicitud, al tipificar como delito la ausencia de respuesta o el incumplimiento del aviso del Comisionado[37].

Artículo 58: Facultad del Comisionado de datos para obtener información de una entidad responsable de datos

83. El Artículo 58 introduce el mecanismo del interrogatorio o recopilación de datos preliminares, a saber, el aviso de solicitud de información. El artículo también indica cuándo se debe utilizar como recurso ese aviso y la forma en que se puede entregar a la parte pertinente. En línea con la consideración general de usar las tecnologías para facilitar la transmisión rápida, el párrafo 2 prevé la posibilidad de la creación de un formulario para facilitar la presentación de la información.

84. Los párrafos 3 y 4 insisten en las cuestiones relativas a la exención abordadas en puntos anteriores del modelo de texto. Estas se incluyen para evitar posibles dudas sobre el tratamiento de esos temas.

Artículo 59: Contenido y forma del aviso de solicitud de información

85. El Artículo 59 describe el contenido que debe tener un aviso de solicitud de información, que en esencia comunica a la parte que lo recibe sus derechos para iniciar un proceso para protegerse con arreglo al marco del modelo de texto.

Artículo 60: Tipificación del incumplimiento de un aviso de solicitud de información como infracción

86. El Artículo 60 plantea que la falta de respuesta a un aviso de solicitud de información se considerará una violación material de la Ley, y el infractor podrá quedar sujeto a sanciones y penas de conformidad con las disposiciones de la Ley. Además, el párrafo 3 estipula una defensa razonable en ese juicio sumario.

Artículo 61: Recurso del Comisionado de datos ante una respuesta insuficiente a un aviso

87. El Artículo 61 estipula cómo debe actuar el Comisionado de datos en caso de que considere que la respuesta a una solicitud de información es insuficiente, por ejemplo, ordenando el cese de las operaciones relacionadas con la recopilación, tratamiento y divulgación de información personal.

---

35 Componente básico 3.5 para políticas: "La ley o mandato jurídico concederá al jefe de este organismo las atribuciones de investigación necesarias para facilitar la ejecución de las funciones contempladas en el marco de la protección de datos".

36 Componente básico 3.7 para políticas: "El organismo designado podrá llevar a cabo auditorías o investigaciones sobre las operaciones realizadas por personas a las que sea aplicable el marco, ya sea por propia iniciativa o en respuesta a reclamaciones de los ciudadanos. El reglamento determinará quién debe asumir los costes derivados de esas auditorías o investigaciones".

37 Componente básico 3.8 para políticas: "Las personas a quienes se aplica la ley deberán cooperar con el mencionado organismo en el ejercicio de sus funciones, bajo pena de sanciones civiles y/o penales".

88. Los Artículos 62 a 66 establecen el procedimiento adecuado por el cual el Comisionado de datos puede emprender una auditoría o investigación, lo que incluye la recepción de una denuncia hecha por una persona, la notificación subsiguiente a la entidad responsable de los datos de la existencia de una investigación en curso, y la concesión de facultades de entrada, allanamiento e incautación (sujetas a la emisión de una orden y la presencia de un agente de policía)[38] .

Artículo 62: Respuesta del Comisionado de datos sobre la recepción de una queja

89. El Artículo 62 aborda la obligación del Comisionado de datos de actuar de diferentes maneras tras la recepción de una queja. Entre estos actos obligatorios pueden mencionarse la iniciación de una investigación y la notificación al demandante de los resultados de la investigación en un plazo razonable. El párrafo 3 refuerza las disposiciones anteriores relativas al papel de los agentes que actúan en nombre de una persona que inicia este proceso.

Artículo 63: Forma y contenido de una queja

90. El Artículo 63 describe la forma general a que debe ajustarse la queja presentada por un demandante, y obliga al Comisionado a prestar la asistencia que razonablemente considere necesaria para garantizar que la queja se presenta de la forma adecuada. El Comisionado de datos no debe ayudar en cuanto al contenido de la queja.

Artículo 64: Inicio de una investigación por el Comisionado de datos a raíz de una queja

91. El Artículo 64 describe el proceso que el Comisionado de datos debe seguir para la intervención de la entidad responsable de los datos en la resolución de una queja. El mecanismo propuesto (el aviso de investigación) se debe notificar al jefe de la entidad responsable de los datos, antes del inicio de una investigación.

Artículo 65: Atribuciones generales de allanamiento e incautación de bienes en el curso de una investigación

92. El Artículo 65 otorga al Comisionado de datos atribuciones generales para entrar en los locales de una entidad responsable de datos, emprender un allanamiento y, en caso necesario, incautarse de la documentación pertinente en el curso de una investigación. El párrafo 2 de este artículo limita la aplicación de esta atribución general, en el sentido de que primero será preciso obtener una orden judicial, y que durante los actos mencionados los funcionarios de la Oficina del Comisionado de datos deberán estar acompañados por un agente de policía.

Artículo 66: Exenciones de la incautación

93. El Artículo 66 insiste en que las disposiciones anteriores que establecen que los documentos de particulares están exentos del tratamiento en virtud de esta Ley son igualmente aplicables en el caso de la inspección e incautación.

94. Una vez completada la investigación, puede suceder que el Comisario de datos estime que la entidad responsable de los datos no actúa de acuerdo con sus obligaciones en materia de protección de la privacidad. En este caso, los Artículos 67 a 69 establecen el mecanismo y el proceso en virtud de los cuales el Comisionado de datos podrá emitir instrucciones a las entidades que, a su juicio, están operando de una manera incompatible con la Ley.

[38] Componente básico 3.9 para políticas: "Este organismo podrá solicitar la presentación de ciertos documentos para facilitar sus investigaciones, y las personas pertinentes tendrán la obligación de presentarlos. Si se justifica, el organismo podrá obtener una orden judicial para lograrlo".

Artículo 67: Aviso de ejecución

95. El Artículo 67 faculta al Comisionado de datos a utilizar el mecanismo propuesto (el envío de un aviso de ejecución), delimita la aplicación adecuada de este mecanismo y, para evitar cualquier duda, establece el destinatario del mismo, a saber, la entidad responsable de los datos.

Artículo 68: Forma y contenido del aviso de ejecución

96. El Artículo 68 describe la forma específica del aviso de ejecución, y atribuye a este mecanismo la necesaria autoridad vinculante para ordenar a las entidades responsables de datos infractoras que actúen para rectificar dicho incumplimiento. Este artículo también establece el mecanismo, y la forma que debe tener ese mecanismo, para que la entidad responsable de datos responda al aviso de ejecución, y prevé un plazo máximo para esa respuesta. De esta manera, las entidades responsables de los datos quedan obligadas a responder o cumplir con las instrucciones incluidas en el aviso de ejecución.

Artículo 69: Tipificación del incumplimiento del aviso de ejecución como infracción

97. El Artículo 69 establece que el incumplimiento de un aviso de ejecución como se indica en el Artículo 68 se considerará una infracción grave de la Ley y expondrá a la entidad responsable de los datos a sanciones penales[39].

Artículo 70: Condiciones de la investigación

98. El Artículo 70 establece además las condiciones logísticas en que deberían realizarse las investigaciones. El párrafo 1 exige que todas las investigaciones se lleven a cabo haciendo hincapié en su carácter confidencial.

99. El párrafo 2 dispone que cada parte podrá presentar sus argumentos al Comisionado de datos durante el curso de las investigaciones. Sin embargo, señala que en esta etapa de la investigación se prohíbe la presencia de cualquiera de las partes durante las argumentaciones de la otra.

Artículo 71: Remisión de asuntos al Comisario de policía

100. El Artículo 71 establece la forma adecuada de actuar del Comisionado de datos para remitir un expediente a la persona adecuada cuando considere que se ha producido una violación de la Ley.

Artículo 72: Informe anual del Comisionado de datos al Parlamento

101. El Artículo 72 obliga al Comisionado de datos a presentar un informe sobre sus actividades al Parlamento, en línea con las mejores prácticas parlamentarias[40].

[39] Componente básico 3.8 para políticas, *sic.*

[40] Componente básico 3.11 para políticas: "Este organismo presentará anualmente un informe al Parlamento/Consejo Legislativo sobre las actividades realizadas durante el año anterior".

PARTE VIII – ESTABLECIMIENTO DE DELITOS Y SANCIONES POR INCUMPLIMIENTO DE LAS DISPOSICIONES

102. La **Parte VIII de la Ley modelo** describe los delitos asociados al incumplimiento de ciertas disposiciones de la Ley.

Artículo 73: Infracción por recopilación de información personal sin el debido aviso al titular de los datos

103. El Artículo 73 considera que la violación del Artículo 8 es un delito. Cuando las jurisdicciones decidan hacer una distinción entre información personal sensible y no sensible, existirá la posibilidad de establecer sanciones diferentes según se considere que la violación se ha perpetrado con información personal o con información personal sensible. Cuando se aplique este enfoque, se aconsejan sanciones más severas si el incumplimiento se relaciona con este último tipo de información.

104. Aunque las obligaciones consagradas en las disposiciones 8 a 15 y 20 son fundamentales para la aplicación efectiva de la protección de datos, las violaciones de las mismas se pueden resolver sin la imposición de sanciones penales. Sin embargo, se sugiere que, debido a sus consecuencias en los acuerdos comerciales internacionales, las infracciones del Artículo 19 se consideren de mayor gravedad que las demás.

Artículo 74: Infracción por transferencia de datos personales a otras jurisdicciones sin la autorización pertinente

105. En consecuencia, el Artículo 74 define como delito penal la violación de la disposición del Artículo 19 en particular, y proporciona la definición de la sanción típica asociada a ese delito[41].

Artículo 75: Infracción por obstrucción de la labor de un agente del Comisionado de datos

106. El Artículo 75 trata de la obstrucción, directa o indirecta, de la labor de agentes autorizados del Comisionado de datos en el ejercicio de sus funciones durante una investigación y describe la sanción típica asociada a este delito.

Artículo 76: Infracción por presentación de declaraciones falsas al Comisionado de datos o sus agentes

107. El Artículo 76 trata de las personas que se considera que han abusado de los derechos conferidos por la Parte III de la Ley. Los delitos tipificados y las sanciones descritas deben ser disuasorios para evitar el abuso irritante de estas disposiciones facultativas, pues de otro modo se socavaría la viabilidad operativa de la entidad responsable de los datos, de la Oficina del Comisionado de datos o de ambas.

[41] Componente básico 5.10 [6.6] para políticas: "La ley o mandato jurídico establece sanciones civiles y penales por el incumplimiento de las disposiciones referidas al uso o tratamiento [divulgación] de la información personal. Dichas sanciones podrán imponerse a la parte que trata los datos, o a cualquier funcionario o director que según se demuestre haya incumplido intencionalmente la ley o mandato jurídico".

Artículo 77: Infracción por violación del juramento de confidencialidad

108. El Artículo 77 tiene por objeto ocuparse de las personas que violan el juramento de respeto de la confidencialidad prestado en el momento de asumir funciones en la Oficina del Comisionado de datos. El objetivo de esta disposición es limitar la frecuencia de estos hechos y asegurar el mantenimiento de la confianza del público en la Oficina.

109. Las infracciones a las disposiciones de la Ley que no están explícitamente descritas en esta parte o en otros artículos generales serán abordadas por los tribunales en virtud del derecho civil.

PARTE IX – DISPOSICIONES GENERALES PARA FACILITAR LA APLICACIÓN DEL MARCO

110. La **Parte IX de la Ley modelo** prevé diversas consideraciones que resultarán provechosas para la vigencia efectiva de los principales aspectos de la Ley descritos en los artículos anteriores.

Artículo 78: Protección de los denunciantes

111. El Artículo 78 prevé la protección de aquellas personas que mientras trabajan para una entidad responsable de datos toman conocimiento de actos de dicha entidad que se oponen a los objetivos de esta Ley o a las disposiciones de la misma y voluntariamente informan a la autoridad competente sobre tales actos. Esta disposición de "protección de los denunciantes" está orientada a brindar tranquilidad a los empleados que actúan en favor del interés público, limitando toda reacción punitiva por parte del jefe de la entidad responsable de los datos. El objetivo de la disposición es crear un mayor número de vías para informar a las autoridades sobre hechos delictivos contra la privacidad, a fin de lograr una rápida rectificación de la situación y/o cumplimiento de la Ley.

Artículo 79: Tasas aplicables por los servicios del Comisionado de datos

112. El Artículo 79 dispone que el Ministro, con el asesoramiento del Comisionado de datos, establecerá una tabla de tasas aplicables por los servicios prestados por esa Oficina. De esta forma se trata de facilitar la recuperación de una parte de los costes asociados con el funcionamiento de la Oficina.

Artículo 80: Establecimiento por el Ministerio de las reglamentaciones necesarias

113. El Artículo 80 prevé una disposición general que habilita al Ministro correspondiente a dictar las reglamentaciones necesarias para dar efecto a disposiciones particulares de la Ley, o proporcionar explicaciones al respecto.

Artículo 81: Función de los tribunales

114. El Artículo 81 aclara el papel de los tribunales como foro de apelación de última instancia al que podrá recurrir cualquiera de las partes que no quede satisfecha con el resultado de un proceso de resolución de controversias llevado a cabo por el Comisionado de datos. Este artículo también refuerza el poder de los tribunales para imponer sanciones civiles por infracciones de la Ley que no se consideren delito en virtud de la Parte VIII de la Ley[42] [43] [44].

[42] Componente básico 4.8 para políticas, *sic.*
[43] Componente básico 5.10 para políticas, *sic.*
[44] Componente básico 6.6 para políticas, *sic.*

ANEXOS

Anexo 1

Participantes en el primer taller de consulta para el Grupo de trabajo del proyecto HIPCAR, sobre el marco legislativo de las TIC – Temas sobre la sociedad de la información Gros Islet, Santa Lucía, 8 a 12 de marzo de 2010

Participantes designados oficialmente y observadores

País	Organización	Apellido	Nombre
Antigua y Barbuda	Ministerio de Información, Radiodifusión, Telecomunicaciones, Ciencia y Tecnología	SAMUEL	Clement
Bahamas	Autoridad Reguladora de los Servicios Públicos y la Competencia	DORSETT	Donavon
Barbados	Ministerio de Finanzas, Inversiones, Telecomunicaciones y Energía	BOURNE	Reginald
Barbados	Ministerio de Industria y Comercio	COPPIN	Chesterfield
Barbados	Cable & Wireless (Barbados) Ltd.	MEDFORD	Glenda E.
Barbados	Ministerio de Industria y Comercio	NICHOLLS	Anthony
Belice	Comisión de Servicios Públicos	SMITH	Kingsley
Granada	Comisión Reguladora Nacional de las Telecomunicaciones	FERGUSON	Ruggles
Granada	Comisión Reguladora Nacional de las Telecomunicaciones	ROBERTS	Vincent
Guyana	Comisión de Servicios Públicos	PERSAUD	Vidiahar
Guyana	Oficina del Primer Ministro	RAMOTAR	Alexei
Guyana	Dependencia Nacional de Gestión de Frecuencias	SINGH	Valmikki
Jamaica	University of the West Indies	DUNN	Hopeton S.
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Saint Kitts y Nevis	Ministerio de Información y Tecnología	BOWRIN	Pierre G.
Saint Kitts y Nevis	Ministerio de la Fiscalía General, Justicia y Asuntos Jurídicos	POWELL WILLIAMS	Tashna
Saint Kitts y Nevis	Ministerio de Promoción de la Juventud, Deportes, Tecnología de la Información, Telecomunicaciones y Correos	WHARTON	Wesley
Santa Lucía	Ministerio de Comunicaciones, Obras Públicas, Transporte y Servicios Públicos	FELICIEN	Barrymore
Santa Lucía	Ministerio de Comunicaciones, Obras Públicas, Transporte y Servicios Públicos	FLOOD	Michael R.
Santa Lucía	Ministerio de Comunicaciones, Obras Públicas, Transporte y Servicios Públicos	JEAN	Allison A.
San Vicente y las Granadinas	Ministerio de Telecomunicaciones, Ciencia, Tecnología e Industria	ALEXANDER	K. Andre
San Vicente y las Granadinas	Ministerio de Telecomunicaciones, Ciencia, Tecnología e Industria	FRASER	Suenel

Anexo 1

País	Organización	Apellido	Nombre
Suriname	Telecommunicatie Autoriteit Suriname / Autoridad de Telecomunicaciones de Surinam	LETER	Meredith
Suriname	Ministerio de Justicia y Policía, Departamento de Legislación	SITALDIN	Randhir
Trinidad y Tobago	Ministerio de la Administración Pública, División de Servicios Jurídicos	MAHARAJ	Vashti
Trinidad y Tobago	Autoridad de Telecomunicaciones de Trinidad y Tobago	PHILIP	Corinne
Trinidad y Tobago	Ministerio de la Administración Pública, Secretaría de las TIC	SWIFT	Kevon

Participantes de organizaciones regionales/internacionales

Organización	Apellido	Nombre
Secretaría de la Comunidad del Caribe (CARICOM)	JOSEPH	Simone
Comunidad Virtual de las TIC del Caribe (CIVIC)	GEORGE	Gerry
Comunidad Virtual de las TIC del Caribe (CIVIC)	WILLIAMS	Deirdre
Unión de Telecomunicaciones del Caribe (CTU)	WILSON	Selby
Delegación de la Comisión Europea en Barbados y el Caribe Oriental (EC)	HJALMEFJORD	Bo
Autoridad de Telecomunicaciones del Caribe Oriental (ECTEL)	CHARLES	Embert
Autoridad de Telecomunicaciones del Caribe Oriental (ECTEL)	GILCHRIST	John
Autoridad de Telecomunicaciones del Caribe Oriental (ECTEL)	HÉCTOR	Cheryl
Unión Internacional de Telecomunicaciones (UIT)	CROSS	Philip
Unión Internacional de Telecomunicaciones (UIT)	LUDWIG	Kerstin
Oficina de Negociaciones Comerciales (antes CRNM), Secretaría de la Comunidad del Caribe (CARICOM)	BROWNE	Derek E.
Secretaría de la Organización de Estados del Caribe Oriental (OECS)	FRANCIS	Karlene

Consultores del HIPCAR participantes en el taller

Apellido	Nombre
MARTINS DE ALMEIDA	Gilberto
GERCKE	Marco
MORGAN[45]	J Paul
PRESCOD	Kwesi

[45] Presidente del taller.

Anexo 2

Participantes en el segundo taller de consulta (Fase B) del Grupo de trabajo del proyecto HIPCAR, sobre el marco legislativo de las TIC – Temas sobre la sociedad de la información

Frigate Bay, Saint Kitts y Nevis, 19 a 22 de julio de 2010

Participantes designados oficialmente y observadores

País	Organización	Apellido	Nombre
Antigua y Barbuda	Ministerio de Información, Radiodifusión, Telecomunicaciones, Ciencia y Tecnología	SAMUEL	Clement
Bahamas	Autoridad Reguladora de los Servicios Públicos y la Competencia	DORSETT	Donavon
Barbados	Ministerio de Finanzas, Inversiones, Telecomunicaciones y Energía	BOURNE	Reginald
Barbados	Oficina de Negociaciones Comerciales	BROWNE	Derek
Barbados	Ministerio de Asuntos Económicos, Empoderamiento, Innovación y Comercio	NICHOLLS	Anthony
Belice	Ministerio de Finanzas	LONGWORTH	Michelle
Belice	Comisión de Servicios Públicos	PEYREFITTE	Michael
Dominica	Ministerio de la Información, Telecomunicaciones y Fomento de la Ciudadanía	CADETTE	Sylvester
Dominica	Ministerio de Asuntos Jurídicos	RICHARDS-XAVIER	Pearl
Granada	Comisión Nacional Reguladora de las Telecomunicaciones	FERGUSON	Ruggles
Granada	Comisión Nacional Reguladora de las Telecomunicaciones	ROBERTS	Vincent
Guyana	Comisión de Servicios Públicos	PERSAUD	Vidiahar
Guyana	Oficina del Presidente	RAMOTAR	Alexei
Guyana	Unidad Nacional de Gestión de Frecuencias	SINGH	Valmikki
Jamaica	Oficina del Primer Ministro	MURRAY	Wahkeen
Jamaica	Fiscalía General del Estado	SOLTAU-ROBINSON	Stacey-Ann
Jamaica	Grupo Digicel	GORTON	Andrew
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Saint Kitts y Nevis	Ministerio de Seguridad Nacional	ARCHIBALD	Keisha
Saint Kitts y Nevis	Departamento de Tecnología	BOWRIN	Pierre
Saint Kitts y Nevis	Proyecto ICT4EDC	BROWNE	Nima
Saint Kitts y Nevis	Gobierno de Saint Kitts y Nevis	CHIVERTON	Eurta
Saint Kitts y Nevis	Departamento de Tecnología	HERBERT	Christopher
Saint Kitts y Nevis	Ministerio de Promoción de la Juventud, Deportes, Tecnología de la Información, Telecomunicaciones y Correos	LAZAAR	Lloyd
Saint Kitts y Nevis	Ministerio de Finanzas, Unidad de Información Financiera	MASON	Tracey
Saint Kitts y Nevis	Ministerio de Desarrollo Sostenible	MUSSENDEN	Amicia

Anexo 2

País	Organización	Apellido	Nombre
Saint Kitts y Nevis	Ministerio de Promoción de la Juventud, Deportes, Tecnología de la Información, Telecomunicaciones y Correos	PHILLIP	Glen
Saint Kitts y Nevis	Fiscalía General del Estado	POWELL WILLIAMS	Tashna
Saint Kitts y Nevis	Ministerio de Hacienda, Unidad de Información Financiera	SOMERSALL-BERRY	Jacqueline
Saint Kitts y Nevis	Ministerio de Promoción de la Juventud, Deportes, Tecnología de la Información, Telecomunicaciones y Correos	WHARTON	Wesley
Santa Lucía	Ministerio de Comunicaciones, Obras Públicas, Transporte y Servicios Públicos	DANIEL	Ivor
Santa Lucía	Ministerio de Comunicaciones, Obras Públicas, Transporte y Servicios Públicos	FELICIEN	Barrymore
Santa Lucía	Cable & Wireless (Santa Lucía) Ltd.	LEEVY	Tara
Santa Lucía	Fiscalía General del Estado	VIDAL-JULES	Gillian
San Vicente y las Granadinas	Ministerio de Telecomunicaciones, Ciencia, Tecnología e Industria	ALEXANDER	K. Andre
San Vicente y las Granadinas	Ministerio de Telecomunicaciones, Ciencia, Tecnología e Industria	FRASER	Suenel
Suriname	Telecommunicatiebedrijf Suriname (TELESUR)	JEFFREY	Joan
Suriname	Telecommunicatie Autoriteit Suriname / Autoridad de Telecomunicaciones de Suriname	LETER	Meredith
Suriname	Ministerio de Justicia y Policía	SITLADIN	Vyaiendra
Suriname	Ministerio de Transportes, Comunicaciones y Turismo	SMITH	Lygia
Trinidad y Tobago	Oficina del Primer Ministro, División de Información	MAHARAJ	Rishi
Trinidad y Tobago	Ministerio de Administración Pública, División de Servicios Jurídicos	MAHARAJ	Vashti
Trinidad y Tobago	Autoridad de Telecomunicaciones de Trinidad y Tobago	PHILIP	Corinne
Trinidad y Tobago	Ministerio de Administración Pública, Secretaría de las TIC	SWIFT	Kevon

Anexo 2

Participantes de organizaciones regionales/internacionales

Organización	Apellido	Nombre
Secretaría de la Comunidad del Caribe (CARICOM)	JOSEPH	Simone
Comunidad Virtual de las TIC del Caribe (CIVIC)	HOPE	Hallam
Comunidad Virtual de las TIC del Caribe (CIVIC)	ONU	Telojo
Telecomunicaciones del Caribe Oriental (ECTEL)	WRIGHT	Ro Ann
Unión Internacional de Telecomunicaciones (UIT)	CROSS	Philip
Unión Internacional de Telecomunicaciones (UIT)	LUDWIG	Kerstin
Secretaría de la Organización de Estados del Caribe Oriental (OECS)	FRANCIS	Karlene

Consultores del HIPCAR participantes en el taller

Apellido	Nombre
GERCKE	Marco
MORGAN[46]	J Paul
PRESCOD	Kwesi

[46] Taller de Presidente.

Unión Internacional de Telecomunicaciones
Oficina de Desarrollo de las Telecomunicaciones (BDT)
Place des Nations
CH-1211 Ginebra

E-mail: bdtmail@itu.int
www.itu.int/ITU-D/projects/ITU_EC_ACP/

Ginebra, 2013