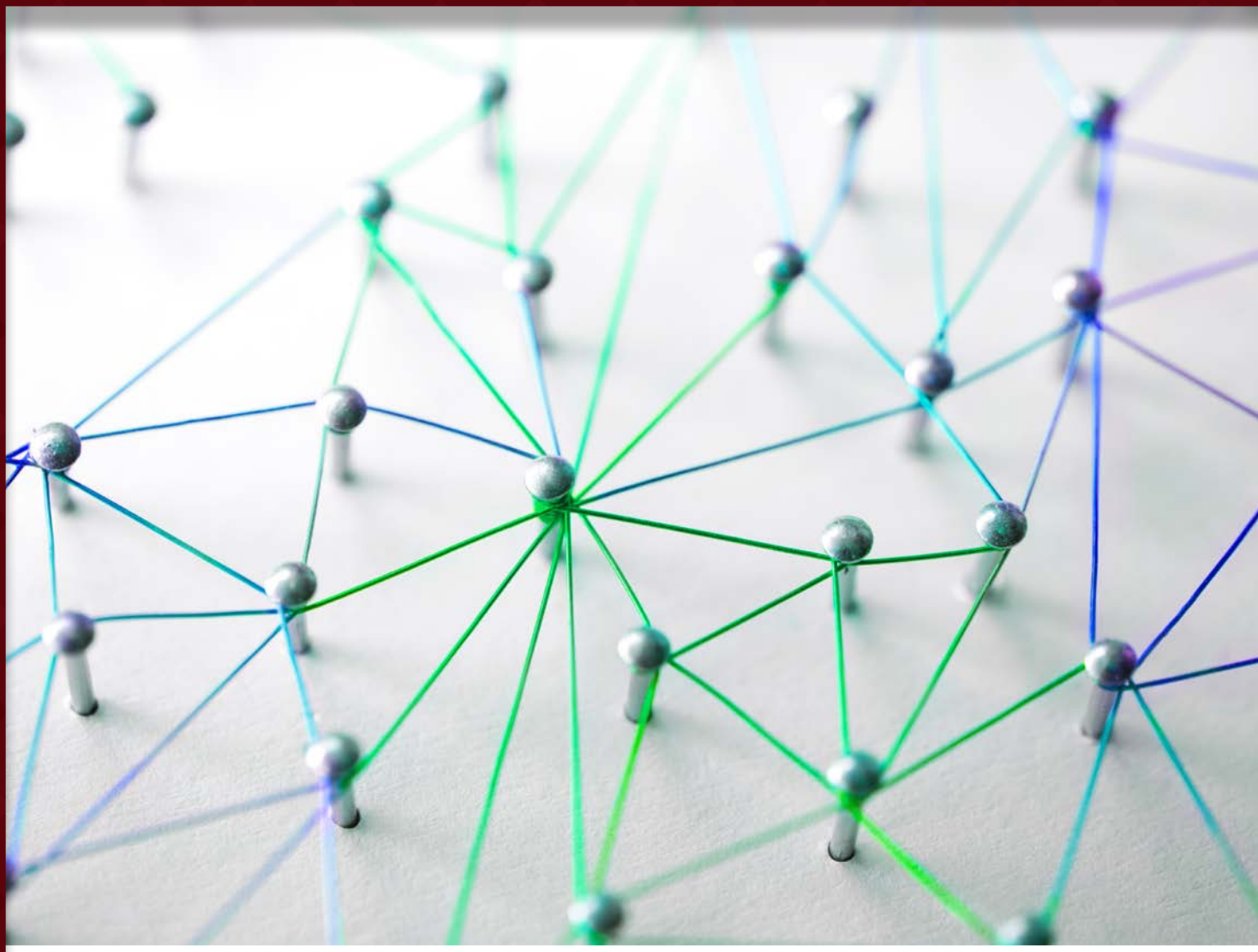
# REVISTA PDP

## Revista Uruguaya de Protección de Datos Personales

NÚMERO 4 - agosto, 2019

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES




**DOCTRINA**

- *CARLA BARBOZA*
- *EDUARDO BERTONI / SOFÍA DOMÍNGUEZ BARANDICA*
- *GRAHAM GREENLEAF*
- *DARA HALLINAN*
- *JUAN ANTONIO TRAVIESO*
- *FERNANDO VARGAS*

**CONVENIO 108 Y TEXTO EXPLICATIVO**

**DICTÁMENES**

**NOTA DE INTERÉS**

*ACTUALIZACIÓN DE LA NORMATIVA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES*

**ENTREVISTA**

*CONSEJO EJECUTIVO URCDP*

# ÍNDICE


Pág. 3
## DOCTRINA

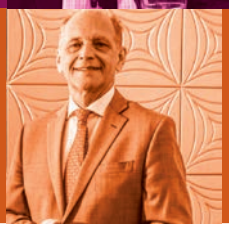
Pág. 4
CARLA **BARBOZA**
**LA PROTECCIÓN DE DATOS PERSONALES EN EL MARCO DE LA ACTIVIDAD EMPRESARIAL; UNA VISIÓN PRÁCTICA**

Pág. 11
EDUARDO **BERTONI**
SOFÍA **DOMÍNGUEZ BARANDICA**
**HACIA UNA NUEVA LEY DE PROTECCIÓN DE LOS DATOS PERSONALES EN ARGENTINA**

Pág. 17
GRAHAM **GREENLEAF**
**ASIA'S DATA PRIVACY DILEMMAS, 2014-19: NATIONAL DIVERGENCES, CROSS-BORDER GRIDLOCK**

Pág. 42
DARA **HALLINAN**
**RIGHTS AND FREEDOMS IN THE GDPR: AN OVERLOOKED SUBSTANTIVE NOVELTY**

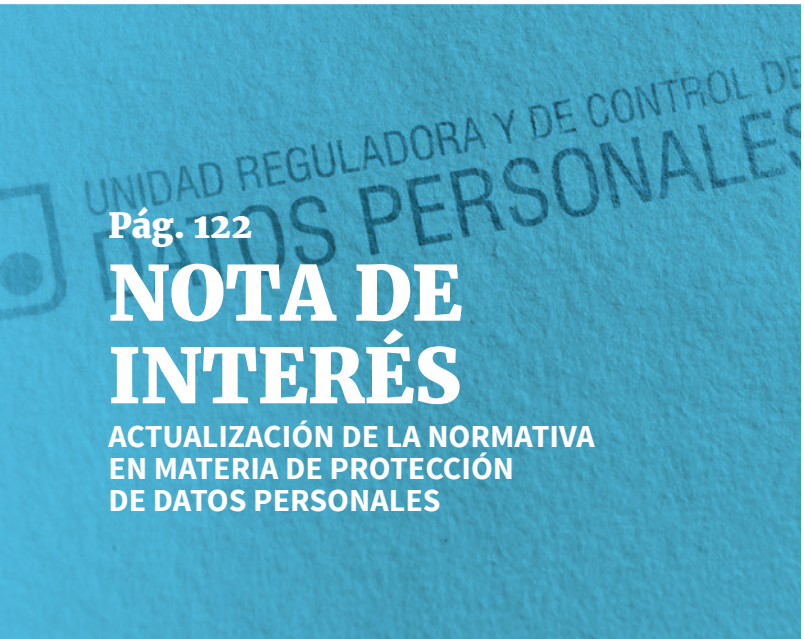
Pág. 52
JUAN ANTONIO **TRAVIESO**
**DESPROTECCIÓN DE DATOS PERSONALES. LA SALIDA DEL PRECIPICIO POR UN CAMINO VIRTUOSO**



Pág. 60
FERNANDO **VARGAS**
**EL ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES EN EL DERECHO URUGUAYO**

Pág. 68
## CONVENIO 108

Pág. 106
## DICTÁMENES




Pág. 122
## NOTA DE INTERÉS
**ACTUALIZACIÓN DE LA NORMATIVA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES**

Pág. 130
## ENTREVISTA
Consejo Ejecutivo
**URCDP**

# PRÓLOGO

Con gran satisfacción tengo el honor de presentar la cuarta edición de la *Revista Uruguaya de Protección de Datos Personales* que publica anualmente la Unidad Reguladora y de Control de Datos Personales.

El propósito de la Revista es hacer llegar a nuestros lectores el estado de situación de la protección de datos personales en Uruguay y en el resto del mundo. Por ello se congregan especialistas locales e internacionales, que aportan conocimientos, experiencias y miradas complementarias que tienen su punto de encuentro en estas páginas.

Los tiempos cambian y la realidad con ellos. Cuando hace diez años se constituía la Unidad Reguladora y de Control de Datos Personales, el ranking de las diez mayores compañías globales estaba dominado por empresas dedicadas al rubro "petróleo y gas" y en la actualidad lo está por empresas de tecnología que tienen como principal foco de su negocio el tratamiento de datos personales. Esto ratifica que la frase "los datos son el petróleo del siglo XXI" no es una ingeniosa metáfora, sino una realidad constatable.

Si hace una década el legislador entendió conveniente regular los datos personales, cuánto más urgente se vuelve hoy con una situación global de semejante escala. Ante ella surgen algunas preguntas inevitables. ¿Cuál es la realidad a la que nos enfrentamos hoy? ¿Son apropiadas las mismas herramientas jurídicas e institucionales para la realidad actual? ¿Qué acciones ha tomado nuestra república para adecuarse a los cambios experimentados? ¿Cuáles son los modelos seguidos en las distintas regiones del mundo? ¿Cuáles son los principales paradigmas actuales?

Estas y otras preguntas encuentran respuesta o abren nuevos caminos para reflexionar sobre estos temas en las páginas que siguen. Invito al lector a entrar en ellas con inquietud y sentido crítico, ya que si logramos despertar la curiosidad y el involucramiento en este tema habremos logrado nuestro propósito.

La dignidad humana está en juego y la defensa del derecho a la protección de datos personales no admite el camino de la autocomplacencia sino el de cuestionarse cada paso con la mayor amplitud de pensamiento.

MAG. FEDERICO MONTEVERDE

# DOCTRINA

CARLA
**BARBOZA**

EDUARDO
**BERTONI**

SOFÍA
**DOMÍNGUEZ BARANDICA**

GRAHAM
**GREENLEAF**

DARA
**HALLINAN**

JUAN ANTONIO
**TRAVIESO**

FERNANDO
**VARGAS**

# LA PROTECCIÓN DE DATOS PERSONALES EN EL MARCO DE LA ACTIVIDAD EMPRESARIAL;
*una visión práctica*


CARLA
**BARBOZA**

*Carla Barboza es actualmente Head of Government Relations en Argentina, Paraguay y Uruguay para Equifax.*
*Anteriormente fue Directora de Asuntos Legales para Equifax Uruguay desde 2016.*
*Dirigió, y participó en las Áreas Legales de los proyectos industriales (celulosa, energía, y terminales portuarias) más relevantes de los últimos 15 años en Uruguay.*
*Fue Gerente de Sostenibilidad de ARPEL (Asociación de Empresas de Petróleo y Gas de América Latina y el Caribe) durante 2013 y 2014.*
*Es Abogada graduada en la Universidad de Montevideo, Uruguay. Ha realizado cursos de especialización en gerenciamiento de proyectos y estrategias de sostenibilidad corporativa, así como de posgrados en derecho ambiental, tanto en Uruguay como en el exterior.*






## RESUMEN


La autora releva distintas prácticas de las empresas privadas que procuran dar cumplimiento de la normativa de protección de datos personales. Centra además buena parte del análisis en las hipótesis de transferencias internacionales de datos, para finalizar con consideraciones relacionadas con la actualización de la normativa nacional en la materia y sus impactos.


---

En el presente artículo abordaremos los aspectos prácticos relacionados con la implementación y cumplimiento de la normativa de protección de datos personales, en el marco de las actividades habituales de las compañías privadas en Uruguay. Analizaremos las distintas figuras en las que una compañía puede actuar, distinguiendo las obligaciones y responsabilidades según realice el tratamiento de los datos en calidad de responsable de la base de datos, o de encargado de tratamiento.

## IMPORTANCIA DEL TEMA

Este asunto reviste especial importancia cuando nos situamos en el marco de una compañía nacional o multinacional, cuyas actividades implican el procesamiento de bases de datos propias y/o de terceros, sobre todo en el actual contexto de desarrollo tecnológico y transformación digital.

Considerando el marco regulatorio vigente en Uruguay ya hace más de 10 años y en particular, la profundización de la normativa que en línea con el Nuevo Reglamento Europeo entró en vigencia este año, los desafíos – y también las oportunidades- no son menores tanto para los regulados como para los reguladores.

En ese contexto, analizaremos los aspectos legales generales a tomar en cuenta por los responsables de bases de datos y encargados de tratamiento (ubicados en el país o en el extranjero) a quienes les resulte aplicable la normativa local.

### *1. EL TRATAMIENTO DE DATOS PERSONALES A NIVEL NACIONAL*

#### *1. a. RESPONSABLES DE BASES DE DATOS Y EL PRINCIPIO DE FINALIDAD*

Uno de los primeros aspectos que una compañía debe considerar a la hora de recolectar datos personales para fines propios, ya sea para su tratamiento como objeto principal de su actividad o como consecuencia de la misma, es la finalidad con la cual los datos van a ser utilizados.

Definir de antemano la finalidad con la que se van a tratar los datos recolectados, es una tarea que no puede dejarse pendiente. Sobre todo por la relevancia que lo anterior tiene para identificar y distinguir en qué base de datos se van a incorporar (o si corresponde la creación de una base nueva), y en el cumplimento de otros principios directamente relacionados, como los de proporcionalidad, minimización y privacidad por diseño y por defecto.

**El principio de finalidad** está especialmente consagrado en nuestra legislación[1] estableciendo que *"Los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención..."*.

En base a lo anterior, se deberán considerar tantas bases de datos como finalidades tenga el tratamiento de los datos recolectados. A modo de ejemplo, todos los datos que se recopilen con relación o en ocasión de una relación de trabajo, se van a incorporar a una base de datos que tendrá como finalidad administrar las distintas etapas y aspectos de esa relación de trabajo, con independencia de los medios, el momento y los soportes en lo que los datos se recopilen y/o registren.

Siguiendo con lo anterior y con otros ejemplos, nuestra normativa regula a los *"Datos Especialmente Protegidos"*[2], identificando dentro de esta categoría a los datos de naturaleza sensible, de salud, telecomunicaciones, publicidad, y actividad comercial y crediticia.

Cada una de esas finalidades, implicará la creación de distintas bases de datos, para las que regirán diferentes aspectos específicos en materia de: **tipo de datos personales a recolectar (campos de la base), fuentes de datos permitidas que nutrirán a la base, período de conservación, derechos de los titulares, medidas técnicas y organizativas para preservar la seguridad y confidencialidad, entre otros.**

En virtud del **principio de legalidad**[3], cada base de datos existente o creada en base a los criterios anteriores debe estar debidamente registrada ante la Unidad Reguladora y de Control de Datos Personales (en adelante "URCDP") dentro del plazo máximo de 90 días desde su creación, proporcionando la información que se especifica en el Decreto Reglamentario[4], pudiendo utilizar además para ello

1 *Ley 18.331, Art. 7*
2 *Ley 18.331, CAPITULO IV*
3 *Ley 18.331, Art. 6*
4 *Decreto 414/009, TITULO III, Régimen Registral*

el mecanismo web de **Sistema de Registro de Bases de Datos**[5].

Cada responsable de bases de datos, podrá además contar con un **Código de Conducta**, en el que se detallarán los aspectos relevantes del procesamiento de datos que realiza la empresa en cuestión, incluyendo aspectos de la **normativa nacional e internacional** aplicables, así como aquellos vinculados a las **políticas corporativas internas** de la empresa en cuestión, que hacen al tratamiento de datos. Estos códigos de conducta, por lo general pretenden integrar las actividades de la empresa, la protección de los datos personales, y la conducta de sus empleados y directivos al respecto.

La existencia y **registro**[6] de dicho código, como más adelante se verá, cobra especial relevancia para el marco de las actividades de empresas multinacionales, ya que es uno de los mecanismos habilitantes para la transferencia internacional de datos propios, entre la matriz y sus filiales y/o sucursales, y entre éstas.

Finalmente cada responsable o propietario de bases de datos, deberá considerar especialmente los **derechos que los titulares de los datos**[7] tienen, respecto a los datos incluidos en las bases de datos de su propiedad. Los mismos pueden variar según el tipo de base de que se trate (distinguidas, como vimos, según su finalidad), pero generalmente hablamos de los derechos de: acceso, así como los de rectificación, actualización, inclusión o supresión.

El derecho de acceso otorga al titular del dato, la potestad de obtener toda la información que sobre sí mismo obre en una base de datos, previa acreditación de su identificación, existiendo plazos específicos de respuesta por parte del responsable, en un plazo muy breve de tan solo 5 días hábiles. Este derecho se concede de forma gratuita a intervalos de seis meses, salvo que el titular demuestre que medie nuevamente un interés legítimo en un plazo menor. Por su parte, los derechos de rectificación y supresión, implican por lo general que el titular del dato pueda acreditar el error o falsedad del dato, mediante un procedimiento especialmente establecido a esos efectos[8], todo lo cual debe ser respondido siempre, sea accediendo o denegando la solicitud, en un plazo de 5 días hábiles.

Existen casos, en donde por la naturaleza de la base de datos o por las fuentes permitidas, la Ley le otorga garantías adicionales a los titulares, como sucede con las bases de publicidad[9], donde se establece el deber del responsable de bloquear o suprimir el dato en cualquier momento y ante la sola solicitud del titular.

Al margen de las obligaciones legales antes consideradas, cabe señalar que en los hechos, establecer mecanismos de contacto entre el responsable de una base de datos con los titulares, resulta de mucha utilidad; produce una retroalimentación en materia de actualización de datos, lo que redunda en una mejor calidad de los datos, y ofrece al titular una instancia para controlar la exactitud de sus datos.

### *1. b. PRESTADORES DE SERVICIOS INFORMATIZADOS DE DATOS PERSONALES, Y LA IMPORTANCIA DEL CONTRATO EN URUGUAY.*

Otro caso de relevancia en materia de tratamiento de datos, se da cuando una compañía además de tratar los datos personales que surgen como consecuencia lógica de sus actividades (bases de datos propias), también procesa **datos de terceros** a través de la prestación de distintos servicios a sus clientes. En estos casos, procesa datos que no le son propios por cuenta y orden de sus clientes, bajo la figura del encargado de tratamiento.

En este caso, y si bien bajo la regulación vigente su celebración no es estrictamente obligatoria, **el contrato** entre el encargado de tratamiento (empresa que presta el servicio) y el cliente (responsable de sus bases), es altamente recomendable, ya que será el instrumento que regule específicamente los aspectos vinculados a la protección de dichos datos, tomando como plataforma la normativa aplicable[10].

En ese sentido, en un contrato de esas características se entiende importante incluir **cláusulas** especiales relativas a: i) el carácter especial del encargado de tratamiento, que actuará siempre **por cuenta y orden** del cliente (responsable de la base de datos), ii) declaración por parte del cliente del **objeto y finalidad** del tratamiento encargado, iii) determinación de las etapas y/o acciones que implicará el **procesamiento de los datos**, iv) **confidencialidad**, v) **responsabilidad de cada una de las partes atendiendo a su calidad de responsable y encargado**, respectivamente, y, en caso que exista un **"sub-encargado de tratamiento"**: declarar tal situación por parte del encargado, estableciendo los datos de contacto de dicha empresa, y que la otra parte (el cliente o responsable) autorice la **comunicación de sus datos** al tercero que intervendrá en el proceso del tratamiento de los datos para los mismos fines y con las mismas limitaciones que los encargados al encargado principal.[11]

Dentro de la dinámica de las relaciones comerciales y en aquellos casos en donde por disposiciones legales o por la naturaleza de los datos o de las fuentes, una de las partes está habilitada a comunicar datos de su propia base a terceros, puede ocurrir que una de las partes asuma un doble rol. Esto es: actúa como encargado de tratamiento de los datos provistos por su cliente, pero a su vez, es responsable de bases de datos propias, cuya información el cliente desea consultar para incorporar dichos datos también al procesamiento encargado. Ejemplo de lo anterior sucede cuando un cliente le encarga a una empresa de informes comerciales, un tratamiento de datos determinado por su cuenta y orden, proveyéndole a esos efectos datos provenientes de sus propias bases, pero también datos sobre cumplimento e incumplimiento de obligaciones que obtiene de la base de datos informes comerciales.

En estos casos, resulta muy útil que el contrato contenga cláusulas de **"antecedentes" y "definiciones relativas al procesamiento"**, para que el flujo de datos entre ambas partes sea estrictamente el permitido por la regulación vigente, así como como las **responsabilidades** de cada una en el proceso, estén bien delimitadas.

Finalmente, en estos casos es importante considerar en los contratos los aspectos especiales vinculados a las **regulaciones específicas de la propia industria** de la empresa que encarga el procesamiento. A modo de ejemplo, si quien encarga el procesamiento de datos propios es una entidad regulada por el Banco Central del Uruguay, puede estar obligada a cumplir con ciertos requisitos que puede ser necesario incorporar al contrato.

## *2. EL TRATAMIENTO DE DATOS PERSONALES EN EL EXTERIOR*

### *2. a. ASPECTOS A CONSIDERAR CON RELACIÓN A LAS TRANSFERENCIAS INTERNACIONALES.*

La transferencia internacional de datos es sin lugar a dudas un tema de gran relevancia para las compañías multinacionales que operan en Uruguay.

Nuestra normativa regula distintos escenarios vinculados a este tema.

Así, si el tratamiento de datos implica la transferencia internacional de datos propios de una compañía establecida en Uruguay a otros países, será importante considerar que la legislación vigente **prohíbe la transferencia internacional de datos a países que no ofrezcan niveles adecuados de protección de datos, con ciertas excepciones.**[12] De acuerdo a la Resolución de la URCDP[13], los países que ofrecen un nivel adecuado de protección de datos son: los países miembros de la Unión Europea, y aquellos países no miembros pero que hayan obtenido una nota de adecuación de la Comisión Europea. La forma que adoptó la URCDP para identificar los países con niveles de protección adecuados ha sido sin dudas un acierto dado que permite a Uruguay mantenerse actualizado y siempre en línea con los criterios de la Comisión Europea. Prueba de ello es que a través de este criterio, Uruguay reconoce como adecuadas, al igual que los países de la Unión Europea, a las empresas ubicadas en Estados Unidos adheridas al Privacy Shield Framework. Es decir, la transferencia internacional de datos de responsables de bases, en las situaciones antes mencionadas, **no está prohibida.**

Sin embargo, puede suceder que por la forma de organizarse una empresa, o por necesidades vinculadas a procesos que se desarrollan en más de una jurisdicción, entre otros aspectos, sea necesario implementar **transferencias internacionales de datos personales a países que no forman parte de los ya mencionados.** En el caso de una empresa multinacional, será importante considerar si la empresa que va a realizar el tratamiento en el exterior **es una empresa del mismo grupo que la que se encuentra en Uruguay.** Si la respuesta es positiva, **y se confirma además que existe un Código de Conducta registrado** ante la URCDP, la transferencia podrá realizarse de igual forma. De ahí la relevancia para las empresas multinacionales de tener un Código de Conducta de las características que se detallan en el apartado "I-A" de este artículo, debidamente registrado ante el regulador de datos personales. Si por el contrario: i) el exportador de datos no es una empresa multinacional, o ii) como se abordará más adelante, estamos ante el caso de una empresa multinacional ubicada en Uruguay, que necesita implementar una transferencia internacional de datos hacia una empresa no perteneciente al grupo, y para ambos casos (i y ii) la jurisdicción de destino no es adecuada, o siendo una empresa americana la importadora de los datos no está adherida a Privacy Shield; entonces la forma en que generalmente se deberá proceder es **solicitar la autorización de transferencia internacional de datos ante la URCDP**[14].

5 *https://www.gub.uy/unidad-reguladora-control-datos-personales/registro-bases-datos*

6 *Decreto 414/009, Art.36*

7 *Ley 18.331, CAPITULO III*

8 *Ley18.331, Art. 15*

9 *Ley 18.331, Art. 21*

10 *Ley 18.331, Art. 30*

11 *Ley 18.331, Art. 15*

12 *Ley 18.331, Art. 23*

13 *Resolución N° 4/2019*

14 *Decreto 414/009, Arts. 34 y 35*

Para **determinar** si estamos ante un caso que requiera aplicar una u otra **solución habilitante** de la transferencia internacional, **es importante plantearse la pregunta** respecto a dónde serán procesados los datos, y específicamente, dónde estará localizado físicamente el "data center" de los procesadores o sub-procesadores en el exterior, ya sea en la misma jurisdicción del exterior, o eventualmente en otra (y en ese caso se deberá volver a evaluar las reglas de transferencia internacional de acuerdo a los parámetros ya indicados). Es sustancial entones tener en claro el flujo de los datos implícito en el procesamiento internacional, y entender cuáles son las partes involucradas, así como las tareas que realizan cada una de ellas.

### *2. b. ASPECTOS DE TRANSFERENCIA INTERNACIONAL A CONSIDERAR POR PRESTADORES DE SERVICIOS INFORMATIZADOS DE DATOS PERSONALES.*

Tal como se comentó en el punto "I-B", una empresa privada puede también procesar datos de terceros, a través de la prestación de distintos servicios a sus clientes (bases de datos de clientes).

En ese caso, tendríamos un procesador (o encargado de tratamiento o prestador de servicios informatizados de datos personales) en Uruguay, al cual su cliente (responsable de sus bases de datos) le instruye un determinado procesamiento de datos. Sin embargo el procesador encargaría, (sea por razones de almacenamiento, escalabilidad, disponibilidad de recursos u otros motivos) dicho procesamiento en todo o en parte a un sub-procesador ubicado en el exterior. Esto es cada vez más habitual, en un contexto de desarrollo de las plataformas regionales de procesamientos de datos, y de soluciones de "cloud computing" para el "hosteo" de datos prestados por entidades del exterior.

En este caso corresponderá antes que nada, de parte del procesador uruguayo considerar los siguientes aspectos: i) jurisdicción donde se localiza el "data center" del sub-procesador, de manera de apuntar a que la jurisdicción del importador de datos sea una a la que no esté prohibida la transferencia internacional, sin embargo, ii) en caso de una transferencia internacional a una jurisdicción no segura, deberá presentarse el contrato entre procesador de Uruguay y el sub-procesador del exterior a la URCDP para su autorización.

Una vez que se verifique que **el destino de los datos objeto del sub-procesamiento** es una jurisdicción de las contempladas por la normativa local que no requieren autorización del regulador de datos de transferencia internacional, u obtenida dicha autorización de la URCDP (en caso que sea un país distinto a los contemplados por la normativa nacional vigente) deberá prestarse **especial atención a los contratos que servirán de estructura de la operativa.**

Es recomendable que **el contrato entre el procesador de Uruguay y el sub-procesador del exterior,** contemple especialmente cláusulas vinculadas a los aspectos de protección de datos como se regulan en Uruguay, o como es de estilo, incluir como anexo al contrato un "Data Processing Agreement" o "DPA", donde las partes pauten exclusivamente los temas vinculados al procesamiento y a la protección de datos personales. En ese sentido, en un "DPA" es aconsejable considerar los siguientes temas según sea la envergadura del procesamiento en el exterior: alcance y roles de las partes en el procesamiento de datos, definiciones, naturaleza del procesamiento (refiere al servicio que estará prestando el sub- procesador), tipo de datos sometidos al sub-procesamiento, duración del sub-procesamiento, tipo de titulares de datos (clientes, empleados, proveedores, entre otros), confidencialidad, medidas de seguridad para el sub-procesamiento, medidas de seudonimización (si existieren), aspectos vinculados a los sub-procesadores del sub-procesador (sub-procesadores autorizados desde el inicio por las partes, y mecanismos de aprobación de sub- procesadores, obligaciones de los sub- procesadores, responsabilidad del sub-procesador respecto al cumplimiento con el "DPA" por parte de sus sucesivos sub-procesadores), derechos de los titulares de los datos y responsabilidades de las partes para dar respuesta al ejercicio de los mismos, notificaciones en caso de incidentes de seguridad, mecanismos de auditorías, responsabilidades del sub-procesador en materia de estudios de impacto de privacidad que el procesador realice, así como en lo que le pueda corresponder al sub-procesador en materia de medidas técnicas y organizativas a las que el procesador se haya comprometido con el responsable de la base (el cliente).

Por otro lado, en el **contrato de procesamiento de datos entre el procesador en Uruguay y su cliente,** además de los aspectos ya mencionados en el punto **"I-B"**, deberá indicarse el lugar de localización del sub-procesador del exterior, objeto, duración, y autorización de dicha comunicación de datos, en un todo de acuerdo con la normativa nacional.

## *3. ACTUALIZACIONES A LA LEY DE PROTECCIÓN DE DATOS PERSONALES Y NUEVAS OBLIGACIONES*

El 1° de enero entró en vigencia el proceso de profundización normativa de Uruguay en materia de protección de datos, a través de los arts. 37 a 40 de la Ley 19.670. Revisten especial relevancia los siguientes conceptos que la legislación introduce:

### *3. a. RESPONSABILIDAD PROACTIVA*

Constituye uno de los principales cambios ya que en los hechos implica un cambio radical en el abordaje que deben realizar las empresas. Los tiempos en que se podía esperar y confiar en que nada sucedería, han quedado en el pasado. La regulación ahora impone una actuación pro-activa y desde el inicio, tal como lo sugiere el término. Constituye en definitiva un robustecimiento del principio de responsabilidad[15], ya recogido en la primera versión de la ley[16] pero con efectos relevantes.

Las diferencias radican especialmente en los siguientes aspectos:(i) el principio de responsabilidad le atañe además al **encargado de tratamiento**, siendo ahora también responsable por las violaciones a la ley, (ii) se vuelve obligatorio el **ejercicio de una responsabilidad proactiva**, tanto para responsables como para encargados de tratamiento, que en los hechos implicará la adopción de medidas previas, paralelas, y posteriores al tratamiento de los datos, que apunten a dar cumplimiento a las normas de protección de datos, las que además deberán estar documentadas, para demostrar su efectiva implementación.

En este contexto de responsabilidad proactiva, la privacidad por diseño y por defecto, así como la evaluación de impacto a la protección de datos personales, son tres conceptos fundamentales que se introducen al marco normativo nacional.

**Privacidad por diseño**, implica tanto para responsables como para encargados, **diseñar** sus bases de datos, procesos, productos o tecnologías considerando desde esa instancia los aspectos de protección de datos necesarios con el objetivo de cumplir con la normativa en la materia.

**Privacidad por defecto**, conlleva que el responsable y el encargado de tratamiento, deberán diseñar los procesamientos de tal manera que solamente sean tratados los datos personales necesarios (considerando aspectos como el lazo de conservación, extensión del tratamiento, y comunicación) para cada una de las finalidades previstas.

Por su parte, la **evaluación de impacto a la protección de datos personales** o como se la conoce internacionalmente: "PIA" ("Privacy Impact Assessment"), es una herramienta de gestión que permite reconocer riesgos y medidas de eliminación o mitigación de los mismos, considerando la expectativa de privacidad que pueden tener los titulares de los datos para cada tipo de tratamiento. Se sugiere en estos casos elaborar internamente **formularios de fácil compresión** para las distintas áreas involucradas, de manera que queden plasmadas en un documento las distintas fases de un proyecto, los riesgos identificados en materia de protección de datos, así como las medidas técnicas y organizativas propuestas para su eliminación o mitigación. Es recomendable también que el modelo de dicho formulario cuente con una **guía sencilla a modo de "screening"** que sirva de ayuda para identificar cuándo un proyecto debe ser sometido a un proceso de "PIA". Finalmente y dependiendo de la envergadura del procesamiento de datos personales que habitualmente implemente una empresa, es aconsejable también considerar una **política interna de privacidad** que contenga la visión de la compañía respecto al tema protección de datos personales en cumplimiento con las normas aplicables, la conducta esperada de empleados y directores al respecto, así como la enunciación de los instrumentos de gestión vigentes que se deberán aplicar.

Finalmente, cabe señalar que el artículo 39 de la ley 19.670, establece que la reglamentación determinará las medidas que correspondan para dar cumplimiento con el principio de responsabilidad proactiva, así como la oportunidad para su revisión y actualización.

### *3. b. RESPUESTAS A INCIDENTES DE SEGURIDAD*

El artículo 8 Decreto 414/09 ya hacía referencia a aspectos vinculados a las vulneraciones de seguridad, estableciendo que cuando el responsable de una base de datos o el encargado de tratamiento, tomara conocimiento de tal extremo, y siempre y cuando fuera susceptible de afectar de manera "significativa" los derechos de los interesados, se debía informar a los mismos.

La nueva normativa en la materia[17], introduce una nueva obligación para responsables y encargados de informar pormenorizadamente respecto a la ocurrencia de la vulneración, así como las medidas que adopte: (i) a los titulares de los datos, y (ii) **a la URCDP**, la que coordinará el curso de acción que corresponda con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay (CERTuy). **También se aclara que la reglamentación determinará el contenido de la información correspondiente a la vulneración de seguridad.**

Las empresas que tratan datos personales de manera habitual, por lo general cuentan con **políticas internas y/o certificaciones de seguridad**, que im-

15 *Ley 19.670, Art.39*

16 *Ley 18.331, Art.12.*

17 *Ley 19.670, Art.38*

plican medidas técnicas y organizativas con el fin de salvaguardar la integridad, confidencialidad y disponibilidad de la información.

Sin perjuicio de lo anterior, y en materia de comunicación de **vulneraciones de seguridad**, será importante que la reglamentación refiera a algunas cuestiones que hoy se plantean como interrogantes: (i) ya no se refiere más la afectación "significativa" de los derechos de los titulares, y por tanto sería relevante que se aclarara en qué casos de vulneraciones efectivamente se debe proceder con las comunicaciones, (ii) dado que el encargado de tratamiento también deberá hacerlo, sería conveniente considerar la forma en que deberá actuar frente al responsable en estos casos, y (iii) es primordial tomar en cuenta que estas circunstancias implican la entrada en acción de equipos especializados en seguridad (entre otros), y que son procesos muy intensos y dinámicos, durante los cuales varias líneas de acción se disparan en forma paralela, para neutralizar la situación o mitigarla, así como para ir recabando datos de lo sucedido en el contexto de una investigación. Así, "minuto a minuto" puede ir cambiando el contexto conocido por la empresa, y frente a esa realidad, será esencial que la reglamentación diferencie el plazo y el contenido de la comunicación a la URCDP; del plazo y del contenido de la comunicación a los titulares de los datos, considerando a tales efectos, aspectos relativos a la minimización de daños, pero también a la exactitud de la información que se comunique a los titulares.

### *3. c. DELEGADO DE PROTECCIÓN DE DATOS*

Finalmente, la nueva normativa establece que las entidades privadas que traten datos sensibles como negocio principal y las que realicen el tratamiento de grandes volúmenes de datos, deberán designar un **delegado de protección de datos.**[18]

Si bien se describen las generalidades de las funciones que el delegado debe llevar a cabo, será importante conocer mediante la reglamentación las características técnicas requeridas para el ejercicio de ese rol, y si el mismo puede ser llevado a cabo por un dependiente de la empresa o es una función que se pueda tercerizar.

## *4. CONCLUSIÓN FINAL*

Una vez más, Uruguay ha marcado su postura de adecuarse a las nuevas disposiciones en materia de protección de datos personales a través de la nueva normativa y la reglamentación que se espera en los próximos tiempos.

Alinear las operaciones existentes de una empresa al nuevo contexto normativo, exigirá invertir en nuevos recursos destinados a la formalización de procesos, así como en tecnologías que hagan más eficiente y seguro el procesamiento de datos personales.

El acompañamiento desde la perspectiva educativa por parte de las distintas autoridades competentes, especialmente en las primeras etapas, será esencial para lograr la efectiva implementación de la regulación, considerando el justo balance que debe existir entre los desafíos y los beneficios que el tema presenta.

# BIBLIOGRAFÍA:


- Ley 18.331 de Protección de Datos Personales y Acción de Habeas Data, del 8 de agosto de 2008 y sus modificativas.
- Ley 19.670, artículos 37 a 40, del 15 de octubre de 2018.
- Decreto 414/009, del 15 de setiembre de 2009.
- Resolución N° 4/2019 de la Unidad Reguladora y de Control de Datos Personales.
- Reglamento Europeo N° 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Código de Conducta Equifax Uruguay S.A, registrado por Resolución del Consejo Ejecutivo de la Unidad Reguladora y de Control de Protección de Datos Personales, de fecha 17 de julio de 2013.


18 *Ley 19.670, Art. 40*

# HACIA UNA NUEVA LEY DE PROTECCIÓN DE LOS DATOS PERSONALES EN ARGENTINA


EDUARDO
**BERTONI**

*Es el Director de la Agencia de Acceso a la Información Pública, actualmente la autoridad de control de la Ley Nº 25.326 de Protección de los Datos Personales y la Ley Nº 27.275 de Derecho de Acceso a la Información Pública en Argentina (AAIP). Es abogado, Doctor en Derecho de la Universidad de Buenos Aires y entre 2002-2005 fue Relator Especial de la Comisión Interamericana de Derechos Humanos para la Libertad de Expresión. Es Profesor de la Facultad de Derecho de la Universidad de Buenos Aires y de la Escuela de Derecho de la Universidad de Nueva York (NYU). Fundador del Centro de Estudios en Libertad de Expresión y Acceso a la Información de la Universidad de Palermo, Argentina. Ha publicado varios libros en carácter de autor o editor, siendo el más reciente "Difamación en Internet. Problemas de Jurisdicción y Ley Aplicable", Editorial Ad-Hoc, Buenos Aires (2015).*

SOFÍA
**DOMÍNGUEZ BARANDICA**

*Es asesora jurídica en la Agencia de Acceso a la Información Pública (AAIP). Es abogada, egresada de la Universidad Torcuato Di Tella.*


## SUMARIO


- RESUMEN
- HACIA UNA NUEVA LEY DE PROTECCIÓN DE LOS DATOS PERSONALES EN ARGENTINA

## RESUMEN

Los autores del artículo reseñan las circunstancias que motivaron la redacción del proyecto de Ley de Protección de Datos de la República Argentina, sus objetivos, antecedentes y principales cambios con respecto a la normativa vigente en el citado país.


## HACIA UNA NUEVA LEY DE PROTECCIÓN DE LOS DATOS PERSONALES EN ARGENTINA[1]

La protección de los datos personales se encuentra explícitamente garantizada en Argentina a través de la acción de hábeas data prevista en el artículo 43, tercer párrafo, de la Constitución Nacional, acción que fue incorporada en oportunidad de la reforma constitucional del año 1994. Posteriormente, se sancionó la Ley Nº 25.326 de Protección de los Datos Personales, norma de orden público que regula los principios aplicables en la materia, así como también el procedimiento de la acción de hábeas data. La mencionada ley fue sancionada en octubre del 2000 y entró en vigencia al año siguiente.

No se puede objetar que la tecnología ha evolucionado en los últimos dieciocho años a un ritmo vertiginoso, impactando en gran medida en la protección de los datos personales. Basta señalar que, por ejemplo, Facebook surgió en 2004 y Dropbox en 2007 para darse cuenta de que el escenario en el que se sancionó la Ley Nº 25.326 cambió radicalmente. Esta nueva realidad de la tecnología ha traído enormes desafíos en el campo del ejercicio de los derechos. Los beneficios son innegables, pero también lo son las nuevas potenciales vulneraciones a la privacidad.

Por otro lado, se debe destacar que actualmente se presenta un nuevo contexto regulatorio internacional en esta materia a raíz de la entrada en vigencia del Reglamento Europeo de Protección de Datos (en adelante, Reglamento (UE) 2016/679).

Sin duda el Reglamento (UE) 2016/679 ha tenido un impacto significativo a nivel internacional. Ello se debe principalmente a dos razones: (a) su aplicación extraterritorial; y (b) la regla en materia de transferencias internacionales que, en principio, únicamente permite se transfieran datos a terceros países -no Miembros de la UE- que cuenten con un nivel de protección adecuado.[2] En este sentido, se considera que un país es adecuado cuando su sistema legal y el modo en que éste es aplicado en la realidad garantiza ciertos derechos y obligaciones considerados esenciales por la UE[3].

Si bien la Argentina es uno de los pocos países latinoamericanos que ha logrado obtener una decisión de adecuación por parte de la Comisión Europea[4], esta situación podría cambiar a raíz de la adopción del Reglamento (UE) 2016/679, ya que éste además de receptar cambios sustanciales respecto a la anterior Directiva 95/46/CE, prevé un procedimiento de revisión periódica por parte de la Comisión Europea para verificar los acontecimientos relevantes en el tercer país cuyo nivel de protección haya sido declarado adecuado.[5] Si la revisión revelara que alguno de estos países ya no garantiza un nivel de protección adecuado, la Comisión tendría la potestad de suspender la decisión de adecuación.[6]

Por lo expresado hasta aquí, la entonces Dirección Nacional de Protección de Datos Personales, dependiente del Ministerio de Justicia y Derechos Humanos (en adelante, la DNPDP)[7] tomó la iniciativa en 2016 de elaborar un proyecto de ley de protección de datos personales para reformar la ley vigente. El desafío de esta tarea consistió en elaborar una nueva normativa destinada a proteger los datos personales y la privacidad de las personas, sin ser un obstáculo para la innovación y el desarrollo tecnológico y que, además, cumpliera con estándares internacionales.

El proyecto elaborado fue el resultado de un proceso que se llevó a cabo en el marco del programa "Justicia 2020", creado por el Ministerio de Justicia y Derechos Humanos, como un espacio de participación ciudadana e institucional para la elaboración, implementación y seguimiento de iniciativas y políticas de Estado.[8]

Este proceso tuvo dos etapas. Durante la primera, se realizaron reuniones de trabajo con diferentes actores interesados en la materia, provenientes del sector privado, del ámbito académico y de la sociedad civil para debatir sobre la necesidad de una reforma.[9] El resultado de esas reuniones fue compilado en el documento "Ley de Protección de los Datos Personales en Argentina (Sugerencias y aportes recibidos en el proceso de reflexión sobre la necesidad de su reforma - Agosto-Diciembre 2016)" y publicado en el sitio web de la AAIP.[10]

En este proceso de reflexión, se discutieron distintos aspectos de la legislación vigente y se escucharon propuestas de modificaciones a la Ley Nº 25.326, siendo uniforme la opinión respecto de la necesidad de una reforma. Además se debatió acerca de la importancia de adecuar la legislación a los estándares internacionales en materia de protección de datos, contenidos en el Reglamento (UE) 2016/679 como en otros instrumentos internacionales.[11]

Uno de los temas mayormente abordados durante la serie de reuniones fue el mantenimiento del consentimiento del titular de los datos como principio rector para su tratamiento. En general, una mayoría destacó la necesidad de flexibilizar el concepto de consentimiento receptado en la ley vigente. Sustentaron su postura en que en un mundo en el que se producen continuamente transacciones que implican tratamiento de datos personales cuando una persona utiliza servicios y productos en Internet, no es realista esperar que las personas deban recibir y procesar solicitudes de consentimiento para cada interacción que conlleve el uso de sus datos. En este sentido, se sugirió que, de reformarse la ley, ésta permita un consentimiento transparente pero implícito, sujeto al contexto en el cual un servicio se utilice, y restrinja el requerimiento de consentimiento explícito a situaciones específicas donde, por ejemplo, se traten datos sensibles.

Otro tema abordado en la mayoría de las reuniones fue la incorporación del principio de responsabilidad demostrada (o proactiva) a la ley argentina sobre protección de datos. Hubo consenso generalizado respecto de la necesidad de que se adopte un sistema de responsabilidad demostrada, por el cual los responsables y otros sujetos que realicen tratamiento de datos se encuentren obligados a demostrar el cumplimiento de la ley. Se defendió, siguiendo la tendencia internacional, que al incorporar este principio se podría abandonar la obligación de registro de bases de datos.

A su vez, un aspecto de la ley vigente que varios criticaron fue el diseño institucional de la autoridad de control. Todos aquellos que hicieron referencia a este tema coincidieron en la necesidad de que la ley de protección de datos personales contemple

---

1 *El presente artículo fue inicialmente publicado en la Revista Latinoamericana de Protección de Datos Personales, Número 4, Número especial: Reforma de la ley argentina de protección de datos personales, CDYT, Buenos Aires, 2017. En la presente versión, se realizaron algunas modificaciones y añadidos a los fines de su actualización.*

2 *Artículo 45.1 del Reglamento (UE) 2016/679.*

3 *Sentencia del Tribunal de Justicia de la Unión Europea del 6 de octubre de 2015 en el asunto C-362/14, Maximilian Schrems v. Data Protection Commissioner, consid. 73, 74, 75 y 96; Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, Brussels, 10.1.2017, COM(2017) 7 final, pages 6-7.*

4 *Decisión de la Comisión C (2003) 1731 de fecha 30 de junio de 2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina. Publicación oficial: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32003D0490&from=EN, última consulta: 18/06/2019.*

5 *En efecto, actualmente la República Argentina se encuentra en proceso de revisión de su decisión de adecuación a la regulación europea de protección de datos personales.*

6 *Artículo 45 del Reglamento (UE) 2016/679.*

7 *En Argentina, el diseño institucional de la autoridad de control en materia de protección de datos personales fue modificado. En efecto, mediante el Decreto Nº 746/2017, se adicionó a las funciones de la Agencia de Acceso a la Información Pública – autoridad creada en el marco de la Ley Nº 27.275, como ente autárquico que funciona con autonomía funcional en el ámbito del Poder Ejecutivo Nacional- la de actuar como autoridad de aplicación de la Ley N° 25.326. Posteriormente, mediante el Decreto Nº 899/2017 se ratificó lo ya dispuesto por el Decreto Nº 746/2017, sustituyendo el artículo 29 del Anexo I del Decreto Nº 1558/01 -que designaba a la Dirección Nacional de Protección de Datos Personales en el ámbito de Ministerio de Justicia y Derechos Humanos, como órgano de control de la Ley Nº 25.326- por el siguiente: "Artículo 29.- La Agencia de Acceso a la Información Pública, conforme los términos del artículo 19 de la Ley N° 27.275, sustituido por el artículo 11 del Decreto N° 746/17, es el órgano de control de la Ley Nº 25.326". Si bien actualmente la Dirección Nacional de Protección de Datos Personales sigue existiendo como una dirección dependiente de la AAIP, a efectos prácticos en el presente artículo se hará referencia a la "DNPDP" cuando se trate de la entonces Dirección Nacional de Protección de Datos Personales dependiente del Ministerio de Justicia y Derechos Humanos y a la "AAIP" cuando se trate de la Dirección Nacional de Protección de Datos Personales dependiente de la Agencia de Acceso a la Información Pública.*

8 *Para acceder al sitio oficial de Justicia 2020, ingrese al siguiente enlace: https://www.justicia2020.gob.ar/, última consulta: 18/06/2019.*

9 *Los participantes que acudieron al proceso de reflexión convocado por la DNPDP fueron los siguientes: Sector privado: Accenture, Asociación de Bancos Argentinos (ADEBA), Asociación de Bancos de la Argentina (ABA), Asociación de Marketing Directo e Interactivo de Argentina (AMDIA), Cámara Argentina de Comercio Electrónico (CACE), Cámara Argentina de Internet (CABASE), Cámara de Comercio de los Estados Unidos de América en la Argentina (AmCham Argentina), Confederación Argentina de la Mediana Empresa (CAME), Facebook, Google, GSMA, IBM, Information Technology Industry Council(ITI), INTEL, MercadoLibre, Microsoft, Telecom, Telefónica. Académicos y particulares: Alejandro Castillo, Juan Darío Veltani, Guillermo F. Peyrano, Horacio R. Granero, Leonor Guini, Mariano Javier Peruzzotti, Mariano M. Del Río, Matilde S. Martínez, Natalia Eugenia Roda, Oscar Puccinelli, Pablo A. Palazzi, Paula Vargas, Silvia Iglesias. Sociedad civil: Asociación Civil por la Igualdad y la Justicia (ACIJ), Asociación por los Derechos Civiles (ADC), Centre for Information Policy Leadership (CIPL), Fundación Poder Ciudadano, Fundación Sadosky, Fundación Vía Libre, Information Accountability Foundation (IAF).*

10 *Para acceder al documento, ingrese al siguiente sitio:https://www.argentina.gob.ar/sites/default/files/documento_aportes_reforma_ley25326_0.pdf, última consulta: 18/06/2019.*

11 *A lo largo de las reuniones, además de indicar se tuviera en cuenta el Reglamento (UE) 2016/679 como modelo para una eventual reforma, se sugirieron otros modelos; entre ellos, el APEC Privacy Framework y el APEC Cross Border Privacy Rules (CBPR) system , así como el Acuerdo Transpacífico de Cooperación Económica. Un sector muy minoritario recomendó también tener en cuenta el informe del Comité Jurídico Interamericano, titulado "Privacidad y protección de datos personales" de 2015.*

una expansión de la capacidad de la DNPDP para cumplir con sus funciones de contralor. Para ello, sugirieron se aumente la autonomía de la DNPDP y se garantice su adecuado financiamiento.[12]

Esta primera etapa de consultas fue seguida por la elaboración de un primer anteproyecto de ley por parte de la DNPDP, en el que no sólo se tomaron en cuenta los comentarios recibidos en el proceso de reflexión, sino también regulaciones existentes a nivel internacional específicas en la materia, como el Reglamento (UE) 2016/679, el Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108) y el Convenio sobre la Ciberdelincuencia (Convención de Budapest). Asimismo, se tomó como referencia legislación comparada sancionada en los últimos años, como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México, la Ley de Protección de Datos Personales Nº 29.733 de Perú, la Ley Estatutaria 1581 de 2012 de Colombia y sus respectivas reglamentaciones y la Ley de Protección de Información Personal y de Documentos Electrónicos de Canadá *(Personal Information Protection and Electronic Documents Act - PIPEDA)*, entre otras. También se tomaron en cuenta los Estándares de Protección de Datos Personales para los Estados Iberoamericanos y el Informe del Comité Jurídico Interamericano sobre Privacidad y Protección de Datos Personales.

En la segunda etapa del proceso, este anteproyecto fue sometido a discusión y consulta pública, nuevamente en el marco de la plataforma "Justicia 2020", recibiéndose comentarios y sugerencias sobre el texto que se había elaborado.[13] Luego de analizar los documentos recibidos, se elaboró una segunda versión del anteproyecto[14].

Esta versión del anteproyecto fue sometido a la revisión de distintas dependencias del Poder Ejecutivo nacional y finalmente el 19 de septiembre de 2018 el proyecto –con algunas modificaciones-[15] fue enviado al Congreso de la Nación mediante Mensaje MEN-2018-147-APN-PTE[16]. Si bien, como se indicó anteriormente, uno de los principales factores que impulsaron a la DNPDP a activar un proceso para reformar la ley vigente fue la necesidad de que Argentina continúe siendo un país con legislación adecuada conforme a los lineamientos del nuevo Reglamento (UE) 2016/679, se debe recalcar que el proyecto no es bajo ninguna medida una copia exacta de la mencionada regulación europea. Es cierto que el proyecto recepta aquellos aspectos que pueden considerarse esenciales del Reglamento (UE) 2016/679, pero a su vez, presenta ciertas aristas que difieren, sin contradecirla, de la normativa europea y responden más bien al contexto argentino. Para ello, se tomaron como referencia la experiencia de la DNPDP, jurisprudencia local en la materia y legislación comparada.

En síntesis, los principales cambios que se proponen y que creemos oportuno destacar son los siguientes:

- El proyecto sigue los lineamientos más modernos en materia de protección de datos, entendiendo que la normativa se aplicará aun cuando, bajo ciertos supuestos, los responsables de tratar los datos no se encuentren en territorio nacional.
- El eje central pasa a ser el dato personal objeto de tratamiento, y no las bases de datos, como ocurre con la ley vigente.
- Se dispone que la aplicación de la ley no podrá afectar al tratamiento de datos que realicen los medios de comunicación en el ejercicio de la libertad de expresión. Específicamente, en relación con el derecho de supresión, el proyecto aclara que este derecho no procederá cuando el tratamiento de datos persiga un fin público o sea necesario para ejercer el derecho a la libertad de expresión e información.
- Se incorpora el principio de responsabilidad demostrada. Al receptar este principio, se abandona la obligación de registro de bases de datos, imposición que según la experiencia de la DNPDP no ha mejorado la protección de la privacidad de las personas.
- Se incluye la evaluación de impacto y la obligación de notificar incidentes de seguridad, entre las medidas destinadas a garantizar un tratamiento adecuado de los datos personales y el cumplimiento de las obligaciones dispuestas por la ley.
- Se flexibilizan las normas relacionadas al consentimiento, con el fin de estar más acorde a la era digital. El proyecto prevé que el consentimiento puede ser obtenido de forma expresa o tácita. La forma del consentimiento estará sujeta al contexto en el que se recepten los datos personales y al tipo de dato en cuestión.
- El interés legítimo pasa a ser una base legal admitida expresamente para el tratamiento de datos personales.
- Se incorporan parámetros especiales para el tratamiento de datos de niñas, niños y adolescentes, resaltando la importancia que para ello tiene el respeto a la Convención sobre los Derechos del Niño.
- Se aclara que el consentimiento del titular del datos, los mecanismos de autorregulación vinculante y las cláusulas contractuales que contengan mecanismos de protección de datos acordes con las disposiciones de la ley son bases legales para realizar transferencias internacionales.
- Se crea la figura del delegado de protección de datos cuya designación será obligatoria para algunos casos específicamente definidos en la ley, a saber: tratamiento de datos por parte de autoridades u organismos públicos, tratamiento de datos sensibles como parte de la actividad principal del responsable o encargado del tratamiento, y tratamiento de datos a gran escala.
- Se aumenta el monto máximo de las multas. Asimismo, se contemplan otras sanciones por incumplimiento de la ley, como la suspensión o cierre temporal de actividades relacionadas con el tratamiento de datos e incluso el cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.

Sobre algunos de estos puntos, cabe hacer una aclaración. En primer lugar, debe destacarse que el proyecto, al igual que el Reglamento (UE) 2016/679, resalta la importancia de garantizar el ejercicio de la libertad de expresión, siendo éste un valor fundamental en una sociedad democrática. En este sentido, se establece ya desde el artículo 3 que la ley no podrá afectar al tratamiento de datos que realicen los medios de comunicación en el ejercicio de la libertad de expresión.

Esta regla que fija el proyecto de ley tiene implicancias en el derecho de supresión de datos personales, derecho que el Reglamento (UE) 2016/679 parece asimilar al derecho al olvido. Como es sabido, el denominado "derecho al olvido" ha traído muchas discusiones teóricas y críticas sobre su alcance dado que una deficiente implementación podría devenir en violaciones a otros derechos fundamentales, como la libertad de expresión o el acceso a la información pública. Por este motivo, el proyecto, si bien reconoce este derecho bajo la figura del derecho de supresión, aclara especialmente que este derecho no procede cuando el tratamiento de datos persiga un fin público o sea necesario para ejercer el derecho a la libertad de expresión e información.

En segundo lugar, es relevante hacer referencia a los cambios que trae aparejados la normativa proyectada en materia de transferencias internacionales. Bajo la ley vigente, en principio, se prohíbe la transferencia de datos personales a países que no proporcionen un nivel adecuado de protección.[17] La ley luego prevé algunas excepciones a esta regla[18], pero la práctica ha demostrado que son limitadas y muy pocas aplican al sector privado[19].

Si bien se puede sostener que la rigidez de estas normas fue flexibilizada por el Decreto Reglamentario al incluir al consentimiento del titular de los datos como una base legal para la transferencia internacional y también, aunque de forma no muy clara, a los sistemas de autorregulación y a las cláusulas contractuales,[20] la DNPDP estimó conveniente aclarar esta situación en el proyecto.

12 *Al momento de la elaboración del anteproyecto, la DNPDP era la autoridad de control de la Ley Nº 25.326. Posteriormente a la publicación de la segunda versión del anteproyecto, éste fue sometido a la revisión del Poder Ejecutivo nacional. Durante ese proceso, mediante una modificación normativa del diseño institucional, se designó a la AAIP como nueva autoridad de control, tal como se consigna en la nota al pie 8. En virtud de este cambio normativo, la autoridad de control se reconstituyó como un ente autárquico con autonomía funcional en el ámbito del Poder Ejecutivo nacional. De esta manera, no solo se cumplió con lo postulado durante el proceso de consulta, sino también con el estándar de independencia exigido por el Reglamento (UE) 2016/679.*

13 *Por ejemplo, se recibieron documentos de la Asociación de Bancos Argentinos (ADEBA), la Asociación de Bancos de la Argentina (ABA), la Asociación de Marketing Directo e Interactivo de Argentina (AMDIA), la Cámara Argentina de Comercio Electrónico (CACE), la Cámara Argentina de Internet (CABASE), la Cámara de Comercio de los Estados Unidos de América en la Argentina (AmCham Argentina), Information Technology Industry Council(ITI), Telecom, de algunas organizaciones de la sociedad civil y de varios académicos.*

14 *Para acceder al documento, ingrese al siguiente sitio: https://www.argentina.gob.ar/sites/default/files/anteproyecto_reforma_ley_proteccion_de_los_datos_personales_nueva_version.pdf, última consulta: 18/06/2019.*

15 *Los artículos que fueron objeto de modificaciones sustanciales fueron aquellos referidos a la prestación de servicios de información crediticia y los que conforman el Capítulo 8, atinentes a la autoridad de control.*

16 *Para acceder al documento, ingrese al siguiente sitio: https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf, última consulta: 18/06/2019.*

17 *Artículo 12 inc. 1 de la Ley Nº 25.326.*

18 *Artículo 12 inc. 2 de la Ley Nº 25.326.*

19 *Palazzi, Pablo A., Transferencia internacional de datos personales. Nueva regulación de la Dirección Nacional de Protección de Datos Personales, La Ley, Tomo La Ley 2017-A.*

20 *A pesar de que esta situación fue medianamente aclarada con el dictado de la Disposición Nº 60 – E/2016, la DNPDP consideró igualmente necesario dejar sentadas de forma más clara las bases legales para realizar una transferencia internacional en el proyecto.*

Por ello el proyecto concentra en un artículo todas las bases legales para realizar transferencias internacionales que actualmente se encuentran dispersas entre la Ley N° 25.326, su Decreto Reglamentario y la Disposición Nº 60 – E/2016[21]. Además recepta algunas condiciones adicionales, a saber: a) cuando sea efectuada a cualquier sociedad del mismo grupo económico del responsable del tratamiento, en tanto los datos personales sean utilizados para finalidades que no sean incompatibles con las que originaron su recolección; b) cuando sea necesaria en virtud de un contrato celebrado o por celebrar en interés inequívoco del titular de los datos, por el responsable del tratamiento y un tercero; c) cuando sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia; d) cuando sea necesaria para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; y e) cuando sea necesaria para el mantenimiento o cumplimiento de una relación jurídica entre el responsable del tratamiento y el titular de los datos.

El objetivo que persigue este cambio en materia de transferencias internacionales es que se brinde mayor claridad al sistema, para que ya no existan grises o contradicciones como existen hoy entre la ley y la reglamentación, y a su vez se promueva un escenario más apto para la inversión y la innovación en la Argentina, sin que por ello se deje de proteger la privacidad de las personas.

Demás está decir que lo expresado hasta aquí son apenas trazos muy gruesos de algunos de los aspectos más relevantes de la normativa proyectada. Su lectura y análisis darán comprensión a cabalidad del profundo cambio que se propone.

---

21 *La Disposición Nº 60 – E/2016 de la DNPDP presenta una lista de los países que son considerados adecuados bajo la legislación argentina, sujeta a futuras modificaciones. A su vez, presenta dos contratos modelo a ser utilizados por las partes que deseen transferir datos personales a países no adecuados. Estos modelos pueden ser útiles para comprender a qué refiere el proyecto cuando establece que las cláusulas contractuales deberán ser "acordes a las disposiciones previstas en la ley".*

# ASIA'S DATA PRIVACY DILEMMAS, 2014-19:

## *National divergences, cross-border gridlock*


GRAHAM
**GREENLEAF**

*Es Profesor de Derecho y Sistemas de Información en la UNSW Australia en Sydney, donde realiza investigación sobre las relaciones entre la tecnología y el derecho. Ha trabajado en protección de datos desde mediados de los años ´70. Su libro de 2014, "Asian Data Privacy Laws" analiza las leyes de privacidad en los 28 países asiáticos. Es Editor para Asia-Pacífico de "Privacy Laws & Business International Report", y publica encuestas bianuales de las leyes de privacidad en el mundo. Ha completado numerosas consultorías para la Comisión Europea en privacidad de datos en países de Asia-Pacífico. En 2018 fue invitado a participar en Bruselas, en el lanzamiento del Reglamento General de Protección de Datos (RGPD) de la UE. Es miembro del Consejo Consultivo del Convenio 108+ y del Grupo Experto de Lineamientos de la OCDE.*


## SUMARIO


**RESUMEN**

**ABSTRACT**

**INTRODUCTION: A HALF-DECADE OF CHANGE**

- TAKE-UP OF DATA PRIVACY LAWS – REGIONAL COMPARISON

**NATIONAL DATA PRIVACY LAWS IN ASIA 2014-19**

- NEW DATA PRIVACY LAWS – ONLY ONE 'POST-GDPR'
  - *THAILAND – CAN A JUNTA DELIVER ADEQUACY?*
  - *CHINA – AN ALTERNATIVE MODEL?*
- REVISED LAWS
  - *JAPAN – THE ILLUSION OR REALITY OF ADEQUACY?*
  - *KOREA – A DIFFERENT PATH TO ADEQUACY*
- BILLS IN PROGRESS – THE GDPR MEETS DATA LOCALISATION
  - *INDONESIA – DRAFTS WITH STRONG GDPR INFLUENCES*
  - *INDIA – AFTER PUTTASWAMY, WHERE IS THE BILL?*
- PROGRESS IN OTHER ASIAN JURISDICTIONS
  - *NORTH-EAST ASIA – LITTLE CHANGE IN TAIWAN AND MACAU*
  - *HONG KONG SAR – DEFICITS IN POWERS, BUT TRANSPARENCY CONTINUES*
  - *SOUTH-EAST ASIA (ASEAN) – THE PHILIPPINES (ENERGETIC) AND MALAYSIA (INACTIVE)*
  - *VIETNAM – LIGHTER DATA LOCALISATION*
  - *SINGAPORE – ENFORCEMENT AND RESISTANCE*
  - *SOUTH ASIA (SAARC) – LITTLE TO SEE*
  - *BHUTAN – DATA PRIVACY AS GROSS NATIONAL HAPPINESS*

**INTERNATIONAL STANDARDS, DATA EXPORTS AND LOCALISATION**

- *ASIA'S LACK OF REGIONAL STANDARDS*
- *THE G20'S 'OSAKA TRACK', THE WTO AND BRICS DISSENT*
- *THE CPTPP LIMITS LOCALISATION AND EXPORT RESTRICTIONS*
- *APEC-CBPRS' CONTINUING FAILURE*
- *WILL THE EU'S 'ADEQUATE' LIST EXPAND IN ASIA?*
- *OTHER 'APPROPRIATE SAFEGUARDS' FOR TRANSFERS FROM THE EU (AND ELSEWHERE)*

**CONCLUSIONS: NO GRAND SOLUTIONS LIKELY**

- *NATIONAL LAWS AND PRACTICES – UNEVEN EMULATION AND 'GDPR CREEP'*
- *INTERNATIONAL COMMITMENTS – GRIDLOCK AD INFINITUM?*
- *DATA PRIVACY DILEMMAS IN ASIA*

## RESUMEN

En 2014, trece de los 28 países de Asia sancionaron leyes de protección de datos. Todos ellos implementaron los diez principios mínimos (Primera generación) para una ley de protección de datos que se ha consolidado en los instrumentos de la OCDE y el Consejo de Europa de 1980/81. También implementaron poco más de la mitad de los adicionales diez principios (Segunda generación) que distinguieron la Directiva de protección de datos de la UE de 1995. En relación de flujos transfronterizos, una variedad de instrumentos pelean por la primacía.

Cinco años después, mucho ha cambiado en Asia, a pesar de que el número de países con leyes de protección de datos se ha elevado solo a 15 (agregando China y Bhutan). Leyes actualizadas incluyen aquellas de Tailandia, la primera ley con una fuerte influencia del RGPD, y en Japón y Corea, afectados por su apuesta a una adecuación a la UE. India e Indonesia tienen leyes con fuerte influencia del RGPD, pero -como China- también poseen fuertes compromisos con la localización de los datos. Este artículo releva todos estos desarrollos nacionales en término de cuáles son los nuevos modelos para leyes de protección de datos que están emergiendo en Asia.

El resultado global de los desarrollos nacionales de este lustro es que la media de las leyes asiáticas ha virado de la inclusión de 5/10 principios de "segunda generación" o principios "europeos", a 6/10. Mas aún, hay al menos 40 instancias de principios de "tercera generación" tipificados por innovaciones del RGPD de la UE que han sido adoptados por las leyes asiáticas, el más popular de los cuáles es el conjunto de requerimientos para la notificación de vulneraciones de seguridad. La sanción de leyes influenciadas por el RGPD en India e Indonesia fortalecerá estas tendencias. No obstante, la ausencia de estándar regionales significativos en Asia (en comparación con África o América Latina) implica que la adopción de principios particulares no es uniforme, y la "convergencia" no es para ésta un concepto muy valioso.

A pesar de que numerosos instrumentos internacionales y sus efectos son influyentes en Asia (el acuerdo de libre comercio CPTPP, APEC-CBRs, Convenio 108+, y la adecuación del RGPD), ninguno de estos se ha convertido en dominante, o no parece que vaya a serlo. Como resultado, los países individualmente podrán optar por involucrarse con ellos en función de sus intereses nacionales y otras obligaciones. Este nuevo elemento de las leyes de localización de datos es influyente en varios países, está distorsionando alianzas tradicionales, y está causando el surgimiento de nuevos modelos para leyes de protección de datos, particularmente aquellos que incluyen la localización de datos.


Thanks to Privacy Laws & Business International Report for publishing many of the articles cited herein, to Oxford University Press for publishing Asian Data Privacy Laws: Trade and Human Rights Perspectives (2014), and to Jill Matthews for editing. Responsibility for all content remains with the author.


## ABSTRACT

In 2014, thirteen of the 28 countries in Asia[1] had enacted data privacy laws. They all implemented the ten minimum ('1st generation') principles for a data protection law which had consolidated in the 1980/81 OECD and Council of Europe instruments. They also implemented a little over half of the additional ten '2nd generation' principles which distinguished the 1995 EU data protection Directive. In relation to cross-border transfers, a variety of instruments contended for primacy.

Five years later, much has changed in Asia, although the number of countries with data privacy laws has only risen to 15 (adding China and Bhutan). Amended laws include those in Thailand, the first law with strong GDPR influences, and in Japan and Korea, affected by their bids for EU adequacy. India and Indonesia have Bills with strong GDPR influences, but – like China – also strong commitments to data localization. This article assesses all these national developments in terms of whether new models for Asian data privacy laws are emerging.

The overall result of this half-decade of national developments is that the average of Asian laws has moved from the inclusion of 5/10 '2nd generation' or 'European' principles, to 6/10. Furthermore, there are at least 40 instances of '3rd generation' principles typified by the innovations of the EU's GDPR being adopted in Asian laws, the most popular being data breach notification requirements. Enactment of GDPR-influenced laws in India and Indonesia will strengthen these trends. However, the absence of any significant regional standards in Asia (in comparison with Africa or Latin America) means that the adoption of particular principles is not uniform, and 'convergence' is not a very valuable concept in Asia.


1 *From Japan to Afghanistan going E-W and China to Timor Leste going N-S.*





Although numerous international instruments and their effects are influential in Asia (the CPTPP free trade agreement, APEC-CBPRs, Convention 108+, and GDPR adequacy), none of these have become dominant, or are likely to. As a result, individual countries will choose to engage with them as suits their national interests and other obligations.

The new element of data localization laws is influential in quite a few countries, is disrupting traditional alliances, and is causing new models for data privacy laws to emerge, particularly those including data localization.

---

## INTRODUCTION: A HALF-DECADE OF CHANGE

Five years ago in 2014, 13 of the 28 countries in Asia[2] had enacted data privacy laws. My overall conclusion about the standards adopted by those laws[3] was that, with minor exceptions, they all implemented the ten minimum ('1st generation') principles for a data protection law found in the 1980/81 OECD privacy Guidelines and Council of Europe data protection Convention 108. On average, they also implemented a little over half of the additional ten '2nd generation' principles which distinguished the 1995 EU data protection Directive (and in most cases the 2001 amending protocol to Convention 108). Asia's laws had thus advanced from the 1980s' minimum standards 'half way' toward the higher standards of the Directive.[4] This was less than the average standard of data privacy laws outside Europe, as assessed in 2012, which was enactment of 6.9 of the 10 '2nd generation' principles, largely because European influences on many Latin American and African countries were stronger than in Asia.[5]

In relation to enforcement, using the standards of 'responsive regulation' theory,[6] my conclusion was that South Korea and the Macau SAR had 'the widest range of enforcement mechanisms', and made effective use of them.[7] Hong Kong, while lacking legislative enforcement mechanisms until 2012, compensated by very vigorous enforcement activity. The laws in some countries like Singapore, Malaysia and the Philippines were too recent for assessment. There was little credible evidence of enforcement in Japan, Taiwan and India. Related to this, the previous 'Asian civil law model' of Ministry-based enforcement was now limited to these three countries of 'regulatory failure', plus Vietnam, and was in decline. The alternative model of a specialist data protection authority (DPA), though not necessarily an independent one, had been adopted by the newest Asian laws (Singapore, Malaysia and the Philippines), and the other earlier laws.

In mid-2019, there are now 15 Asian countries with data privacy laws meeting minimum standards, with China and Bhutan being the new entrants, plus Thailand having enacted a completely new law to replace an old and useless one. Japan has also enacted a major revision of its law, Korea various lesser revisions (and one ongoing), and there are smaller changes in other countries. Very significant wholesale replacement laws are in the process of enactment in India and Indonesia. It is therefore an opportune time to review the conclusions reached in my 2014 book, in light of a further half-decade. The details of these changes to national laws and practices are the subject of the first half of this article. References to specific sections of legislation may be found in the articles cited herein, but are generally not included in this survey.

Such a review must also take into account the multilateral instruments (treaties, declarations, guidelines etc) that affect the content and interaction of Asian data privacy laws, particularly on the crucial topic of data export restrictions, and its newly-recognised cousin, data localisation. In 2014 I dismissed the idea of a regional data privacy treaty in Asia as unrealistic, and likewise any idea of a new treaty originating from the UN, whereas the 'globalisation' of Convention 108 was seen as more realistic (but with no attempt to suggest what Asian countries might accede to it). 'Interoperability' between EU standards and APEC-CBPRs was described as 'an unrealistic goal'.[8] The second part of the article reviews changes in these multilateral arrangements over the past five years.

2 *From Japan to Afghanistan going E-W and China to Timor Leste going N-S.*

3 *G. Greenleaf Asian Data Privacy Laws: Trade and Human Rights Perspectives (OUP, 2014, paperback 2017), pp. 502-3 summary, and preceding chapter.*

4 *The 'principles' included in these ten include the Directive's requirements of and independent DPA, and access to judicial remedies, more accurately described as 'standards' than 'principles'.*

5 *The 'principles' included in these ten include the Directive's requirements of and independent DPA, and access to judicial remedies, more accurately described as 'standards' than 'principles'.*

6 *Greenleaf, Asian Data Privacy Laws, pp. 62-75.*

7 *Greenleaf, Asian Data Privacy Laws, pp. 526-7, and preceding chapter.*

8 *Greenleaf, Asian Data Privacy Laws, pp. 550-1.*

### TAKE-UP OF DATA PRIVACY LAWS – REGIONAL COMPARISON

The following Table[9] provides a regional analysis of the 135 countries that now have data privacy laws.[10] Of the total of 231 countries, the 135 with data privacy laws constitute 58%, and since about 2014 (then 115 countries with laws) the majority of countries have had such laws. Asia, now with 15 of 28 countries (54%) is close to the global average. Of the larger regions (20 countries or more) outside Europe, Latin America (55%) is much the same as Asia, and Africa (46%) is next. Data privacy laws are indeed global: the only region with less that 40% of countries having them is the Pacific Islands, with none.

| Region | Countries | DP Laws | % |
|---|---|---|---|
| Africa | 58 | 27 | 46% |
| Caribbean | 29 | 12 | 41% |
| Other European | 29 | 26 | 90% |
| EU | 28 | 28 | 100% |
| Asia | 28 | 15 | 54% |
| Latin America | 22 | 12 | 55% |
| Middle East | 14 | 8 | 57% |
| Pacific Islands | 13 | 0 | 0% |
| Central Asia | 6 | 3 | 50% |
| N. America | 2 | 2 | 100% |
| Australasia | 2 | 2 | 100% |
| TOTAL | 231 | 135 | 58% |

9 *In the Table, the whole number of countries in a region is compared with the number of countries with data privacy laws, and the percentage result then shown. The number of 'countries per region' is based, with modifications to accommodate my division into regions, on Internet World Stats, Country List <http://www.internetworldstats.com/list1.htm#geo>. The total of 231 countries includes non-UN members, and sub-national regions with distinct top-level domains (such as Hong Kong or Jersey), and therefore is at least as extensive as the criteria I use for a 'country'. All such lists commence from slightly differing assumptions.*

10 *For 135 countries, Uganda, Nigeria and Kyrgyzstan must be added to the 132 countries with laws listed in G. Greenleaf 'Global Tables of Data Privacy Laws and Bills (6th Ed January 2019)' (2019) Supplement to 157 Privacy Laws & Business International Report (PLBIR) 16 pgs <https://ssrn.com/abstract=3380794>.*

## NATIONAL DATA PRIVACY LAWS IN ASIA 2014-19

Although in the last five years Asia has not experienced the speed of change of data privacy laws of the preceding five years, there has still been substantial change, taking into account new laws, revised laws, enforcement changes, and particularly Bills in progress.

### NEW DATA PRIVACY LAWS – ONLY ONE 'POST-GDPR'

The most significant legislative changes in Asia since 2014 are that Thailand and China now have much stronger data privacy laws, with Thailand significantly influenced by the EU's 'GDPR model', and China developing what may be an alternative model of its own.

***Thailand – Can a junta deliver adequacy?***

A military coup in 2014 imposed a junta government, which in February 2019 enacted a data privacy law to replace an old and ineffective law applying only to the public sector. This occurred three weeks before Thailand's first general elections since the coup. A military-backed party now leads a coalition government, including a Prime Minister and Cabinet members from the previous military government, and a largely appointed upper house.

Thailand's *Personal Data Protection Act* (PDPA) will come into force on 28 May 2020, a year after it was gazetted. It is based on a GDPR-influenced Bill proposed by the junta government in May 2018,[11] but it has many differences from that Bill. Only some of the notable points on which the Act differs from that 2018 Bill, which take a different approach to the EU's GDPR, or are significant internationally, are discussed here.

The PDPA is a comprehensive Act, unlike the private-sector-only laws in the rest of ASEAN (Philippines excepted). It exempts few parts of the private sector (credit reporting has a separate law) or public sector (courts, legislature, security and law enforcement), but further exemptions can be made by decree.

The PDPA has some stronger principles influenced by the GDPR, including the data subject's right to data portability; the right to object; data breach notifications to both the data subject and the DPA; minimal collection requirements; data retention restrictions; and strong consent requirements. Genetic and biometric data have been added to the categories of 'sensitive personal data', consistent with the GDPR. Appointment of data protection officers (DPOs) will be required, with exceptions for a 'small sized business' (criteria to be specified by PDPC). Some notable aspects of the GDPR, such as the right to be forgotten, and protections in relation to automated processing, are not included.

11 *The 2018 Bill is examined in G. Greenleaf and A. Suriyawongkul 'Thailand's draft data protection Bill: Many strengths, too many uncertainties' (2018) 153 Privacy Laws & Business International Report, 23-2*

The PDPA will have extra-territorial effect (similar to the GDPR) in relation to marketing to, or monitoring of, persons in Thailand. Processing outside Thailand by a controller or processor located in Thailand is also covered.

A Personal Data Protection Committee (PDPC) is established as the primary body to administer the law, but it has no legislatively guaranteed independence. There is also an Office of the PDPC, which is a government department. Expert Committees will determine complaints. Many breaches of the PDPA can result in administrative fines, for which the highest maximum amount is 3 million baht (approx. US$100K). This is now a low maximum by international standards, but may still be a deterrent to some local businesses. Data subjects have a right to seek compensation from a court for any breaches of the Act (and with few defences provided), and the court may impose additional compensation up to double the original amount (ie 'triple damages').

Data exports from Thailand can occur to countries which have an 'adequate level of protection', as determined by the PDPC. However, 'adequate' is to be determined by criteria set by the PDPC, so it cannot be assumed that it will mean the same as it does in the EU. Additional provisions allowing data exports include a form of Binding Corporate Rules (BCRs), and undefined 'appropriate safeguards', both to be based on standards set by PDPC.

The main significance of the Thai law is that it is the first explicitly 'GDPR-based' law to yet be enacted in Asia. However, there are GDPR-influenced draft Bills in India and Indonesia.

***China – An alternative model?***

From 2011-14 China enacted five main largely consistent laws and regulations dealing with data privacy, at various levels in its complex legislative hierarchy. A number of omissions (particularly lack of subject access) meant that they were close to, but did not quite comprise, the minimum requirements for a data privacy law.[12]

12 *Greenleaf Asian Data Privacy Laws (2014), pp. 225-6, and preceding chapter.*

The data privacy provisions of China's *Cybersecurity Law* of 2016 were China's most comprehensive and broadly applicable set of data privacy principles up to 2017, going beyond the previous laws.[13] However, that law was still missing explicit user access rights, requirements on data quality and special provisions for sensitive data, as well as having no specialist data protection authority (DPA), and being of uncertain scope in relation to the public sector. The omission (or ambiguity) of the first of these – explicit subject access rights – meant that China's law as a whole did not yet include one of the most fundamental elements of a data privacy law. However, these doubts are now sufficiently resolved. The *E-Commerce Law* of 2018 (in force 1 January 2019), a law of China's second highest legislative body, is both of wide scope within the private sector, and explicitly provides that users may make 'inquiries' concerning their information.[14] Since then, there have been two further significant developments.

The recommended standard entitled *Information Security Techniques - Personal Information Security Specification* promulgated by China's National Standardization Committee, and effective 1 May 2018[15] is an important step forward in the evolution of China's data privacy protections because of its comprehensive scope; the potential breadth of its definition of 'personal information' (possibly broader than any other Chinese laws, or European laws); inclusion for the first time of extra protections for 'personal sensitive information'; explicit inclusion of a right access; collection minimization, and appeals against automated processing. The suggested obligations in relation to subject access, minimum collection of data, and restrictions on automated processing, are not found in other (enforceable) laws. Although only a 'standard', businesses must think twice before failing to observe a recommended standard, and it is probably realistic to consider the requirements of the 'standard' to already be part of China's data privacy law.

13 *G Greenleaf and S Livingston 'China's Cybersecurity Law – also a data privacy law?' (2016) 144 Privacy Laws & Business International Report, 1-7 <https://ssrn.com/abstract=2958658>*

14 *E-Commerce Law of the People's Republic of China (Standing Committee of the National People's Congress, 31 August 2018) Art 24 "Where e-business operators receive applications for inquiries, modification, or deletion of user information, they shall promptly make the inquiry, or modify or delete the user information, after identity verification' (Source: China Law Translate).*

15 *G. Greenleaf and S. Livingston, 'China's Personal Information Standard: The Long March to a Privacy Law' (2017) 150 Privacy Laws & Business International Report 25-28. < https://ssrn.com/abstract=3128593>*

China has not yet finished its data privacy legislation agenda. A 'Personal Information Protection Law' and a 'Data Security Law', are each listed separately on the work program for the current National People's Congress (NPC).[16] They are 'Class I Projects: Draft laws for which the conditions are relatively mature and which are planned to be submitted for deliberation during the term (69 projects)', and should 'in principle' be completed within the 13th NPC's term, which will end in March 2023.' It may turn out that the above 'standard' is a test-bed for what will eventually be China's comprehensive data privacy law.

It must always be borne in mind that China's data protection laws co-exist with the Social Credit System (SCS), which is emerging as the world's most pervasive and potentially totalitarian surveillance system, but as yet is far from complete.[17] The relationship between the SCS and data privacy laws is unclear.

Two years after the *Cybersecurity Law* came into force, China is still finalising the data export and data localisation rules based on that law. On June 13, 2019, the Cyberspace Administration of China (CAC) issued, for a month's consultation, the draft *Measures on Security Assessment of the Cross-border Transfer of Personal Information* ('draft Measure on Security Assessment').[18] This second iteration of these Measures imposes them more broadly than before: 'all network operators are obliged to undergo the security assessment process before they may transfer personal information collected in the course of their operations in China to recipients outside China',[19] not only Critical Information Infrastructure operators. There are numerous requirements for the security assessment, and then further rules concerning notice to, opt-in and opt-out by data subjects, and assumption of liability by exporters. These requirements have compared with the EU's SCCs and BCRs, but the security assessment aspect makes them very different.[20]

The general data localisation provisions of the *Cybersecurity Law* have been in force since 2017, providing that all personal data and 'important data' held by 'critical information infrastructure' operators (CIIOs) must be stored in China.[21] The Law does not itself define 'critical information infrastructure', so its meaning has to be inferred from other documents.[22] However, because implementing regulations for the data localisation aspects are not included in the 2019 version of the draft *Measures on Security Assessment*, there is still uncertainty about what China's localization policies require.

There are many respects in which China's data privacy laws could be emulated (and promoted by China) as a model for data privacy regulation which is an alternative to the 'western' (more accurately 'European') model: (i) inclusion of enforceable principles which at least meet the '1st generation' criteria of the OECD Guidelines and Convention 108 (1980/81 versions); (ii) inclusion of strong data localisation requirements and data export restrictions which are more oriented to protection of State or national interests than to protection of individual citizens; (iii) the absence of a central (let alone independent) data protection authority (DPA); (iv) data privacy laws to be subordinate to data surveillance laws (such as those governing the Social Credit System); (v) optional whether the public sector is covered. Such an 'authoritarian model' of data privacy protection may have an appeal outside China, underwritten by China's economic weight and success.

16 *NPC Observer <https://npcobserver.com/2018/09/07/translation-13th-npc-standing-committee-five-year-legislative-plan/>*

17 *For an authoritative assessment, see R. Creemers 'China's Social Credit System: An Evolving Practice of Control' (May 9, 2018) <https://ssrn.com/abstract=3175792 or http://dx.doi.org/10.2139/ssrn.3175792>; also Y. Chen and A. Cheung 'The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System' (2017) Vol. 12, No. 2, The Journal of Comparative Law 356-378 < https://ssrn.com/abstract=2992537>; for recent information, K. Needham 'Millions are on the move in China, and Big Data is watching' Sydney Morning Herald, 6 February 2019 <https://www.smh.com.au/world/asia/millions-are-on-the-move-in-china-and-big-data-is-watching-20190204-p50vlf.html>*

18 *Draft Measure on Security Assessment (China), unofficial English translation <https://www.insideprivacy.com/wp-content/uploads/sites/6/2019/06/Measures-for-Security-Assessment-of-the-Cross-Border-Transfer-of-Personal-Information_bilingual.pdf>*

19 *Yan Luo, Zhijing Yu and Nicholas Shepherd 'China Seeks Public Comments on Draft Measures related to the Cross-border Transfer of Personal Information' Inside Privacy, 13 June 2019*

20 *Yan Luo, Zhijing Yu and Nicholas Shepherd, ibid.*

21 *See for background S. Livingston and G. Greenleaf 'PRC's New Data Export Rules: 'Adequacy with Chinese Characteristics'?' (2017) 147 Privacy Laws & Business International Report 9-12; <https://ssrn.com/abstract=3026914>.*

22 *Livingston and Greenleaf 'PRC's New Data Export Rules' ibid.*





## REVISED LAWS

Japan's law has been revised, but is not of a high standard (except for Europeans), whereas Korea is taking a different path.

***Japan – The illusion or reality of adequacy?***

Japan's data privacy laws, of which the centrepiece was the Act on the Protection of Personal Information (PPIA) of 2003, were characterised by me in 2014 as 'weak and obscure', with ambiguous and low-grade principles, and no credible evidence of enforcement. 'The illusion of protection' was the chapter title.[23]

In 2015 Japan enacted reforms to bring Japan's PPIA closer to international standards, including creation of a data protection authority, the Personal Information Protection Commission (PPC), which has enforcement powers, jurisdiction over the private sector (only), and requirements to act independently. The Bill enacted was significantly stronger than was indicated by early drafts. Nevertheless, its principles had many weaknesses, including a narrow concept of 'personal information'; low standards for both change of use (allowing 'duly related' uses) and disclosure to third parties (an 'opt out' procedure); no deletion requirements; obscure provisions on access and correction; no extra protection for sensitive information; and an exemption for businesses 'considered unlikely to violate the individual's rights'.[24] The enforcement provisions are minimal, with no clear provisions for the making of complaints; PPC powers to issue administrative fines limited to about US$10,000; criminal procedures that, on past experience, will never be used; and no rights to individuals to obtain compensation from the PPC or the courts.

A significant part of the 2015 PPIA reforms were 'big data' provisions concerning use of allegedly 'anonymised' data. A new concept of 'anonymous process information' (API) was introduced, but because it follows a prescribed method of anonymisation, rather than objective criteria of non-identifiability, it was obvious that it would not be consistent with EU approaches to this topic. Although API is not 'personal information', many protective provisions similar to those applied to personal information apply to API.

The European Commission decided in January 2019 that Japan's data protection system met the GDPR art. 45 requirements for a positive adequacy decision.[25] There were a number of unusual aspects of the approaches that Japan and the EU took to finalising this decision, some of which are:[26]

- Japan's post-2015 law fell short of EU requirements in four respects which Japan's PPC (DPA) addressed by making Supplementary Rules to remedy those deficiencies.[27] However, these Rules only apply to personal data originating from the EU (thus probably primarily affecting EU citizens), and do not apply to personal data sourced from Japan, or from other foreign countries. The question of whether the concept of 'essentially equivalent' protections, as required by the GDPR and the CJEU, can be satisfied by laws which, in effect, give a lower level of protection to Japanese citizens, is not addressed in the Decision,[28] but the Commission says it is 'Japan's choice' to take this approach.[29]
- GDPR art. 45 explicitly requires 'effective and enforceable data subject rights' and 'effective judicial and administrative redress'. The EDPB states that these are 'of paramount' importance' and that infringements 'should be punished in practice' and compensation awarded.[30]

23 *Greenleaf, Asian Data Privacy Laws (2014) pp. 263-5 and the preceding Ch. 8 'Japan – The Illusion of Protection.'*

24 *For details see G. Greenleaf, Japan: Toward International Standards – Except for 'Big Data' (June 19, 2015). (2015) 135 Privacy Laws & Business International Report, 12-14 < https://ssrn.com/abstract=2649556>*

25 *[European Union] Commission Implementing Decision of 23.1.2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information < https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf >*

26 *For detailed critical analysis, see G. Greenleaf 'Japan's Proposed EU Adequacy Assessment: Substantive Issues and Procedural Hurdles' (2018) 154 Privacy Laws & Business International Report, 1, 3-8; extended online version at <https://ssrn.com/abstract=3219728>; G. Greenleaf 'Questioning 'Adequacy' (Pt I) – Japan' (2017) 150 Privacy Laws & Business International Report, 1, 6-11 <https://papers.ssrn.com/abstract_id=3096370>; G. Greenleaf 'Japan and Korea: Different Paths to EU Adequacy' (2019) 156 Privacy Laws & Business International Report, 9-11. <https://ssrn.com/abstract=3323980>.*

27 *(European) COMMISSION IMPLEMENTING DECISION of 23.1.2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information ('Japan Final Decision'), Brussels, 23.1.2019 , C(2019) 304 final; Final Decision paras. (15)-(16).*

28 *If insistence on changes which are not restricted to EU-sourced data is considered to be likely to breach the EU's obligations under GATS art. 14, the Decision could but does not state this.*

29 *Commission statement (B. Gencarelli) to the EU Partliament LIBE Committee, 26 September 2018.*

30 *See Greenleaf 'Japan's Proposed EU Adequacy Assessment' 2018, p. 7.*

Despite it being clear that enforcement and redress must be demonstrated in practice, and not only exist on paper, the Decision ignores this. It lists many examples of where the PPC or the courts can, in theory under legislative provisions, take enforcement actions, but it does not give any examples of specific penalties issued or compensation granted, either administrative or judicial.[31]

- A strong aspect of the Decision is that it makes it clear that the 'Japanese back door', which allowed personal data exports from Japan to overseas companies merely because they are certified under the APEC CBPRs scheme, has been shut in relation to any data originating from the EU, by one of the Supplementary Rules.[32] Such onward transfers now require the consent of the individual data subject in the EU, which is an improvement but still open to criticisms.[33] Under the GDPR, consent is not a basis for transfer to third countries, but is only a very constrained derogation, which the EDPB considers must remain the exception not the rule.[34]
- The Decision is very thorough in explaining where and why Japan's laws meet GDPR standards, but there remain apparent 'gaps' between the GDPR and explicit provisions of Japan's laws. These include: requirements for data protection by design and by default; data portability; mandatory DPIAs; mandatory DPOs; and de-linking ('right to be forgotten'). There is also very weak protections for automated decision-making,[35] and data breach notification requirements which are voluntary,[36] both of very limited scope. While it is clear that 'essentially equivalent' protection does not require the inclusion of every GDPR innovation, the Decision does not provide valuable criteria for assessing what is and is not required.

Unless any of matters is called into question by the CJEU in its interpretation of the GDPR, the Commission's decision disposes of them. Both the European Parliament[37] and the European Data Protection Board (EDPB),[38] in their opinions on the Commission's draft Decision, neither endorse nor reject it. On my interpretation, they each implied but did not expressly state that the Commission had failed to demonstrate the adequacy of Japan's protections. However, they accepted the inevitability of a positive adequacy Decision. The EDPB invited the Commission to review 'this adequacy finding' at least every two years, not four years, and the Commission will do so. The result is that this first adequacy Decision under the GDPR, while very valuable to the EU in demonstrating that positive decisions in relation to its largest trading partners are possible, does not appear to be a strong or clear precedent for future adequacy decisions.

***Korea – A different path to adequacy***

Korea's has a number of data privacy laws, of which the most significant are the Network Act, covering information content service providers (ICSPs), the Credit Information Act and the Personal Information Protection Act (PIPA) which covers all sectors not covered by other Acts, and has an independent DPA (the PIPC), but one without sufficient powers. Overall, these laws remain the strongest laws in Asia, and by 2014 already included (although not uniformly) many elements of the 1995 Directive and anticipated some elements of the GDPR.[39] Although some aspects of Korea's laws are still in the process of amendment for the purposes of its adequacy application to the EU (discussed below), there have also been numerous changes to strengthen enforcement provisions in Korea's data privacy laws since 2014. Only two of the most important are mentioned here.[40]

Problems caused by difficulties of obtaining proof of damage for consumers in civil damages actions following massive data spills were addressed by amendments to all the relevant laws in 2014-15. They provided that defendants may be required by a court to pay statutory damages of up to KRW 3 million (around US$3,000) to each affected user for a negligent or wilful violation of a data protection requirement that causes data loss, theft, or leakage, without the user having to prove actual damage resulting from such violation, and for punitive damages of up to three times the actual damages of the data subject ('treble damages') if the data subject can prove: (i) an intentional or grossly-negligent violation of the law by the handler; (ii) that the data subject's personal information was lost, stolen, leaked, forged, falsified or damaged due to such violation; and (iii) the actual amount of damages resulting from such a violation.[41] The PIPA amendment also added a statutory damages provision that allows a data subject to claim up to KRW 3 million (around US$3,000) in damages when the data subject can prove (i) wilful misconduct or negligence of the handler, and (ii) the fact that data subject's personal information was lost, stolen, leaked, forged, falsified or damaged because of the wilful misconduct or negligence. These provisions for statutory and punitive damages remain in advance of those required by the GDPR.

The Network Act was also amended in 2014 to provide that ICSPs may be required by the Korean Communications Commission (KCC) to pay administrative fines of up to 3% (previously 1%) of the ICSP's annual turnover for failure to obtain user consent prior to the collection and use of personal information. The Credit Information Act was similarly amended in 2015, and similar amendments to PIPA are in the legislative process. The first application of these major penalties was in relation to the 'Interpark data leak'[42] which resulted in KCC imposing a fine ('administrative surcharge') of 4.5 billion won (around US$4.5 million) on one of the largest Korean online shopping malls. Cyber criminals, allegedly associated with North Korea, fraudulently obtained personal information of 10.3 million customers, and attempted to blackmail the company for KRW 3 billion (around US$3 million). The fine was imposed for negligent failure to protect customer data, and was 60 times higher than previous fines. Korea's progressive enactment of administrative fines of up to 3% of turnover from 2014 onward was in advance of the EU, and the Interpark fine of US$4.5 million was larger than any fine in the EU prior to CNIL's fine against Google of 50 million euros in January 2019, now dwarfed by the UK ICOs proposed July 2019 fines against British Airways (£183 million) and Marriott (£99 million). This fine is also the largest in Asia, approximately five times larger than the largest Singaporean fine.

Korea is seeking an adequacy assessment from the EU, with progress being described by the European Commission as being 'at an advanced stage'.[43] Bills to comprehensively amend Korea's four main data privacy laws were introduced into Korea's National Assembly in November 2018 to advance this goal, but are not yet enacted. The key Bill is the *Partial Amendment to the Personal Information Protection Act.*[44] The Bills have three main purposes[45], each of which is discussed further here.[46]

- Korea's previously proposed scope of an adequacy decision was limited to those parts of the private sector under the 'Network Act' and the jurisdiction of the Korean Communications Commission (KCC). This was primarily because the Personal Information Protection Commission (PIPC), while independent in its decision-making, did not have any independent powers to enforce its decisions but had to rely upon enforcement by the Ministry of the Interior and Safety (MOIS). The Korean government and the European Commission agreed that this approach was too narrow to provide meaningful benefits to EU-Korean trade, from either the Korean or EU perspectives. Korea therefore proposed to make the PIPC a 'central administrative agency' under the Prime Minister, with independent authority over all situations of processing of personal information, and to transfer to it all powers and functions of the Ministry under PIPA, and of KCC under the Network Act. PIPC is also to be empowered to investigate violations and to impose administrative fines up to 3% of turnover, the power currently held by KCC

31 *Japan Final Decision ,Paras. (97)-(112).*

32 *Japan Final Decision, paras (75)-(80); see Greenleaf 2018, pp. 5-7 for reasons why this was necessary.*

33 *Greenleaf, 2018, p.6.*

34 *Greenleaf, 2018, p.6.*

35 *Japan Final Decision, paras. (93)-(94).*

36 *Japan Final Decision, paras. (57)-(59).*

37 *European Parliament, Opinion on the draft Decision concerning Japan, 13 December 2018, para. [27].*

38 *European Data Protection Board (EDPB), Opinion on the draft Decision concerning Japan, 13 December 2018, para. [30]*

39 *See Greenleaf, Asian Data Privacy Laws, Ch. 5 'South Korea – The Most Innovative Law'.*

40 *For details of many of the changes summarised in the following, see Kwang-Bae Park and Hwan-Kyoung Ko, 'Amendments to the Credit Information Act Promulgated on March 11, 2015', Lee & Ko Data Protection / Privacy Newsletter, March 2015 <http://www.leeko.com/newsl/dpp/201503/dpp1503_eng01.html>; Kwang-Bae Park and Hwan-Kyoung Ko, "Amendment to the Personal Information Protection Act Passed in the National Assembly on July 6, 2015 - Adoption of punitive damages, statutory damages provisions", Lee & Ko Data Protection / Privacy Newsletter, July 2015. <http://www.leeko.com/newsl/dpp/201507/dpp1507_eng1.html>; Kwang-Bae Park and Hwan-Kyoung Ko, "MOGAHA Announces Updated 'Standards of Personal Information Security Measures'" Lee & Ko Data Protection / Privacy Newsletter, February 2015.*

41 *PIPA (Korea), art. 39(3); Network Act (Korea), art. 32(2).*

42 *Whon-il Park 'Interpark data leak' (KoreanLII, 2017) <http://koreanlii.or.kr/w/index.php/Interpark_data_leak>.*

43 *European Commission Media Release 'Commissioner Jourová's intervention at the event "The General Data Protection Regulation one year on: Taking stock in the EU and beyond" Brussels, 13 June 2019 <http://europa.eu/rapid/press-release_SPEECH-19-2999_en.htm>*

44 *All sections quoted are from an unofficial draft translation provided by the KCC.*

45 *Kwang Bae Park et al 'Korea's Proposed Overhaul of Data Protection Laws' (156) Privacy Laws & Business International Report*

46 *All of these points are discussed in more detail, with section references to Bills, in G. Greenleaf 'Japan and Korea: different paths to EU adequacy' (2019) 156 Privacy Laws & Business International Report 9-11 <https://ssrn.com/abstract=3323980>.*

but not by PIPC. The European Commission will have to assess whether these no doubt welcome proposals will meet the GDPR's technical standards for the necessary powers and independence of a DPA. These reforms represent a considerable shift in bureaucratic power, and it still remains to be see the extent to which they will be enacted.

- Similar to Japan, Korea is now proposing to deal with aspects of 'big data' processing directly in PIPA, rather than under the 2016 'Big Data Guidelines', which had no clear legal status. The PIPA Bill distinguishes personal information, pseudonymized information and anonymized information in ways which are appear to be consistent with the GDPR. However, to accommodate 'big data' processing, the Bill provides that a controller 'may process pseudonymized information without the consent of the data subject for the purpose of statistics, scientific researches, public-interest archiving, etc.'. 'Process' includes disclosure to third parties, so this is an area of considerable privacy dangers, particularly in the breadth of meaning of 'statistics' and 'scientific research', which will raise significant issues in adequacy discussions with the EU.
- Various other provisions in the reform Bills will, if enacted, move Korea's laws closer to the GDPR. One has a 'data portability' right, and includes limits on automated decision-making. To address a perceived weaknesses in Korea's current laws concerning data exports, compared with GDPR standards, 'special provisions regarding (i) safeguards to be implemented for the cross-border transfer of personal information, (ii) restrictions on the onward transfer of personal information, [and] (iii) the designation of a local representative'.[47] Some overseas providers of information services within Korea will be required to nominate a 'domestic agent' (local representative) to carry out duties of a chief privacy officer and fulfill reporting obligations, and the overseas provider will be liable for their failures to do so. Transfer of personal data overseas will generally require the consent of the data subject, based on notifications, including of the data to be transferred, the country of the recipient, the recipient's identity, the purpose of transfer and the duration of retention of data, and the transferor must take any other protective measures required by Presidential Decree. The same restrictions purport to apply to any further onward transfers by that recipient, but whether such an exercise of extra-territorial jurisdiction will be effective is questionable.

When and to what extent these proposed reforms are enacted will have a significant effect on the nature of the EU's adequacy assessment of Korea. Although adequacy negotiations are not public, Korea's approach appears to be very different from that taken by Japan, because there is no equivalent to Japan's Supplementary Rules which apply stronger GDPR-like provisions only to EU-origin personal data but not to Japan-origin data. The Korean approach has been to strengthen its law through legislation applying to all personal data, irrespective of its source, although it is likely that Presidential Decrees will be needed to clarify some issues between Korea and the EU, once adequacy negotiations advance further. It will be very valuable to the privacy of the Korean people, and also to the future of the EU concept of adequacy, if Korea continues its inclusive approach by making such Decrees apply to all personal data, irrespective of its source, and rejects Japan's insular approach.

## BILLS IN PROGRESS – THE GDPR MEETS DATA LOCALISATION

The largest and third largest countries in Asia by population, India and Indonesia, each of which is advancing economically at a rapid rate, are likely to enact data privacy laws within the next year or two. These laws which will be comparable to that of Thailand, being laws enacted by democracies, covering both public and private sectors, with a DPA (possibly one which is independent), and with many principles influenced by the EU's GDPR, but also with data localisation provisions. If and when enacted, these laws will change the landscape of data privacy in Asia.

### *Indonesia – Drafts with strong GDPR influences*

Indonesia already has a data privacy law which meets minimum standards, partly from a pre-2014 law and regulation which constituted 'a short enforceable privacy code',[48] and significantly expanded into a minimum standards data privacy law by a regulation in 2016.[49] However, these laws remain largely unenforced, mainly because there is no data protection authority to oversee them. Various branches of the Indonesian government have been drafting a comprehensive new law since 2015 or earlier. The Minister of Communication and Informatics (MOCI) (Kementerian Komunikasi dan Informatika (Kominfo) in Bahasa) has lead responsibility for the drafting of a comprehensive Data Protection Bill, in consultation with other government bodies. An internal government version (April 2018) is the basis of the following summary,[50] but the final version will inevitably differ from any drafts.

The main point to be made is that the draft Bill has many strengths, when compared with the GDPR as a global high standard. GDPR-compatibility is one of the Indonesian government's objectives. The Bill provides comprehensive coverage of both private and public sectors, and of all persons in Indonesia. There is some extra-territorial coverage (but not based on GDPR criteria), relating to acts outside Indonesia which have consequences in Indonesia, or harm Indonesia's national interests. There are few exemptions from the whole Act, with most exceptions only from specific principles, and no general exemption for publicly available information.

The principles included are extensive, covering all basic principles plus the following: a vague right to request limitation of processing; opt-in (consent) required for both pseudonymous processing and direct marketing; and data breach notification to individuals required. 'Specific' (or sensitive) personal data includes the conventional categories (excluding religious beliefs), plus genetics and biometrics.

A Commission (DPA) is established to administer the law, responsible directly to the President. It may investigate and adjudicate on infringements; to conduct mediation between parties, with agreed results of mediation being enforceable. This approach of initial mediation by Commission members, and if that fails, arbitration, with a right of either party to take the dispute to a court, is similar to South Korea.

The DPA may impose administrative penalty sanctions of at least US$75,000 (1BN rupiah), and up to 25 times as much (25 BN rupiah). Compensation claims may be made to a court, or to the Commission, for any infringements. Criminal offences apply to many breaches of the Act, the most severe with potential sentences of 10 years gaol.

Personal data transfers outside Indonesia may be justified in various ways: the consent of the data subject; or the law of the recipient country providing 'an equal or higher level of protection' than Indonesia's; or based on contract or international agreements; or an exemption from the Commission. The Commission may determine a White List based on strength of foreign laws.

On the other hand, there are many apparent limitations of the Bill, when compared with the GDPR (although some may result from inadequate translation). There is no automatic destruction of personal data once the purpose of collection is completed, it must be requested. The Commission does not appear to have legislatively guaranteed independence or tenure (but perhaps this may arise otherwise under Indonesian law). Many new GDPR principles do not appear to be included, such as: separate obligations imposed on processors; requirements for Data Protection Officers (DPOs); Data Protection Impact Assessments (DPIAs); data portability; and a right to have human review of automated decisions. Indonesia already has a version of the 'right to be forgotten' from a 2016 amendment, but its implementation depends on regulations yet to be made (and is otherwise left to the Courts). It is not stated in this Bill.

Despite these limitations (some of which may be resolved by translation clarifications), my initial overall assessment is that a Bill like this, if enacted, would be one of the stronger laws in Asia, with standards much higher than the minimum standards for a data privacy law, placing Indonesia among the Asian counties with the strongest GDPR influences.

Current data export restrictions in Indonesia are complex and obscure.[51] However, there are several

47 *Park et al, cited above.*

48 *G. Greenleaf Asian Data Privacy Laws (2014), pp. 374-388, concerning Article 26 of Law No 11 of 2008 concerning Electronic Information and Transactions (Law 11/2008) and Government Regulation No 82 of 2012 on the Implementation of the Electronic Transactions and Information Law (GR 82/2012)*

49 *Regulation No 20 of 2016 concerning Personal Data Protection in Electronic Systems (MCI 20/2016), an implementing measure mandated by GR 82/2012, added considerable detail to both previous laws, and provides a two-year transition period for full compliance (ie to 1 December 2018). ; see A. A. Rahman 'Indonesia to Introduce Personal Data Protection Rules in Electronic Systems' (2016) <https://andinadityarahman.com/indonesia-to-introduce-personal-data-protection-rules-in-electronic-systems/>; More detailed version: 'Indonesia Enacts Personal Data Regulation' (2017) 145 Privacy Laws & Business International Report 1.*

50 *The government subsequently released another, less developed, version for public discussion – see Baker & McKenzie 'Indonesia: Government Pushes Draft Data Protection Law' Global Compliance News May 18 2018 <https://globalcompliancenews.com/indonesia-draft-data-protection-law-20180518/> .*

51 *J. P. Kusumah and D. Kobrata Jurisdictional Report – Indonesia in C. Girot (Ed.) Regulation of Cross-Border Transfers of Personal Data in Asia (ABLI, 2018), paras. 19-20, 30-39, and 61 <https://abli.asia/PUBLICATIONS/Regulation_of_Cross-border_Transfers_of_Personal_Data_in_Asia>.*

Indonesian regulations already requiring 'data localisation', in the following areas:

- *Electronic system providers (ESPs) offering public services* – Data centres/recovery centres must be located in Indonesia, but provided a copy of the data is kept in Indonesia, it does not appear that there is a prohibition on a copy being transferred abroad. The question of what is a 'public service' is complex.[52] These provisions have 'already been used to request a major foreign company to establish its data centre in Indonesia' and 'it appears that the data localisation requirement can apply to foreign entities if the processing or storing of personal data by the foreign entity is considered to have legal implication within Indonesian jurisdiction and/or to have legal implications outside Indonesian jurisdiction but harms the national interest'.[53]
- *ESPs in the financial sector* – All ESPs in the financial sector are required to store in Indonesia all transaction data (in effect, any action with legal consequences made by using a computer, computer network and/or other electronic media).[54]
- *Data centres of banks and insurers* – Separately from questions of electronic transactions, banks must locate their data centres and disaster recovery centres in Indonesia, for all data. Similar requirements apply to insurance, but only for specified types of data. Applications can be made for exceptions.[55]

Although Indonesia has data localisation laws, as do China, Vietnam and India (next discussed), each of these countries' approaches to data localisation is different, as will be discussed in the conclusions.

***India – After Puttaswamy, where is the Bill?***

At present, India's data protection law is based on an incoherent and largely ignored set of Rules under s43A of the *Information Technology Act*, as amended in 2011. It is probably Asia's weakest data privacy law, from the perspective of citizens' rights. Two applications by India to the EU for a positive adequacy assessment, before and after the 2011 amendments, were unsuccessful, as they should have been. India attempted to demand 'data secure status' as part of EU trade negotiations but was also rebuffed. Various reform Bills failed to proceed.[56]

Since 24 August 2017, the new starting point for understanding of data privacy in India is the unanimous decision of a nine judge 'constitution bench' of India's Supreme Court in *Puttaswamy v Union of India*[57] that India's Constitution recognises an inalienable and inherent right of privacy as a fundamental constitutional right. It is an implied right, because privacy is not explicitly mentioned in the Constitution, but it is implied by Article 21's protections of life and liberty, and is also protected by other constitutional provisions providing procedural guarantees. Privacy protection is also required by India's ratification of the UN's *International Covenant on Civil and Political Rights* (ICCPR), article 17 of which protects privacy. The decision will affect private sector practices ('horizontal effect') as well as actions by the Indian state ('vertical effect'). The Court identified three main aspects of privacy: privacy of the body; privacy of information; and privacy of choice. *Puttaswamy* held that governments could only interfere with the fundamental right of privacy if they observed three conditions: 'first, there is a legitimate state interest in restricting the right; second, that the restriction is necessary and proportionate to achieve the interest; third that the restriction is by law.'[58]

Subsequent smaller constitution benches are now deciding the constitutionality of various pieces of legislation, and practices, in light of the fundamental right of privacy. In *Navtej Johar v Union of India* a unanimous five judge Constitution Bench held[59] that India's criminalization of homosexual conduct (s. 377 of the Criminal Code) was unconstitutional post-*Puttaswamy*). The Indian government decided not to oppose the petition, saying it would leave the decision to the Court. The decision may have wide implications within India.[60] Outside India, the decision has already been followed by Botswana's High Court to declare unconstitutional a similar provision.[61]

A five judge constitution bench heard the challenge to the constitutionality of India's 'Aadhaar' (biometric ID) system, and the *Aadhaar Act 2016*. Puttaswamy was again the lead petitioner.[62] The court held by a 4/1 majority that the Aadhaar scheme was capable of being constitutionally valid, but that many aspects of the current *Aadhaar Act 2016* were unconstitutional. Legislation intended to 'remedy' these constitutional deficiencies, and in particular to enable Aadhaar use by the private sector, was enacted in July 2019.[63]

It is very likely that, in order to protect the constitutionality of other legislation and practices, the Indian government will have to legislate comprehensively to protect privacy in relation to both the public and private sectors in India, and to do so consistently with the requirements of *Puttaswamy #1*. The Indian government therefore commissioned the Report[64] of the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna ('Srikrishna Report'), delivered in July 2018, accompanied by a draft *Personal Data Protection Bill 2018* ('Srikrishna Bill').[65] Despite submissions on the draft Bill closing on 10 September 2018, following which the government had undertaken to produce a Bill for introduction to Parliament, no such Bill had emerged by mid-2019. However, the world's largest election had preoccupied India for many months until June 2019. The new IT Minister has announced that one of his key priorities will be to pass the Srikrishna Bill in this Parliamentary session.

It is difficult to adequately convey comparisons between two such complex pieces of legislation as the Srikrishna draft Bill and the GDPR, each of approximately 100 clauses.[66] Only the most important points of comparison are summarised here.

The Data Protection Authority of India (DPAI) to be established, although described as 'independent' is subject to broad instructions from the government. The DPAI will have a very wide range of enforcement powers, influenced by 'responsive regulation' theory.[67] These include imposition of administrative penalties of 2% to 4% of the data fiduciaries' 'total worldwide turnover of the preceding financial year.'

The Bill provides broad coverage of the private and public sectors, with definitions of 'personal data' and 'sensitive data' similar to the GDPR. Data minimisation, a strong interpretation of consent, and demonstrable grounds for lawful processing, are very similar to the EU. Other obligations of data controllers ('data fiduciaries') cover many significant new elements of the GDPR, including demonstrable accountability, privacy by design and data breach notification. The rights of data subject ('data principals') include data portability and the 'right to be forgotten'. However, some of the more bureaucratic obligations will only apply to 'significant data fiduciaries', designated by the DPAI (and a few others): registration; data protection impact assessments (DPIAs); data protection officers (DPOs); record-keeping to demonstrate compliance; and annual audits. 'Small entities' with less than US$30,000 turnover per year, are also excused from some other obligations. The few significant GDPR elements not included in the Srikrishna Bill include the following: privacy by default; protections against automated processing; an explicit right to object to or block processing; and an explicit direct marketing opt out.

The Srikrishna Bill's data localisation and data export requirements create complex combinations of obligations because it distinguishes between three results:

- *Local copy requirement (localisation #1):* All personal data must be located on a server in India (s. 40(1)), with government

52 *Kusumah and Kobrata, 2018, paras. 41-51.*

53 *Kusumah and Kobrata, 2018, paras. 47-48.*

54 *Kusumah and Kobrata, 2018, para. 52.*

55 *Kusumah and Kobrata, 2018, paras. 53-57.*

56 *G. Greenleaf Asian Data Privacy Laws (OUP, 2014), pp. 432-3, and preceding chapter.*

57 *Justice K.S. Puttaswamy (Retd.) v. Union of India 2017 (10) SCALE 1.*

58 *ibid*

59 *Navtej Singh Johar & Ors. v. Union of India thr. Secretary Ministry of Law and Justice W. P. (Crl.) No. 76 of 2016 (Supreme Court of India) (decided 6 September 2018)*

60 *Alok Prasanna Kumar 'Section 377 judgment could form beginning of a body of path-breaking jurisprudence in India' Scroll 6 September 2018 <https://scroll.in/article/893468/section-377-judgment-could-form-beginning-of-a-body-of-path-breaking-jurisprudence-in-india>; Gautam Bhatia 'The Indian Supreme Court Reserves Judgment on the De-criminalisation of Homosexuality' Oxford Human Rights Hub, 15 August 2018 <http://ohrh.law.ox.ac.uk/the-indian-supreme-court-reserves-judgment-on-the-de-criminalisation-of-homosexuality/>*

61 *Motshidiemang v Attorney General (Lesbians, Gays and Bisexuals of Botswana (LEGABIBO), Amicus Curiae) (2019) High Court of Botswana, 11 June 2019.*

62 *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar judgment), Supreme Court of India, 26 September 2018 <https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf>, 1448 pages.*

63 *Aadhaar and Other Laws (Amendt.) Act, 2019; see 'Parliament passes Aadhaar amendment bill' Deccan Herald, 9 July 2019 <https://www.deccanherald.com/national/national-politics/parliament-passes-aadhaar-amendment-bill-745933.html>*

64 *Committee of Experts under the Chairmanship of Justice B.N. Srikrishna A Free and Fair Digital Economy Protecting Privacy, Empowering Indians, 2018 < http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf >*

65 *Personal Data Protection Bill 2018 <http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf>*

66 *For a longer comparison, see G. Greenleaf 'GDPR-Lite and Requiring Strengthening – Submission on the Draft Personal Data Protection Bill to the Ministry of Electronics and Information Technology (India)' (20 September, 2018). UNSW Law Research Paper No. 18-83 <https://ssrn.com/abstract=3252286 >.*

67 *The Srikrishna Report p. 151 cites G.Greenleaf Asian Data Privacy Laws (OUP, 2014) as their basis for stating that 'a responsive regulatory framework equipped with a range of tools has been found by us to be of critical importance' referring to Chapter 3, part 4 'Standards for enforcement mechanisms and 'responsive regulation'.*

exemptions allowed except for sensitive data. Localisation is already being required for some financial transactions.

- *Export prohibitions (localisation #2):* Categories of 'critical personal data' (CPD) specified by government cannot be exported, except to a destination held 'adequate' (SCCs or BCRs would not be sufficient), or for emergencies
- *Export permission requirements (localisation #3):* All non-CPD can be exported, but only if an export exception is satisfied, including adequacy of destination (as determined by the DPIA), or CSCs or BCRs where the exporter retains liability; or DPIA-designated emergency situations. If the conditions are not met, the data is unable to be exported, and in effect in category (ii).

India's data localisation is as complex as China's, but without the overriding requirement of 'security assessments' of data fiduciaries being carried out by State agencies. There is little doubt that some version of such a general data localisation policy will be enacted in India, as it is also consistent with India's draft Electronic Commerce Policy (February 2019).[68]

The Bill also has extraterritorial effects similar to the EU, applying to overseas companies targeting or profiling persons in India, and to Indian companies carrying out processing overseas. There is also a Government power to exempt specified processing of personal data of foreign nationals not present in India (an 'outsourcing exemption', like in the Philippines), which we might expect would be applied to the USA, but India would guarantee not to apply it to data originating from the EU.

Looking at the Srikrishna draft Bill overall, my conclusions are:[69]

1. The draft Bill sets out a serious and modern law, influenced heavily by the GDPR and including most of its elements. However, its tripartite distinction, in terms of the extent of obligations, between 'significant', normal, and 'small' data fiduciaries is the first to attempt to 'moderate' the GDPR in the this way. It could be an appealing model for other developing economies to take. However, it is potentially open to abuse, if the DPIA does not declare some data fiduciaries to be 'significant' when it is clear that they should. The effect of this on EU adequacy considerations remains to be seen.
2. The Report and Bill both reflect a very different regulatory philosophy from the EU GDPR's radical dispersal of decision-making responsibility (and liability for wrong decisions) to data controllers. The Indian model is more prescriptive, but a justifiable regulatory option, provided it does not give excessive discretion to the government or the Data Protection Authority.
3. The very broad exemptions from most of the Act for processing in the interests of State security or relating to law enforcement, although purportedly constrained by legality, necessity and proportionality (are dangerously vague). The DPAI also has discretion to expand the grounds of lawful processing.
4. The Bill's data localisation requirements adopt an unjustifiable generic approach to data localisation, through blanket local copy requirements (with exceptions to be specified by government), and export prohibitions also specified by government.

If the Srikrishna Bill is enacted in something close to its current form, Asia will have another new model for data privacy laws: strong GDPR influences; different obligations on different classes of data fiduciaries; and complex data localisation requirements.

## PROGRESS IN OTHER ASIAN JURISDICTIONS

Bhutan's law is new. There have been only minor legislative changes in the other eight Asian jurisdictions with laws, but there have been some significant internal changes in operations.

### *North-east Asia – Little change in Taiwan and Macau*

Taiwan continues not to have any specialised data protection authority, so the effectiveness or enforcement of its *Personal Information Protection Act* (PIPA) is difficult to gauge. Amendments in 2016 to Taiwan's Act added enhanced protection for special categories of sensitive data, but made compliance easier by relaxing the consent requirement for ordinary (non-sensitive personal data, and reduced the risk of criminal liability for violations of the PIPA. It has stated that it 'hopes

68 *For a summary see Sneha Johari 'India's Draft Ecommerce Policy is really a Digital Economy Policy, impacts the whole ecosystem' Medianama, 26 February 2019 <https://www.medianama.com/2019/02/223-india-draft-e-commerce-policy/>.*

69 *G. Greenleaf 'GDPR-Lite and Requiring Strengthening' cited above.*





to participate' in APEC CBPRs.[70] In the absence of a DPA, Taiwan's National Development Council (NDC) has opened a data protection coordination office, and has submitted a self-evaluation report on Taiwan's data protection to the EU, in order to commence adequacy discussions.[71]

Macau's Office for Personal Data Protection (GPDP) still has not been formally established by its own legislation, but continues to operate as a 'project' under the Chief Executive's Office, twelve years after the PDPA was enacted. It continues to have one of Asia's most transparent enforcement practices (like Singapore, but no longer Hong Kong), publishing around 20 complaint resolutions notes per annum[72] (in English translations, even though English is not an official language in Macau), as well as the occasional authorisation of data exports.[73]

### *Hong Kong SAR – Deficits in powers, but transparency continues*

In 2014 Hong Kong's data privacy regime could be considered one of the most effective in Asia, possibly 'Asia's leader in data privacy', despite a relatively weak Act, because of a vigorous enforcement regime.[74] Since then, under a new Commissioner (PCPD), the vigour of enforcement seemed initially to have diminished, but since 2017 has again become transparent from the PCPD website.[75] This includes the resumption of casenotes (complaint summary), of up to 15 per annum; Administrative Appeal Board case summaries; and summaries of the few court decisions on the Ordinance, plus some examples of minor prosecutions of breaches included under 'News'. The PCPD has also resumed publishing investigation report under s. 48(2), previously a favoured means of enforcement which enabled 'name and shame' as an enforcement technique. There have now been five such reports against public and private sector bodies since 2015, which although modest compared with 31 such reports from 2010-14, indicates that PCPD enforcement continues.

In June 2019 PCPD issued a s48(2) report in relation to the data breach by Cathay Pacific affecting 9.4 million people,[76] and which has potential implications for EU extra-territorial jurisdiction. However, the PCPD could only order that the airline take measure to prevent and remediate the manifest security breaches that had occurred, because it has no powers to issue administrative fines. This demonstrates that the Hong Kong legislation is inadequate to deal with the scale of breaches that now occur, particularly in light of the UK ICO's proposed fine of £183 million against British Airways for a data breach of similar scale. While the local visibility and transparency of the PCPD continues, its enforcement powers are now unjustifiably outdated and insufficient. Hong Kong no longer leads in Asian data protection.

### *South-east Asia (ASEAN) – The Philippines (energetic) and Malaysia (inactive)*

The Philippines Data Privacy Act (DP Act), enacted in 2012, included more than the minimum '1st generation' principles, such as deletion rights, protection of sensitive information, data portability (in advance of the GDPR, and data breach notification, but no data export restrictions. Its enforcement regime appeared to have a broad and serious 'toolkit'. Much was uncertain because of vague and ambiguous drafting.[77] This otherwise potentially strong Act was also marred by an exemption from the Act of any personal data collected legally in foreign jurisdictions but 'being processed in the Philippines' – in other words, an exemption for any outsourced processing – which is likely to make any EU finding of adequacy impossible to obtain.[78]

Although theoretically coming into force in 2012, the Act remained dormant until 2016, because until a National Privacy Commission (NPC) was appointed, and made Implementing Rules and Regulations (IRR), very few of its provisions were enforceable, and none were enforced. Outgoing President Aquino appointed the three NPC Commissioners shortly before

70 *Taiwan Executive Yuan Taiwan's achievements during 2016 APEC Economic Leaders' Week', 8 December 2016 <http://english.ey.gov.tw/News_Hot_Topic.aspx?n=9CAC6D643D2B87F8&sms=C7706D6F9D246174>.*

71 *'EU lauds Taiwan's efforts to push for talks on data transfer deal' Taiwan News, 11 March 2019 < https://www.taiwannews.com.tw/en/news/3655633> .*

72 *OPDP (Macau) 'Complaint Case Notes' <http://www.gpdp.gov.mo/index.php?m=content&c=index&a=lists&catid=209> .*

73 *OPDP (Macau) 'Authorisations' <http://www.gpdp.gov.mo/index.php?m=content&c=index&a=lists&catid=206> .*

74 *Greenleaf, Asian Data Privacy Laws (2014), pp. 120-1 and preceding chapter.*

75 *See 'Compliance and enforcement' on PDPC (HK) website <https://www.pcpd.org.hk/>.*

76 *PCPD Media Statement (HK) 'Cathay Data Breach Incident-Personal Data Security & Retention Principles Contravened-Lax Data Governance' 6 June 2019 <https://www.pcpd.org.hk/english/news_events/media_statements/press_20190606.html>.*

77 *Greenleaf, Asian Data Privacy Laws (2014), pp. 352-3.*

78 *Greenleaf, Asian Data Privacy Laws (2014), p. 348.*

leaving office.[79] The NPC rapidly issued finalized IRRs so that the Act became effective.[80] The NPC has taken a very activist approach to publicising the Act and to some aspects of enforcement. It recommended the criminal prosecution under the Act of the head of the Philippines' Electoral Commission, for negligently allowing a massive data breach, as well as restorative measures by the agency.[81] The NPC has not yet published results of other investigations in any routine way (unlike Singapore or Macau), but in 2018 released all its Advisory Opinions, many of which are based on quite specific enquiries to the NPC.[82] With about 70 opinions in 2017, this is a very substantial body of authoritative interpretation of the DP Act, unless and until contradicted by court decisions. It is a novel form of transparency.

Malaysia's *Personal Data Protection Act 2010* (PDPA) is limited to the private sector, with a non-independent Commissioner, and has few principles beyond the minimum.[83] After five years, Malaysia's Department of Personal Data Protection has shown few visible signs of enforcing the PDPA, despite that Act being in force for six years. One reason is that, in effect, the Malaysian PDPA can only be enforced through prosecutions, and those must be with the consent of the Public Prosecutor. There is nothing on the PDPC website to indicate that the Commissioner has yet taken any steps to enforce the Act, such as reports of investigated complaints.[84] Three cases have been reported where 'processing personal data without certification of registration' (essentially, failure to pay registration fees) has resulted in small fines.[85] A new Regulation allows the Commissioner to offer to compound specified offences – in effect to allow a fine to be paid instead of prosecution. In 2017 a previous Commissioner proposed a 'White List' of countries with supposedly 'adequate' laws for data export purposes, but which included the USA and China without any justification. This has not been formally adopted as yet, and may have been abandoned. Following the electorate's decisive dismissal of Malaysia's scandal-plagued government in May 2018, the new Minister claims that the PDPA is being reviewed, including in light of the GDPR which he implied required 'comprehensive changes to business practices'.[86] It is reported that this will involve a data breach notification regime,[87] but no other details are available, and there is no time-frame.

***Vietnam – Lighter data localisation***

Vietnam's data privacy laws, which are scattered across various regulations and sectors, were 2014 'a reasonable approximation of the basic principles set out in the 1980 OECD Guidelines or the … APEC Privacy Framework'. However, they lacked any of the elements found in the EU 1995 Directive, or the GDPR, except perhaps some ability to prevent continuing processing.[88] The most recent post-2014 addition, the Law on Cyber-Information Security (CISL), a highest-level law enacted by the National Assembly, significantly expands Vietnam's existing data privacy laws, in that it sets out what is probably the most comprehensive set of data privacy principles yet found in a Vietnamese law. Its scope is limited to commercial processing and only in cyberspace,[89] although it defines 'cyberspace' so as to suggests that the scope also includes VPNs and possibly certain intranets. Like China, Vietnam has no overall Data Protection Authority, but relies on Ministry-based enforcement, details of which are not readily available.

A 2013 law required some businesses to have a server located in Vietnam, if state authorities so requested, a limited sectoral data localisation requirement. Vietnam currently has no explicit legislation on data export restrictions, but consent or government approval is required for overseas transfers.[90] Vietnam enacted a controversial *Law on Cyber Security* in June 2018 introducing data localisation requirements, but also imposing severe penalties on the publication of anything considered to be anti-State activities. It 'imposes tremendous obligations on both onshore and, especially, offshore companies providing online services to customers in Vietnam'.[91] However, the data localization requirements are less strict than in previous drafts: 'The adopted version of the law seems to relax these restrictions by requiring the online service providers to store the Vietnamese users' information within Vietnam for a certain period of time. However, during the statutory retention time, the law does not appear to expressly prohibit the online service providers from duplicating the data and transferring/storing such duplicated data outside of Vietnam.'[92] 'Another requirement found in previous drafts', the same authors note, 'that offshore service providers must locate servers in Vietnam, has been removed from the final version. However, by requiring offshore service providers to "store" Vietnamese users' information in Vietnam, the offshore service providers, as a practical matter, will likely need to locate servers in Vietnam, either by directly owning/operating the servers or leasing servers owned/operated by other service providers in Vietnam, to store such information'.

***Singapore – Enforcement and resistance***

In 2014, before Singapore's *Personal Data Protection Act* (PDPA) had come into full operation, it presented as an Act with 'an exceptionally limited scope, perhaps the narrowest of any Asian law', but one which 'does appear to have a serious and multi-faceted enforcement pyramid', so that businesses would be wise to take its limited requirements seriously.[93] The last five years have borne out these assessments, as documented elsewhere by me[94] and in relation to enforcement in a 2018 report by Chia to the Asian Business Law Institute.[95] Only the distinctive aspects of Singapore's law in operation, and proposed reforms to it, are discussed here.

The Personal Data Protection Commission (PDPC) has proven to be a serious regulator, even though legislative changes have clarified that it does not have independence from government.[96] It reports details of its decisions regularly,[97] with respondents always named, giving transparency likely to affect respondent behaviour and encourage complainants. In Singapore, a small and compliance-conscious jurisdiction, 'name and shame' is likely to be an effective sanction. PDPC may issue administrative fines up to S$1 million. In practice, fines in the S$10K-S$30K range are common, and S$50K not unusual. Other than Korea, no other Asian law results in fines of this magnitude, this often, low though they now are by European standards. In January 2019 the PDPC fined Singapore Health Services (SingHealth) S$250,000, and Integrated Health Information Systems (IHIS), S$750,000 (US $550,000), its largest fines to date, for what the PDPC called the 'worst breach of personal data in Singapore's history,' resulting in the disclosure of personal data for 1.5 million patients and the outpatient prescription records of approximately 160,000 patients.[98]

A mandatory data breach notification scheme is supported by PDPC, based on 'a consistent risk-based approach, and a higher threshold for notification to affected individuals as well as to PDPC', and is likely to result in legislation. In February 2019, the Minister announced that Singapore is considering, as part of an ongoing review of the Personal Data Protection Act (PDPA), introducing data portability.[99] These are the only proposals to strengthen the relatively weak principles in Singapore's law in the direction of the GDPR. Other proposed reforms are likely to weaken

79 *G. Greenleaf, Philippines Appoints Privacy Commission in Time for Mass Electoral Data Hack (2016) 141 Privacy Laws & Business International Report, 22-23 <https://ssrn.com/abstract=2824419>*

80 *G. Greenleaf, Philippines Puts Key Privacy Rules in Place but NPC Faces Pressure (2016) 143 Privacy Laws & Business International Report, 19-21 <https://ssrn.com/abstract=2895600>*

81 *See the Philippines section in G. Greenleaf '2014-2017 Update to Graham Greenleaf's Asian Data Privacy Laws - Trade and Human Rights Perspectives' (July 12, 2017). UNSW Law Research Paper No. 17-47 <https://ssrn.com/abstract=3000766>.*

82 *NPC Advisory Opinions (Philippines) <https://privacy.gov.ph/advisory-opinions/>*

83 *Greenleaf, 2014, pp. 322-355.*

84 *PDPC (Malaysia) <http://www.pdp.gov.my/index.php/en/mengenai-kami/maklumat-organisasi/pejabat-pesuruhjaya>*

85 *Kherk Ying Chew 'Malaysia: Enforcement of the Personal Data Protection Act 2010' Baker & McKenzie, 1 November, 2017 <https://globalcompliancenews.com/malaysia-enforcement-personal-data-protection-20171101/>*

86 *Bernama 'Personal Data Protection Act under review – Gobind' MalaysiaKini 18 March 2019 <https://www.malaysiakini.com/news/468441>*

87 *Yuet Ming Tham 'Important Changes to the Malaysia Data Privacy Regime' Sidley 9 April 2019 <https://www.sidley.com/en/insights/newsupdates/2019/04/important-changes-to-the-malaysia-data-privacy-regime>*

88 *Greenleaf, 2014, pp. 368-372.*

89 *C. Schaefer and G. Greenleaf 'Vietnam's Cyber-Security Law Strengthens Privacy… A Bit' (2016) 141 Privacy Laws & Business International Report, 26-27<https://ssrn.com/abstract=2824405>.*

90 *Waewpen Piemwichai Jurisdictional Report – Vietnam in C. Girot (Ed.) Regulation of Cross-Border Transfers of Personal Data in Asia, (ABLI, February 2018) , paras. 18-45 <http://abli.asia/PUBLICATIONS/Data-Privacy-Project>.*

91 *W. Piemwichai and Tu Ngoc Trinh 'Vietnam's New Cybersecurity Law Will Have Major Impact on Online Service Providers', Tilleke & Gibbons, June 18 2018 <https://www.tilleke.com/index.php?q=resources/vietnam%E2%80%99s-new-cybersecurity-law-will-have-major-impact-online-service-providers>*

92 *Piemwichai and Trinh, ibid.*

93 *Greenleaf, Asian Data Privacy Laws, pp. 314-5.*

94 *G. Greenleaf 'The Asian context of Singapore's Law', Chapter 8 of S. Chesterman (Ed) Data Protection Law in Singapore (2nd Ed) (Academy Press, 2018).*

95 *Ken Chia 'Jurisdiction Report – Singapore' in C. Girot (Ed.) Regulation of Cross-Border Transfers of Personal Data in Asia, February 2018 <http://abli.asia/PUBLICATIONS/Data-Privacy-Project>*

96 *For details see Greenleaf 'The Asian context of Singapore's Law' 2018, paras. 8.64-65.*

97 *PIPC decisions <https://www.pdpc.gov.sg/Commissions-Decisions/Data-Protection-Enforcement-Cases>,*

98 *In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012 and Singapore Health Services Pte. Ltd and Integrated Health Information Systems Pte. Ltd [2019] SGPDPC 3*

99 *K. Kwang 'Singapore plans data portability requirement as part of PDPA update' Channel News Asia, 25 February 2019 <https://www.channelnewsasia.com/news/singapore/singapore-personal-data-protection-act-portability-rights-move-11287772>*

Singapore's law, from a consumer perspective: Guidelines concerning 'anonymisation' or de-identification of personal data appear to leave more scope for use of personal data than European standards; PDPC suggestions of a 'regulatory sandbox' are probably aimed at allowing 'big data' experiments based on these Guidelines, or further weakening of them; and PDPC is proposing to weaken the significance of consent even further.

Singapore is attempting to develop a multi-faceted approach to the problems of cross-border data traffic.[100] PDPC has developed its own recommended (not mandatory) Standard Contract Clauses (SCCs) for transfers. Singapore stated its intention to participate in the APEC APEC-CBPRs in July 2017, but has not yet appointed an 'Accountability Agent' (AA), so cannot do so yet. Possible policy directions include mutual recognition (within ASEAN and beyond) of both CBPRs certifications (once Singapore is fully involved), and Trustmarks. PDPC and its controlling Department (IMDA) called for Singapore-based organisations to participate in Singapore's Data Protection Trustmark (DPTM) certification, which requires an evaluation by one of three independent assessment bodies to determine whether they are able to meet their obligations under the PDPA. It is described as a 'local certification scheme' with no mutual recognition of other schemes at this stage,[101] The Minister states that Singapore will align its own proposed Trustmark standards with APEC-CBPRs standards. DPTM certification therefore does not authorise data exports to APEC-CBPRs certified companies in the US. According to Chia 'Singapore is also exploring other avenues of bilateral or multilateral co-operation with foreign counterparts in the area of data protection, such as free trade negotiations, and mutual recognition of data protection regimes between Singapore and its key trade and economic partners.' A separate regime for international data transfers operates in the banking sector, prevailing in the event of inconsistency with the PDPA.

The result of all these developments is that Singapore, along with Japan (despite its 'adequate' status) lead the group of Asian countries that wish to have little to do with strengthening their laws in the directions suggested by the example of the EU, or the arguments put forward by proponents of human rights. On the other hand, they do not support the 'data sovereignty' approaches of counties favouring data localisation (sometimes influenced by China). For these countries, a limited amount of data protection is a requirement for trust in online business, including cross-border transfers, but that is all. I will call them 'the resisters'.

***South Asia (SAARC) – Bills pending***

The SAARC region (South Asian Area of Regional Cooperation), comprising the eight states of South Asia (India, Sri Lanka, Bangladesh, Pakistan, Bhutan, Nepal, Maldives and Afghanistan), is the Asian sub-region with the least development of data privacy laws. Nepal has a public sector law,[102] and Bhutan a comprehensive but otherwise limited new 2018 law (discussed below). There are some minor but no major developments in the other jurisdictions,[103] except a draft private sector *Personal Data Protection Bill 2018* in Pakistan and a Ministry proposal for a comprehensive, GDPR-influenced, Personal Data Protection Bill in Sri Lanka. If enacted, these two Bills would be major developments.

***Bhutan – Data privacy as gross national happiness***

The land-locked kingdom of Bhutan is known internationally for favouring a measure of 'Gross National Happiness' rather than GDP. It can now add to its GNH the *Information, Communications and Media Act of Bhutan 2018*,[104] passed by the National Assembly in 2017, and in force from mid-2018. Although the data protection principles in the Act are stated briefly, they do more than give Bhutan a minimal data privacy law, because they include seven of the ten 'second generation' principles (see the Table in the Conclusion). Although only applying to provision of the 'ICT and Media Sectors', and providers and users of their service. 'ICT services' are given a very broad meaning, and will normally include public facilities (and thus the public sector), so the law will cover almost any use of electronic information. The act establishes a Bhutan Infocomm and Media Authority which is not fully independent, but has powers to investigate and resolve complaints. There are provisions for compensation, and for offences.

100 *See generally Chia 'Jurisdiction Report – Singapore' paras 1, 21-23 and 83-93,*

101 *IMDA 'Data Protection Trustmark Certification' 29 August 2018 <https://www.imda.gov.sg/dptm>; see also Anne L. Petterd, Andy Leck, Ken Chia and Ren Jun Lim 'Singapore launches pilot Data Protection Trustmark certification scheme' Baker & McKenzie/Lexology 30 August 2018.*

102 *Greenleaf, Asian Data Privacy Laws, pp. 436-446.*

103 *G. Greenleaf 'Privacy in South Asian (SAARC) States: Reasons for Optimism' (2017) 149 Privacy Laws & Business International Report 18-20 <https://ssrn.com/abstract=3113158>.*

104 *Information, Communications and Media Act of Bhutan, 2018 <https://www.dit.gov.bt/information-communications-and-media-act-bhutan-2018>.*

## INTERNATIONAL STANDARDS, DATA EXPORTS AND LOCALISATION

Agreed standards for data privacy laws, whether within a geographical region such as Asia, or at an international level, can have two main effects on international data flows. Adherence to them by legislation can result in increased convergence of standards, making countries more willing to allow personal data concerning their citizens to be exported to countries with similar standards. If common standards for such personal data exports can be agreed upon between countries, then businesses within and without those countries have a reduced compliance burden.

The context of the problem has continued to change, and undue focus on the difficulties of transfers from the EU (and their solutions) is unhelpful. This is because almost all data privacy laws have data export restrictions (of many different kinds), and every new or revised law multiplies the complexity of every other country's problems of obtaining data imports.

This part of the paper examines the extent to which the international mechanism discussed in 2014 have (and have not) developed over the past five years. It will help explain why it is unlikely for the near future that Asia will develop a significant degree of convergence or data export consistency. The Singapore-based Asian Business Law Institute (ABLI)[105] has a multi-year project to explore possible mechanism to reduce problems of personal data transfers between countries within Asia, and also outside Asia. The project has already generated exceptionally valuable research on the position in each country,[106] but it is unsurprising that solutions have not yet emerged.

***Asia's lack of regional standards***

There is still no Asia-wide enforceable regional data privacy agreement, nor any such agreement at the sub-regional level. The only sub-regional agreement is the 2016 *ASEAN Framework on Personal Data Protection*[107] which is a non-binding 'record of Participants' intentions' with no practical effects and no obligations concerning implementation. It refers to the APEC Privacy Framework, and includes principles similar to those APEC principles, but with the addition of a principle concerning cessation of retention of personal data.

The closest Asia comes to regional standards are the supra-regional standards resulting from some Asian jurisdictions (but not India and the rest of South Asia) being part of APEC and its Cross-border Privacy Rules system (CBPRs, see below), and the APEC-related free trade agreement, the Comprehensive and Progress Trans-Pacific Partnership (CPTPP, see below).

Africa and Latin America are both more advanced than Asia in the development of regional data privacy standards. In Africa the ECOWAS Supplementary Act of 2013 on data privacy,[108] with a relatively high level of protections approaching those of the 1995 EU data protection Directive, is now in force between 15 west African states, ten of which have enacted data privacy laws. The African Union 'Malabo Convention' of 2014, dealing with both cybercrime and data protection, and with standards similar to ECOWAS, is not yet in force. It has five of the required 15 ratifications, and a further 11 signatories from the 54 AU member states. The network of Latin American data protection authorities (abbreviated as RIPD or RedIP) finalized in 2017 the *Standards for Personal Data Protection for Ibero-American States,*[109] at the request of the XXVth *Ibero-American Summit of Heads of State and Government* in 2016. This 'RIPD Standard' has a strong consistency with the EU's GDPR and with Convention 108+. It is a standard, not a binding commitment to legislate, but there is at present activity within the Organisation of American States (OAS), which includes all 35 independent states in the Americas, toward developing such a binding agreement.

***The G20's 'Osaka Track', the WTO and BRICS dissent***

Since he introduced the term at the January 2019 Davos World Economic Forum, Japanese Prime Minister Abe has hoped to make the concept of 'Data Free Flow with Trust' (DFFT) one of the centerpieces of Japan's hosting of the 2019 G20 Leader's Summit in Osaka. The June summit produced two declarations which may have a long-

105 *Asian Business Law Institute (ABLI) 'Convergence of the rules and standards for cross-border data transfers in Asia' Project < https://abli.asia/PROJECTS/Data-Privacy-Project> .*

106 *C. Girot (Ed.) Regulation of Cross-Border Transfers of Personal Data in Asia (ABLI, 2018), <https://abli.asia/PUBLICATIONS/Regulation_of_Cross-border_Transfers_of_Personal_Data_in_Asia>.*

107 *Telecommunications and IT Ministers of the ASEAN member states 'ASEAN Framework on Personal Data Protection' <http://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf> November 2016.*

108 *Supplementary Act on Personal Data Protection within ECOWAS <http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf >.*

109 *RIPD Standard 2017 <http://www.redipd.es/documentacion/common/Estandares_eng_Con_logo_RIPD.pdf>.*

term effect on global data privacy rules, but their significance is far from certain due to their vague terms, and to the number of significant countries that are as yet staying outside of the processes that have been established.

The *G20 Osaka Leaders' Declaration,*[110] endorsed by all G20 leaders, includes a section 'Innovation: Digitalization, Data Free Flow with Trust' (arts.10-12, 3 of 43), is very bland, but refers to the challenges of data privacy in the context of IP rights and cybersecurity:

> *Cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development, while raising challenges related to privacy, data protection, intellectual property rights, and security. By continuing to address these challenges, we can further facilitate data free flow and strengthen consumer and business trust. In this respect, it is necessary that legal frameworks, both domestic and international, should be respected.*

The *Osaka Declaration on Digital Economy*[111] was made by 24 countries, including the US, China, Russian, the EU, Latin American and east Asian countries.[112] However four potentially significant countries did not participate: India, Egypt, Indonesia and South Africa. The Osaka Declaration was downgraded to a secondary event in order to avoid singling out the four countries that had yet not signed on.[113] The signatories declared the launch of the 'Osaka Track', described as 'a process which demonstrates our commitment to promote international policy discussions, *inter alia*, international rule-making on trade-related aspects of electronic commerce at the WTO'. They confirmed their 'commitment to seek to achieve a high standard agreement with the participation of as many WTO Members as possible', noting that 78 WTO Members are 'on board' with the Joint Statement on Electronic Commerce issued in Davos on 25 January 2019. They resolved to aim for substantial progress in the negotiations by the 12th WTO Ministerial Conference in June 2020. Abe has announced Japan will organize a meeting of 'Osaka Track' participants, possible as early as July 2019.[114]

India is refusing to support this Davos e-commerce initiative, its Commerce and Industry Minister, Piyush Goyal, arguing in Osaka that 'developing countries need time and policy space to build deepest understanding of the subject and formulate their won legal and regulatory framework before meaningfully engaging in e-commerce negotiations'.[115] Goyal reiterated India's policy favouring data localisation, reflecting the Modi government's policy that data is a national asset, not primarily an individual right, as set out in its draft e-commerce policy (as discussed above in relation to India).

'Data Free Flow with Trust' may be a new label, but it is not a new concept when applied to data privacy, even if it is new in relation to IP or cybersecurity. The idea that free flow of personal data could only be guaranteed by trust between countries has been around since at least 1980. It appeared in the original OECD privacy Guidelines and Council of Europe data protection Convention as trust induced by adherence to minimum standards of data protection. Agreement on what constitutes the 'minimum standards' has been the problem. It is not clear why shifting discussions back to a WTO forum will have any effect in relation to data privacy, although it might in relation to IP and cybersecurity.

The new element is the number of countries introducing data localization policies and laws (in varying forms), which can affect all three areas of concern because they are not necessarily limited to personal data. India and Indonesia's general data privacy laws are still in draft, but they already have some data localization laws. So do China, Vietnam and Russia, but they signed the Osaka Track statement, indicating that participation does not signal any particular view about data localization. The Joint Statement[116] by the leaders of the BRICS countries (both those that did not sign on to the Osaka Track), stressed the centrality of the WTO to a rules-based multilateral trading system, in contrast to the current view of the USA, but otherwise there was no explicit 'BRICS solidarity' evident. Indian trade Minister Piyush Goyal said that data was a 'new form of wealth', important for development, and there was a need to take into account the requirements of developing countries within WTO discussions rather than outside them.[117] There are no longer any simple division on these issues, but rather a global fragmentation of views.

***The CPTPP limits localisation and export restrictions***

In 2017-18 the previous Trans Pacific Partnership (TPP) was scrapped after President Trump refused US ratification, but it was then replaced by the 11 other parties proceeding with the *Comprehensive and Progressive Trans-Pacific Partnership* (CPTPP), which was largely the same in its provisions which impose significant limitations on the ability of parties to enact data export restrictions or data localisation requirements, beyond those found in the WTO's General Agreement on Trade in Services (GATS), art. XIV. Japan, Malaysia, Singapore and Vietnam are the Asian jurisdictions which are signatories to the CPTPP. Korea, Indonesia, the Philippines and Thailand are not signatories to the CPTPP, although they are entitled to accede to it because they are APEC members. So is China, but very unlikely to sign.

CPTPP came into force between its six initial ratifying parties, including Japan and Singapore, on 30 December 2018.[118] Vietnam was to commence on 14 January 2019. The US-Mexico-Canada FTA has similar provisions but is not yet in force. The data localisation and data export provisions in these free trade agreements (FTAs) may be inconsistent with provisions in the laws of some of these countries (including provisions necessary for EU adequacy), and also with their other international obligations such as in Convention 108.[119] As parties to CPTPP, it is arguable that Japan, New Zealand and Canada may already have made commitments inconsistent with being considered adequate by the EU; and Mexico may have done similarly in relation to its commitments under Convention 108.

Will these potential inconsistencies lead to litigation or diplomatic enforcement activities? In a different context, in February 2018, the threats to privacy legislation posed by FTAs became more real, when the US reiterated complaints against Chinese legislation restricting personal data exports, under the WTO's General Agreement on Trade in Services, (GATS, 1995). The US has not yet attempted to join the CPTPP (after abandoning the TPP), but it might do so, in which case the likelihood of enforcement actions would increase.[120]

Another Asia-Pacific FTA is now under negotiation, under strict secrecy, the *Regional Comprehensive Economic Partnership* (RCEP).[121] It is not yet known what privacy-related clauses this agreement might contain. Australia, China, Japan, Korea, New Zealand, India, Singapore, Thailand, Malaysia, Indonesia, Vietnam and other ASEAN countries are involved in the negotiations, so it is potentially very important because neither China nor India are involved in CPTPP.

***APEC-CBPRs' continuing failure***

All APEC members have endorsed the *APEC Privacy Framework*, a largely '1980s' standard based on the OECD Guidelines, as revised in 2013, but with some additional weaknesses, particularly its 'accountability' principle of allowing data exports subject to 'due diligence'. There are no enforcement mechanisms.[122] This endorsement does not carry any legal obligations with it – it is not a treaty. However, the Framework is the foundational standard on which the APEC CBPRs is based, standards well below those of the GDPR (or the Directive).

In 2017-18 Singapore, Australia and Taiwan ('Chinese Taipei' in APEC-speak) were approved to participate in the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules System (CBPRs). APEC's Electronic Commerce Steering Group Joint Oversight Panel (ECSG-JOP) held that their laws met APEC requirements. Mexico (2014), Canada (2014), and Korea (2016) obtained approval earlier. If and when any of these six countries appoint 'Accountability Agents' (AAs), then companies in their jurisdictions can apply to be certified as CBPRs-compliant. Until then,

110 *G20 Osaka Leaders' Declaration, June 2019 <https://g20.org/pdf/documents/en/FINAL_G20_Osaka_Leaders_Declaration.pdf>*

111 *Osaka Declaration on Digital Economy <https://www.meti.go.jp/press/2019/06/20190628001/20190628001_01.pdf >.*

112 *Argentina, Australia, Brazil, Canada, China, the European Union, France, Germany, Italy, Japan, Mexico, Republic of Korea, Russian Federation, Saudi Arabia, Turkey, United Kingdom, United States, Spain, Chile, Netherlands, Senegal, Singapore, Thailand, and Viet Nam.*

113 *Satoshi Sugiyama 'Abe heralds launch of 'Osaka Track' framework for free cross-border data flow at G20' The Japan Times, 28 June 2019, <https://www.japantimes.co.jp/news/2019/06/28/national/abe-heralds-launch-osaka-track-framework-free-cross-border-data-flow-g20/> .*

114 *'G20 leaders' joint declaration again omits 'protectionism' The Japan News, 30 June 2019 <http://the-japan-news.com/news/article/0005843262.*

115 *Aditi Agrawal 'Piyush Goyal at G20: Data is a sovereign asset, free trade can't justify its free flow' Medianama, 11 June 2019.*

116 *Joint Statement on BRICS Leaders' Informal Meeting on the margins of G20 Summit, 28 June 2019 <http://pib.nic.in/PressReleseDetail.aspx?PRID=1576270>; Signed by the leaders of Brazil, Russia, India, China and South Africa.*

117 *'G20 summit: India does not sign Osaka declaration on cross-border data flow' < https://scroll.in/latest/928811/g20-summit-india-does-not-sign-osaka-declaration-on-cross-border-data-flow>*

118 *Australia, Canada, Japan, Mexico, New Zealand and Singapore (with Vietnam to commence on 14 January 2019) – See DFAT Australia CPTPP site <https://dfat.gov.au/trade/agreements/in-force/cptpp/Pages/comprehensive-and-progressive-agreement-for-trans-pacific-partnership.aspx>.*

119 *G. Greenleaf 'Asia-Pacific free trade deals clash with GDPR and Convention 108' (2018) 156 Privacy Laws & Business International Report, 32-34.*

120 *ibid*

121 *Australia Department of Foreign Affairs and Trade Regional Comprehensive Economic Partnership – About the RCEP Negotiations <https://dfat.gov.au/trade/agreements/negotiations/rcep/Pages/regional-comprehensive-economic-partnership.aspx>.*

122 *Greenleaf, Asian Data Privacy Laws, 2014, pp. 33-37.*

'participation' in APEC CBPRs has no practical effect. None of these countries has yet appointed an AA. Canada called for applicants to be AAs in 2017.[123] It seems that some countries say they wish to participate in APEC CBPRs, and take preparatory steps, but then do not do so.

As at mid-2019, only the US (26 companies certified since 2013[124]) and Japan (3 companies certified since 2016[125]) have appointed AAs,[126] so after six years of operation, APEC CBPRs only involves a tiny number of US and Japanese companies. CBPRs is therefore of negligible practical significance as yet. The European Commission states in its Decision concerning Japan's adequacy assessment that certification of a company as APEC CBPRs compliant cannot be the basis for any onward transfer of EU-origin personal data from a country that is held to be GDPR-adequate.[127] This will further diminish the business case for CBPRs. On the other hand, APEC CBPRs has been recognised in the proposed USMCA tripartite free trade agreement (not yet finalised).

| APEC economy | Approved to join APEC-CBPRs | Accountability Agent appointed | No. of Companies certified |
|---|---|---|---|
| **USA** | **2012** | **2013** | **26** |
| **Japan** | **2014** | **2015** | **3** |
| Canada | 2014 | - | 0 |
| Mexico | 2014 | - | 0 |
| Korea | 2016 | - | 0 |
| Singapore | 2017 | - | 0 |
| Taiwan | 2018 | - | 0 |
| Australia | 2018 | - | 0 |
| Other 11 in APEC | - | - | 0 |

123 *See Gazette <http://www.gazette.gc.ca/rp-pr/p1/2017/2017-01-21/pdf/g1-15103.pdf > at p. 242.*

124 *TrustAct APEC CBPR Certified Companies < https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list> as at 15 July 2019.*

125 *See JIPDEC's APEC CBPRs Certified Companies list <https://english.jipdec.or.jp/protection_org/cbpr/list.html> (as at 15 July 2019).*

126 *APEC CBPRs Accountability Agents listing < http://cbprs.org/accountability-agents/> .*

127 *[European Union] Commission Implementing Decision of 23.1.2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information < https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf >*

***Little Asian progress for Convention 108+***

The 'modernisation' of data protection Convention 108 was completed, by the parties to the existing Convention agreeing to a Protocol amending it, on 18 May 2018. The new version (called '108+' to distinguish it) will not come into force for some years.[128] The standards required by 108+ of the laws of acceding countries are higher than those of Convention 108, arguably mid-way between 108 and the GDPR.[129] Since it became open for signature on 10 October 2018, any new countries wishing to accede will have to accede to both the Protocol (ie to 108+) as well as to Convention 108. The UN Special Rapporteur on the Right to Privacy (SRP) has recommended that all UN member states should accede to Convention 108+ and implement its provisions in their domestic law, and where possible to implement additional GDPR principles, while leaving the door open to a broader international agreement at a later date.[130] The EU also endorses accession to Convention 108 by countries seeking a positive adequacy assessment (GDPR, recital 105). Parties to 108+ commit to allowing free flow of personal data to other parties, in return for the same benefit,[131] obligations enforceable only by diplomatic means.

Convention 108 has had reasonable success since its 'globalisation' started with the completion of Uruguay's accession in 2013. It now has 55 Parties, with three from Latin America (Uruguay, Mexico and Argentina), and five from Africa (Tunisia, Cape Verde, Senegal, Mauritius and Morocco). Burkina Faso remains eligible to accede to 108.

However, Convention 108 has had a lack of success in Asia with no accessions as yet, although Japan, Korea, the Philippines and Indonesia are accredited as Observers. The task of attracting accessions to Convention 108+ may be more difficult because of the higher standards that acceding countries must meet. Of the 15 countries in Asia with data privacy laws many will not be able to meet the basic Convention 108+ requirements that a Party must be a State that can claim to be democratic, with a data privacy law that covers both its public and private sectors, and includes an independent DPA. These various criteria rule out nine of the 15: China, Vietnam, Taiwan, Hong Kong, Macau, Singapore, Malaysia, Nepal and Bhutan. Indonesia and India would be ineligible on their current limited laws, but may not be if their new Bills are enacted, subject only to the question of whether these laws would meet the higher standards of 108+. That leaves only Thailand, Japan, Korea and the Philippines as possible 108+ accessions as at mid-2019. The junta-appointed upper house in Thailand raises issues in relation to democracy. The Duterte government's Trumpish antipathy to international institutions like the International Criminal Court make a Philippines accession request unlikely in the short term, although its DPA says it is looking into the possibility.[132] Japan no longer needs 108+ to assist its EU adequacy case, and is preoccupied with its 'Osaka Track', the consistency of which with 108+ is too early to assess. The legislation currently before the Korean legislature would improve its position in relation to 108+ as well as EU adequacy, and the Korean government may be positively disposed toward accession, but has not made any announcement to this effect.

In summary, Asia seems at present unlikely to be a major source of the continuing globalization of Convention 108+, less so than Africa or Latin America. However, new laws and policies, including in any of India, Indonesia, Korea, Japan or the Philippines, could change this momentum.

***Will the EU's 'adequate' list expand in Asia?***

The GDPR coming fully into force on 25 May 2018 created a more concrete 'international standard': those countries which wish to obtain or retain a finding by the European Commission that they 'ensure an adequate level of protection' must satisfy the requirements of art. 45. Which Asian countries, other than Japan and Korea, could do so? The Japanese adequacy decision has shown how low (or 'reasonable') a benchmark the GDPR adequacy standard can be, not much different from the Directive except that there must now be credible protection of private sector data against public sector accesses.

Although otherwise credible in relation to its private sector (at least by the 'Japan standard'), Singapore is disqualified by the lack of independence of its DPA. Malaysia likewise. Taiwan has no DPA, and would not realistically be able to obtain a positive adequacy assessment until it does. Perhaps, on the Japanese standard, the Philippines could apply, but it would not be so important to the EU that the answer is 'yes', and (at best) any data imported into the Philippines from the EU for the purposes of further processing would have to be excluded from the scope of such a determination, because the Philippines data privacy law does not apply to such data. Thailand has expressed interest in applying for an adequacy determination, but the extent of independence of its DPA would need to be examined. It seems unlikely that Chinese politics would allow Hong Kong or Macau to apply, and in any event Hong Kong does not have any data export restrictions. Whether India or Indonesia might become credible applicants is unknown. Although the position is no doubt more complex than these brief observations suggest, and is always subject to amendments arising from negotiations (as was the case with Japan), it is nevertheless apparent that there are no easy roads to positive adequacy determinations yet to be found in Asia.

***Other 'appropriate safeguards' for transfers from the EU (and elsewhere)***

As the European Commission insists quite often, art. 45 adequacy decisions are not the only basis for approved transfers of personal data between the EU and other countries. Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), approved codes and approved certification mechanisms, providing 'appropriate safeguards' under art. 46 can support large-scale transfers. However, uncertainty will surround the effectiveness of SCCs (and other mechanisms) at least until the CJEU delivers its decision in the 'Schrems #2' case, only now being heard, challenging the validity of the use of SCCs for data transfers to the USA, because of the extent of US government access to such data.

Whatever the position in the EU, these same mechanisms, if adopted in Asian data privacy laws, may provide parts of the answers for cross-border transfers within and outside Asia. Singapore has a particular interest in developing such mechanisms.

128 *For details see G. Greenleaf (2018) 'Modernised' data protection Convention 108+ and the GDPR' 154 Privacy Laws & Business International Report 22-3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3279984>.*

129 *G. Greenleaf 'Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives' (2016) 142 Privacy Laws & Business International Report,14-17 <https://ssrn.com/abstract=2892947>.*

130 *United Nations General Assembly, seventy-third session Report of the Special Rapporteur on the right to privacy, 17 October 2018, para. 117(e) <http://www.worldlii.org/int/other/UNSRPPub/2018/11.html>.*

131 *There is an exception allowing higher regional standards to also be required, such as adequacy under the EU GDPR.*

132 *L. Hunt 'Does Duterte's War on the International Criminal Court Really Matter?' The Diplomat 5 April 2018.*

## CONCLUSIONS: NO GRAND SOLUTIONS LIKELY

With the passage of the last half-decade, Asia remains the most economically significant region of the global least likely to adopt uniform answers to the dilemmas of data privacy law. Convergence of national laws is only likely to occur in a limited and uneven way, and no single international instrument is likely to dominate the resolution of cross-border issues.

***National laws and practices – Uneven emulation and 'GDPR creep'***

The lack of any regional data privacy standard or agreement across the Asian region, or any significant standards at a sub-regional level such as ASEAN, means there is no easy path to convergence of standards in national legislation. Inconsistency continues, as it did pre-2014. The average implementation of 2nd generation (EU Directive influenced) principles across the eleven Asian jurisdictions with laws in 2014 was slightly more than 5 of the 10 principles (see Introduction). In 2019, the fourteen Asian laws covering the private sector[133] include on average just over 6 of these principles. The increases are primarily due to the new Thai law and the 2015 reforms of Japan's law, but the inclusion of both China's 2016 Law (and accompanying 'standard'), and Bhutan's law, have also increased the average.

| 2nd Generation – 'European standards' | EU Directive | Asian laws including standard | No. |
|---|---|---|---|
| *Data retention limits* (destruction or anonymisation) after processing achieved | EU Dir 6(1)(e)<br>*GDPR 5(1)(e)* | Bhutan, HK, Indonesia, Japan, Korea, Malaysia, Macau, Philippines, Taiwan, Singapore, Thailand, Vietnam | 12 |
| *Recourse to the courts* to enforce data privacy rights (incl. compensation, and appeals from decisions of DPAs) | EU Dir 22, 23<br>*GDPR 78, 79, 82* | Bhutan, China, HK, India, Indonesia, Korea, Macau, Philippines, Taiwan, Singapore, Thailand, Vietnam | 12 |
| *Minimum necessary collection* for the purpose (not only 'limited') | EU Dir 6(1)(c), 7<br>*GDPR 5(1)(c)* | Bhutan, China, HK, India, Korea, Malaysia, Macau, Taiwan, Singapore, Thailand | 10 |
| *Restricted data exports* based on data protection provided by recipient country ('adequate'), or alternative guarantees | EU Dir 25<br>*GDPR 44-49* | China, India, Japan, Korea, Malaysia, Macau, Singapore, Thailand, Taiwan | 9 |
| *Specialised Data Protection Authority(-ies)* (DPA) required | EU Dir 28<br>*GDPR 51-59, 77* | Bhutan, HK, Japan, Malaysia, Korea, Macau, Philippines, Singapore, Thailand | 9 |
| *Additional protections for sensitive data* in defined categories | EU Dir 8<br>*GDPR 9, 10* | Bhutan, China, Japan, Korea, Malaysia, Macau, Philippines, Taiwan, Thailand | 9 |
| *Rights to object to processing, including to 'opt-out' of direct marketing uses* of personal data | EU Dir 14(a), (b)<br>*GDPR 21* | Bhutan, China, HK, Korea, Malaysia, Macau, Taiwan, Thailand, Vietnam | 9 |
| General requirement, and exhaustive definition, of *legitimate processing'* | EU Dir 6(1)(a)<br>*GDPR 5(1)(a), 6* | Bhutan, China, Korea, Malaysia, Macau, Philippines, Taiwan, Thailand | 8 |
| *Prior notification to or checking by DPA of some sensitive processing* | EU Dir 20<br>*GDPR 36* | HK, Japan, Korea, Malaysia, Macau | 5 |
| *Limits on automated decision-making* (incl. right to know processing logic) | EU Dir 15, 12(a)<br>*GDPR 22* | China, Macau, Philippines | 3 |
| | | Av. over 14 countries = 6.1/10 principles | 86 |

Some of the innovations of the EU's GDPR are also already found in Asian laws. These include: data breach notification to DPA for serious breaches (China, Korea, Philippines, Thailand, Vietnam, and of limited scope in Japan), or to data subjects if of high risk (Indonesia, Taiwan, Philippines, Korea, Thailand); collective actions before DPAs or courts by public interest privacy groups (China, Korea; Philippines, Taiwan, Vietnam); DPAs able to issue administrative fines (Japan, Korea, Singapore, Taiwan, Thailand); Mandatory DPOs (Korea; Thailand); right to portability (Philippines, Thailand); extra-territorial jurisdictions based on 'targeting' (Thailand); and 'right to be forgotten' (Indonesia). This list is not comprehensive, but at least 40 examples of principles similar to GDPR innovations have already been enacted across Asia.

The main conclusion that appears from the developments in national laws since 2014 is that, while the lack of any regional standard or agreement means that national developments are not likely to be uniform, there is a measurable development of stronger data privacy principles in Asian laws, both in the increased extent of enactment of '2nd generation' 'European principles', and in the extent of uptake of new '3rd generation' principles, prompted by the GDPR. 'Convergence' is not a term applicable in Asia, except to indicate that overall standards continue to become stronger – slowly, unevenly, but in a consistent direction.

Irrespective of what GDPR-like elements are included in Asian national laws, and irrespective of the likelihood of the extra-territorial jurisdictions of the GDPR applying to companies based in Asia, it is possible that the 'unofficial' or de-facto effects of the GDPR in Asia are even more important. This 'GDPR creep' consists of both 'vertical effects' (companies headquartered outside Asia requiring their subsidiaries in Asia to be 'GDPR-compliant'), and 'horizontal effects' (companies based outside Asia requiring their suppliers of services located in Asia to be 'GDPR-compliant').[134]

***International commitments – Gridlock ad infinitum?***

None of the multinational instruments discussed above are likely to dominate all the others in coverage or effectiveness: the 'Osaka track' provokes dissent and has no clear objectives; the CPTPP data export and localisation clauses are unlikely to be enforced unless the US 'rejoins'; APEC-CBPRs remains a propaganda piece, not a reality; Convention 108+ has few prospects of accession; and candidates for EU adequacy are equally scarce. No initiative has adherents among a majority of significant Asian countries. At present, with no single answer to these problems, the pragmatic approach for any country may be to adopt a mix of 'solutions' – with the risk that some may be contradictory – including development of various 'appropriate safeguards'.

***Data privacy dilemmas in Asia***

On the Asian front of the Data Wars, it is increasingly difficult to know how many sides there are, or whose side various countries are on. Hostilities between the EU and the USA continue, but China must now be counted as a third combatant, considered hostile by both the EU and USA because of its strong stand on data localisation, which hits a sympathetic chord in many other countries, such as India and Vietnam, under the name of 'data sovereignty'. The result is confusion for allies of the main contenders (if they can decide who they are) and for neutrals caught in between. This seem likely to continue indefinitely.

133 *Nepal's law, which only covers the public sector, is omitted for this purpose.*

134 *G. Greenleaf '"GDPR Creep" for Australian Businesses But Gap in Laws Widens' (2018) 154 Privacy Laws & Business International Report 1, 4-5 <https://ssrn.com/abstract=3226835>.*

# RIGHTS AND FREEDOMS IN THE GDPR:

*An overlooked substantive novelty*

DARA
**HALLINAN**

*Estudió derecho en Reino Unido y en Alemania y completó un Master en Derechos Humanos y Democracia en Italia y Estonia. Desde 2011 hasta 2016 trabajó en Fraunhofer ISI in Karlsruhe, luego de lo cual se unió a FIZ Karlsruhe. El foco de su trabajo es la interacción entre el derecho, las nuevas tecnologías –particularmente TIC y biotecnologías- y la sociedad. Escribió su PhD en la Vrije Universiteit Brussel en la regulación óptima para la privacidad genética en biobancos e investigación genómica a través del derecho a la protección de datos. Es Director de Programa en la Conferencia "Computers Privacy and Data Protection" y editor de la publicación bi-semanal de la UE "Data Protection Insider".*

## SUMARIO

RESUMEN
ABSTRACT
1. INTRODUCTION
2. THE EARLY DEVELOPMENT OF EU DATA PROTECTION LAW
3. THE DATA PROTECTION DIRECTIVE
4. THE GENERAL DATA PROTECTION REGULATION
5. THE USE OF THE CONCEPT OF RIGHTS AND FREEDOMS IN THE GDPR
6. THE SCOPE OF THE CONCEPT OF RIGHTS AND FREEDOMS IN THE GDPR
7. META-OBSERVATIONS ON THE CONCEPT OF RIGHTS AND FREEDOMS IN THE GDPR
8. OPEN QUESTIONS CONCERNING THE CONCEPT OF RIGHTS AND FREEDOMS IN THE GDPR
9. CONCLUSION
BIBLIOGRAPHY





## RESUMEN

El Reglamento General de Protección de Datos (RGPD) fue aprobado a comienzos de 2016 y está vigente desde comienzos de 2018. Se ha escrito mucho respecto de las formas en que el RGPD es una novedad con relación a su predecesora, la Directiva 95/46. Un aspecto sustancialmente novedoso que ha sido largamente ignorado, sin embargo, es la generación y el uso del concepto de "derechos y libertades" como punto base referencial para identificar la legitimación y salvaguarda en cualquier instancia del tratamiento de datos. Esta contribución desarrolla esta consideración novedosa: el rango de usos del concepto, el alcance sustancial del concepto, y la variación del concepto en la aproximación que la ley de protección de datos europea toma para regular el tratamiento de la información.

## ABSTRACT

The General Data Protection Regulation (GDPR) came into force in early 2016 and has applied since early 2018. Much ink has been spilled elaborating the ways in which the GDPR is substantively novel in relation to its forerunner, Directive 95/46. One aspect of substantive novelty which has been largely overlooked, however, is the appearance and use of the concept of 'rights and freedoms' as a base reference point for identifying the legitimacy and safeguards relevant for any instance of data processing. This contribution elaborates this novelty considering: the range of uses of the concept, the substantive scope of the concept and the shift the concept implies in the approach European data protection law takes to regulating information processing.

## 1. INTRODUCTION

After a lengthy legislative process, the General Data Protection Regulation (GDPR) came into force in Europe in early 2016 and has applied since early 2018. With its applicability, the GDPR replaced Directive 95/46 – the hitherto overarching instrument of European data protection law – and ushered in a new era in the regulation of personal data processing both in Europe and around the world.

Both during and following the legislative process leading to adoption, there have been discussions as to the novelty of the GDPR. Certain commentators have noted the significance of the European level direct applicability of the Regulation. Other commentators have remarked on the procedural novelties in the Regulation – for example the procedures outlining cooperation and consistency in Data Protection Authorities' interpretation of the GDPR.

Naturally, commentators have also spilled ink discussing the substantive novelties of the GDPR. Truly novel data protection principles such as Data Protection Impact Assessment obligations outlined in Article 35 GDPR or Data Portability obligations outlined in Article 20 have received much attention. Yet, there are aspects of substantive novelty in the GDPR which have been largely overlooked. With this in mind, this contribution makes the following point:

*The concept of rights and freedoms, which appears numerous times, in numerous different substantive provisions of the GDPR, constitutes a significant, but overlooked, substantive novelty in European data protection law.*

The contribution begins by offering – for the reader who may not be familiar – a background to the development of European data protection law, at both national and European level, prior to the adoption of the GDPR (sections 1 and 2). The contribution then moves to outline the background and substance of the GDPR (section 3). The contribution then outlines the role of the concept of rights and freedoms, its scope and its substantive novelty in European data protection (sections 5-7). Finally, the contribution highlights some open questions associated with the concept (section 8).

## 2. THE EARLY DEVELOPMENT OF EU DATA PROTECTION LAW

Data protection laws first appeared in Europe at national level. As far back as the early 1970s, European states had already started to pass laws designed to regulate new information processing technologies. Over the subsequent decades, from narrow beginnings, these laws saw remarkable substantive development.

The first generation of European data protection laws appeared in states in the early 1970s. These laws emerged in response to social concerns related to proposals by national governments on the deployment of large-scale centralised data processing systems to support bureaucracy. Specifically, these concerns focused on the social undesirability of the automated and inhuman bureaucracies imagined to be ushered in by such systems. Unsurprisingly, the substantive content

of these early laws was heavily influenced by the processing context from which they emerged. In terms of scope, laws were tailored to public processing in centralised systems. In terms of substance, laws consisted of technical provisions regulating systems' operation. Ex ante, laws required prior registration. During processing, laws legislated for the correct use of technology. Obligations on data security, secrecy and accuracy were central.

Over the subsequent two decades, European society saw drastic changes in the technologies involved in information processing as well as the deployment of these technologies. Computers became increasingly small, numerous and used for an increasing range of bureaucratic and business tasks in an increasing range of organisations. In turn, technologies were developed to link computers together in networks. In parallel, the social concerns connected with computers – and increasingly networks of computers - also changed. In particular, focus shifted from concerns directly connected with administrations, to concerns connected with individuals' rights in information. Increasingly, concerns arose in relation to ensuring individuals had, and could maintain, control over the use of their information by third parties – concerns of informational self-determination.

As a result of technical and social evolutions, European data protection law underwent a number of cycles of renewal. Mayer-Schönberger refers to three subsequent 'generations' of data protection laws. Throughout these generations, three types of development are significant. First, laws expanded in scope to encompass both public and private data processing operations. Second, in terms of content, laws increasingly focused on the protection of individual rights. This focus took the form of granting individuals increasing granularity of control over their personal data as well as of providing extra protection – such as strict prohibitions – where control was seen to be illusory. Third, laws adopted an increasingly technologically neutral, principles-based approaches – employing increasingly abstract provisions aimed at being adaptable to both technological and social change.

Whilst generations of European data protection laws might be identified since the 1970s, the reality on the ground was that that laws in different states displayed significant differences. Not all states adopted data protection laws, and amongst those that did, laws did not necessarily have equivalent scope or equivalent substantive provisions. These differences spurred moves at European level to harmonise laws across European states. The most significant harmonisation initiative came, in 1995, via the European Union.

## 3. THE DATA PROTECTION DIRECTIVE

There had been prior efforts at harmonizing European data protection law. Most noteworthy were efforts by the Organisation for Economic Cooperation and Development and the Council of Europe. Unfortunately, these proved insufficient to deliver the substantial harmony the European Union felt required for delivering the goal of an integrated single market. Accordingly, in 1990, the European Union began the legislative process for an encompassing European level data protection legislation. The result of this legislative process was the adoption, in 1995, of Directive 95/46 – the Data Protection Directive.

The purpose of the Directive was to balance competing interests in data processing. On the one hand, the Directive recognised the possibility for data processing to impact data subjects' fundamental rights. On the other hand, the Directive recognised the legitimate interests of public and private actors in processing personal data. This was reflected in Article 1 of the Directive which clarified the purpose of the law as being: '[protecting] the fundamental rights and freedoms of natural persons, and in particular their right to privacy [whilst allowing the] free flow of data between Member States'. In pursuing this aim, the Directive pursues a highly technological neutral and principles-based approach providing a system of what De Hert refers to as 'procedural justice' – i.e. a system in which the normative legitimacy of personal data processing is accepted whilst being subjected to substantive safeguards.

The Directive had a very broad material scope. According to Article 3, the law applied to all processing of personal data regardless of whether this processing was manual or automated and regardless of whether processing took place in the public or private sector. Precisely how the law applied however, was dependent on the type of personal data being processed. The Directive outlined two categories of personal data: normal personal data; and sensitive personal data. Normal personal data constituted all personal data not explicitly classified as sensitive. The range of types of personal data classified as sensitive were exhaustively outlined in Article 8. Processing of types of personal data classified as sensitive were regarded as carrying a higher risk to individual's rights and were thus subject to a higher standard of protection.

Generally speaking, the substantive principles outlined by the Directive could be broken down into six categories – six building blocks: oversight – including the obligation for the controller to notify the Data Protection Authority prior to processing; legitimate processing – in order to legitimate processing, the data controller needed to secure the consent of the data subject or fall under one of the other, exhaustively listed, public interest justifications; data subject rights – in relation to all data processing operations, the data subject was endowed with a range of ongoing rights in relation to their personal data; data controller obligations – in relation to all data processing, data controllers were subject to certain obligations, not least the key data processing principles; and finally, sanctions – in cases of violations of the principles of the Directive, data controllers were subject to penalties.

The Directive remained the unchallenged lynchpin of European data protection law for 15 years. In the course of time, however, the Directive started to show its age. On the one hand, technological progress and societal use of computers and other information technologies had evolved, again, at a startling pace. On the other hand, the legal landscape out of which the Directive had emerged had also changed. In particular, the Treaty of Lisbon elevated data protection to the status of a constitutional right in the EU legal order as well as – in Article 16 of the Treaty on the Function of the European Union – provided the EU with clear competence to legislate on data protection.[1] By 2010, it was thus time for a renewal of EU data protection law.

## 4. THE GENERAL DATA PROTECTION REGULATION

This renewal began with the European Commission's adoption of the Communication: 'A comprehensive approach on personal data protection in the European Union'. A long and hard legislative process followed. Indeed, in front of the European Parliament, the process was the subject of a level of lobbying activity never priorly experienced. Eventually, however, the process came to an end with the adoption of Regulation 679/2016: the GDPR. The GDPR came into force in early 2016 and has applied, as binding law, replacing Directive 95/46, since early 2018.

The purpose of the GDPR remains largely unchanged from that of Directive 95/46. The GDPR still seeks to balance the same set of competing interests in data processing as Directive 95/46. This is exemplified in Article 1 of the Regulation which mirrors Article 1 of Directive 95/46: 'This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data [whilst allowing the] free movement of personal data within the Union'. The legal approach the GDPR takes to balancing these competing interests also mirrors that of Directive 95/46. The GDPR also pursues a highly technologically neutral, principles-based, legislative approach. The GDPR also functions based on the provision of procedural justice whilst recognising, in principle, the normative legitimacy of personal data processing.

In terms of material scope, the GDPR retains the key applicability criteria outlined by the Directive. The GDPR applies to the processing of personal data regardless of whether this is by manual or automated means and regardless of whether this is undertaken by a public or private entity. The GDPR does, however, take a novel approach to territorial scope. Whilst Directive 95/46 was unclear on extraterritorial applicability, the GDPR makes clear it applies whenever EU citizens' personal data are being processed. Article 3 clarifies applicability extends to: 'the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to... the offering of goods or service...to... data subjects in the Union; or... the monitoring of...behaviour as far as their behaviour takes place within the Union'.

In terms of substantive provisions, the GDPR inherits the majority from Directive 95/46. The GDPR retains each of the six categories of substantive provisions in the Directive without adding any new categories of its own. Within each category, the GDPR retains most provisions present in Directive 95/46. There are some truly novel provisions outlined in the GDPR – for example, the data subject Data Portability Right outlined in Article 20, the data controller Data Breach Notification obligation outlined in Article 34 and the data controller Data Protection Impact Assessment obligation in Article 35. There are also certain provisions which have undergone significant substantive change – for example, the scale of administrative fines outlined in Article

1 *Prior to the provision of this ground, the EU had legislated on data protection via its competence in relation to the single market.*

84(5) is colossal in comparison to that elaborated in the Directive.

Unsurprisingly, commentators have spent much time on the analysis of the substantive novelty of the GDPR in relation to Directive 95/46. For the most part, in seeking novelty, commentators have looked to the clearly novel provisions, or clearly novel aspects of provisions in the GDPR – outlined in the paragraph above. Commentators have, however, largely overlooked one significant aspect of novelty in the GDPR: the use of the concept of 'rights and freedoms'.

## 5. THE USE OF THE CONCEPT OF RIGHTS AND FREEDOMS IN THE GDPR

The concept of rights and freedoms appears seventy-seven times in a substantive capacity in the GDPR. This number alone dwarfs the twenty-five references to the concept in Directive 95/46. The concept can be seen to appear in three different substantive forms in the GDPR. The first form mirrors the use of the concept in Directive 95/46. The second form builds significantly on the use of the concept in Directive 95/46. The third form is completely novel to the GDPR.

First, the concept of rights and freedoms appears as a scoping concept for the purpose of the GDPR. As discussed above – in section 4 – the concept is used in Article 1 of the GDPR as determinative of purpose of the law: 'This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.' This use of the concept in relation to the elaboration of purpose mirrors that of Article 1 of Directive 95/46: 'In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data .' This replication of purpose should be unsurprising, since at least the second generation of national laws in the late 1970s, the aim of protecting rights and freedoms has been central to European data protection law.

Second, the concept of rights and freedoms appears as a normative framework to be considered in specifying, in context, the applicability of other concrete data protection provisions in the GDPR. The concept appears in this capacity in numerous provisions. The concept appears, for example, in relation to determining when data controllers may rely on legitimate interest processing justifications in Article 6, how data controllers must discharge obligations concerning automated decision making in Article 22, how data controllers must discharge security and confidentiality obligations under Article 32 and how data controllers must discharge data breach obligations in Article 33. The concept did appear in a similar role in Directive 95/46. In the Directive, however, the concept only explicitly appeared in this role once, in relation to the legitimate interest processing justification.[2]

Third, the concept of rights and freedoms appears as a stand-alone normative framework. The GDPR outlines the need for data controllers to engage in a general consideration of how data subjects' rights and freedoms might be impacted by data processing. In light of this consideration, data controllers are subsequently obliged to consider whether processing is normatively legitimate and, if so, under what conditions. These obligations are, in particular, outlined in Article 25 on Data Protection by Design and Default and Article 35 on Data Protection Impact Assessments. These general considerations are detached from the consideration of concrete data protection principles outlined elsewhere in the GDPR. Accordingly, they may require data controllers to go over and above what is explicitly required in the black-letter text of the GDPR. There are no comparable provisions identifiable in Directive 95/46.

This section has clarified the uses and novelty of the concept of rights and freedoms in the GDPR. With this clarification, however, comes a significant question: what does the concept of rights and freedoms used in the GDPR encompass?

## 6. THE SCOPE OF THE CONCEPT OF RIGHTS AND FREEDOMS IN THE GDPR

The scope of the concept of rights and freedoms in the GDPR is not explicitly clarified in the text of the Regulation. Consequently, commentators have offered different interpretations. Jandt, for example, referring to the concept in the context of the Article 35 Data Protection Impact Assessment obligation, suggests: 'Despite the relatively general formulation of 'rights and freedoms of data subjects'...not every interference with fundamental rights need be considered in the assessment.'[3] Yet, it is hard to see which argumentation could support such a limited understanding of the concept. In fact, it seems clear the concept must encompass the full range of rights and freedoms outlined in foundational European human and fundamental rights documents.

The concept of rights and freedoms has a clear, base-line, meaning in EU law: the range of rights and freedoms outlined in foundational European fundamental and human rights documents. Specifically, the concept refers to the catalogues of rights and freedoms outlined in the two key European fundamental and human rights instruments: the European Convention of Human Rights (ECHR); and the Charter of Fundamental Rights of the European Union (CFEU). Given the foundational nature of the concept in EU law, it is very hard to imagine that the EU legislator has mistakenly or carelessly used the term when only a limited, or truncated, set of rights was intended. Thus, unless evidence can be found in the text of the GDPR, or in associated jurisprudence, that the concept refers to some limited set of rights, the base-line meaning must be taken as correct.

There is, however, no such evidence in the text of the GDPR. The purpose of the GDPR is explicitly clarified as being to protect rights and freedoms, with no caveats. There is no indication a sui generis, limited, concept of 'rights and freedoms', is intended. This should be no surprise. As De Hert observes: '[data protection law is] a piece of furniture in...other existing chambers of the constitutional state'. There is also no indication a limited concept of rights and freedoms is intended in any of the specific substantive provisions outlined in the GDPR. In relation to the Article 25 Data Protection Data Protection by Design and Default obligation, for example, there is only one reference to the concept. This reference, without further caveat or clarification, simply elaborates the need to take into account, when implementing the provision: 'the risks of varying likelihood and severity for rights and freedoms'.

There is also no such evidence available in supporting jurisprudence. The Article 29 Working Party – the body previously responsible for offering European level interpretation of EU data protection law principles – have given the concept some consideration.[4] In particular, the Working Party considered the concept in their recent opinion on the Article 35 Data Protection Impact Assessment obligation. In this opinion, the Article 29 Working Party explicitly recognised the concept in data protection law has a broad scope: 'the reference to "the rights and freedoms" of the data subjects primarily concerns the right to privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement...' This clarification is not a one-off. Indeed, the approach resonates with previous Article 29 Working Party declarations on Directive 95/46 – for example on the risk-based approach.

The above sections have clarified the technical novelty of the deployment of the concept of rights and freedoms in the GDPR and elaborated the concept can only refer to the full range of rights and freedoms outlined in foundational European fundamental and human rights instruments. Taking the observations in these chapters at face-value, certain meta-observations can be made about the significance of the use of the concept in the GDPR for European data protection law generally.

## 7. META-OBSERVATIONS ON THE CONCEPT OF RIGHTS AND FREEDOMS IN THE GDPR

The previous sections have painted a somewhat dry, technical, picture of the substantive novelty of the concept of rights and freedoms in the GDPR. Looking closer, however, the use of the concept can be seen to represent a deep shift in the approach of European data protection law to dealing with the regulation of information processing and the data processing ecosystem to which it relates. In this regard, three meta-observations seem particularly relevant.

First, the use of the concept of rights and freedoms in the GDPR represents a conceptual shift in legal approach in European data protection law. This shift constitutes a move away from the presumption that concrete data protection principles, defined by the legislator *ex ante*, will be adequate in providing protection for the harms which arise in all cases of data processing. Now – especially as a result of the third substantive form of the concept, outlined in section 5 – the data controller is placed, in relation to each processing operation, in the position of performing the normative calculation as to whether processing is legitimate and in relation to which safeguards are necessary. The data controller is placed, in a meta-regulatory approach, framed by the concept of fundamental rights and freedoms, in the position of legislator. Whilst this may seem a surprise move, it is arguably a natural development in

2 *The concept did appear, however, in relation to other provisions in jurisprudence clarifying the application of Directive 95/46.*

3 *Author translation of: 'Trotz der relative allgemein gehaltenen Formulierung „Risiken für die Rechte und Freiheiten der betroffenen Personen" sind nicht jegliche (Grund-) Rechtsbeeinträchtigungen in die Bewertung einzubeziehen.'*

4 *The body has been subsequently replaced by the European Data Protection Board.*

European data protection law. Recall, in sections 2-4, the observation that data protection law has always played catch up with technological developments and the social issues they pose. The shift of normative burden to the data controller is a logical response.

Second, such a meta-regulatory approach will have impacts on the position and function of European Data Protection Authorities. Two consequences seem particularly significant. First, Data Protection Authorities, in principle, can no longer be conceptualised as being limited technical executive agencies responsible for overseeing compliance with concrete data protection principles. Now, they must play a more normative, standard-setting, role in defining the legitimacy of processing operations and relevant safeguards irrespective of concrete data protection principles. In other words, they shift toward being fundamental rights agencies in relation to information processing. Second, certain Data Protection Authorities will need to reorient their approaches to data controllers. Owing to the lack of *ex ante* normative clarity, these two groups will need to work together more collaboratively in establishing clarity in relation to adequate protection of fundamental rights and freedoms.

Third, such a meta-regulatory approach will, itself, create winners and losers amongst data controllers. The obligation on data controllers to perform quasi-legislative functions requires these data controllers to engage in subtle normative considerations. To effectively execute such considerations then requires suitable organisational structures and the devotion of resources to those structures. Large scale data controllers – for example US multinationals – are have experience, and already structured to efficiently engage in, quasi-legislative standard-setting behaviour. Indeed, precisely for this reason, certain larger data controllers have been vocal in their support for meta-regulative legislative thrusts in European data protection in the past – specifically the risk-based approach. Smaller data controllers, however, are unlikely to have either the experience to understand the normative considerations required of them, how to structure their organisational approaches nor, necessarily, adequate resources.

Taking a legalistic and face-value approach to the conceptualisation of data protection principles is, however, a risky business. There is scarcely another area of law in which the law on the books is so flexible, subject to divergent interpretation and to stakeholder influence. Accordingly, despite the observations made in this section, several questions remain unanswered.

## 8. OPEN QUESTIONS CONCERNING THE CONCEPT OF RIGHTS AND FREEDOMS IN THE GDPR

The range of unanswered questions and uncertainties is broad. Indeed, perhaps the use of the concept of rights and freedoms raises more questions than it answers. Three questions, however, seem particularly poignant.

First: how can the concept of rights and freedoms be a basis for identifying data protection standards? The catalogue of rights and freedoms in foundational European instruments constitute high level principles, fleshed out in specific situations by case law. The vast majority of these principles were not designed with data processing in mind – indeed, only the right to data protection was specifically designed with computerized information processing in mind. In turn, the vast majority of relevant case law is neither designed for computerized information processing nor is necessarily scalable across all processing sectors. Two significant issues thus remain open. First: how can the catalogue of rights and freedoms be considered such that they can, conceptually, function as a scalable framework for the distillation of data processing obligations. Second: how can this conceptual approach be transferred into a practical framework which can be used, by data controllers, to distil when, and under what conditions data processing, is legitimate.

How should the concept of rights and freedoms apply to private actors? The catalogue of rights and freedoms in foundational European instruments describe the relationship between individuals and the state. Their use as a framework to establish data processing obligations relating to state actors is thus – except for the issue outlined in the paragraph above – unproblematic. How such concepts relate to private actors, however, is less clear. There are European legal concepts – such as the German Drittwirkung principle – which clarify how certain rights may apply to private actors in certain cases. These do not, however, provide comprehensive accounts of accounts of the applicability of fundamental rights to private actors. Two significant issues thus remain unresolved. First, to what extent can principles built on the relationship between states and individuals be logically applied to relationships between private actors and individuals in information processing. Second, how can the concept of rights and freedoms function as a practical framework in which private actors can distil when, and under what conditions, data processing is legitimate.

How will the concept of rights and freedoms be interpreted by Data Protection Authorities? Data Protection Authorities under the GDPR have considerable power. They are the entities tasked with providing clarity to the uncertainties inherent in the GDPR's provisions. They are also the entities which decide when, and to what degree, infringements of the GDPR are subject to sanctions. In this regard, how Data Protection Authorities choose to interpret the scope of the concept of rights and freedoms, the instances in which these substantive interpretations become relevant – for example in relation to which provisions – and how they choose to act on infringements of these interpretations will be definitive. It will make a huge difference, for example, whether Data Protection Authorities choose to treat the concept as a practically unusable oddity – regardless of what a positivistic reading of the law would suggest – or a solid benchmark against which processing legitimacy can be measured and sanctioned.

Accordingly – regardless of what the law states and the significance this superficially may be imbued with – there remain key open questions in relation to how the concept of rights and freedoms can, and will, conceptually and practically, be built into the corpus of European data protection law. Only as the answers to these questions crystalize over time, will the true substantive significance of the concept of rights and freedoms in the GDPR become clear.

## 9. CONCLUSION

Since early in the legislative process, commentators and scholars have sought to highlight the substantive novelties of the GDPR in relation to its predecessor, Directive 95/46. Commentators have noted, for example, the appearance of clearly novel substantive provisions – for example Data Portability rights and Data Protection Impact Assessment obligations – as well as significant substantive alterations to pre-existing provisions – for example the scale of possible administrative fines. There are aspects of substantive novelty in the GDPR, however, which have largely flown under the radar.

One such overlooked aspect of substantive novelty is the use of the concept of 'rights and freedoms'. The concept appears in three substantive forms in the GDPR. The first form is that of a scoping concept for the purpose of the law. This use of the concept is not novel. The second form is as a normative framework to be used in specifying the details of applicability of other concrete provisions in the GDPR. This use of the concept displays novelty in relation to the range of provisions in which it appears. The third form is as a stand-alone normative framework for evaluating the legitimacy and conditions of data processing over and above those elaborated by specific concrete data protection provisions. In this final form, the use of the concept is completely novel in the GDPR.

Contrary to the position of certain commentators, there is only one plausible definition available for the concept of rights and freedoms in the GDPR: the full catalogue of rights and freedoms outlined in foundational European fundamental and human rights instruments – in particular in the European Convention on Fundamental Rights and in the Charter of Fundamental Rights of the European Union.

In this regard, the use of the concept, theoretically at least, represents a deep shift in how European data protection law regulates information processing and the processing ecosystem this creates. Three aspects of this shift are particularly significant. First, the use of the concept represents a shift away from legislative attempts to identify, ex ante, data protection principles and towards a meta-regulatory approach in which the data controller is put in the position of evaluating the normative legitimacy and relevant safeguards in relation to a processing operation. Second, such a meta-regulatory approach will have impacts on the position and function of European Data Protection Authorities. These move from being technical agencies toward being guardians of fundamental rights in information. Third, such a meta-regulatory approach will create winners and losers amongst data controllers. Large controllers will be much better placed to engage in the required normative considerations.

Despite the above, there remain several open questions around the concept of rights and freedoms in the European data protection ecosystem. Indeed, only as the answers to these questions become clear, over time and practise, will the true significance of the use of the concept in the GDPR will become clear. Three questions, in particular, seem poignant. First, how can the concept of rights and freedoms be a basis for identifying data protection standards? Second, how should the concept of rights and freedoms apply in relation to private actors' processing? Finally, how will the concept of rights and freedoms be interpreted by Data Protection Authorities – they are, after all, the bodies who must eventually give life to the concept?

## BIBLIOGRAPHY

Albrecht, Jan Philipp, Lobbyism and the EU data protection reform, 12.02.2013. Available at: https://www.janalbrecht.eu/2013/02/2013-02-12-lobbyism-and-the-eu-data-protection-reform/. Last consulted: 20.04.2019.

Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 17/EN WP 248 rev.01, 2017.

Article 29 Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, 14/EN WP 218, 2014.

Bygrave, Lee, Data Protection Law: Approaching Its Rationale, Logic and Limits, Kluwer, London, 2002.

Clifford, Damian, Ausloos, Jef, Data Protection and the Role of Fairness, Yearbook of European Law, vol. 0, 2018, 1-58.

Commission of the European Communities, Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and information security, COM(90) 314 final, 1990.

Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14, ETS 005, 1950, Article 8, (Protocol 11, ETS 155, 1998), (Protocol 14, CETS 194, 2010).

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 1981.

Dalla Corte, Lorenzo, A Right to a Rule: On the substance and essence of the fundamental right to personal data protection, in Ronald Leenes, Dara Hallinan, Serge Gutwirth and Paul de Hert (eds.), Data Protection and Democracy, Hart, Oxford, Forthcoming 2019.

Datenschutzkonferenz, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier 18, 2018. Available at: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf. Last consulted: 19 November 2018.

De Hert, Paul, Citizens' Data and Technology: An optimistic perspective, Dutch Data Protection Authority, The Hague, 2009.

De Hert, Paul, Papakonstantinou, Vagelis, The new General Data Protection Regulation: Still a sound system for the protection of individuals?, Computer Law and Security Review, vol. 32, 2016, pp 179-194.

De Hert, Paul, Papakonstantinou, Vagelis, Wright, David et. al., The proposed Regulation and the construction of a principles-driven system for individual data protection, Innovation, vol. 26, no. 1-2, pp. 133-144.

Demetzou, Katerina, A teleological interpretation of the Scope of Risk in the GDPR, in Ronald Leenes, Dara Hallinan, Serge Gutwirth and Paul de Hert (eds.), Data Protection and Democracy, Hart, Oxford, Forthcoming 2019.

European Commission, A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 2010.

European Parliament and Council, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J., L 281/31, 23.11.1995.

European Parliament and Council, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J., L 119/1, 04.05.2016.

European Union, Charter of Fundamental Rights of the European Union, O.J., 326/02, 26.10.2012.

European Union, Treaty of Lisbon: Amending the Treaty on European Union and the Treaty Establishing the European Community, O.J., C306/01, 17.12.2007.

Gellert, Raphael, Understanding the risk-based approach to data protection: An analysis of the links between law, regulation, and risk, Vrije Universiteit Brussel, PhD Thesis, 2017

González Fuster, Gloria, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer, Heidelberg, 2014.

Jandt, Silke, Art. 35: Datenschutz-Folgenabschätzung, in Jürgen Kühling and Benedikt Buchner (eds.) DatenschutzGrundverordnung/BDSG, Beck, Munich, 2018, pp. 685-706.

Kosta, Eleni, Consent in European Data Protection Law, Martinus Nijhoff, Leiden, 2013.

Kuner, Christopher, The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Bloomberg BNA Privacy and Security Law Report, February 6, 2012, pp. 1-15.

Levy-Abegnoli, Julie, Viviane Reding: Data protection regulation one more step towards digital single market, The Parliament Magazine, 23 May 2016. Available at: https://www.theparliamentmagazine.eu/articles/interview/viviane-reding-data-protection-regulation-one-more-step-towards-digital-single. Last consulted: 20.04.2019.

Lynsky, Orla, The Foundations of EU Data Protection Law, Oxford University Press, Oxford, 2015.

Mayer-Schönberger, Viktor, Generational Development of Data Protection in Europe, in Technology and Privacy: The New Landscape, Phillip Agre and Marc Rotenberg (eds.), MIT Press, Cambridge, 1997, pp. 219-242.

Moerel, Lokke, Big Data Protection - How to make the Draft EU Regulation on Data Protection Future Proof, Tilburg University, Tilburg, 2014.

Organisation for Economic Cooperation and Development, OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 1980.

Schütz, Philip, Karaboga, Murat, Akteure, Interessenlagen und Regulierungspraxis im Datenschutz: Eine politikwissenschaftliche Perspektive, Fraunhofer ISI, Karlsruhe, 2015.

# DESPROTECCIÓN DE DATOS PERSONALES.

*La salida del precipicio por un camino virtuoso*


JUAN ANTONIO
**TRAVIESO**

*Juan Antonio Travieso. Doctor en Derecho. Profesor Titular de Derecho Internacional Público y de Derechos Humanos y Garantías, de la Facultad de Derecho de la Universidad de Buenos Aires. Autor de 15 libros y más de 100 publicaciones científicas. Premio UNESCO. Personalidad Destacada del Derecho declarado por la Legislatura de la Ciudad de Buenos Aires.*


## SUMARIO


**RESUMEN**

**I. INTRODUCCIÓN**

**II. LOS DATOS PERSONALES EN FOCO**

1. INFORME DE LA CÁMARA DE LOS COMUNES DEL REINO UNIDO: DESINFORMACIÓN Y NOTICIAS FALSAS. INFORME FINAL, EMITIDO EL 14 DE FEBRERO DE 2019.

*a. Obligaciones*

*b. Propaganda Política, Marketing y alfabetismo digital.*

*c. El Consentimiento*

2. WASHINGTON PONE EN LA MIRA EL PODER DE LAS CUATRO GRANDES TECNOLOGÍA.

3. AHORA OTRO PROBLEMA: FACEBOOK Y LAS CRIPTOMONEDAS.

**III. EL REGLAMENTO DE LA UNIÓN EUROPEA 679/2016 (RGDP) URUGUAY Y ARGENTINA**

**IV. EL FUTURO**

**V. CONCLUSIONES.UN NUEVO CAMINO: HACIA UN CÓDIGO DE ÉTICA EN DATOS PERSONALES**







## RESUMEN

El desarrollo de la tecnología ha puesto en tela de juicio todos los avances en materia de protección de datos personales. El problema se agrava con relación al crecimiento inusitado de las compañías superpoderosas tales como Facebook, Amazon, Google, Instagram, etc. Por otra parte la información constituye una mina de oro para la política para influir en las decisiones, alterando de alguna manera los procesos democráticos habituales. Otro factor a tener en cuenta es el avance de algunas compañías en el campo de las criptomonedas , en ámbitos muy regulados y con la intención de eludir regulaciones de los órganos de control . Toda esta situación genera un ámbito de desprotección de datos personales y la necesida de impulsar un camino virtuoso por medio de la ética


---

## I. INTRODUCCIÓN

Desde el patio de entrada de este trabajo se propone una petición de principios con un esquema dual. Nos encontramos ante un cruce de caminos y estamos perplejos. Por ahora, nuestro propósito inicial es superar el precipicio en el que estamos cayendo en cámara lenta.

La salida, como siempre es hacia arriba, pero no nos adelantaremos.

A veces suele considerarse que la protección de datos personales es sólo un capítulo, el más pequeño de las innovaciones tecnológicas. El tema es que la innovación tecnológica, en si, no es mala, lo malo es cuando se utiliza la innovación para afectar la privacidad de las personas.

Volviendo a la innovación, lo cierto es que estamos viviendo una época de grandes revoluciones y cambios. Hace pocos día en una entrevista Pat Gelsinger, director ejecutivo de VMware, opinó sobre la nube, la movilidad, la internet de las cosas y la Argentina. Hay que tener en cuenta que el entrevistados es el ejecutivo que ocupa el segundo puesto entre los más influyentes del mundo según el ranking 2018 elaborado por la revista Fortune. En la citada entrevista se le preguntó por las claves de las tecnologías "superpoderosas": cómputo en la nube, dispositivos móviles, internet de las cosas (IoT) e inteligencia artificial (IA). Lo interesante es que Gelsinger descarta la impresión 3D, la nanotecnología, el blockchain, la realidad virtual y los drones.

La respuesta tiene que ver con la realidad de que las tecnologías superpoderosas están penetrando en todas las industrias y en la sociedad a escala mundial y por tanto en la vida privada de cada uno de nosotros. Por ejemplo el cómputo en la nube, permite que todos podamos acceder a servicios que antes eran para unos pocos, y los dispositivos móviles ya están en casi el 60% de la población mundial y por otra parte, las cosas conectadas e inteligentes atraviesan todas las industrias e incluso están llegando a los hogares y a la vida privada.

Todas estas informaciones que ilustran sobre la realidad real y no virtual enfocan distintos aspectos, pero soslayan la existencia de datos alrededor de todas las tecnologías superpoderosas que se desarrollan como una gigantesca generadora de peligros y daños concretos a las personas.

De esta manera el derecho a ser dejado a solas de Brandeis, se transforma en una entelequia del siglo pasado. En ese sentido, hace pocos días escribimos un artículo donde reclamábamos por la privacidad perdida[1].

Ahora, continuamos con el tema y tratamos de alertar con miras a potenciar y revitalizar ese derecho para resguardar nuestra privacidad[2].

Mientras tanto nuestros celulares blanquean nuestras caras con su luz. Nosotros nos sentimos seguros, protegidos y equivocados.

## II. LOS DATOS PERSONALES EN FOCO

### 1. INFORME DE LA CÁMARA DE LOS COMUNES DEL REINO UNIDO: DESINFORMACIÓN Y NOTICIAS FALSAS. INFORME FINAL, EMITIDO EL 14 DE FEBRERO DE 2019.

Alarmados por la llamadas noticias falsas, (fake news) la Cámara de los Comunes del Reino Unido, propuso una e investigación parlamentaria que culmino con un extenso informe muy relacionado con los datos personales, pues la política, o mejor dicho la mala política abre el mundo de los datos privados con intenciones antijurídicas.

Así pues, la Cámara de los Comunes del Reino Unido, utilizó una metodología muy apropiada para encarar los problemas vinculados con el tema ex-

1 *Juan Antonio Travieso "En Busca de la Privacidad Perdida "Carpenter vs Estados Unidos". La Ley. 22 de marzo 2019*

2 *Juan Antonio Travieso "Régimen Jurídico de los Datos Personales , Abeledo Perrot 2014, Buenos Aires, Argentina*

puesto. Se trata de un reporte muy bien escrito y organizado. Compila casi 2 años de trabajo con los whistleblowers de Cambridge Analítica y otros.

Como se recordará. La cuestión se presentó luego de las escandalosas revelaciones del affaire Cambridge Analitics. Ese caso, disparó investigaciones y trabajos y luego de dos años de labor, el informe resulto una caja de resonancia de problemas muy serios que se hallan relacionados en el hecho de que es necesario una acción regulatoria toda vez que no se puede admitir que las grandes empresas de tecnología crezcan exponencialmente sin limitación o supervisión regulatoria apropiada. Lo cierto es que es necesario que los estados y sus gobiernos regulen este caos.

Como expresamos, el informe pone de relieve varios estudios relacionados con la actividad de las empresas Cambridge Analytics y Facebook, y cuestiones más amplias relativas a la utilización de datos personales por las compañías de medios sociales y la forma en que dichas empresas son responsables de la difusión de información errónea y desinformación. Cabe resaltar que se trata de información errónea pero que sobrevuela sobre los datos personales, que constituyen el material más valioso.

El interés del citado informe para las empresas de tecnología y redes sociales es evidente, ya que se dirige a ellas expresamente y propone cambios regulatorios concretos. En cuanto a las empresas en general, consideramos que deben seguir de cerca los avances de este tema, que interesará cada vez más a sus clientes y al público toda vez que pone en foco su privacidad. Y los datos personales.

Lo que se pone en tela de juicio es el "data compliance" de dichas industrias que deberá tomar en consideración las tendencias reflejadas que impactarán sobre los gobiernos y parlamentos y de manera intensa influirán en el entramado de los partidos políticos y la democracia.

*a. Obligaciones*

Todas las empresas se encuentran obligadas a proteger sus bases de datos y asegurar que la información será utilizada respetando el principio de finalidad y que no será accedida por terceros.

Aun cuando la información no sea su "core business", prácticamente todas las empresas manejan datos de sus clientes, en muchos casos masivamente y online. Por ello, tomar las medidas técnicas de seguridad apropiadas y manifestarse respecto de este tema en sus políticas de privacidad y normas de autorregulación, puede ser muy útil a fin de minimizar los riesgos a los que refiere el informe citado.

*b. Propaganda Política, Marketing y alfabetismo digital.*

El informe verifica que las empresas que procesan datos con fines de propaganda política recurren a los mecanismos del marketing digital. Es interesante que las empresas y otros actores de buena fe, que recurren a instrumentos de marketing directo estén alertados y atentos a estos usos ocultos o no manifiestos de las herramientas del marketing, para evitar ser usadas y expuestas en su reputación comercial.

Otro punto muy interesante referido en el informe tiene relación con el denominado alfabetismo digital. Evidentemente, se trata de un saber indispensable para los ciudadanos del mundo, a fin de ejercer plenamente su voluntad y libertad y además es un área en la que cualquier empresa debe contribuir, por ejemplo, como parte de sus programas de Responsabilidad Social Empresaria.

*c. El Consentimiento*

Se trata de un tema especialmente considerado por el informe. Para advertir lo señalado, seguidamente se acompañan las referencias al consentimiento en el informe de la Cámara de los Comunes:

En el punto 57 y ss. se menciona la multa máxima de (£500,000) impuesta por el ICO (Information Commissioner's Office) británico a Facebook en 2018, bajo la normativa anterior de protección de datos personales por falta de transparencia y por "permitir a las aplicaciones y a los desarrolladores de aplicaciones recolectar información personal de clientes que no habían dado su consentimiento.

En el punto 64 y ss. se hace referencia a Facebook y el "Consent Decree 2011" (Decreto de Consentimiento 2011) de la FTC ("Federal Trade Commission"), subrayándolo como un ejemplo del contraste entre los protocolos de seguridad de Facebook y sus prácticas. En 2011, la FTC de los Estados Unidos reclamó a Facebook por haber permitido (entre 2007 y 2010) acceso irrestricto a la información del perfil personal de los usuarios por parte de desarrolladores externos de aplicaciones, a pesar de haber informado a dicho usuarios que las App de la plataforma sólo accederían a dicha información en la medida necesaria para operar. En ese caso, Facebook debió acordar que obtendría el consentimiento para compartir datos con terceros, sin embargo, el reporte bajo análisis, señala que la orden de consentimiento de la FTC no





fue cumplida. También se deduce de lo expuesto, que, de haberse cumplido con el consentimiento, el escándalo de Cambridge Analytica se habría podido evitar.

En el punto 64 y ss. se mencionan los "acuerdos de listas blancas" entre Facebook y ciertas empresas, asegurando a éstas mantener pleno acceso a los datos de amigos de usuarios de manera posterior a algunas reformas en Facebook ,que podrían haber afectado esa capacidad. El informe advierte que no es claro en absoluto que se hayan recolectado los consentimientos necesarios para ello.

En el punto 142 se mencionan 1,069,852 emails propagandísticos enviados en 2016 por "Leave.EU" a suscriptores que habían consentido recibir emails de "Leave.EU", pero se destaca que las comunicaciones incluían marketing para servicios "GoSkippy" y descuentos, para lo cual "Leave.EU" no contaba con un consentimiento específico.

Por último, en el punto 190, se mencionan sofisticados sistemas de asociación de datos entre LinkedIn y Facebook que, combinados con otras herramientas, habrían podido ser usados por la empresa AIQ para dar a sus clientes políticos información clave para el targeting de su propaganda digital sin el consentimiento de los titulares de los datos

## 2. WASHINGTON PONE EN LA MIRA EL PODER DE LAS CUATRO GRANDES TECNOLOGÍAS

Con el telón de fondo expuesto, comienza a estallar el problema en la opinión pública estadounidense[3].

Hace pocos día el título de este acápite fue tema periodístico mundial y curiosamente en Estados Unidos de América, se han unido los dos partidos para investigar a los cuatro grandes : Amazon, Facebook, Google y Apple, en una primera etapa poniendo en mira la concentración económica y el monopolio.

Todo comenzó en ocasión del escándalo antes expuesto de Cambridge Analytics, que golpeó la reputación de Facebook abrió un abanico de cuestionamientos sobre los negocios y acciones de todas las empresas gigantes de tecnología.

El tema es la necesidad impostergable de controlar el poder de los gigantes tecnológicos que ha borrado todos los límites entre los dos grandes partidos de Estados Unidos de América.(USA)

3 *https://www.lanacion.com.ar/el-mundo/washington-pone-en-la-mira-el-poder-de-las-cuatro-grandes-tecnologicas-nid2258171*

En ese orden de ideas, hace pocos días la Cámara de representantes de USA anunció la apertura de una investigación sobre el hipotético comportamiento monopólico de los gigantes tecnológicos. El problema es entre Google, Facebook, Amazon y Apple y la necesidad de limitar y restringir de algún modo su poder monopólico. En el terreno de la competencia, a Google se la acusó básicamente de favorecer sus propios productos en las búsquedas que realizan los usuarios y de abusar de su influencia en el mercado publicitario.

Ahora bien, ¿Cuáles son las acciones de las empresas que provocan tales medidas, sus problemas y riesgos?. Veamos.

Con relación a Facebook el problema es que está a punto de convertirse en un monopolio en redes sociales, con la adquisición de Instagram y WhatsApp sin perjuicio de la invasión de la privacidad con relación a los datos personales.

Por otra parte, Amazon, controla la mitad del comercio online, y se la acusa de presionar a los vendedores que utilizan las App vinculadas abusando de su posición de de monopolio en su mercado de aplicaciones.

Google y Apple no levan a la zaga en incumplimientos y las acciones generan abusos y provocan la adopción de medidas.

Lo cierto es que en realidad, el poder de estas empresas comienza a representar un serio peligro para la democracia estadounidense por una parte y por la otra comienza a señalarse la necesidad de acciones regulatorias.

El problema es que estas industrias, de reciente data, han ido creciendo en control y poder económico de manera desmesurada, afectando la privacidad, los datos personales y en especial todo el sistema democrático.

El control quedará a cargo del Departamento de Justicia para Apple y Google y por otra parte, Amazon y Facebook quedarán bajo la supervisión de la FTC. Todos estos anuncios llevaron a que la cotización bursátil de las acciones de las cuatro compañías en algunos casos, como con Facebook llegaron a caer un 7%.

La cuestión tiene tal importancia que las cuatro compañías ya llevan gastado más de 55 millones de dólares en prácticas de lobby durante 2018. ¿Que ha sucedido con estas empresas?

El tema de la privacidad recién hace algunos años ha despertado la alarma en las personas. Todos hemos disfrutado y disfrutamos de la tecnología, sin imaginar que detrás de los progresos e inno-

vaciones, la cuestión clave consistía en adueñarse de la mina de oro de los datos personales.

Por ese motivo es que crece la intención de regular el proceder de estas empresas superpoderosas.

### 3. AHORA OTRO PROBLEMA: FACEBOOK Y LAS CRIPTOMONEDAS

El 22 de junio de 2019 un nueva noticia impactó en los medios. Ahora el tema es que Facebook intenta lanzar al mercado una criptomoneda a la que denominará "Libra".

Esta noticia ha generado un clima de desconfianza de los reguladores de todo el mundo. Ahora, no sólo desafían a los reguladores de datos personales, sino también a los Bancos Centrales del mundo entero.

Facebook ha informado que el proyecto Libra será lanzado en 2020 con la participación de Visa y MasterCard. De inmediato comenzaron a llover las críticas. El ministro de Finanzas Francés, Bruno Le Maire advirtió que la competencia soberana de crear moneda es privativa de los Estados, en plena coincidencia con el Gobernador del Banco de Inglaterra.

Se insiste que los bancos centrales y demás reguladores van a fijar las reglas de juego y Facebook deberá aceptarlas.

Hay que recordar que en el mundo de las finanzas hay principios férreos como la vigilancia y la protección del consumidor asegurándose los datos personales y la privacidad de las personas.

Distintos especialistas y personalidades han insistido en que se debe adoptar una posición clara, toda vez que el proyecto de moneda de Facebook constituye una prueba para la credibilidad de los gobiernos y los bancos centrales.

Ese es el panorama, pero al parecer la actividad regulatoria y de control no podrá ser eludida.

Pero hay algo más. Como expresamos, Facebook anunciará a finales de junio de 2019 su propia criptomoneda y además le permitirá a los empleados que trabajen en el proyecto que cobren parte de su sueldo en dicha moneda.

De acuerdo a un informe de The Information, Facebook planea ceder el control de la criptomoneda a terceros para asegurar así que el activo digital no esté totalmente centralizado.

Estos terceros pagaran hasta US$ 10 millones para actuar como nodos -es decir, tener la capacidad de validar transacciones- en la red para el token desarrollado por la compañía creada por Mark Zuckerberg.

Esta moneda, que estará integrada como herramienta de pago en todos los otros productos de la red social -WhatsApp, Facebook Messenger e Instagram-también estará disponible a través de cajeros automáticos físicos.

Hace pocos días, el Financial Times dio a conocer que la Commodity Futures Trading Commission (CFTC) de los Estados Unidos está en conversaciones con Facebook sobre su moneda. Asimismo, durante mayo de 2019 Facebook adquirió la marca "Libra" para su proyecto y también registró una nueva empresa en el Registro Mercantil de Ginebra, Suiza, Libra Networks LLC.

Como se advierte el panorama es de alta movilidad.

## III. EL REGLAMENTO DE LA UNIÓN EUROPEA 679/2016 (RGDP) URUGUAY Y ARGENTINA

Ahora bien, en el plano de los deslizamientos y antijuricidades expuestas, observamos que, por el contrario, en el ámbito de la Unión Europea el panorama es de control, regulación y buenas prácticas generando un circulo virtuoso.

Así entonces, y dentro de este mismo orden de ideas y concepto, en la Unión Europea se ha sancionado el Reglamento de la Unión Europea (RGDP) 679/2016 que entro en vigor desde el 25 de mayo de 2018 que deroga la Directiva 95/46.

Ante esta situación cabe preguntarse el motivo del interés en el RGDP. La respuesta es porque trata de estados de protección equivalente y protección adecuada como lo son entre otros, la República Oriental del Uruguay[4] y la República Argentina[5].

Entre otras normas, y en síntesis, las nuevas disposiciones del RGDP tratan sobre obligaciones rigurosas para las empresas que trabajan con datos, actualizaciones y revisiones periódicas, obligaciones en materia de transparencia y salvaguardias claras

Entre otros derechos se han establecido normas sobe transparencia, información, acceso, rectificación, derecho al olvido, limitación del tratamiento y portabilidad de datos.

4 *Uruguay. Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012*

5 *Argentina. Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003*





Por otra parte, asimismo hay también nuevas exigencias y personas a cargo del control interno de los datos personales como el Responsable y encargado del tratamiento de datos personales, delegado de protección de datos.

Todo ello implica un escenario donde impera la seguridad de datos personales, la Evaluación de Impacto, códigos de conducta y certificación, y Transferencia de datos personales a terceros.

También de manera resumida, las nuevas normas vigentes en la Unión Europea (RGDP) poseen varios pasos:

- Contemplar la privacidad en todos los procesos de la organización.
- La privacidad desarrollada desde el diseño (PBD).
- Establecer políticas de privacidad claras y fácilmente accesibles para los titulares del dato.
- Configurar por defecto como activadas, las opciones de privacidad.
- Permitir que los titulares de los datos ejecuten controles legales.
- Limitar la recolección de los datos a los estrictamente necesarios para el negocio.
- Asegurar los datos personales recabados dentro de un ámbito en el que todos sean responsables de la privacidad.

Cabe aclarar que por su parte la República Oriental del Uruguay ha producido cambios recientes en su legislación sobre Protección de Datos Personales.

Así pues, en enero de 2019 entró en vigencia la nueva Ley de Rendición de Cuentas, que incorpora importantes modificaciones a la legislación nacional sobre Protección de Datos Personales con el fin ofrecer mayores garantías a los uruguayos.

Asimismo, en octubre de 2018 fue promulgada la Ley de Rendición de Cuentas N°19.670, vigente desde enero de 2019, la cual contiene cuatro artículos que incorporan importantes modificaciones a la normativa de Protección de Datos Personales en Uruguay.

Dichos cambios tienen el objetivo de alinear la legislación nacional con los nuevos desarrollos en la materia, ofreciendo así mayores garantías a las personas para la protección de sus datos personales.

Los cambios a la legislación sobre Protección de Datos Personales (introducidos por los artículos 37 a 40 de la Ley de Rendición de Cuentas) son los siguientes:

- Ampliación del ámbito de aplicación de la Ley de Protección de Datos Personales
- Nuevas obligaciones para responsables y encargados de bases de datos
- Modificaciones al "principio de responsabilidad

El artículo 39 de la Ley de Rendición de Cuentas sustituye el antiguo artículo 12 de la Ley 18.331 de Protección de Datos Personales. La nueva redacción impone modificaciones al "principio de responsabilidad", estableciendo que tanto el responsable como el encargado de una base de datos son responsables de la violación de las disposiciones de la ley de protección de datos personales y **creación de la figura del "delegado de protección de datos".**

En lo que respecta a la República Argentina, como es de público conocimiento, la Dirección Nacional de Protección de Datos Personales dependiente de la Agencia de Acceso a la Información Pública (AAIP), elaboró un Anteproyecto que puso a consideración de entidades públicas, privadas, especialistas y público en general.

En ese sentido, se ha presentado al Poder Legislativo un Anteproyecto que se debatió y luego se presentaron sugerencias algunas de las cuales fueron receptadas.

La versión final fue elevada por la Agencia de Acceso a la Información Pública (AAIP)a consideración del Poder Ejecutivo Nacional y el 19 de Septiembre pasado ingresó al Senado de la Nación en las Comisiones de Asuntos Constitucionales y Derechos y Garantías.

En líneas generales el objetivos es actualizar las normas del año 2000 adecuarlas al Reglamento de Protección de Datos Personales de la Unión Europea. (RGDP) y en ese sentido, pues, se trata de actualizar el régimen legal sobre protección de datos personales vigente por medio de la adopción de normas más adecuadas a la realidad actual.

Otro objetivo, es ajustar las normas argentinas al Reglamento de Protección de Datos Personales aprobado en la Unión Europea y que entro en vigencia a partir del 25 de mayo de 2018.

Por otra parte, en la Argentina, además de lo expuesto, debe tenerse presente que de acuerdo con el Cap. XI, art. 89, las disposiciones del proyecto de Ley, entrarán en vigencia a los dos años de su publicación en el Boletín Oficial y, mientras tanto se mantiene la vigencia de las Leyes 25326, 26343

y 26951, sus normas reglamentarias y la restante normativa dictada por la Dirección Nacional de Protección de Datos Personales. Ello significa que el Proyecto, además de ser aprobado, requiere dos años más para entrar en vigencia.

## IV. EL FUTURO

Hemos analizado los cuestionamientos actuales en el ámbito de la protección de datos personales.

Pero es el caso que con la RGDP se ha instalado una pared de fuego que tanto la República Oriental del Uruguay y la Argentina han receptado en sus normas.

Ahora, en el plano virtuoso vemos los progresos que se avecinan en materia de protección de datos personales tales como modernización, aprovechamiento por parte de las empresas de un mercado único digital, menor burocracia, menores costos, más confianza de los consumidores, cooperación transfronteriza , libre circulación de datos siempre como finalidad la protección de personas físicas en el tratamiento de datos personales

Ante esos propósitos generales se plantea qué hacer y qué diligencias se deben ejecutar además de las reformas legislativas efectuadas y en curso.

Como siempre consideramos que todo lo que las empresas hagan en pos de una mayor transparencia en el uso de los datos, constituye un activo para ellas; estableciendo una ventaja competitiva frente a las demás.

Pero además, con el nuevo instituto de responsabilidad proactiva y la disminución de sanciones prevista para las empresas que hayan tomado las medidas apropiadas de prevención (ambos previstos en el Reglamento General de Protección de Datos (RGDP)y el proyecto de ley argentino de 2018), todas las medidas diligentes de protección que se adopten,-por sobre los estándares mínimos-, serán cada vez menos un "costo" y cada vez más la única vía eficiente de protección legal y reputacional para las empresas.

Otro punto que se destaca en algunas noticias es la relación de las "fake news" con el RGDP. Si bien Europa avanza en nuevas leyes contra la desinformación, ya existe en la RGDP una herramienta apta contra este flagelo digital. Al respecto, se menciona toda la información que el RGDP ordena transparentar en relación al tratamiento de datos con fines de marketing, lo cual importaría tener que revelar si los mismos son utilizados con fines propagandísticos.

Del mismo modo, se menciona el consentimiento que el RGDP ordena recolectar para cada uso en particular, lo que significaría que los usuarios puedan oponerse a que su información sea utilizada para influirlos políticamente.

Por otra parte, recordemos, además, las onerosas sanciones previstas en RGDP, de 20 millones de euros o el 4% de la facturación anual global, que sin duda contribuyen a su efecto disuasivo.

Parece ser una faceta no tan explorada o explotada del RGDP (la de ser una herramienta legal anti-fake news), pero que evidentemente existe en potencia y puede ser útil mientras no existen instrumentos legislativos más específicos.

## V. CONCLUSIONES.UN NUEVO CAMINO: HACIA UN CÓDIGO DE ÉTICA EN DATOS PERSONALES

Estimamos que hay una marcada tendencia a extremar los recaudos normativos hacia un tipo de regulación estricta sobre todo en áreas como publicidad proselitista, sin perjuicio de su posible e hipotética extensión a otros sectores, eventualmente comerciales.

Los diarios y la prensa están regulados, pero la publicidad en Facebook y Twitter y otras redes no tiene el mismo nivel de escrutinio regulatorio. Facebook va a tratar de evitar toda regulación y los ejemplos en Francia y Alemania nos dan una pauta del posible futuro en el Reino Unido.

Los políticos son reacios a regular porque ven a Facebook como un elemento de proselitismo de bajo costo y alta eficacia[6].

Lo cierto es que Facebook es una suma de incumplimientos y Zuckerberg ha optado por el negocio, en contraposición con la protección de datos. Es un tema de costos y aparentemente, los costos de las sanciones son inferiores a las ganancias, sin perjuicio del desprestigio que está haciendo mermar la participación mundial en Facebook.

Hasta ahora el sistema aplicado por Facebook ha sido incumplir y corregir después. Este año Facebook tendrá multas del orden del billón de dólares, tanto en USA como en Europa, y no solamente por la vigencia de los nuevos estándares de sanción de la RGDP.

Así pues, no dudamos en insistir en que consideramos que todo lo que las empresas hagan en pos de una mayor transparencia en el uso de los datos, constituye un activo para ellas; una ventaja competitiva frente a otras.

Insistimos en lo expuesto: evitar siempre las sanciones y multas y el costo reputacional.

Lo expuesto es condición necesaria pero no suficiente.

Falta un componente esencial: La ética[7].

¿Porque hay que insistir en la ética? ¿Por qué hay que tratar la ética junto con la tecnología, mezclada con el derecho? A veces tenemos la sensación de que este tema, parece extraño a las normas y más cercano a las reuniones de religiosos o de expertos en marketing de la palabra, en big data. Aquí, ingresamos en la relación entre ética, derecho y también tecnología. Un buen método de abordaje, puede ser por medio de la disciplina del derecho que, como la tecnología, ha irrumpido y se ha afianzado en la actualidad: el derecho Internacional de los Derechos Humanos (DIDH) que se ha establecido con inusitada velocidad, casi como la tecnología, salvando las diferencias.

Lo cierto es que la sociedad de la tecnología también esta interrelacionada con la ética. Afortunadamente, los cambios e innovaciones de la sociedad, en los distintos sectores, tienen a la ética como principal componente.

La lucha por los valores forma parte de la lucha para que la sociedad global además de global sea vivible. Para ello, es condición necesaria, pero no suficiente el compromiso personal con la ética. Hace falta el compromiso personal, nacional y por encima de las naciones el compromiso supranacional Porque no es el tema de aumentar la tecnología, sino aumentar la ética

Por tanto proponemos poner en práctica y funciones un Centro de Ética de datos que habrá de poner límites y establecerá estándares de cumplimiento, por medio del código de ética.

El Código de Ética debe ser desarrollado por expertos técnicos y supervisado por el regulador independiente, con el fin de fijar por escrito lo que es y no es aceptable en las redes sociales. Esto debe incluir contenidos ilícitos y nocivos y por supuesto buenas prácticas.

Prometimos salir del precipicio. Nuestro rumbo es el camino de la ética.

6 *Ver Bolsonaro en Brasil, Cambridge Analítica en Nigeria: https://www.theguardian.com/uk-news/2018/apr/04/cambridge-analytica-used-violent-video-to-try-to-influence-nigerian-election*

7 *Juan Antonio Travieso. Derecho y Tecnología: Historias y Dilemas. Editorial Publicia. España. 2018*

# EL ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES

*en el Derecho Uruguayo*


FERNANDO
**VARGAS**

*Fernando Vargas Coytinho es egresado en el año 1981 de la Facultad de Derecho y Ciencias Sociales de la Universidad de la República (UdelaR).*
*Actualmente es Socio Director del Estudio Vargas Abogados de la República Oriental del Uruguay.*
*Docente de las cátedras de Informática Jurídica y Derecho de las Telecomunicaciones de las Facultades de Derecho de la Universidad de Montevideo (UM) y de la Universidad Católica del Uruguay "Dámaso Antonio Larrañaga" (UCUDAL) y de la Universidad de la Empresa (UDE).*
*Asesor Legal de la Cámara Uruguaya de Tecnologías de la Información (CUTI); del Centro de Ensayo de Software (CES) y de la Federación de Asociaciones de Latinoamérica, El Caribe y España de Entidades de Tecnologías de la Información (ALETI).*
*Socio fundador y Director de Infojur, primera empresa uruguaya especializada en informática jurídica y de "El Derecho Digital", primer periódico jurídico digital uruguayo editado exclusivamente en Internet desde el año 1999. (www.elderechodigital.com).*


## SUMARIO


**RESUMEN**

**1. EL ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES**

**2. DEFINICIONES**

**3. RESPONSABLE DE LA BASE Y ENCARGADO DEL TRATAMIENTO. SUS DIFERENCIAS**

**4. CONTRATO DE ARRENDAMIENTO DE SERVICIOS (O DE OBRA)**

**5. LOS EMPLEADOS DEPENDIENTES**

**6. ÁMBITO TERRITORIAL**

**7. SEGURIDAD**

**8. SECRETO PROFESIONAL**

**9. RÉGIMEN DE RESPONSABILIDADES Y SANCIONES**

**10. CONSERVACIÓN Y DESTRUCCIÓN DE DOCUMENTOS**

**11. IMPUGNACIÓN DE VALORACIONES PERSONALES E INTELIGENCIA ARTIFICIAL**

**12. EL REGLAMENTO EUROPEO (RGPD) Y LOS ENCARGADOS DEL TRATAMIENTO**

**13. CONCLUSIONES**

**NORMATIVA ACTUALIZADA.**






## RESUMEN


En el artículo el autor desarrolla importantes conceptos vinculados a la figura del encargado de protección de datos, diferenciándolo de otras figuras existentes en la legislación nacional en la materia.

Se incluyen además de la evolución de la figura, el impacto de las nuevas modificaciones resultantes de la Ley N° 19.670 en las obligaciones y responsabilidades de los encargados.

Incluye entre los temas tratados el ejercicio de derechos ante los encargados y reseña la forma de tratamiento recibida por la figura en normas regionales a nivel internacional como el Reglamento General de Protección de Datos de la Unión Europea.

Reglamento referido. El manejo de grandes cantidades de información tratada y transferida a distintos puntos del mundo impone que los Estados traten de adoptar medidas de prevención y protección.

El objeto de este trabajo consistirá -justamente- en el examen de ambos tópicos, la figura del Encargados del tratamiento de los datos personales en el derecho uruguayo y cómo les afecta el Reglamento europeo cuando su comitente pertenece a la Unión.


## EL ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES EN EL DERECHO URUGUAYO

Transcurridos ya diez años desde la sanción de la Ley No. 18.331 y su Decreto Reglamentario No. 414/009, resulta oportuno analizar la evolución de la figura del Encargado del tratamiento de datos personales. Y si bien la misma no fue especialmente concebida para un tipo particular de organizaciones, sí es claro que el avance de la tecnología ha llevado a que las empresas de ese Sector -tanto de desarrollo de software y prestación de servicios informáticos como de comercio electrónico- son quienes han cumplido primordialmente esta función tan particular. Por eso nos proponemos en este trabajo abordar los principales aspectos que presenta esta actividad para las empresas del Sector tecnológico.

A su vez, la sanción en la Unión Europea del Reglamento General de Protección de Datos (RGPD o DPGR en inglés) y su reciente vigencia, ha generado una serie de consecuencias (y muchas dudas, obviamente) respecto a su incidencia en la actividad de las empresas uruguayas de tecnología que se desempeñan como Encargados del tratamiento de datos personales para Responsables europeos.

Cada vez más los cambios legislativos que surgen como consecuencia más o menos directa de avances tecnológicos no se limitan a los fenómenos ocurridos o producidos en una sola jurisdicción física, sino que tienen alcance y repercusiones internacionales. Justamente es éste el caso del

## 1. EL ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES

En nuestro país la Ley No. 18.331, de 11 de agosto de 2008 sobre Protección de Datos Personales (PDP) creó la figura del Encargado del tratamiento de datos y trajo aparejada una serie de consecuencias prácticas y jurídicas para la mayoría de las empresas del Sector tecnológico que tratan datos de manera informatizada para otras empresas.

Cabe precisar que además de la regulación que les será aplicable a estas empresas como titulares de sus propias bases de datos, muchas de ellas estarán a cargo de la gestión informatizada de las bases de datos de sus clientes, configurando así lo que la ley denomina "Encargado del tratamiento".

## 2. DEFINICIONES

La Ley define qué se entiende por "Bases de datos"; "dato personal" y "dato sensible", previendo la existencia de varios sujetos involucrados en su tratamiento. Así surge la figura del "Responsable de la base de datos o del tratamiento"; del "Titular de los datos"; del "Tercero"; del "Usuario de datos"; del "Destinatario" y del "Encargado del tratamiento". Cada una de estas figuras cuenta con definición concreta y regulación específica. Como dijimos, el objeto de este trabajo se centrará exclusivamente en el análisis de la figura del "Encargado del tratamiento" y las distintas connotaciones que la misma presenta.

El art. 4, literal H entiende por **"Encargado del tratamiento"** a la *"persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento"* Y agrega el propio art. 4, en su literal M qué se entiende por *"Tratamiento de datos: operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permitan el procesamiento de datos personales, así como también*

*su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias."*

Por tanto, si una empresa contrata acciones de marketing directo; desarrollos de inteligencia artificial para el tratamiento de los datos personales que se suben a su site, minería de esos datos; procesamiento informatizado; hospedaje web o de bases de datos en servidores de terceros, en la nube, etc. se estará bajo el ámbito de aplicación de la Ley.

A partir de esta definición y del relacionamiento de esta figura con las otras que mencionamos, así como del resto de la regulación que la normativa prevé, se extrae una serie de consecuencias jurídicas y prácticas que examinaremos a continuación y constituyen el objeto de este trabajo.

## 3. RESPONSABLE DE LA BASE Y ENCARGADO DEL TRATAMIENTO. SUS DIFERENCIAS

Se entiende por "Responsable de la base de datos o del tratamiento" a la *"persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento."* O sea, el Responsable de la base es "el dueño" de la base, el que en tal calidad dispone sobre la suerte de la misma y puede contratar determinados servicios para que otra persona física o jurídica, trate esos datos.

Mientras tanto, el "Encargado del tratamiento" como vimos, es la "persona física o jurídica, pública o privada, que sola o en conjunto" trata esos datos personales para el Responsable de la base. Parece que las diferencias son claras. El Encargado es una tercera entidad (empresa o profesional independiente) a la cual se le contrata un servicio determinado, en este caso, se la contratará para que preste el servicio de tratamiento de datos para el Responsable de la base de datos.

En todos los casos el relacionamiento jurídico que se establecerá entre ambos será de orden contractual y normalmente consistirá en un contrato de arrendamientos de servicios (o de obra), que tendrá por objeto principal que el comitente encarga a un tercero actividades que suponen el tratamiento de los datos que contienen las bases de datos de su propiedad. De esta forma, quedan claramente diferenciadas ambas figuras, las cuales tienen en la normativa una regulación particular en cuanto a sus responsabilidades.

## 4. CONTRATO DE ARRENDAMIENTO DE SERVICIOS (O DE OBRA)

No existe en la Ley ninguna obligación que establezca la existencia de un contrato de arrendamiento de servicios específico entre el Responsable de la base y el Encargado del tratamiento con el fin de establecer el alcance del tratamiento de los datos. Sin embargo, en nuestra opinión, su suscripción deviene imprescindible. Y aquí conviene diferenciar el contrato de servicios general (como podría ser la realización de marketing corporativo o alojamiento en la nube) con éste de Encargado del tratamiento.

El art. 30 de la Ley, bajo el acápite de "Prestación de servicios informatizados de datos personales" establece que *"Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aún para su conservación."* En este contrato específico -que podríamos calificar como accesorio al principal- se establecerán todos los derechos y obligaciones que tiene cada una de las partes a la luz de la normativa. Deberá preverse que el Encargado del tratamiento tratará los datos según las instrucciones que se le confieran; que no los utilizará con fines distintos a los previstos; que guardará secreto y confidencialidad sobre su contenido y –por tanto- que no los comunicará a otras personas fuera de la relación contractual. Más adelante volveremos sobre estos aspectos contractuales cuando veamos el Reglamento europeo.

Entendemos que resulta de especial significación la inclusión de cláusulas que prevean detalladamente el alcance de las obligaciones y responsabilidades de cada parte, ya que el Responsable de la base de datos tendrá frente a los órganos de control las suyas propias y las derivadas de los presuntos incumplimientos o violaciones en que pueda incurrir o hacerle incurrir el Encargado del tratamiento.

El texto original de la ley fue modificado de modo de subsanar la contradicción que existía entre el "Principio de responsabilidad" previsto en el art. 12 "El Responsable de la base de datos es responsable de la violación de las disposiciones de la presente ley" y el art. 35 que facultaba al órgano de control a sancionar también al Encargado del tratamiento. En la redacción actual, el artículo 12 establece que *"El responsable de la base de datos o tratamiento y el encargado, en su caso, serán responsables por violación de las disposiciones de la presente ley."*





El contrato deberá establecer específicamente –entre otros puntos de interés- qué pasará en caso que el Encargado del tratamiento incurra en incumplimientos que sometan al Responsable de la base a sanciones por parte de las autoridades o por reclamaciones de terceros. Dado que el Encargado del tratamiento tendrá sus propias responsabilidades y las que le genere al Responsable de la base como consecuencia de sus posibles incumplimientos al contrato, deberá establecerse de forma expresa y clara la posibilidad de repetición entre ambos; garantías de cumplimiento y eventuales retenciones o suspensiones del pago del precio del arrendamiento para compensar las sanciones que afronte el Responsable.

Se introduce en nuestro ordenamiento, sin mencionarlo específicamente como tal, el ***"principio de responsabilidad proactiva"*** que también contempla el Reglamento europeo.

*"En ejercicio de una responsabilidad proactiva, deberán adoptar las medidas técnicas y organizativas apropiadas ..."* Resulta claro que de no tomarse a tiempo medidas preventivas o correctivas, técnicas u organizativas, una falla de seguridad puede irrogar importantes perjuicios para los titulares de los datos, ya sean materiales o no. Discriminación, daño a la reputación, apropiación de identidad digital, patrimonio financiero, confidencialidad, etc. son algunos de los más notorios.

Por ello se exige al Encargado del tratamiento que adopte inmediatamente medidas que eliminen, reduzcan o minimicen los eventuales daños y que informe con toda la diligencia posible a la autoridad competente. La propia norma encomendó a la reglamentación determinar las medidas específicas que corresponderán en cada caso.

## 5. LOS EMPLEADOS DEPENDIENTES

A partir de la modalidad contractual que venimos de analizar en el literal anterior, corresponde analizar la situación jurídica de los dependientes del Responsable de la base y del Encargado del tratamiento.

En una primera lectura, la definición tan amplia conferida por la ley al Encargado del tratamiento (persona que trate datos personales por cuenta del titular de la base) haría pensar que los empleados dependientes del Responsable de la base encuadrarían dentro de esa categoría y todas las disposiciones atinentes al Encargado del tratamiento serían aplicables a ellos. Sin embargo, no participamos de esta solución ya que la propia norma, en su art. 4 literal J), prevé la existencia de "personas autorizadas para tratar los datos bajo la autoridad directa del responsable ...", siendo ésta la situación exacta a nuestro entender. No se trata de un Encargado del tratamiento en el concepto de la ley, sino que son los propios dependientes del Responsable de la base que trabajan con los datos bajo la responsabilidad directa de su empleador.

La misma situación se plantea respecto a los dependientes del Encargado del tratamiento, para quienes postulamos una solución idéntica. Los empleados dependientes del Encargado del tratamiento no se constituyen a su vez en Encargados de tratamiento ellos mismos, sino que son personas autorizadas a tratar los datos bajo la responsabilidad de su empleador.

A su vez, el art. 4, lit. B) define a la comunicación de datos como *"toda revelación de datos realizada a una persona distinta del titular de los datos"*, mientras que el art. 17 agrega que *"Los datos personales objeto de tratamiento sólo podrán ser comunicados ... con el previo consentimiento del titular de los datos al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permiten hacerlo".*

Una consecuencia práctica que se deriva de esta problemática está relacionada al consentimiento previo del titular de los datos, pues si los dependientes y empresas subcontratadas fueran considerados Encargados del tratamiento -y a su vez se entiende que para con ellos existe comunicación en los términos de la Ley-, tendría que requerirse el consentimiento previo del titular ya que los datos sólo podrían ser comunicados *"con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar el destinatario o los elementos que permitan hacerlo"*

La reglamentación aclaró un poco este punto. El art. 14 in fine del Decreto 414/009 previó que "No se considera comunicación o cesión de datos el acceso por parte de un encargado de tratamiento, que resulte necesario para la prestación de un servicio al responsable, salvo que este acceso implique la existencia de un nuevo vínculo entre el encargado del tratamiento y el titular".

## 6. ÁMBITO TERRITORIAL

El artículo 37 de la ley No. 19.670, de 15 de octubre de 2018 dispuso que el tratamiento de datos por parte de un Encargado del tratamiento se regirá por la normativa uruguaya cuando se encuentre establecido en territorio uruguayo.

También será de aplicación nuestra legislación, cuando el tratamiento esté relacionado con bienes o servicios dirigidos a los habitantes del país; se refieran a su comportamiento; cuando existan normas internacionales o disposiciones contractuales al respecto y, particularmente si los medios utilizados para el tratamiento se encuentran en el territorio nacional. Agrega que tratándose de un tratamiento que implique exclusivamente el "tránsito" de los datos, el Responsable podrá exceptuarse de la normativa designando un representante ante el organismo de control.

Esta norma vino a reforzar jerárquicamente, modificándolo de manera parcial, al artículo 3 del Decreto reglamentario del año 2009. Ahora se incluye expresamente al Encargado del tratamiento. Una vez que se apruebe la reglamentación se podrá profundizar respecto al alcance que pretende dársele a la misma, aunque ya puede pronosticarse que muchas empresas de primer orden internacional se verán afectadas por este cambio.

## 7. SEGURIDAD

Otra de las novedades introducidas recientemente en la legislación patria que alcanza al Encargado del tratamiento de los datos, la constituye el artículo 38 de la ley No. 19.670, de 15 de octubre de 2018. Al igual que en el caso anterior, veremos luego que ambas disposiciones están "inspiradas" y son similares al Reglamento europeo.

En efecto, se genera una nueva obligación para el Encargado imponiéndosele que cuando *"tome conocimiento de la ocurrencia de la vulneración de seguridad, deberá informar inmediata y pormenorizadamente"* a los titulares de los datos y al órgano de contralor (URCDP), así como de las medidas que hubiere adoptado.

## 8. SECRETO PROFESIONAL

Hasta ahora constituía una práctica habitual en la celebración de contratos de arrendamiento de servicios que implicaban también el manejo de datos a cargo del comitente por parte de una empresa contratada, incluir una o más cláusulas sobre la confidencialidad y reserva que debía mantenerse.

A partir de la Ley, sin importar si existe o no esta cláusula contractual, se le asigna la calidad de "secreto profesional (art. 302 del Código Penal)" a la obligación que tienen los que por *"su situación laboral u otra forma de relación con el responsable de una base de datos, están obligadas a guardar estricto silencio."* (art. 11) Esta norma alcanza a los empleados dependientes del Responsable de la base de datos y a cualquier contratista que acceda a los datos -como sería el caso del Encargado del tratamiento-, aún a los dependientes de este último. La obligación no tiene plazo de finalización, ya que el párrafo final del artículo establece que *"... subsistirá aún después de finalizada la relación con el responsable de la base de datos."*

## 9. RÉGIMEN DE RESPONSABILIDADES Y SANCIONES

El art. 35 determina que *"El órgano de control podrá aplicar las siguientes sanciones a los responsables de las bases de datos, encargados de tratamiento de datos personales y demás sujetos alcanzados por el régimen legal, en caso que se violen las normas de la presente ley, las que se graduarán en atención a la gravedad, reiteración o reincidencia de la infracción cometida"*

De aquí que el Encargado del tratamiento tiene legitimación pasiva para ser sancionado directamente por el órgano de control en caso de que viole alguna disposición de la ley. Esta es la primera cuestión que surge al estudiar este artículo, pero no es la única.

El numeral 4 del artículo incluye dentro de la gama de sanciones posibles la *"Suspensión de la base de datos respectiva por el plazo de cinco días"*. Esta medida extrema afectará siempre al Responsable de la base ya que no podrá contar con la misma por el tiempo que dure la suspensión. Sin embargo, como vimos, la sanción puede derivar de su propio incumplimiento o del que incurra el Encargado del tratamiento.

En las otras sanciones previstas (observación, apercibimiento o multa) el órgano de control, al comprobar que el Responsable de la base no es quien directamente dio mérito al incumplimiento, podría optar por sancionar exclusivamente al Encargado del tratamiento si es éste el que incurrió en responsabilidad. Pero en el caso de suspensión administrativa o judicial de la base por responsabilidad del Encargado del tratamiento, siempre se verá afectado el Responsable de la base y esta posibilidad deberá ser contemplada en el contrato de arrendamiento de servicios suscrito entre ambos.

Por último en cuanto a este punto, resulta de dudosa constitucionalidad la posibilidad que tiene el órgano de control para clausurar la base de datos por una medida administrativa. En efecto, el artículo 35 faculta a la URCDP a promover ante los órganos jurisdiccionales competentes la clausura de la base de datos. Hasta ahí parece razonable y ajustado a derecho el procedimiento, pero el párrafo siguiente de este artículo prevé que *"... quedará habilitada a disponerla por sí en caso que el Juez no se pronunciare dentro de dicho término"*. De esta forma, la clausura temporal sería tomada directamente en sede administrativa sin las mínimas garantías del caso para el administrado (Responsable de la base) pues en ningún lado se establece la posibilidad de que el mismo ejerza su derecho constitucional al debido proceso.

## 10. CONSERVACIÓN Y DESTRUCCIÓN DE DOCUMENTOS

El art. 30 de la ley prevé la hipótesis específica de la empresa informática que es contratada por el dueño de la base de datos para realizar el tratamiento informático de los mismos. Así, establece que *"Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aún para su conservación."*

Este párrafo presupone lo que ya habíamos visto en cuanto a la tercerización del tratamiento informático de los datos en una empresa de tecnología y la necesidad de la suscripción de un contrato adicional al de arrendamiento de servicios, el cual deberá regular el alcance de esta tarea específica.

Más adelante, el artículo dice que una vez cumplido el contrato *"los datos personales tratados deberán ser destruidos"*. Este es el principio general que sienta la norma, aunque no es de carácter absoluto pues agrega que puede existir una autorización expresa para que los mantenga en su poder si *"razonablemente se presume la posibilidad de ulteriores encargos"*. En este caso el plazo máximo de conservación de los datos será de "hasta dos años".

## 11. IMPUGNACIÓN DE VALORACIONES PERSONALES E INTELIGENCIA ARTIFICIAL

Este es a nuestro entender un tema realmente trascendente de la Ley. Bajo el acápite de "Derecho a la impugnación de valoraciones personales", el art. 16 establece que *"las personas tienen derecho a no verse sometidas a una decisión con efectos jurídicos que les afecte de manera significativa"* en base al tratamiento automatizado de datos.

En este caso, se le otorga el derecho a obtener del Responsable de la base información *"tanto sobre los criterios de valoración como sobre el programa utilizado en el tratamiento que sirvió para adoptar la decisión manifestada en el acto."*

Esto significa que si una persona se presenta ante el Responsable de una base de datos, creyéndose "afectada de manera significativa" por una decisión que se tomó sobre su comportamiento, el Responsable de la base deberá proporcionarle los criterios de valoración que utiliza y proveerle el acceso al programa de ordenador empleado para el tratamiento de los datos.

Pero resulta que, en la mayoría de los casos, ni unos ni otros están en poder del dueño de la base. Es frecuente que empresas especializadas en este tipo de tratamiento (inteligencia artificial, minería de datos, por ejemplo) provean estos servicios de manera tercerizada a los Responsables de las bases. Con el agravante que en muchos casos ni siquiera son empresas que se encuentran instaladas en el mismo territorio que el Responsable. Y obviamente que estas empresas cuidan celosamente ese "know How" que les permite desarrollar el programa y que el mismo constituye un secreto comercial de la empresa. El responsable sólo contará con una licencia de uso pero no tendrá el código fuente, los algoritmos ni los criterios de ponderación.

Y un elemento no menor. Los programas de inteligencia artificial presentan el problema de las ***"cajas negras"***. Como se sabe, estos sistemas funcionan fundamentalmente por algoritmos, entendidos estos como *"un conjunto ordenado y finito de operaciones que permite hallar la solución de un problema"* (Real Academia Española) Ahora bien, los algoritmos que utilizan los datos personales de los usuarios son quienes originan el comportamiento del sistema, ya sea para sugerirnos música, películas, publicidad o resultados en una búsqueda conceptual. La justicia, el acierto o la ausencia de error en el resultado dependerá de cómo estén configurados y diseñados esos algoritmos. Y el problema no sería mayor si sólo se tratara de una película o canción errónea, pero resulta que estos algoritmos pueden determinar que una persona sea impedida de acceder a un trabajo, de ingresar a un evento o -lo que es mucho peor- de ser ingresado a una base de datos de posibles delincuentes reincidentes o a quienes no se le otorgue una libertad anticipada.

Esto nos lleva a dos conclusiones, por un lado, la configuración y diseño de esos algoritmos son

secretos comerciales fuertemente resguardados por los creadores, quienes no permiten el acceso a los mismos. Pero aún en el caso que se pudiera acceder al código de programación, en muchos casos esos algoritmos trabajan con las denominadas ***"cajas negras"*** lo que implica que ni los propios creadores del sistema pueden explicar los resultados y el proceso que llevó a la toma de decisión final.

Cómo encontrar una solución que permita articular la norma (art. 16 in fine de la ley) con esta realidad es tarea de jueces, legisladores y fundamentalmente de los órganos de control especializados, quienes deberán considerar la evolución de la tecnología que les impone estas situaciones.

## 12. EL REGLAMENTO EUROPEO (RGPD) Y LOS ENCARGADOS DEL TRATAMIENTO

Lo primero que hay que tener en cuenta es que el Reglamento se aplica tanto a Responsables como Encargados del tratamiento establecidos en la Unión, independientemente que el tratamiento de los datos se realice o no en el territorio europeo (art. 3, numeral 1). En este último caso existiría una transferencia internacional de datos.

También se aplica el Reglamento, según el mismo artículo 3 numeral 2, cuando se trata de responsables o encargados que residen fuera de la Unión pero ofrecen bienes, servicios o realizan un control del comportamiento de los titulares de los datos que sí residen en la Unión.

El propio Reglamento en sus Considerandos, luego de afirmar que "*La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental*" (1) explica "*La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial ... Estos avances requieren un marco más sólido y coherente para la protección de datos ... Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas.*" (6)

En el mismo sentido, el Considerando 23 expone detalladamente este criterio: "*Con el fin de garantizar que las personas físicas no se vean privadas de la protección a la que tienen derecho en virtud del presente Reglamento, el tratamiento de datos personales de interesados que residen en la Unión por un responsable o un encargado no establecido en la Unión debe regirse por el presente Reglamento si las actividades de tratamiento se refieren a la oferta de bienes o servicios a dichos interesados, independientemente de que medie pago.*"

El artículo 28 del Reglamento contempla específicamente la figura del Encargado del tratamiento. Analizaremos los aspectos más destacados que se relacionen directamente con el objeto de este numeral, o sea, lo que puede alcanzar a las empresas de tecnología de nuestro país que presten servicios para Responsables o Encargados del tratamiento europeos alcanzados por el Reglamento, destacándose lo siguiente:

a. El Responsable deberá elegir un Encargado que "ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas"

b. El Encargado deberá requerir autorización previa y escrita del Responsable cuando deba recurrir a otro Encargado del tratamiento.

c. Se requerirá un contrato u otro acto jurídico específico que vincule al Responsable con el Encargado. El documento debe ser escrito, admitiéndose el formato electrónico. La norma detalla pormenorizadamente el alcance de dicho contrato, destacándose la necesidad de autorizar la transferencia internacional de los datos fuera del territorio de la Unión y la posibilidad de recurrir a un sub Encargado del tratamiento.

d. Si se contrata un sub Encargado deberá cumplir con todas las obligaciones previstas en el contrato principal entre el Responsable y el Encargado que lo subcontrató.

e. Garantizar la obligación de confidencialidad respecto a las personas que intervengan en el tratamiento.

f. Colaborar con el Responsable para responder las solicitudes de ejercicio de los derechos que tienen los titulares de los datos, así como para elaborar informes que permitan al Responsable comprobar que ha cumplido con sus obligaciones legales.

g. Deberá devolver al Responsable o suprimir los datos una vez que concluya su actuación, excepto que se acuerdo lo contrario en cumplimiento de otras normas.

h. Deberá llevar un registro de las categorías de actividades de tratamiento que ha efectuado para el Responsable. Estos registros también deberán ser escritos y se podrán emitir en formato electrónico.

i. Aplicará medidas técnicas y organizativas apropiadas para garantizar una seguridad adecuada a los datos que trata. Estas medidas deberán estar en consonancia con el alcance, la naturaleza y los fines del tratamiento, así como con los costos en relación a las probabilidades y riesgos para los titulares de los datos.

j. El Encargado deberá notificar inmediatamente ("sin dilación indebida" dice el art. 33) al Responsable cualquier violación de seguridad que conozca, lo que implicará la previsión de un procedimiento específico a tales fines.

Por último, aunque no menos importante, se prevé que el Encargado del tratamiento ***"designará"*** un Delegado de protección de datos cuando sus actividades consistan en operaciones que requieran "una observación habitual y sistemática de interesados a gran escala" o también cuando "consistan en el tratamiento a gran escala de categorías especiales de datos personales" (datos sensibles y relativos antecedentes penales)

## 13. CONCLUSIONES

De lo expuesto, cabe concluir que el transcurso de más de un decenio de aprobada la ley de protección de datos personales en nuestro país, así como la reciente sanción y entrada en vigencia del Reglamento europeo sobre esta temática, supuso para las empresas pertenecientes al Sector TICs que actúan como Encargados del tratamiento de datos personales, una serie de beneficios y obligaciones en su actuación.

Respecto a los primeros es claro que la normativa aprobada, consistente con los estándares internacionales más altos, conjuntamente con el reconocimiento a nuestro país en el año 2012 por parte de la Unión Europea de un nivel de protección adecuado de los datos personales transferidos, produjo un ámbito propicio para el desarrollo de actividades de este tipo y fue aprovechado por las empresas del sector tecnológico.

A su vez, esta nueva normativa obliga a las empresas a profesionalizar su gestión, y no sólo en los aspectos técnicos sino también en su infraestructura comercial y jurídica, de modo de adecuarse a los requerimientos nacionales e internacionales.

Indirectamente, esta adecuación les posibilita cumplir con gran parte de las previsiones del Reglamento europeo, lo que agranda enormemente sus posibilidades de trabajo.

Podríamos decir que "la mesa está servida" así que ahora sólo dependerá de las empresas, de sus expectativas y capacidades, para aprovechar esta coyuntura internacional.

***Normativa actualizada.***


1. Ley No. 18.331 de 11 de agosto de 2008
2. Decreto No. 664/008 de 22 de diciembre de 2008.
3. Decreto Reglamentario No. 414/009 de 31 de agosto de 2009
4. Decreto No. 437/009 de 28 de setiembre de 2009
5. Ley No. 18.719 de 27 de diciembre de 2010, arts. 152 a 156.
6. Ley No. 18.996 de 7 de noviembre de 2012.
7. Ley No. 19.355 de 19 de diciembre de 2015, arts. 83 y 84.
8. Ley No. 19.438 de 14 de octubre de 2016.
9. Ley No. 19.670 de 15 e octubre de 2018, art. 39.
10. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

# CONVENIO 108 Y TEXTO EXPLICATIVO



**TRADUCCIÓN N°. 025/2019. CONVENIO PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO DE DATOS PERSONALES**

/Documento extendido en 18 fojas, redactado en idiomas inglés y francés. En el margen inferior, las páginas se encuentran numeradas y obra la leyenda "Convenio 108+". A solicitud de parte interesada, se traduce únicamente el texto en idioma inglés. A continuación, se traducen las primeras 8 fojas./

/A fojas 1:/

/Obra imagen con personas y números./

**Convenio 108+**

Convenio para la protección de las personas con respecto al tratamiento de datos personales

www.coe.int/dataprotection

/Obra bandera del Consejo de Europa./

Consejo de Europa

/Al dorso de fojas 1:/

**Convenio 108+**

Convenio para la protección de las personas con respecto al tratamiento de datos personales

Consejo de Europa

/A fojas 2:/

Edición en francés:

*Convention 108+*

*Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel*



Foto: Shutterstock

Diseño gráfico de la portada: Departamento de Producción de Documentos y Publicaciones (SPDP, por sus siglas en inglés), Consejo de Europa



Impreso en el Consejo de Europa

/Al dorso de fojas 2:/

**Contenido**

DECISIÓN DEL COMITÉ DE MINISTROS: 5

CONVENIO PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO DE DATOS PERSONALES ACTUALIZADO: 7

INFORME EXPLICATIVO: 15

/A fojas 3. Página en blanco/

/Al dorso de fojas 3:/

**Decisión del Comité de Ministros**

Sesión N° 128 del Comité de Ministros, Elsinor, 18 de mayo de 2018

Decisiones

El Comité de Ministros

1. tomó nota de la Opinión n° 296 (2017) de la Asamblea Parlamentaria con respecto al borrador del Protocolo modificando el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos Personales (ETS n° 108);

2. adoptó el Protocolo modificando el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos Personales (ETS n° 108), tal como aparece en el documento CM(2018)2-final, y, como instrumento relacionado con el Protocolo, aprobó el Informe Explicativo, tal como aparece en el documento CM(2018)2-addfinal;

3. recalcó la importancia de una rápida adhesión del máximo de los Estados Partes del Convenio N° 108 al Protocolo, a los efectos de facilitar la formación de un régimen legal general sobre la protección de datos de acuerdo con el Convenio actualizado, así como asegurar la mayor representación posible de los Estados en el Comité del Convenio;

4. decidió abrir el Protocolo a suscripción el 25 de junio de 2018* durante la tercera parte de la sesión de la Asamblea Parlamentaria, en Estrasburgo;

/nota al pie de página*:/ El Comité de Ministros decidió posponer la apertura a suscripción hasta el 10 de octubre de 2018).

5. insistió a los Estados miembros y a otras Partes del Convenio a tomar sin demora las medidas necesarias para permitir que el Protocolo entre en vigencia en un plazo de tres años a partir de su apertura a suscripción y a iniciar de forma inmediata, pero en cualquier caso en un plazo no mayor a un año a partir de la fecha en la cual el Protocolo fue abierto a suscripción, el proceso de adecuación de las leyes nacionales para ratificar, aprobar o aceptar dicho Protocolo;

6. destacó que, luego de la entrada en vigencia del Convenio modificado de acuerdo con las disposiciones del Artículo 37(2) del Protocolo, solo aquellos Estados que hayan ratificado, aprobado o aceptado el Protocolo se verán obligados por las obligaciones que surjan del Convenio modificado;

7. indicó a sus Ministros Adjuntos que revisen semestralmente, comenzando por primera vez al cumplirse un año de la apertura del Protocolo a suscripción, el progreso general de ratificación, en base a la información a ser brindada al Secretario General por cada Estado miembro y otras Partes del Convenio por lo menos un mes antes de dicha revisión.

/A fojas 4. Página en blanco/

/Del dorso de fojas 4 a fojas 8:/

**Convenio para la Protección de las Personas con respecto al Tratamiento de Datos Personales Actualizado*** /nota al pie de página*:/ Protocolo de enmienda del Convenio para la Protección de las Personas con respecto al Tratamiento de Datos Personales, adoptado por el Comité de Ministros en su sesión N° 128 en Elsinor el 18 de mayo de 2018.

**Preámbulo**

Los Estados Miembros del Consejo de Europa, y los demás signatarios del presente,

Considerando que el objetivo del Consejo de Europa es lograr una mayor unión entre sus miembros, basándose particularmente en el respeto de la ley, los derechos humanos y las libertades fundamentales;

Considerando que es necesario asegurar la dignidad humana y la protección de los derechos humanos, así como las libertades fundamentales de cada individuo y considerando la diversificación, intensificación y globalización del tratamiento de datos y el flujo de datos personales, la autonomía personal teniendo en cuenta el derecho de los individuos a controlar sus datos personales y el tratamiento de dichos datos;

Recordando que el derecho a la protección de datos personales debe ser considerado con referencia a su rol en la sociedad y que debe ser conciliado con otros derechos humanos y libertades fundamentales, incluyendo la libertad de expresión;

Considerando que el presente Convenio permite tomar en cuenta, en la implementación de las normas establecidas en el mismo, el principio de derecho al acceso a documentos públicos;

Reconociendo que es necesario promover a nivel mundial los valores fundamentales de respeto de la privacidad y de la protección de datos personales, y así contribuir al libre flujo de información entre las personas;





Reconociendo el interés de reafirmar la cooperación internacional entre las Partes del Convenio,

Acuerdan lo siguiente:

**Capítulo I – Disposiciones Generales**

**Artículo 1 – Objeto**

El objeto del presente Convenio es proteger a todos los individuos, sin importar su nacionalidad o residencia, con respecto al tratamiento de sus datos personales, de manera de contribuir al respeto de sus derechos humanos y libertades fundamentales y, en particular, al derecho a la privacidad.

**Artículo 2 – Definiciones**

A los efectos del presente Convenio:

a. “datos personales” significa cualquier información con respecto a un individuo identificado o identificable (“titular de datos”);

b. “tratamiento de datos” significa cualquier operación o conjunto de operaciones llevadas a cabo sobre los datos personales, tales como su recopilación, almacenamiento, preservación, alteración, recuperación, divulgación, suministro, eliminación o destrucción, o llevar a cabo operaciones lógicas y/o aritméticas sobre dichos datos;

c. cuando no se utiliza tratamiento automatizado, “tratamiento de datos” significa una operación o conjunto de operaciones llevadas a cabo sobre los datos personales dentro de un conjunto estructurado de dichos datos, que son accesibles o recuperables de acuerdo con criterios específicos;

d. “responsable del tratamiento” significa la persona física o jurídica, autoridad pública, servicio, agencia o cualquier otro organismo que, individual o conjuntamente con otros, tiene poder de decisión respecto al tratamiento de datos;

e. “destinatario” significa una persona física o jurídica, autoridad pública, servicio, agencia o cualquier otro organismo a la cual se le revelan o suministran datos;

f. “encargado del tratamiento” significa una persona física o jurídica, autoridad pública, servicio, agencia o cualquier otro organismo que trate los datos personales en nombre del responsable del tratamiento.

**Artículo 3 – Alcance**

1. Cada Parte asume la obligación de aplicar este Convenio al tratamiento de datos dentro de su jurisdicción en los sectores público y privado, garantizando de este modo el derecho a la protección de los datos personales de cada individuo.

2. El presente Convenio no se aplicará al tratamiento de datos llevado a cabo por un individuo en el curso de actividades exclusivamente personales o domésticas.

**Capítulo II – Principios básicos para la protección de datos personales**

**Artículo 4 – Obligaciones de las partes**

1. Cada Parte deberá tomar las medidas necesarias conforme a sus leyes para poder efectivizar las disposiciones del presente Convenio y asegurar su aplicación efectiva.

2. Cada Parte deberá tomar dichas medidas, las que deberán haber entrado en vigencia al momento de la ratificación o adhesión al presente Convenio.

3. Cada Parte asume la obligación de:

a. permitir al Comité del Convenio previsto por el Capítulo VI la evaluación de la efectividad de las medidas tomadas conforme a sus leyes para efectivizar las disposiciones del presente Convenio; y

b. contribuir activamente con este proceso de evaluación.

**Artículo 5 – Legitimidad del tratamiento de datos y calidad de los datos**

1. El tratamiento de datos deberá ser proporcional al fin legítimo perseguido y reflejará en todas las etapas de tratamiento un equilibrio justo entre todos los intereses involucrados, ya sean públicos o privados, así como los derechos y las libertades en juego.

2. Cada parte deberá prever que el tratamiento de datos se llevará a cabo en base al consentimiento libre, específico, informado e inequívoco del titular de datos o sobre otro fundamento legal legítimo.

3. El tratamiento de datos personales deberá realizarse conforme a la ley.

4. Durante su tratamiento, los datos personales deberán:

a. tratarse de forma justa y transparente;

b. recopilarse con propósitos explícitos, específicos y legítimos y no tratarse de forma incompatible con dichos propósitos; el tratamiento adicional con el propósito de archivo en interés público, investigaciones científicas o históricas o propósitos estadísticos si se encontrara sujeto a las garantías apropiadas, será compatible con dichos propósitos;

c. ser adecuados, relevantes y no excesivos en relación con el propósito en función del cual están siendo tratados;

d. ser precisos y, cuando fuere necesario, mantenerse actualizados;

e. preservarse de forma tal que permitan identificar a los titulares de datos, por no más tiempo que el necesario para los propósitos en función de los cuales se tratan dichos datos.

**Artículo 6 – Categorías especiales de datos**

1. El tratamiento de: datos genéticos; datos personales relacionados con delitos, procesos penales y sentencias penales de condena, y medidas de seguridad relacionadas; datos biométricos que identifican únicamente a una persona; datos personales por la información que revelan en relación con los orígenes raciales o étnicos, opiniones políticas, afiliaciones sindicales, creencias religiosas u otras, salud o vida sexual, estará permitido únicamente cuando se consagren garantías apropiadas conforme a la ley, complementando aquellas del presente Convenio.

2. Dichas garantías deberán proteger de los riesgos que el tratamiento de datos sensibles podría presentar para los intereses, derechos y libertades fundamentales del titular de datos, particularmente el riesgo de discriminación.

**Artículo 7 – Seguridad de los datos**

1. Cada Parte deberá prever que el responsable del tratamiento y, si correspondiere, el encargado del tratamiento, deberá tomar medidas de seguridad apropiadas contra riesgos como acceso accidental o no autorizado, destrucción, pérdida, uso, modificación o divulgación de datos personales.

2. Cada Parte deberá prever que el responsable del tratamiento deberá notificar, sin demora, al menos a la autoridad de control competente según lo dispuesto por el Artículo 15 del presente Convenio, aquellas violaciones a los datos que puedan interferir gravemente con los derechos y las libertades fundamentales de los titulares de datos.

**Artículo 8 – Transparencia del tratamiento**

1. Cada parte deberá prever que el responsable del tratamiento deberá informar a los titulares de datos:

a. su identidad y residencia habitual o establecimiento;

b. los fundamentos legales y los propósitos del tratamiento a realizarse;

c. las categorías de los datos personales tratados;

d. los destinatarios o las categorías de destinatarios de los datos personales, si los hubiere; y

e. las formas de ejercer los derechos establecidos en el Artículo 9, así como cualquier otra información adicional necesaria con el fin de asegurar el tratamiento justo y transparente de los datos personales.

2. El párrafo 1 no será aplicable cuando el titular de datos ya posea la información correspondiente.

3. Si los datos personales no fueren recopilados del titular de datos y el tratamiento estuviere establecido especialmente por la ley o proporcionar dicha información fuere imposible o implicare esfuerzos desmedidos, el responsable del tratamiento no estará obligado a proporcionar dicha información.

**Artículo 9 – Derechos del titular de datos**

1. Cada individuo tendrá derecho a:

a. no estar sujeto a una decisión que lo afecte significativamente, basándose únicamente en un tratamiento automatizado de datos sin considerar sus opiniones;

b. obtener, cuando así lo solicitare, en intervalos razonables y sin demora o gastos excesivos, confirmación del tratamiento de los datos personales relacionados con su persona, la comunicación en forma inteligible de los datos tratados, toda la información disponible sobre su origen, el período de conservación así como cualquier otra información que el responsable del tratamiento deba proporcionar con el fin de asegurar la transparencia del tratamiento conforme al Artículo 8, párrafo 1;

c. obtener, cuando así lo solicitare, conocimiento del razonamiento subyacente al tratamiento de datos cuando los resultados de dicho tratamiento se le aplicaren;

d. oponerse en cualquier momento, por fundamentos relacionados con su situación, al tratamiento de datos personales que lo involucren, salvo si el responsable del tratamiento demostrara fundamentos legítimos para el tratamiento superiores a sus intereses o derechos o libertades fundamentales;

e. obtener, cuando así lo solicitare, exento de costos y sin demoras excesivas, la rectificación o eliminación, según sea el caso, de dichos datos si estos estuvieron siendo o hubieren sido tratados en forma contraria a las disposiciones del presente Convenio;

f. obtener una solución jurídica según el Artículo 12 cuando sus derechos de conformidad con el presente Convenio hubieren sido violados;

g. beneficiarse, cualquiera sea su nacionalidad o residencia, de la asistencia de una autoridad de control según lo dispuesto en el Artículo 15, para ejercer sus derechos de conformidad con el presente Convenio.

2. El párrafo 1.a, no será aplicable si la decisión ha sido autorizada por una ley a la cual el responsable del tratamiento está sujeto y que también establece medidas apropiadas para garantizar los derechos, las libertades e intereses legítimos del titular de datos.

**Artículo 10 – Obligaciones adicionales**

1. Cada Parte deberá prever que los responsables del tratamiento y, si correspondiere, los encargados del tratamiento, tomen todas las medidas necesarias para cumplir con las obligaciones del presente Convenio y sean capaces de demostrar, sujetos a las leyes locales adoptadas de acuerdo con el Artículo 11, párrafo 3, en particular a la autoridad de control competente según lo establecido en el Artículo 15, que el tratamiento de datos bajo su control cumple con las disposiciones del presente Convenio.

2. Cada Parte deberá prever que los responsables del tratamiento y, si correspondiere, los encargados del tratamiento, examinen el probable impacto del tratamiento de datos sobre los derechos y las libertades fundamentales de los titulares de datos, previo al comienzo de dicho tratamiento, y deberán diseñar el tratamiento de datos de manera tal que se prevenga o minimice el riesgo de interferencia con dichos derechos o libertades fundamentales.

3. Cada Parte deberá prever que los responsables del tratamiento y, si correspondiere, los encargados del tratamiento, implementen medidas técnicas y organizacionales que tomen en cuenta las implicancias del derecho a la protección de datos personales en todas las etapas del tratamiento de datos.

4. Cada Parte podrá, teniendo en consideración los riesgos en relación con los intereses, derechos y libertades fundamentales de los titulares de datos, adaptar la aplicación de las disposiciones de los párrafos 1, 2 y 3 en la ley que dote de eficacia a las disposiciones del presente Convenio, según la naturaleza y el volumen de los datos, la naturaleza, el alcance y el propósito del tratamiento y, si correspondiere, el tamaño del responsable del tratamiento o encargado del tratamiento.

**Artículo 11 – Excepciones y restricciones**

1. No se permitirá excepción alguna a las disposiciones establecidas en este Capítulo, salvo a las disposiciones del Artículo 5, párrafo 4, Artículo 7, párrafo 2, Artículo 8, párrafo 1, y Artículo 9, si dicha excepción se encuentra prevista por la ley, respeta la esencia de los derechos y las libertades fundamentales y constituye una medida necesaria y proporcionada en una sociedad democrática para:

a. proteger la seguridad nacional, la defensa, la seguridad pública, los intereses económicos y financieros importantes del Estado, la imparcialidad e independencia del poder judicial o la prevención, investigación

y procesamiento de delitos, así como la aplicación de sanciones penales, y otros objetivos esenciales de interés público general;

b. proteger al titular de datos o los derechos y las libertades fundamentales de otros, en particular, la libertad de expresión.

2. Las restricciones para ejercer las disposiciones especificadas en los Artículos 8 y 9 pueden ser previstas por la ley, con respecto al tratamiento de datos con el propósito de archivo en interés público, investigaciones científicas o históricas o propósitos estadísticos cuando no exista riesgo identificable de violación de los derechos y las libertades fundamentales de los titulares de datos.

3. Además de las excepciones permitidas en el párrafo 1 del presente artículo, con referencia a actividades de tratamiento con propósitos de seguridad nacional y defensa, cada Parte podrá prever, por la ley y solo en la medida en que constituya una medida necesaria y proporcionada en una sociedad democrática para cumplir con dicho objetivo, excepciones al Artículo 4, párrafo 3, Artículo 14, párrafos 5 y 6 y Artículo 15, párrafo 2, literales *a, b, c y d.*

Lo anterior es sin perjuicio de que las actividades de tratamiento con propósitos de seguridad nacional y defensa estén sujetas a revisión y supervisión independiente y efectiva, según las leyes locales de la Parte pertinente.

**Artículo 12 – Sanciones y soluciones jurídicas**

Cada parte asume la obligación de establecer sanciones y soluciones jurídicas apropiadas, judiciales y extrajudiciales, para el caso de violaciones a las disposiciones del presente Convenio.

**Artículo 13 – Protección extendida**

Ninguna de las disposiciones del presente capítulo será interpretada como limitando o afectando la posibilidad de que una Parte brinde a los titulares de datos medidas de protección más amplias que aquellas estipuladas en el presente Convenio.

**Capítulo III – Flujos transfronterizos de datos personales**

**Artículo 14 – Flujos transfronterizos de datos personales**

1. Una Parte no podrá, con el solo propósito de proteger los datos personales, prohibir o someter a autorización especial la transferencia de dichos datos a un destinatario que se encuentra sujeto a la jurisdicción de otra Parte del Convenio. No obstante, dicha Parte podrá hacerlo si existe un riesgo real y grave de que la transferencia a otra Parte, o de esa otra Parte a un tercero, pudiera llevar a incumplir las disposiciones del presente Convenio. Una Parte también podrá hacerlo en caso de estar obligada por normas de protección armonizadas, compartidas por Estados pertenecientes a una organización internacional regional.

2. Cuando el destinatario se encuentre sujeto a la jurisdicción de un Estado u organización internacional que no sea Parte del presente Convenio, la transferencia de datos personales solo podrá llevarse a cabo cuando se asegure un nivel de protección apropiado, basándose en las disposiciones del presente Convenio.

3. Un nivel de protección apropiado puede garantizarse mediante:

a. las leyes de ese Estado u organización internacional, incluyendo los tratados o acuerdos internacionales aplicables; o

b. garantías *ad hoc* o garantías estandarizadas aprobadas establecidas en instrumentos legalmente vinculantes y ejecutables adoptados e implementados por las personas involucradas en la transferencia y el tratamiento posterior.

4. Sin perjuicio de las disposiciones de los párrafos anteriores, cada Parte podrá prever que la transferencia de datos personales podrá llevarse a cabo en caso de que:

a. el titular de datos hubiere prestado su consentimiento explícito, específico y libre, luego de haber sido informado de los riesgos en caso de ausencia de garantías apropiadas; o

b. los intereses específicos del titular de datos lo requirieren en su caso particular; o

c. la ley estableciere los intereses legítimos predominantes, en particular intereses públicos importantes, y dicha transferencia constituyere una medida necesaria y proporcionada en una sociedad democrática; o

d. constituyere una medida necesaria y proporcionada en una sociedad democrática para la libertad de expresión.

5. Cada Parte deberá prever que la autoridad de control competente según lo dispuesto en el Artículo 15 del presente Convenio deberá contar con toda la información relevante relacionada con las transferencias de datos mencionadas en el párrafo 3.b y, cuando se solicitare, párrafos 4.b y 4.c.

6. Cada Parte también deberá prever que la autoridad de control tendrá derecho a solicitar que la persona que transfiere datos demuestre la efectividad de las garantías o la existencia de intereses legítimos predominantes y que la autoridad de control podrá, con el fin de proteger los derechos y las libertades fundamentales de los titulares de datos, prohibir dichas transferencias, suspenderlas o someterlas a condiciones.

**Capítulo IV – Autoridades de control**

**Artículo 15 – Autoridades de control**

1. Cada Parte deberá prever una o más autoridades de control, responsables de asegurar el cumplimiento con las disposiciones del presente Convenio.

2. Con este fin, dichas autoridades:

a. tendrán la facultad de investigar e intervenir;

b. deberán llevar a cabo las funciones relacionadas con la transferencia de datos previstas en el Artículo 14, en particular, la aprobación de garantías estandarizadas;

c. tendrán la facultad de emitir decisiones en caso de violaciones a las disposiciones del presente Convenio y podrán, en particular, imponer sanciones administrativas;

d. podrán iniciar procesos judiciales o denunciar a las autoridades judiciales competentes las violaciones a las disposiciones del presente Convenio;

e. deberán promover:

i. la conciencia pública acerca de sus funciones y facultades, así como de sus actividades;

ii. la conciencia pública acerca de los derechos de los titulares de datos y el ejercicio de dichos derechos;

iii. la conciencia de los responsables y los encargados del tratamiento acerca de sus responsabilidades de acuerdo con el presente Convenio;

deberá prestarse atención específica a los derechos a la protección de datos de los niños y otros individuos vulnerables.

3. Las autoridades de control competentes serán consultadas con respecto a las propuestas de medidas legislativas o administrativas sobre el tratamiento de datos personales.

4. Cada autoridad de control competente deberá lidiar con las solicitudes y demandas que presenten los titulares de datos respecto a sus derechos a la protección de datos y deberán mantenerlos informados sobre el progreso correspondiente.

5. Las autoridades de control competentes deberán actuar con total independencia e imparcialidad al cumplir con sus obligaciones y ejercer sus facultades y, al hacerlo, no deberán solicitar ni aceptar instrucciones.

6. Cada Parte deberá asegurarse de que las autoridades de control cuenten con los recursos necesarios para el efectivo cumplimiento de sus funciones y ejercicio de sus facultades.

7. La autoridad de control deberá preparar y publicar un informe periódico resumiendo sus actividades.

8. Los miembros y el personal de las autoridades de control estarán sujetos a obligaciones de confidencialidad con respecto a la información confidencial a la cual tengan acceso, o hayan tenido acceso, en el cumplimiento de sus obligaciones y el ejercicio de sus facultades.

9. Las decisiones de las autoridades de control podrán ser impugnadas judicialmente.

10. Las autoridades de control no tendrán competencia respecto al tratamiento llevado a cabo por organismos que actúen en su calidad judicial.

**Capítulo V – Cooperación y asistencia mutua**

**Artículo 16 – Designación de autoridades de control**

1. Las Partes acuerdan cooperar y prestarse asistencia mutua con el fin de implementar el presente Convenio.

2. A dichos efectos:

a. cada Parte deberá designar una o más autoridades de control según lo dispuesto por el Artículo 15 del presente Convenio, cuyos nombres y domicilios deberá comunicar al Secretario General del Consejo de Europa;

b. cada Parte que haya designado más de una autoridad de control, deberá especificar la competencia de cada autoridad en la comunicación mencionada en el literal anterior.

**Artículo 17 – Formas de cooperación**

1. Las autoridades deberán cooperar entre sí a los efectos necesarios para poder cumplir con sus obligaciones y ejercer sus facultades, y en particular:

a. se proporcionarán asistencia mutua mediante el intercambio de información relevante y útil, cooperando una con la otra con la condición de que, en cuanto a la protección de datos personales, se cumplirán todas las normas y garantías del presente Convenio;

b. coordinarán sus investigaciones e intervenciones, o llevarán a cabo acciones conjuntamente;

c. proporcionarán información y documentación acerca de sus leyes y prácticas administrativas relacionadas con la protección de datos.

2. La información mencionada en el párrafo 1 no incluirá los datos personales que se encuentren siendo tratados, salvo si dichos datos fueren esenciales para la cooperación, o si el titular de datos hubiere prestado su consentimiento explícito, específico, libre e informado para ello.

3. Con el fin de organizar su cooperación y cumplir con las obligaciones establecidas en los párrafos precedentes, las autoridades de control de las Partes formarán una red.

**Artículo 18 – Asistencia a los titulares de datos**

1. Cada Parte deberá asistir a todos los titulares de datos, cualquiera sea su nacionalidad o residencia, a ejercer sus derechos según el Artículo 9 del presente Convenio.

2. Si un titular de datos residiere en el territorio de otra Parte, tendrá la opción de presentar la solicitud a través del delegado de la autoridad de control designada por dicha Parte.

3. Las solicitudes de asistencia deberán contener todos los datos necesarios, entre otros:

a. el nombre, domicilio y cualquier otro dato relevante que identifique al titular de datos que presenta la solicitud;

b. el tratamiento al cual pertenece la solicitud, o su responsable del tratamiento;

c. el propósito de la solicitud.

**Artículo 19 – Garantías**

1. Una autoridad de control que haya recibido información de otra autoridad de control, ya sea acompañando una solicitud o en respuesta a su propia solicitud, no utilizará dicha información más que para el propósito especificado en la solicitud.

2. En ningún caso una autoridad de control podrá presentar una solicitud en nombre de un titular de datos por voluntad propia o sin la aprobación expresa del titular de datos involucrado.

**Artículo 20 – Rechazo de solicitudes**

Una autoridad de control a la cual se le envíe una solicitud según el Artículo 17 del presente Convenio no podrá rehusarse a cumplirla, salvo si:

a. la solicitud no es compatible con sus facultades;

b. la solicitud no cumple con las disposiciones del presente Convenio;

c. cumplir con la solicitud fuera incompatible con la soberanía, seguridad nacional u orden público de la Parte para la cual fue designada, o con los derechos y las libertades fundamentales de los individuos bajo la jurisdicción de dicha Parte.

**Artículo 21 – Costos y procedimientos**

1. La cooperación y asistencia mutua que las Partes se presten según el Artículo 17 y la asistencia que presten a los titulares de datos según los Artículos 9 y 18 no generarán ningún pago de costos u honorarios, salvo los de aquellos incurridos en peritos e intérpretes. La Parte que realice la solicitud se hará cargo de los costos u honorarios de estos últimos.

2. El titular de datos no deberá hacerse cargo de los costos u honorarios relacionados con las medidas tomadas en su nombre en el territorio de otra Parte, salvo aquellos legítimamente pagaderos por los residentes de dicha Parte.

3. Otros detalles relacionados con la cooperación y asistencia mutua, en particular, relacionados con las formas y procedimientos y el idioma a utilizar, serán establecidos directamente entre las Partes involucrados.

**Capítulo VI – Comité del Convenio**

**Artículo 22 – Composición del comité**

1. Se creará un Comité del Convenio luego de que el presente Convenio entre en vigencia.

2. Cada Parte deberá designar un representante al comité y un representante suplente. Cualquier Estado miembro del Consejo de Europa que no sea Parte del Convenio tendrá derecho a que un observador lo represente en el comité.

3. El Comité del Convenio podrá, a través de una decisión tomada por mayoría de dos tercios de los representantes de las Partes, invitar a un observador a ser representado en sus reuniones.

4. Cualquier Parte que no sea miembro del Consejo de Europa contribuirá con la financiación de las actividades del Comité del Convenio, conforme a las modalidades establecidas por el Comité de Ministros de común acuerdo con dicha Parte.

**Artículo 23 – Funciones del comité**

El Comité del Convenio:

a. podrá realizar recomendaciones con el fin de facilitar o mejorar la aplicación del Convenio;

b. podrá realizar propuestas para enmendar el presente Convenio, de acuerdo con el Artículo 25;

c. expresará su opinión con respecto a cualquier propuesta para enmendar el presente Convenio que le sea remitida, de acuerdo con el Artículo 25; párrafo 3;

d. podrá expresar su opinión acerca de cualquier cuestión relacionada con la interpretación o aplicación del presente Convenio;

e. preparará, antes de cualquier adhesión nueva al Convenio, una opinión para el Comité de Ministros relacionada con el nivel de protección de datos personales del candidato a la adhesión y, cuando fuere necesario, recomendará qué medidas se deberán tomar para lograr cumplir con las disposiciones del presente Convenio;

f. podrá evaluar, ante la solicitud de un Estado u organismo internacional, si el nivel de protección de datos personales que este último proporciona se encuentra en cumplimiento con las disposiciones del presente Convenio y, cuando fuere necesario, recomendar qué medidas se deberán tomar para lograr dicho cumplimiento;

g. podrá desarrollar o aprobar los modelos de las garantías estandarizadas que se mencionan en el Artículo 14;

h. examinará la implementación del presente Convenio por las Partes y recomendará qué medidas tomar en caso de que una Parte no cumpliere con el Convenio;

i. facilitará, cuando fuere necesario, una solución amistosa a todas las dificultadas relacionadas con la aplicación del presente Convenio.

**Artículo 24 – Procedimiento**

1. El Secretario General del Consejo de Europa convocará al Comité del Convenio. Su primera reunión se celebrará dentro del plazo de doce meses a partir de la entrada en vigencia del presente Convenio. Posteriormente se reunirá al menos una vez al año o en cualquier otro caso cuando un tercio de los representantes de las Partes soliciten su convocatoria.

2. Luego de cada reunión, el Comité del Convenio presentará al Comité de Ministros del Consejo de Europa un informe acerca de su trabajo y el funcionamiento del presente Convenio.

3. Los sistemas de votación en el Comité del Convenio se establecen en los elementos de las Normas de Procedimiento adjuntas al Protocolo CETS n° [223].

4. El Comité del Convenio redactará los otros elementos de sus Normas de Procedimiento y establecerá, en particular, los procedimientos para la evaluación y examen mencionados en los Artículos 4, párrafo 3, y 23, literal e, f, y h en base a un criterio objetivo.

**Capítulo VII – Enmiendas**

**Artículo 25 – Enmiendas**

1. Una Parte, el Comité de Ministros del Consejo de Europa o el Comité del Convenio podrán proponer enmiendas al presente Convenio.

2. El Secretario General del Consejo de Europa deberá comunicar cualquier propuesta de enmienda a las Partes del presente Convenio, los demás Estados miembros del Consejo de Europa, la Unión Europea y cualquier Estado no miembro u organización internacional que haya sido invitado a adherirse al presente Convenio, de acuerdo con las disposiciones del Artículo 27.

3. Aún más, cualquier enmienda propuesta por una Parte o el Comité de Ministros será comunicada al Comité del Convenio, el cual deberá presentar al Comité de Ministros su opinión acerca de la enmienda propuesta.

4. El Comité de Ministros considerará la enmienda propuesta y cualquier opinión presentada por el Comité del Convenio y podrá aprobar la enmienda.

5. El Comité de Ministros, de acuerdo con el párrafo 4 del presente artículo, enviará a las Partes el texto de la enmienda aprobada para su aceptación.

6. Cualquier enmienda aprobada de acuerdo con el párrafo 4 del presente artículo entrará en vigencia a partir del día treinta desde que todas las Partes hayan informado al Secretario General su aceptación.

7. Aún más, el Comité de Ministros podrá, luego de consultar al Comité del Convenio, decidir unánimemente que una enmienda en particular entrará en vigencia al vencer un período de tres años a partir de la fecha en que se abrió para su aprobación, salvo que una Parte notifique al Secretario General del Consejo de Europa su oposición a su entrada en vigencia. Si dicha oposición fuere notificada, la enmienda entrará en vigencia el primer día del mes siguiente a la fecha en que la Parte del presente Convenio que notificó la oposición hubiere entregado su instrumento de aceptación al Secretario General del Consejo de Europa.

**Capítulo VIII – Cláusulas finales**

**Artículo 26 – Entrada en vigencia**

1. El presente Convenio se abrirá para su suscripción por los Estados miembros del Consejo de Europa y la Unión Europea. Podrá ser ratificado, aceptado o aprobado. Los instrumentos de ratificación, aceptación o aprobación deberán entregarse al Secretario General del Consejo de Europa.





2. El presente Convenio entrará en vigencia el primer día del mes siguiente al vencimiento de un período de tres meses a partir de la fecha en la cual cinco Estados miembros del Consejo de Europa hayan expresado su consentimiento a obligarse por el Convenio conforme a las disposiciones del párrafo precedente.

3. Con respecto a cualquier Parte que posteriormente exprese su consentimiento a obligarse, el Convenio entrará en vigencia el primer día del mes siguiente al vencimiento de un período de tres meses a partir de la fecha en la cual se entregó el instrumento de ratificación, aceptación o aprobación.

Artículo 27 – Adhesión por parte de Estados no miembros u organizaciones internacionales

1. Luego de la entrada en vigencia del presente Convenio, el Comité de Ministros del Consejo de Europa podrá, luego de consultar a las Partes del Convenio y obtener un acuerdo unánime, y de la opinión preparada por el Comité del Convenio de acuerdo con el Artículo 23.e, invitar a cualquier Estado que no sea miembro del Consejo de Europa o a un organismo internacional a adherirse al presente Convenio, mediante decisión tomada por la mayoría prevista en el Artículo 20.d del Estatuto del Consejo de Europa y por el voto unánime de los representantes de los Estados Contratantes que tengan derecho a participar en el Comité de Ministros.

2. Con respecto a cualquier Estado u organización internacional que se adhiera al presente Convenio conforme al párrafo 1 anterior, el Convenio entrará en vigencia el primer día del mes siguiente al vencimiento de un período de tres meses a partir de la fecha en la cual se entregó el instrumento de adhesión al Secretario General del Consejo de Europa.

**Artículo 28 – Cláusula territorial**

1. Cualquier Estado, la Unión Europea u otra organización internacional, podrán, al momento de firmar o entregar su instrumento de ratificación, aprobación o adhesión, especificar el territorio o los territorios en los cuales se aplicará el presente Convenio.

2. Cualquier Estado, la Unión Europea u otra organización internacional, podrán, en cualquier fecha posterior, mediante declaración dirigida al Secretario General del Consejo de Europa, extender la aplicación del presente Convenio a cualquier otro territorio especificado en la declaración. Con respecto a dicho territorio, el Convenio entrará en vigencia el primer día del mes siguiente al vencimiento de un período de tres meses a partir de la fecha en la cual el Secretario General recibió dicha declaración.

3. Cualquier declaración realizada de conformidad con los dos párrafos precedentes podrá, con respecto a cualquier territorio especificado en dicha declaración, ser retirada mediante notificación dirigida al Secretario General. El retiro entrará en vigencia el primer día del mes siguiente al vencimiento de un período de seis meses a partir de la fecha en la cual el Secretario General recibió dicha notificación.

**Artículo 29 – Reservas**

No se podrá realizar ninguna reserva con respecto a las disposiciones del presente Convenio.

**Artículo 30 – Denuncia**

1. Cualquier Parte podrá denunciar en cualquier momento el presente Convenio mediante notificación dirigida al Secretario General del Consejo de Europa.

2. Dicha denuncia entrará en vigencia el primer día del mes siguiente al vencimiento de un período de seis meses a partir de la fecha en la cual el Secretario General recibió dicha notificación.

**Artículo 31 – Notificaciones**

El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo y a cualquier Parte del presente Convenio:

a. cualquier firma;

b. la entrega de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;

c. cualquier fecha de entrada en vigencia del presente Convenio conforme a los Artículos 26, 27 y 28;

d. cualquier acto, notificación o comunicación relacionados con el presente Convenio.

**Apéndice al Protocolo: Elementos para las Normas de Procedimiento del Comité del Convenio**

1. Cada parte tiene derecho de voto y tendrá un único voto.

2. Una mayoría de dos tercios de los representantes de las Partes constituirá quórum para las reuniones del Comité del Convenio. En caso de que el Protocolo de enmienda del Convenio entrare en vigencia conforme a su Artículo 37 (2) antes de su entrada en vigencia con respecto a todos los Estados Contratantes del Convenio, el quórum para las reuniones del Comité del Convenio no deberá ser de menos de 34 Partes del Protocolo.

3. Las decisiones se tomarán por mayoría de cuatro quintos según el Artículo 23. Las decisiones de conformidad con el Artículo 23, literal h, se tomarán por mayoría de cuatro quintos, incluyendo mayoría de votos de los Estados Parte no miembros de una organización de integración regional que sea Parte del Convenio.

4. Cuando el Comité del Convenio tomare decisiones de conformidad con el Artículo 23, literal h, la Parte involucrada en el informe no podrá votar. Cuando dicha decisión tratare de un asunto sujeto a la competencia de una organización de integración regional, la organización y sus Estados miembros no podrán votar.

5. Las decisiones relacionadas con cuestiones de procedimiento se tomarán por mayoría simple.

6. Las organizaciones de integración regional, en asuntos de su competencia, podrán ejercer su derecho a votar en el Comité del Convenio, con un número de votos que sea igual al número de Estados miembros que son Parte del Convenio. Dicha organización no podrá ejercer su derecho a votar si cualquiera de sus Estados miembros ejerciere su derecho.

7. En caso de votar, todas las Partes deberán estar informadas acerca del tema y la hora de la votación, así como si las Partes ejercerán individualmente su derecho a voto o mediante una organización de integración regional en representación de sus Estados miembros.

8. El Comité del Convenio podrá enmendar sus normas de procedimiento por una mayoría de dos tercios, salvo en el caso de los sistemas de votación, los que solo podrán enmendarse por el voto unánime de las Partes, para lo cual se aplicará el Artículo 25 del Convenio.

La suscrita Traductora Pública declara que lo que antecede es traducción fiel del documento adjunto, **Convenio para la Protección de las Personas con respecto al Tratamiento de Datos Personales**, redactado en idioma inglés, de cuya versión al español guarda copia en su archivo con el número 025/2019. Montevideo, 06 de mayo de 2019.

*Traducción Pública realizada*
*por la Traductora Inés Payssé Terra*





**TRADUCCIÓN N°. 058/2019. INFORME EXPLICATIVO DE CONVENIO**

/Documento extendido en 18 fojas, redactado en idiomas inglés y francés. En el margen inferior, las páginas se encuentran numeradas y obra la leyenda "Convenio 108+". A solicitud de parte interesada, se traduce únicamente el texto en idioma inglés. A continuación, se traducen las últimas 11 fojas./

/Del dorso de fojas 8 al dorso de fojas 17:/

**Informe Explicativo**

**I. Introducción**

1. Durante los 35 años que han transcurrido desde que el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos Personales, también llamado Convenio 108 (en adelante, "el Convenio") fue abierto a suscripción, el Convenio ha sido la base de las leyes internacionales de protección de datos de más de 40 países europeos. También ha influenciado políticas y legislaciones mucho más distantes de las orillas europeas. Las nuevas amenazas a los derechos humanos y las libertades fundamentales, especialmente al derecho a la vida privada han dejado claro la necesidad de modernizar el Convenio, a los efectos de abordar estas amenazas contra la privacidad, derivadas del uso de nuevas tecnologías informáticas y de la comunicación, de la globalización de operaciones de tratamiento y del aumento del flujo de datos personales y, al mismo tiempo, para reforzar los mecanismos de evaluación y de seguimiento del Convenio.

2. Se logró un amplio consenso con respecto a los siguientes aspectos de los procesos de modernización: mantener la naturaleza general y tecnológicamente neutral de las disposiciones del Convenio; preservar la coherencia y la compatibilidad del Convenio con otros marcos legales; y reafirmar el carácter abierto del Convenio, el cual le otorga un potencial único como estándar universal. El texto del Convenio es de carácter general y puede ser complementado por textos sectoriales de normas jurídicas no vinculantes / soft law/, especialmente las recomendaciones elaboradas por el Comité de Ministros con la participación de las partes interesadas.

3. El proyecto de modernización se llevó a cabo en el contexto de varias reformas paralelas de instrumentos de protección de datos internacionales, y tomando en cuenta las Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de 1980 (revisadas en 2013), las Directrices de las Naciones Unidas para la Regulación de los Archivos de Datos Personales Informatizados de 1990, el marco /sigue nota al pie de página n° 1/ de la Unión Europea (UE) desde 1995, el marco de Privacidad del foro de Cooperación Económica Asia-Pacífico (2004) y los "Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos personales" /sigue nota al pie de página n° 2/ de 2009. Con respecto a la reforma de protección de datos de la UE, el trabajo se realizó en paralelo y se cuidó especialmente la coherencia de los dos marcos legales. El marco de protección de datos de la UE aporta sustancia y amplía los principios del Convenio 108 y toma en cuenta la adhesión al Convenio 108, especialmente con respecto a las transferencias internacionales /sigue nota al pie de página n° 3/.

4. El Comité Consultivo establecido en el Artículo 18 del Convenio preparó propuestas de proyectos de modernización, adoptadas en la 29a reunión plenaria (27 al 30 de noviembre de 2012) y enviadas al Comité de Ministros. El Comité de Ministros le encargó entonces al Comité ad hoc de protección de datos (CAHDATA, por sus siglas en inglés) que finalizara los proyectos de modernización. Esto se concretó en la tercera reunión del CAHDATA (1 al 3 de diciembre 2014). Además de la finalización del marco de protección de datos de la UE, se estableció otro CAHDATA para tratar los temas pendientes.

La última reunión del CAHDATA (15 y 16 de junio de 2016) concretó las propuestas y las transfirió al Comité de Ministros para ser consideradas y adoptadas.

5. El texto del presente informe explicativo pretende guiar y asistir en la aplicación de las disposiciones del Convenio y otorga indicaciones de cómo los redactores vislumbraron la operativa del Convenio.

6. El Comité de Ministros respaldó el informe explicativo. En este sentido, el informe explicativo forma parte del contexto que se utiliza para verificar el uso de ciertos términos en el Convenio (nota: ref. Artículo 31, párrafos 1 y 2, del Convenio de Viena sobre el Derecho de los Tratados de las Naciones Unidas).

El Comité de Ministros adoptó el Protocolo el 18 de mayo de 2018. El apéndice al Protocolo constituye parte integral del Protocolo y posee el mismo valor legal que las restantes disposiciones del Protocolo.

El Protocolo se abrió a suscripción en Estrasburgo el 10 de octubre de 2018.

**II. Comentarios**

7. El objetivo del presente Protocolo es modernizar el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos Personales del Consejo de Europa (ETS n° 108) y su Protocolo Adicional con respecto a las Autoridades de Control y a los Flujos Transfronterizos de Datos (ETS n° 181) y reforzar su aplicación. Desde el momento de su entrada en vigencia, el Protocolo Adicional será considerado parte integral del Convenio y sus modificaciones.

8. Los informes explicativos del Convenio 108 y de su protocolo adicional siguen siendo relevantes en tanto que aportan el contexto histórico y describen la evolución de ambos instrumentos. A dichos efectos, los mismos se podrán leer en conjunto con el presente documento.

**Preámbulo**

9. El preámbulo reafirma el compromiso de los Estados signatarios con los derechos humanos y las libertades fundamentales.

10. Uno de los objetivos principales del Convenio es colocar a las personas en una posición tal que conozcan, entiendan y controlen el tratamiento de sus datos personales por parte de terceros. Por consiguiente, el preámbulo menciona expresamente el derecho a la autonomía personal y el derecho a controlar los datos personales propios, el cual se deriva en particular del derecho a la privacidad y del derecho a la dignidad humana. La dignidad humana requiere métodos de protección cuando se traten datos personales a los efectos de no considerar a las personas meros objetos.

11. Tomando en consideración el rol del derecho a la protección de datos personales en la sociedad, el preámbulo enfatiza el principio de que los intereses, derechos y libertades fundamentales de los individuos deben, cuando sea necesario, conciliarse los unos con los otros. El Convenio establece ciertas condiciones y limitaciones con respecto al tratamiento de información y a la protección de los datos personales para preservar el delicado equilibro entre los diferentes intereses, derechos y libertades fundamentales. El derecho a la protección de datos debe, por ejemplo, considerarse junto con el derecho a la "libertad de expresión", según lo establece el Artículo 10 del Convenio Europeo de Derechos Humanos (ETS n° 5), el cual incluye la libertad para exponer opiniones y para obtener e impartir información. Además, el Convenio confirma que el ejercicio del derecho a la protección de datos, el cual no es absoluto, no deberá ser utilizado como medio general para impedir el acceso público a documentos públicos /sigue nota al pie de página n° 4/.

12. Mediante los principios que establece y los valores que consagra, el Convenio 108 protege a las personas y sirve como marco para el flujo internacional de datos. Esto es importante ya que el flujo global de información juega un rol cada vez más relevante en la sociedad moderna, pues habilita el ejercicio de derechos y libertades fundamentales, mientras provoca innovación, fomenta el progreso social y económico y juega al mismo tiempo un rol vital asegurando la seguridad pública. El flujo de datos personales en una sociedad de información y comunicación debe respetar los derechos y las libertades fundamentales de las personas. Además, el desarrollo y uso de tecnologías innovadoras también debe respetar estos derechos. Esto ayudará a generar confianza en las innovaciones y nuevas tecnologías y ayudará a continuar su desarrollo.

13. Dado que la cooperación internacional entre autoridades de control es un elemento esencial para la protección efectiva de las personas, el Convenio tiene como objetivo fortalecer dicha cooperación, especialmente exigiéndole a las Partes que se presten asistencia mutua, y otorgando el fundamento legal apropiado para un marco de cooperación e intercambio de información para investigaciones y su ejecución.

**Capítulo I – Disposiciones generales**

**Artículo 1 – Objeto y propósito**

14. El primer artículo describe el objeto y propósito del Convenio. Este artículo se centra en el tema de la protección: se debe proteger a las personas cuando se traten sus datos personales /sigue nota al pie de página n° 5/. Recientemente, se agregó la protección de datos como un derecho fundamental en el Artículo 8 de la Carta de los Derechos Fundamentales de la UE, así como en las Constituciones de varias Partes del Convenio.





15. Las garantías establecidas en el Convenio se extienden a toda persona sin importar su nacionalidad o lugar de residencia. La discriminación entre ciudadanos y nacionales de terceros países está prohibida en la aplicación de las presentes garantías /sigue nota al pie de página n° 6/. Las cláusulas que limiten la protección de datos a los ciudadanos o residentes legales en un Estado serán incompatibles con el Convenio.

**Artículo 2 – Definiciones**

16. Las definiciones usadas en el presente Convenio pretenden asegurar el uso uniforme de los términos para expresar ciertos conceptos fundamentales en la legislación nacional.

***Lit. a. – "datos personales"***

17. "Persona identificable" refiere a una persona que puede ser identificada directa o indirectamente. Una persona no se considerará "identificable" cuando su identificación requiera tiempo, esfuerzo y recursos excesivos. Tal sería el caso, por ejemplo, cuando identificar a un titular de datos requiera operaciones excesivamente complejas, duraderas y costosas. El alcance del término "tiempo, esfuerzo y recursos excesivos" se deberá analizar en cada caso. Por ejemplo, se podría considerar el propósito del tratamiento tomando en cuenta criterios objetivos como costos, beneficios de dicha identificación, tipo de responsable del tratamiento, tecnología usada, etc. Asimismo el desarrollo tecnológico y otros desarrollos podrían cambiar el significado de "tiempo, esfuerzo y recursos excesivos".

18. "Identificable" refiere no solo a la identidad civil o legal del individuo como tal, sino también a lo que puede "individualizar" o diferenciar a una persona de otros (y, por ende, permitir tratar de manera diferente). Esta "individualización" se puede realizar, por ejemplo, refiriéndose a la persona específicamente o a un equipo o conjunto de equipos (computadora, teléfono celular, cámara fotográfica, equipos de videojuegos, etc.) mediante un número de identificación, seudónimo, datos biométricos o genéticos, datos de ubicación, dirección IP u otro elemento identificador. El uso de seudónimos o de un identificador digital/identidad digital no lleva al anonimato de los datos, dado que el titular en todo caso puede ser identificable o individualizado. Por lo tanto, los datos seudónimos deberán considerarse datos personales y se encuentran dentro del alcance de las disposiciones del Convenio. La calidad de las técnicas de creación de seudónimos utilizadas deberá tomarse en cuenta al determinarse si las garantías tomadas para mitigar el riesgo de los titulares de datos han sido apropiadas.

19. Los datos serán considerados anónimos cuando sea imposible reidentificar al titular de datos o si dicha reidentificación requiere tiempo, esfuerzos o recursos excesivos, considerando la tecnología disponible durante el tratamiento y el desarrollo de las tecnologías. Los datos que parecen ser anónimos porque no se encuentran acompañados de ningún elemento identificador obvio podrán, de todas maneras, en algunos casos, permitir la identificación de un individuo (sin requerir tiempo, esfuerzos o recursos excesivos). En este caso, por ejemplo, es posible que el responsable del tratamiento o cualquier persona identifiquen a la persona a través de la combinación de diferentes tipos de datos, como por ejemplo datos físicos, fisiológicos, genéticos, económicos o sociales (combinación de datos de edad, sexo, ocupación, geolocalización, estado familiar, etc.). Cuando este sea el caso, los datos no podrán considerarse anónimos y estarán alcanzados por las disposiciones del Convenio.

20. Cuando los datos sean anónimos, se deberán tomar las medidas apropiadas para evitar la reidentificación de los titulares de datos, y se aplicarán especialmente todas las medidas técnicas para garantizar que la persona no pueda ser, o ya no sea, identificable. Estas se reevaluarán periódicamente ante el rápido avance del desarrollo tecnológico.

***Lit. b. y c. – "tratamiento de datos"***

21. El "tratamiento de datos" comienza con la recolección de datos personales y abarca todas las operaciones realizadas sobre los datos personales, ya sea en forma parcial o totalmente automatizada. Cuando no se utilicen tratamientos automatizados, el tratamiento de datos refiere a una operación o conjunto de operaciones realizadas con respecto a datos personales dentro de una estructura establecida de los datos que sean accesibles o recuperables de acuerdo con un criterio específico, que le permite al responsable del tratamiento o a cualquier otra persona buscar, combinar o correlacionar los datos a un titular de datos específico.

*Lit. d. – "responsable del tratamiento"*

22. "Responsable del tratamiento" refiere a la persona u organismo que tiene la facultad de tomar decisiones relacionadas con los propósitos y medios del tratamiento, ya sea que esta facultad derive de una designación legal o circunstancias de hecho que serán evaluadas caso a caso. En algunos casos, podrán existir múltiples responsables del tratamiento o corresponsables del tratamiento (responsables conjuntamente del tratamiento y posiblemente responsables por diferentes aspectos de dicho tratamiento). Al evaluarse si la persona o el organismo es responsable del tratamiento, se deberá tomar especialmente en cuenta si esa persona u organismo determinan las razones para justificar el tratamiento, dicho de otra forma, sus propósitos y los medios que utilizan para ello. Otros factores relevantes en dicha evaluación incluyen si la persona o el organismo tienen control sobre los métodos del tratamiento, la elección de los datos a tratar y quién tiene permitido el acceso a ellos. Aquellos que no se encuentran directamente sujetos al responsable del tratamiento y llevan a cabo el tratamiento en representación del responsable del tratamiento, y solo siguiendo las instrucciones del responsable del tratamiento, serán considerados encargados del tratamiento. El responsable del tratamiento será responsable por el tratamiento cuando un encargado del tratamiento trate los datos en su representación.

*Lit. e. – "destinatario"*

23. "Destinatario" es un individuo o una entidad que recibe datos personales o a quien se le suministran los datos personales. Dependiendo de las circunstancias, el destinatario podrá ser un responsable del tratamiento o un encargado del tratamiento. Por ejemplo, una empresa puede enviar ciertos datos de sus empleados a un departamento del gobierno que tratará dichos datos como responsable del tratamiento a los efectos impositivos. Los podrá enviar a una empresa que ofrece servicios de almacenamiento y que actuará como encargado del tratamiento. El destinatario puede ser una autoridad pública o una entidad que ha obtenido el derecho a ejercer una función pública, pero cuando los datos recibidos por la autoridad o entidad se trataren dentro del marco de una investigación en particular de acuerdo con la ley aplicable, dicha autoridad o entidad no será considerada destinatario. Las solicitudes de divulgación a autoridades públicas se deberán presentar siempre por escrito, ser fundamentadas y esporádicas y no deberán involucrar la totalidad de un sistema de archivo o llevar a la interconexión de sistemas de archivo. El tratamiento de datos personales realizado por dichas autoridades públicas deberá cumplir con las normas de protección de datos aplicables de acuerdo con los propósitos del tratamiento.

*Lit. f. – "encargado del tratamiento"*

24. "Encargado del tratamiento" es cualquier persona física o jurídica (que no sea empleado del responsable del tratamiento de datos) que trata los datos en representación del responsable del tratamiento y de acuerdo con las instrucciones del responsable del tratamiento. Las instrucciones del responsable del tratamiento establecen el límite de lo que el encargado del tratamiento podrá realizar respecto a los datos personales.

**Artículo 3 – Alcance**

25. De acuerdo con el párrafo 1, cada Parte deberá aplicar el Convenio a todo tratamiento, ya sea en el sector público o privado, dentro de su jurisdicción.

26. El hecho de que el alcance de la protección dependa de la noción de "jurisdicción" de las Partes está justificado por el objetivo de una mayor perduración en el tiempo y el acoplamiento con el desarrollo tecnológico continuo.

27. El párrafo 2 excluye del alcance del Convenio el tratamiento de datos llevado a cabo para actividades exclusivamente personales o domésticas. Dicha exclusión busca evitar la imposición de obligaciones no razonables al tratamiento de datos llevado a cabo por individuos en su esfera privada para actividades relacionadas con el ejercicio de su vida privada. Las actividades personales o domésticas son actividades que están vinculadas cercana y objetivamente a la vida privada de un individuo y que no afectan gravemente la esfera personal de otros. Dichas actividades no poseen aspectos profesionales o comerciales y se relacionan exclusivamente con actividades personales o domésticas, tales como almacenar fotos familiares o privadas en una computadora, crear una lista con los datos de contacto de amigos y familiares, correspondencia, etc. Compartir los datos dentro de la esfera privada abarca particularmente compartirlos en una familia, un círculo de amigos restringido o un círculo limitado en tamaño y basado en una relación personal o una relación particular de confianza.





28. Si las actividades son "actividades exclusivamente personales o domésticas" dependerá de las circunstancias. Por ejemplo, cuando los datos personales se encuentran disponibles para un gran número de personas o para personas claramente externas a la esfera privada, tal como un sitio web público en internet, no se aplicará la exclusión. Asimismo, la operación de un sistema de cámara, que como resultado almacena una filmación de personas en un aparato de filmación continua tal como un disco duro, instalado por un individuo en su hogar con el propósito de proteger la propiedad, salud y vida de los dueños del hogar, pero que cubre, así sea parcialmente, un espacio público y es, en consecuencia, dirigido fuera del lugar privado de la persona que trata los datos de tal forma, no podrá ser considerada una actividad que es exclusivamente "personal o doméstica" /sigue nota al pie de página n° 7/.

29. No obstante, el Convenio se aplica al tratamiento de datos llevado a cabo por los proveedores de los medios para el tratamiento de datos personales para dichas actividades personales o domésticas.

30. A pesar de que el Convenio se refiere al tratamiento de datos relacionados con individuos, las Partes podrán extender la protección en sus leyes locales a datos relacionados con personas jurídicas con el fin de proteger sus intereses legítimos. El Convenio se aplica a individuos vivos: no se pretende aplicarlo al tratamiento de datos personales de personas fallecidas. Sin embargo, esto no impide a las Partes extender la protección a personas fallecidas.

**Capítulo II – Principios básicos de la protección de datos**

**Artículo 4 – Obligaciones de las Partes**

31. Tal como se indica en el artículo 4, el Convenio obliga a las Partes a incorporar sus disposiciones en sus leyes y asegurar su aplicación práctica de manera efectiva; lo que se llevará a cabo de distintos modos dependiendo del sistema legal aplicable y del enfoque respecto a la incorporación de los tratados internacionales.

32. El término "leyes de las Partes" denota, de acuerdo con el sistema legal y constitucional del país en particular, todas las normas vigentes, ya sean legislativas o jurisprudenciales. Deben cumplir con los requisitos cualitativos de accesibilidad y previsibilidad (o "predictibilidad"), por lo que las leyes deberán ser lo suficientemente claras para permitir que los individuos y otras entidades regulen su comportamiento considerando las consecuencias legales de sus actos, y que las personas que puedan verse afectadas por estas leyes tengan acceso a ellas. Incluye normas que establecen obligaciones y confieren derechos a personas (ya sean físicas o jurídicas) o que regulan la organización, facultades y responsabilidades de autoridades públicas o que establecen procedimientos. En particular, incluye las constituciones de los Estados y todas las leyes escritas emanadas de autoridades legislativas (leyes en el sentido formal), así como todas las normas reglamentarias (decretos, reglamentos, resoluciones y directivas administrativas) basadas en dichas leyes. También cubre convenios internacionales aplicables internamente, incluyendo las leyes de la UE. Aún más, incluye toda otra ley de naturaleza general, ya sea de derecho público o privado (incluyendo el derecho contractual), junto con decisiones judiciales en países del common law o, en todos los países, la jurisprudencia establecida que interprete la ley escrita. Además, incluye cualquier norma enmendada de un organismo profesional en el ejercicio de facultades delegadas por el legislador y de acuerdo con sus facultades independientes de creación de leyes.

33. Dichas "leyes de las Partes" podrán ser reforzadas por normas reglamentarias voluntarias en el campo de la protección de datos, tales como códigos de buena práctica o códigos de conducta profesional. Sin embargo, dichas medidas voluntarias no son suficientes para asegurar el cumplimiento íntegro del Convenio por sí solas.

34. Cuando estuvieren involucradas /sigue nota al pie de página n° 8/ organizaciones internacionales, en algunas situaciones, la ley de dicha organización internacional podrá aplicarse directamente a nivel nacional en los Estados miembros de dicha organización, dependiendo de cada sistema legal nacional.

35. La efectividad de la aplicación de las medidas que dan efecto a las disposiciones del Convenio es de crucial importancia. El rol de la autoridad (o autoridades) de control, conjuntamente con cualquier solución jurídica disponible para los titulares de datos, deberán considerarse en la evaluación general de la efectividad de una Parte para implementar las disposiciones del Convenio.

36. En el párrafo 2 se estipula aún más que las Partes involucradas deberán tomar las medidas que dan efecto al Convenio y que estas deberán haber entrado en vigencia al momento de la ratificación o adhesión, esto es, cuando una Parte se encuentre obligada legalmente por el Convenio. Esta disposición busca

que el Comité del Convenio pueda verificar si se tomaron todas las "medidas necesarias" para asegurar que las Partes del Convenio cumplan con sus compromisos y brinden el nivel de protección de datos esperado en su ley nacional. El procedimiento y criterio utilizados para dicha verificación se definirán claramente en las normas de procedimiento del Comité del Convenio.

37. Las Partes se comprometen en el párrafo 3 a contribuir de manera activa en la evaluación del cumplimiento de sus compromisos, con vistas a asegurar una evaluación periódica de la implementación de los principios del Convenio (incluyendo su efectividad). Como posible elemento de esta contribución activa las Partes podrían presentar informes acerca de la aplicación de sus leyes de protección de datos.

38. Al ejercer sus facultades según el párrafo 3, el Comité del Convenio no evaluará si una Parte ha tomado medidas efectivas, si ha utilizado excepciones y restricciones de acuerdo con las disposiciones del Convenio. Según el Artículo 11, párrafo 3, el Comité del Convenio no requerirá a una Parte que proporcione información confidencial.

39. El Comité del Convenio llevará a cabo la evaluación del cumplimento de una Parte basándose en un procedimiento objetivo, justo y transparente establecido por el Comité del Convenio y descripto íntegramente en sus normas de procedimiento.

Artículo 5 – Legitimidad del tratamiento de datos y calidad de los datos

40. El párrafo 1 prevé que el tratamiento de datos debe ser proporcionado, es decir, apropiado en relación con el propósito legítimo buscado y teniendo en cuenta los intereses, derechos y libertades del titular de datos o el interés público. Dicho tratamiento de datos no deberá llevar a una interferencia desproporcionada con estos intereses, derechos y libertades. Se deberá respetar el principio de proporcionalidad en todas las etapas del tratamiento, incluso en la etapa inicial, es decir, cuando se esté decidiendo si llevar a cabo o no el tratamiento.

41. El párrafo 2 establece dos prerrequisitos esenciales alternativos en el tratamiento legítimo: el consentimiento del individuo o un fundamento legítimo establecido por la ley. Los párrafos 1, 2, 3 y 4 del Artículo 5 son acumulativos y deberán respetarse con el fin de asegurar la legitimidad del tratamiento de datos.

42. El consentimiento del titular de datos debe prestarse de manera libre, específica, informada e inequívoca. Dicho consentimiento debe representar la expresión libre de una elección intencional, prestado ya sea por medio de una declaración (que puede ser escrita, incluso por medio electrónicos, u oral) o mediante una clara acción afirmativa y que claramente indique en este contexto específico la aceptación del tratamiento de datos personales propuesto. Por lo tanto, el mero silencio, la inactividad o los formularios o casillas prevalidados no constituirán consentimiento. El consentimiento deberá cubrir todas las actividades de tratamiento llevadas a cabo con el mismo propósito o propósitos (en el caso de propósitos múltiples, se debe prestar consentimiento para cada propósito diferente). Podrían existir casos con decisiones de consentimiento diferentes (por ejemplo, cuando la naturaleza de los datos fuere diferente incluso aunque el propósito fuere el mismo, como datos de salud contra datos de ubicación: en estos casos, el titular de datos podría prestar consentimiento para el tratamiento de sus datos de ubicación pero no para el tratamiento de sus datos de salud). El titular de datos deberá estar informado de las implicancias de su decisión (qué supone el hecho de prestar consentimiento y el alcance de consentimiento). No se podrá ejercer una influencia o presión desmedida (que puede ser económica o de otra naturaleza), ya sea directa o indirecta, sobre el titular de datos. Cuando el titular de datos no tuviere una elección genuina o libre o no pudiere rehusarse o retirar el consentimiento sin perjuicios, el consentimiento no deberá considerarse libre.

43. Por lo general, en el contexto de las investigaciones científicas no es posible identificar por completo el propósito del tratamiento de datos personales con propósitos de investigación científica al momento de recolectar los datos. Por lo tanto, los titulares de datos deberán tener permitido prestar su consentimiento para ciertas áreas de investigación científica de acuerdo con los estándares éticos reconocidos para la investigación científica. Los titulares de datos deberían poder prestar su consentimiento solo a ciertas áreas de investigación o partes de proyectos de investigación en la medida que el propósito planeado lo permita.

44. La expresión de consentimiento no implica la renuncia a la necesidad de respetar los principios básicos para la protección de datos personales establecidos en el Capítulo II del Convenio y la proporcionalidad del tratamiento, por ejemplo, aún debe considerarse.





45. El titular de datos tiene derecho a retirar su consentimiento en cualquier momento (el cual debe distinguirse del derecho separado de oponerse al tratamiento). Esto no afectará la legalidad del tratamiento de datos que ocurrió antes de que el responsable del tratamiento de datos haya recibido el retiro del consentimiento, pero no se podrá continuar el tratamiento de datos, salvo que ello se encuentre justificado por algún otro fundamento legal legítimo.

46. La noción de "fundamento legal legítimo", mencionado en el párrafo 2, abarca, entre otros, el tratamiento de datos necesario para cumplir con un contrato (o medidas precontractuales a solicitud del titular de datos) del cual el titular de datos es parte; el tratamiento de datos necesario para la protección de los intereses vitales del titular de datos o de otra persona; el tratamiento de datos necesario para cumplir con una obligación legal a la cual se encuentra sujeto el responsable del tratamiento; y el tratamiento de datos llevado a cabo en base a razones de interés público o por intereses legítimos superiores del responsable del tratamiento o de un tercero.

47. El tratamiento de datos llevado a cabo en base a razones de interés público debería preverse por la ley, entre otros, para asuntos monetarios, presupuestales e impositivos, salud pública y seguridad social, la prevención, investigación, detección y procesamiento de delitos y aplicación de sanciones penales, la protección de la seguridad nacional, defensa, la prevención, investigación detección y procesamiento de violaciones éticas de las profesiones reguladas, el cumplimiento de demandas de derecho civil y la protección de la independencia judicial y los procesos judiciales. El tratamiento de datos puede servir tanto por una razón de interés público como por los intereses vitales de un titular de datos como, por ejemplo, en el caso de datos tratados con propósitos humanitarios, incluyendo controlar una epidemia que pone en riesgo la vida y su contagio o emergencias humanitarias. Esta última podría ocurrir en situaciones de desastres naturales cuando el tratamiento de datos personales de personas desparecidas fuere necesario durante un tiempo limitado con propósitos relacionados con el contexto de la emergencia, el cual será evaluado caso a caso. También puede ocurrir en situaciones de conflictos armados u otro tipo de violencia /sigue nota al pie de página n°9/. El tratamiento de datos de asociaciones religiosas oficialmente reconocidas llevado a cabo por autoridades públicas con el propósito de alcanzar los objetivos establecidos por el derecho constitucional o el derecho internacional público, también podrá considerarse como llevado a cabo por razones de interés público.

48. Las condiciones del tratamiento legítimo se encuentran establecidas en los párrafos 3 y 4. Los datos personales deben tratarse de conforme a la ley y de manera justa y transparente. Los datos personales también deben haber sido recolectados con propósitos explícitos, específicos y legítimos, y el tratamiento de esos datos particulares debe cumplir con dichos propósitos, o al menos no ser incompatible con ellos. La referencia a "propósitos" específicos indica que tratar datos con propósitos indefinidos, imprecisos o vagos no está permitido. Lo que se considera como propósito legítimo depende de las circunstancias, ya que el objetivo es asegurar un equilibrio entre todos los derechos, libertades e intereses en juego en cada caso; por un lado, el derecho a la protección de datos personales y, por otro, la protección de otros derechos como, por ejemplo, entre los intereses del titular de los datos y los intereses del responsable del tratamiento o de la sociedad.

49. El concepto de uso compatible no debería dificultar la transparencia, certeza legal, predictibilidad o imparcialidad del tratamiento. Los datos personales no deberán ser tratados a posteriori de una forma que el titular de datos pudiere considerar inesperada, inapropiada u objetable de cualquier otra manera. Con el fin de asegurar si el propósito de un tratamiento a posteriori es compatible con el propósito inicial por el cual se recolectaron inicialmente los datos personales, el responsable del tratamiento, luego de cumplir con todos los requisitos para la legalidad del tratamiento original, debería tomar en cuenta, entre otros, cualquier relación entre dichos propósitos y los propósitos del tratamiento a posteriori; el contexto en el cual se recolectaron los datos personales, en particular, las expectativas de los titulares de datos basadas en su relación con el responsable del tratamiento en cuanto a su uso a posteriori; la naturaleza de los datos personales; las consecuencias del tratamiento a posteriori a realizarse para los titulares de datos; y la existencia de garantías apropiadas para las operaciones del tratamiento original y del tratamiento a posteriori planeado.

50. El tratamiento a posteriori de datos personales, mencionado en el párrafo 4.b, con el propósito de archivo en interés público, investigaciones científicas o históricas o propósitos estadísticos, es a priori considerado compatible siempre y cuando existan otras garantías (tales como, por ejemplo, lograr que los datos sean anónimos o utilizar seudónimos, salvo cuando sea necesario retener los datos de forma identificable; normas de secreto profesional; disposiciones que rijan el acceso restringido y la comunicación

de los datos con los propósitos antemencionados, en particular relacionados con estadísticas y archivos públicos; y otras medidas técnicas y organizacionales de seguridad de datos) y que las operaciones, en principio, excluyan cualquier uso de información obtenida para decisiones o medidas relacionadas con un individuo en particular. "Propósitos estadísticos" refiere a la elaboración de encuestas estadísticas o la producción de resultados estadísticos totales. La estadística busca analizar y caracterizar un fenómeno masivo o colectivo en una población dada /sigue nota al pie de página n° 10/. Tanto el sector público como el privado pueden perseguir propósitos estadísticos. El tratamiento de datos con el propósito de "investigaciones científicas" busca suministrar información a los investigadores para contribuir al entendimiento de fenómenos en diferentes áreas científicas (epidemiología, psicología, economía, sociología, lingüística, ciencia política, criminología, etc.) con vistas a establecer principios permanentes, leyes de comportamiento o modelos de causalidad que trasciendan a todos los individuos a los cuales se aplican /sigue nota al pie de página n° 11/. "Propósitos de investigaciones históricas" incluye investigaciones genealógicas. "Propósitos de archivo en interés público" puede incluir también archivos originarios de entidades privadas, que involucren un interés público.

51. Los datos personales que se encuentren siendo tratados deberán ser adecuados, relevantes y no excesivos. Además, los datos deberán ser precisos y, cuando fuere necesario, ser actualizados periódicamente.

52. El requisito del párrafo 4.c en cuanto a que los datos "no sean excesivos" requiere en primer lugar que el tratamiento de datos debe estar limitado a lo necesario para el propósito en función del cual se tratan. Solo deberán tratarse si los propósitos no pueden alcanzarse razonablemente tratando información que no involucra datos personales. Además, este requisito no solo refiere a la cantidad, sino también a la calidad de los datos personales. Los datos personales que son adecuados y relevantes pero que implicarían una interferencia desproporcionada en los derechos y libertades fundamentales en juego deberán ser considerados excesivos y no tratarse.

53. El requisito del párrafo 4.e relacionado con los plazos de almacenamiento de datos personales significa que los datos deberán ser eliminados una vez que se haya logrado el propósito en función del cual se realizó el tratamiento, o que solo deberán ser almacenados de una forma tal que no permita la identificación directa o indirecta del titular de datos.

54. Se permiten ciertas excepciones al Artículo 5, párrafo 4, según lo dispuesto por el Artículo 11, párrafo 1.

**Artículo 6 – Categorías especiales de datos**

55. El tratamiento de ciertos tipos de datos, o el tratamiento de ciertos datos que revelan información sensible, podría interferir con ciertos intereses, derechos y libertades. Por ejemplo, este puede ser el caso cuando existiere riesgo de discriminación o injuria a la dignidad o integridad física de un individuo, cuando se viere afectada la esfera más íntima del titular de datos, como su vida sexual u orientación sexual, o cuando el tratamiento de datos pudiere afectar la presunción de inocencia. Solo deberá permitirse cuando la ley previere garantías adecuadas, que complementen las restantes disposiciones protectoras del Convenio. El requisito de garantías adecuadas, que complementen las disposiciones del Convenio, no excluye la posibilidad prevista en el Artículo 11 de permitir excepciones y restricciones a los derechos de los titulares de datos otorgados según el Artículo 9.

56. Con el fin de evitar efectos adversos para el titular de datos, el tratamiento de datos sensibles con propósitos legítimos debe acompañarse de garantías adecuadas (adaptadas a los riesgos en juego y a los intereses, derechos y libertades a proteger), únicas o acumulativas, tales como, por ejemplo: el consentimiento explícito del titular de datos; una ley que ampare el propósito buscado y los medios de tratamiento o indicando los casos excepcionales en los que el tratamiento de dichos datos estarían permitidos; la obligación de secreto profesional; medidas luego del análisis de riesgos; una medida de seguridad particular y calificada organizacional o técnica (por ejemplo, cifrado de datos).

57. Ciertos tipos específicos de tratamiento de datos pueden implicar un riesgo particular para los titulares de datos independientemente del contexto del tratamiento. Por ejemplo, este es el caso con el tratamiento de datos genéticos, que puede ser abandonado por los individuos y puede revelar información acerca de la salud o filiación de la persona, así como de terceros. Los datos genéticos son todos los datos relacionados con las características genéticas de un individuo que han sido heredadas o adquiridas durante el desarrollo prenatal temprano, que resultan de un análisis de una muestra biológica del individuo involucrado: análisis de cromosomas, ADN o ARN o análisis de cualquier otro elemento que permita obtener información equivalente. Ocurren riesgos similares con el tratamiento de datos relacionado con delitos (incluyendo posibles delitos), sentencias penales de condena (basadas en la ley penal y en el marco de procesos penales) y medidas de seguridad relacionadas (involucrando privación de libertad, por ejemplo) que requieren establecer garantías adecuadas para los derechos y las libertades de los titulares de datos.

58. El tratamiento de datos biométricos, es decir, datos que resultan de un tratamiento de datos específico técnico relacionado con las características físicas, biológicas o fisiológicas de un individuo que permiten una identificación o autenticación exclusiva del individuo, también se considera sensible cuando es utilizado justamente para identificar exclusivamente al titular de datos.

59. El contexto del tratamiento de imágenes es importante para determinar la naturaleza sensible de los datos. Por lo general, el tratamiento de imágenes no involucrará el tratamiento de datos sensibles, ya que las imágenes solo se encontrarán dentro de la definición de datos biométricos cuando sean tratadas a través de un medio técnico específico que permita la identificación o autenticación exclusiva del individuo. Además, cuando el tratamiento de imágenes se planeare para revelar información racial, étnica o de salud (ver el punto siguiente), dicho tratamiento será considerado tratamiento de datos sensibles. Por el contrario, por lo general, las imágenes tratadas mediante un sistema de videovigilancia por meras razones de seguridad en un área de compras no será considerado tratamiento de datos sensibles.

60. El tratamiento de datos sensibles tiene el potencial de afectar de forma adversa los derechos de los titulares de datos cuando se tratan debido a la información específica que revelan. A pesar de que el tratamiento de nombres familiares puede estar libre de riesgos para los individuos en muchas circunstancias (por ejemplo, propósitos de nómina comunes), dicho tratamiento podría, en algunos casos, involucrar datos sensibles, por ejemplo, cuando el propósito sea revelar el origen étnico o las creencias religiosas de los individuos basándose en el origen lingüístico de sus nombres. Información relacionada con la salud incluye información relacionada con la salud física o mental del individuo pasada, presente y futura, y que puede referir a una persona enferma o saludable. El tratamiento de imágenes de personas con lentes gruesos, piernas rotas, piel quemada o cualquier otra característica visible relacionada con la salud de una persona solo puede ser considerado tratamiento de datos sensible cuando el tratamiento se base en la información de salud que pueda extraerse de las fotos.

61. Cuando se tuvieren que tratar datos sensibles con propósitos estadísticos, estos deberán ser recolectados de manera tal que el titular de datos no sea identificable. La recolección de datos sensibles sin datos de identificación es una garantía según el significado establecido en el Artículo 6. Cuando hubiere una necesidad legítima de recolectar datos sensibles con propósitos estadísticos de forma identificable (para que se pueda llevar a cabo una encuesta periódica o longitudinal, por ejemplo), se deben establecer garantías apropiadas /sigue nota al pie de página n° 12/.

**Artículo 7 – Seguridad de los datos**

62. El responsable del tratamiento y, si correspondiere, el encargado del tratamiento deberán tomar medidas de seguridad específicas, tanto de naturaleza técnica como organizacional, para cada tratamiento, tomando en cuenta: las posibles consecuencias adversas para el individuo, la naturaleza de los datos personales, el volumen de los datos personales tratados, el grado de vulnerabilidad de la arquitectura técnica utilizada para el tratamiento, la necesidad de restringir el acceso a los datos, los requisitos relacionados con el almacenamiento a largo plazo, etc.

63. Las medidas de seguridad deberán tomar en cuenta el estado actual de la técnica en los métodos y las técnicas de seguridad de datos en el campo del tratamiento de datos. El costo deberá ser acorde a la seriedad y probabilidad del posible riesgo. Cuando fuere necesario, las medidas de seguridad deberán ser examinadas y actualizadas.

64. A pesar de que las medidas de seguridad buscan prevenir ciertos riesgos, el párrafo 2 contiene una obligación específica para el caso en que de todas formas ocurra una violación a los datos que pueda interferir gravemente con los derechos y libertades fundamentales del individuo. Por ejemplo, la divulgación de datos cubiertos por el secreto profesional, o que pudieren resultar en daños financieros, reputacionales o daños físicos o humillación, podría considerarse una interferencia "grave".

65. Cuando ocurriere dicha violación a los datos, el responsable del tratamiento deberá notificar a las autoridades de control pertinentes el incidente, con sujeción a la excepción establecida en el Artículo 11, párrafo 1. Este es el requisito mínimo. El responsable del tratamiento también deberá notificar a las

autoridades de control las medidas tomadas y/o propuestas para abordar la violación y sus posibles consecuencias.

66. La notificación del responsable del tratamiento a las autoridades de control no excluye otras notificaciones complementarias. Por ejemplo, el responsable del tratamiento también podrá entender necesario notificar a los titulares de datos, en particular, cuando la violación de los datos probablemente resulte en un riesgo importante para los derechos y libertades de los individuos, tales como discriminación, robo o usurpación de identidad, pérdidas financieras, daños a la reputación, pérdida de confidencialidad de los datos protegidos por secreto profesional o cualquier otra desventaja económica o social importante, y suministrarles información adecuada y significativa acerca de, en particular, los puntos de contacto y posibles medidas a tomarse a los efectos de mitigar los efectos adversos de la violación. En los casos en los cuales el responsable del tratamiento no hubiere informado espontáneamente al titular de datos de la violación de los datos, la autoridad de control, tras considerar los probables efectos adversos de la violación, debería poder requerírsele al responsable del tratamiento que así lo haga. También podría ser deseable notificar a otras autoridades relevantes tales como aquellas a cargo de la seguridad de los sistemas informáticos.

**Artículo 8 – Transparencia del tratamiento**

67. El responsable del tratamiento deberá actuar con transparencia a la hora de tratar los datos con el fin de asegurar un tratamiento justo y posibilitar que los titulares de datos comprendan y, por lo tanto, ejerzan plenamente sus derechos en el contexto de dicho tratamiento de datos.

68. El responsable del tratamiento deberá suministrar cierta información esencial de manera proactiva al titular de datos cuando recolecte sus datos directa o indirectamente (no a través del titular de datos, sino a través de un tercero), con sujeción a la posibilidad de establecerse excepciones de acuerdo con el Artículo 11, párrafo 1. La información acerca del nombre y el domicilio del responsable del tratamiento (o corresponsables del tratamiento), los fundamentos legales y los propósitos del tratamiento de datos, las categorías de los datos tratados y destinatarios, así como los medios para ejercer los derechos pueden suministrarse en cualquier formato adecuado (ya sea a través de una página web, herramientas tecnológicas en dispositivos personales, etc.), siempre y cuando la información sea suministrada de manera imparcial y efectiva al titular de datos. Se deberá poder acceder, leer y entender la información presentada fácilmente y esta deberá adaptarse a los titulares de datos pertinentes (por ejemplo, en un lenguaje apto para niños cuando fuere necesario). También se deberá suministrar información adicional necesaria para asegurar el tratamiento justo de los datos o que sea útil para dichos propósitos, tal como el período de conservación, el conocimiento del razonamiento subyacente al tratamiento de datos, o información acerca de transferencias de datos a un destinatario en otra Parte o no Parte (incluyendo si ese no Parte en particular brinda un nivel de protección de datos adecuado, o las medidas tomadas por el responsable del tratamiento para garantizar dicho nivel de protección de datos adecuado).

69. El responsable del tratamiento no estará obligado a suministrar esta información cuando el titular de datos ya la hubiere recibido, o en el caso de una recolección indirecta de los datos a través de terceras partes si el tratamiento estuviere previsto expresamente por la ley, o cuando esto fuera imposible o implicare esfuerzos desmedidos debido a que el titular de datos no es identificable directamente o el responsable del tratamiento no tiene manera alguna de contactar al titular de datos. Esta imposibilidad puede ser tanto de naturaleza legal (por ejemplo, en el contexto de una investigación penal) o de naturaleza práctica (por ejemplo, cuando un responsable del tratamiento solo trata imágenes y no conoce el nombre o los datos de contacto de los titulares de datos).

70. El responsable del tratamiento de datos podrá utilizar cualquier medio disponible, razonable y económico para informar a los titulares de datos de manera colectiva (a través de una página web o una notificación pública) o individual. En caso de que sea imposible hacerlo cuando comienza el tratamiento, puede realizarse en una etapa posterior, por ejemplo, cuando el responsable del tratamiento entre en contacto con el titular de datos, por cualquier nueva razón.

**Artículo 9 – Derechos del titular de datos**

71. Este artículo enumera los derechos que cada individuo debería poder ejercer con respecto al tratamiento de datos personales relacionados con su persona. Cada Parte deberá asegurar, dentro de su ordenamiento legal, que todos esos derechos se encuentren disponibles para cada titular de datos junto a los medios legales, prácticos, adecuados y efectivos necesarios para ejercerlos.





72. Estos derechos incluyen los siguientes:

- el derecho de toda persona a no estar sujeta a una decisión plenamente automatizada que la afecte significativamente sin considerarse sus opiniones (*literal a.*);

- el derecho de toda persona a solicitar que se le confirme el tratamiento de datos relacionado con ella y el derecho a acceder a los datos en intervalos razonables y sin demora o costos excesivos (*literal b.*);

- el derecho de toda persona a recibir, a su solicitud, el conocimiento del razonamiento subyacente al tratamiento de datos cuando los resultados de dicho tratamiento se le aplicaren a ella (*literal c.*);

- el derecho de toda persona a oponerse en base a fundamentos relacionados con su situación a un tratamiento de datos que la involucren, solo si el responsable del tratamiento demostrara fundamentos legítimos para el tratamiento superiores a sus intereses o derechos y libertades fundamentales (*literal d.*);

- el derecho de toda persona a la rectificación o eliminación de datos inexactos, falsos o tratados ilegítimamente (*literal e.*);

- el derecho de toda persona a una solución jurídica si cualquiera de los derechos anteriores no fuera respetado (*literal f.*);

- el derecho de toda persona a obtener asistencia de una autoridad de control (*literal g.*).

73. Es posible que estos derechos deban ser conciliados con otros derechos e intereses legítimos. De acuerdo con el Artículo 11, estos derechos solo podrán limitarse cuando ello estuviere previsto en la ley y ello constituyere una medida necesaria y proporcionada en una sociedad democrática. Por ejemplo, el derecho a la eliminación de datos personales podrá ser restringido en la medida que el tratamiento sea necesario para cumplir con una obligación legal que requiere el tratamiento y a lo cual está sujeto el responsable del tratamiento o para el cumplimiento de una tarea de interés público o en el ejercicio de una autoridad pública que haya sido conferida al responsable del tratamiento.

74. A pesar de que el Convenio no especifica de quién puede el titular de datos obtener la confirmación, información, rectificación, etc., o frente a quién oponerse o expresar sus opiniones, en la mayoría de los casos, será el responsable del tratamiento, o el encargado del tratamiento en su representación. En casos excepcionales, los medios de acceso, rectificación o eliminación pueden involucrar al delegado de la autoridad de control. Con respecto a los datos de salud, los derechos también podrán ejercerse de otra manera que no sea a través de acceso directo. Por ejemplo, podrán ejercerse con la asistencia de un profesional de la salud cuando sea en el interés del titular de datos, en particular para ayudarlo a entender los datos o para asegurar que el estado psicológico del titular de datos sea adecuadamente considerado al transmitírsele la información, de acuerdo con los principios deontológicos, por supuesto.

75. *Literal a.* Es esencial que un individuo que podría estar sujeto a una decisión plenamente automatizada tenga derecho a impugnar dicha decisión presentando, de manera significativa, su opinión y argumentos. En particular, el titular de datos debería tener la oportunidad de corroborar la posible inexactitud de los datos personales antes de su utilización, la irrelevancia del perfil que se aplicará a su situación particular, u otros factores que impactarán en el resultado de la decisión automatizada. Este es el caso en el cual se estigmatiza al individuo mediante la aplicación de un razonamiento algorítmico que resulta en limitar un derecho o rechazar un beneficio social o evaluar su capacidad de crédito solamente mediante un programa de computadora. Sin embargo, un individuo no puede ejercer este derecho si la decisión automatizada se encuentra autorizada por una ley a la cual el responsable del tratamiento se encuentra sujeto y que además establece medidas adecuadas para garantizar los derechos y libertades e intereses legítimos del titular de datos.

76. *Literal b.* El titular de datos debería tener derecho a saber acerca del tratamiento de sus datos personales. El derecho al acceso debería, en principio, estar exento de costos. Sin embargo, la redacción del literal b. busca permitir al responsable del tratamiento, en ciertas condiciones específicas, cobrar una tarifa razonable cuando las solicitudes fueren excesivas y contempla varios enfoques que podrían ser adoptados por una Parte llegado el caso. Dicha tarifa debería ser excepcional y razonable en todos los casos y no debería evitar o disuadir a los titulares de datos de ejercer sus derechos. El responsable del tratamiento o el encargado del tratamiento también podrían rehusarse a responder solicitudes claramente infundadas o excesivas, en particular debido a su carácter repetitivo. El responsable del tratamiento en todos los casos debería justificar dicho rechazo. Para asegurar el ejercicio justo de los derechos de acceso, la comunica-

ción "de manera inteligible" aplica tanto al contenido como a la forma de la comunicación digital estandarizada.

77. *Literal c.* El titular de datos debería tener derecho a conocer el razonamiento subyacente al tratamiento de datos, incluyendo las consecuencias de dicho razonamiento, que conduzca a cualquier conclusión resultante, en particular, en los casos que involucran el uso de algoritmos para la toma de decisiones automatizadas, incluyendo esbozar un perfil. Por ejemplo, en el caso de la calificación crediticia, deberían tener el derecho de conocer la lógica que sustenta el tratamiento de sus datos y que resultará en una decisión de "sí" o "no", y no simplemente información acerca de la decisión en sí. Comprender estos elementos contribuye a ejercer efectivamente otras garantías esenciales, tales como el derecho de oposición y el derecho a quejarse frente a una autoridad de control.

78. *Literal d.* En cuanto al derecho de oposición, el responsable del tratamiento podrá tener un fundamento legítimo para el tratamiento de datos, el cual invalida los intereses o derechos y libertades del titular de datos. Por ejemplo, el establecimiento, ejercicio o defensa de reclamos legales o motivos de seguridad pública podrían considerarse como fundamentos de invalidación legítimos que justifican la continuación del tratamiento. Esto deberá demostrarse caso a caso y si dichos fundamentos legítimos convincentes no pudieren demostrarse al llevar a cabo el tratamiento, ello podría considerarse ilegitimo. El derecho a oponerse opera de manera distinta y separada del derecho de obtener rectificación o eliminación (*literal e.*)

79. Oponerse al tratamiento de datos con propósitos de marketing debería conducir al borrado o eliminación sin condiciones de los datos personales cubiertos por la oposición.

80. El derecho a oponerse podría estar limitado por la ley, por ejemplo, con el propósito de investigar y procesar delitos. En este caso, el titular de datos podrá, según sea la situación, impugnar la legitimidad del tratamiento. Cuando el tratamiento de datos se base en el consentimiento válido prestado por el titular de datos, podrá ejercerse el derecho a retirar el consentimiento en lugar del derecho a oponerse. El titular de datos podrá retirar su consentimiento y posteriormente deberá asumir las posibles consecuencias que deriven de otros textos legales, tal como la obligación de compensar al responsable del tratamiento. Asimismo, cuando el tratamiento de datos se basare en un contrato, el titular de datos podrá tomar las medidas necesarias para revocar el contrato.

81. *Literal e.* La rectificación o la eliminación, cuando sea justificado, deberá estar exenta de costos. En el caso de las rectificaciones o eliminaciones obtenidas de conformidad con el principio establecido en el *literal e.*, dichas rectificaciones o eliminaciones deberían, cuando fuere posible, hacerse saber a los destinatarios de la información original, salvo si ello fuere imposible o implicare esfuerzos desmedidos.

82. El *literal g.* busca asegurar la protección efectiva de los titulares de datos al brindarles el derecho de asistencia de una autoridad de control para ejercitar los derechos establecidos en el Convenio. Cuando el titular de los datos residiere en el territorio de otra Parte, podrá presentar la solicitud a través de un delegado de la autoridad designada por esa Parte. La solicitud de asistencia debería contener información suficiente para permitir identificar el tratamiento de datos en cuestión. Este derecho puede limitarse de acuerdo con el Artículo 11 o adaptarse con el fin de garantizar los intereses de un proceso judicial pendiente.

83. Se permiten ciertas excepciones al Artículo 9 según lo dispuesto por el Artículo 11, párrafo 1.

**Artículo 10 – Obligaciones adicionales**

84. Con el fin de asegurar que el derecho a la protección de los datos personales sea efectiva, se imponen obligaciones adicionales al responsable del tratamiento y, si correspondiere, al encargado(s) del tratamiento.

85. De acuerdo con el *párrafo 1*, la obligación del responsable del tratamiento de asegurar la adecuada protección de los datos se relaciona con la responsabilidad de verificar y poder demostrar que el tratamiento de datos cumple con la ley aplicable. Los principios de protección de datos establecidos en el Convenio, los cuales se aplicarán en todas las etapas del tratamiento, incluyendo la etapa de diseño, buscan proteger a los titulares de datos y también son un mecanismo para generar su confianza. Las medidas adecuadas que el responsable y el encargado del tratamiento podrán tener que tomar para asegurar el cumplimiento incluyen: capacitar empleados; establecer procedimientos de notificación adecuados (por ejemplo, indicar cuándo deben eliminarse los datos del sistema); establecer disposiciones contractuales específicas





delegando el tratamiento con el fin de hacer cumplir con el Convenio; así como establecer procedimientos internos que permitan verificar y demostrar el cumplimiento.

86. Si, de acuerdo con el Artículo 11, párrafo 3, una Parte elige limitar las facultades de una autoridad de control según el significado del Artículo 15 en relación con el tratamiento de actividades con propósitos de seguridad nacional y defensa, el responsable del tratamiento tendrá que demostrar a dicha autoridad de control el cumplimento con los requisitos de protección de los datos para las actividades incluido en la excepción antemencionada.

87. Una posible medida que podría tomar el responsable del tratamiento para facilitar dicha verificación y demostración de cumplimento sería designar un "funcionario de protección de datos", proveyéndolo de medios necesarios para cumplir con su mandato. Dicho funcionario de protección de datos, cuya designación debería notificarse a la autoridad de control, podría ser interno o externo al responsable del tratamiento.

88. El *párrafo 2* aclara que antes de llevar a cabo una actividad de tratamiento de datos, el responsable del tratamiento deberá examinar el posible impacto sobre los derechos o libertades fundamentales de los titulares de datos. Este examen puede realizarse sin formalidades excesivas. También deberá considerarse el principio de proporcionalidad en base a una perspectiva general del tratamiento a realizarse. En algunas circunstancias, cuando, además del responsable del tratamiento, se involucrare el encargado del tratamiento, este también deberá examinar los riesgos. Los desarrolladores de los sistemas de tecnología de la información, incluyendo profesionales de seguridad, o diseñadores, junto con usuarios y peritos podrían ayudar a examinar los riesgos.

89. El *párrafo 3* especifica que con el fin de garantizar un nivel de protección efectivo, los responsables del tratamiento y, si correspondiere, los encargados del tratamiento, deberían asegurarse de integrar cuanto antes los requisitos de protección de los datos, es decir, idealmente en la etapa de arquitectura y diseño del sistema, en operaciones de tratamiento de datos a través de medidas técnicas y organizacionales (protección de datos por diseño). Esta implementación de los requisitos de protección de los datos debería lograrse no solo en cuanto a la tecnología utilizada para tratar los datos, sino que también en cuanto a los procesos de trabajo y administrativos relacionados. Deberían establecerse funcionalidades fáciles de utilizar que faciliten el cumplimento con la ley aplicable. Por ejemplo, debería ofrecerse el acceso en línea seguro a los datos propios de cada titular de datos cuando ello fuere necesario y relevante. También deberían establecerse herramientas fáciles de utilizar para permitir que los titulares de datos lleven sus datos a otro operador de su elección o almacenen los datos ellos mismos (herramientas de portabilidad de datos). Al establecer los requisitos técnicos para configuraciones por defecto, los responsables del tratamiento y los encargados del tratamiento deberían elegir configuraciones estándar de privacidad para que el uso de las aplicaciones y programas no infrinja los derechos de los titulares de datos (protección de datos por defecto), en particular para evitar tratar más datos que los necesarios para lograr el propósito legítimo. Por ejemplo, las redes sociales deberían configurarse por defecto para que las publicaciones o fotografías solo fueron compartidas en círculos restringidos y seleccionados y no con toda la internet.

90. El *párrafo 4* permite a las Partes adaptar las obligaciones adicionales enumeradas en los párrafos 1 a 3 teniendo en cuenta los riesgos para los intereses, derechos y libertades fundamentales de los titulares de datos. Dicha adaptación deberá realizarse teniendo en cuenta la naturaleza y el volumen de los datos procesados, la naturaleza, alcance y propósitos del tratamiento de datos y, en ciertos casos, el tamaño de la entidad que lleve a cabo el tratamiento. Las obligaciones podrían adaptarse, por ejemplo, para no suponer costos excesivos para pequeñas y medianas empresas (PYMES) que tratan solo datos personales no sensibles recibidos de clientes en el marco de actividades comerciales y que no los reutilizan con otros propósitos. Ciertas categorías de tratamiento de datos, tales como el tratamiento que no implica riesgo alguno para el titular de datos, podrán incluso estar exentas de algunas de las obligaciones adicionales establecidas en el presente artículo.

**Artículo 11 – Excepciones y restricciones**

91. No se permite ninguna excepción a las disposiciones del Capítulo II, salvo en el caso de ciertas disposiciones, (Artículo 5, párrafo 4, Artículo 7, párrafo 2, Artículo 8, párrafo 1, y Artículo 9) siempre que dichas excepciones se encuentren previstas por la ley, respeten la esencia de los derechos y libertades fundamentales y sean necesarias en una sociedad democrática en base a los fundamentos enumerados en el literal a. y b. del primer párrafo del Artículo 11. Una medida que es "necesaria en una sociedad democrática" debe buscar un objetivo legítimo y, por lo tanto, satisfacer una necesidad social urgente que no

puede lograrse mediante medios menos intrusivos. Aún más, dicha medida deberá ser proporcionada al objetivo legítimo buscado y las razones aducidas por las autoridades nacionales para justificarla deberán ser relevantes y adecuadas. Dicha medida deberá estar establecida en una ley accesible y previsible, que deberá estar detallada de manera suficiente.

92. El tratamiento de datos personales deberá ser conforme a la ley, justo y transparente en relación con los titulares de datos, y solo se admitirá el tratamiento con propósitos específicos. Esto no inhabilita en sí mismo las actividades de investigación encubierta y videovigilancia que puedan llevar a cabo las autoridades. Dichas actividades podrán realizarse con el propósito de prevenir, investigar, detectar o procesar delitos penales y aplicar sanciones penales, incluyendo la prevención contra amenazas a la seguridad nacional y la seguridad pública, siempre y cuando sean establecidas por la ley y constituyan una medida necesaria y proporcionada en una sociedad democrática con debida consideración de los intereses legítimos de los titulares de datos.

93. La necesidad de dichas excepciones deberá examinarse caso a caso y considerando los objetivos esenciales del interés público general, tal como se detalla en el *literal a. y b.* del primer párrafo. El *literal a.* enumera algunos objetivos del interés público general del Estado o de organizaciones internacionales que pueden requerir excepciones.

94. La noción de "seguridad nacional" deberá interpretarse en base a la jurisprudencia pertinente del Tribunal Europeo de Derechos Humanos /sigue nota al pie de página n° 13/.

95. El término "intereses económicos y financieros importantes" incluye en especial los requisitos de recaudación de impuestos y control de cambio. El término "prevención, investigación y procesamiento de delitos, así como aplicar sanciones penales" en este literal incluye el procesamiento de delitos y la aplicación de las sanciones relacionadas con el mismo. El término "otros objetivos esenciales de interés público general" cubre, entre otros, la prevención, investigación, detección y procesamiento de violaciones éticas en el caso de profesiones reguladas y el cumplimiento de demandas de derecho civil.

96. El *literal b.* refiere a los derechos y libertades fundamentales de partes privadas, tales como aquellos del propio titular de datos (por ejemplo, cuando los intereses vitales de un titular de datos peligraren porque se encuentra desaparecido) o de terceras partes, tales como la libertad de expresión, incluyendo la libertad de expresión periodística, académica, artística o literaria, y el derecho de recibir y transmitir información, confidencialidad de correspondencia y comunicaciones, o secreto comercial o de negocios y otros secretos protegidos legalmente. En particular, esto deberá aplicar al tratamiento de datos personales en el campo audiovisual y en archivos de noticias y bibliotecas de prensa. Con el fin de tomar en cuenta la importancia del derecho a la libertad de expresión en cada sociedad democrática, es necesario interpretar las nociones relacionadas con esa libertad, tal como el periodismo, en líneas generales.

97. El *segundo párrafo* deja abierta la posibilidad de restringir las disposiciones establecidas en el Artículo 8 y 9 en relación con cierto tratamiento de datos llevado a cabo con el propósito de archivo en interés público, investigaciones científicas o históricas o propósitos estadísticos que no suponen un riesgo perceptible de violación de los derechos y las libertades fundamentales de los titulares de datos. Por ejemplo, este podría ser el caso del uso de datos para trabajos estadísticos, tanto en el campo público como el privado, si los datos se publican de forma agregada y se establecen las garantías adecuadas para la protección de los datos (ver párrafo 50).

98. Las excepciones adicionales permitidas al Artículo 4, párrafo 3, Artículo 14, párrafos 5 y 6, y Artículo 15, párrafo 2, *literales a., b., c. y d.*, con respecto a actividades de tratamiento con propósitos de seguridad nacional y defensa se establecen sin perjuicio de los requisitos aplicables relacionados con la independencia y efectividad de los mecanismos de examen y supervisión /sigue nota al pie de página n° 14/.

**Artículo 12 – Sanciones y soluciones jurídicas**

99. A los efectos de que el Convenio garantice un nivel efectivo de protección de datos, la legislación de las Partes deberá reflejar las obligaciones del responsable y del encargado del tratamiento y los derechos del titular de datos estableciendo las sanciones y soluciones jurídicas pertinentes.

100. Cada Parte determinará la naturaleza (civil, administrativa, penal) de estas sanciones judiciales y no judiciales. Estas sanciones deben ser efectivas, proporcionadas y disuasivas. Lo mismo se aplica a las soluciones jurídicas: los titulares de datos deberán tener la posibilidad de impugnar judicialmente una decisión o práctica; las Partes definirán la modalidade para hacerlo. Las soluciones no jurídicas también deberán estar disponibles para los titulares de datos. También podrían considerarse indemnizaciones financieras en el caso de daños materiales y no materiales cuando fuere necesario, ocasionados por el tratamiento, así como establecerse la posibilidad de acciones colectivas.

Artículo 13 – Protección extendida

101. Este artículo se basa en una disposición similar: el Artículo 53 del Convenio Europeo de Derechos Humanos. El Convenio confirma los principios de la ley de protección de datos que todas las Partes deben adoptar. El texto enfatiza que estos principios constituyen solo una base para que las Partes construyan sobre ella un sistema de protección más avanzado. La expresión "medidas de protección más amplias" refiere a un estándar de protección que es superior, no inferior, al requerido por el Convenio.

Capítulo III – Flujo Transfronterizo de Datos Personales /sigue nota al pie de página n° 15./

Artículo 14 – Flujo transfronterizo de datos personales

102. El objetivo de este artículo es facilitar el libre flujo de información a pesar de las fronteras (establecidas en el preámbulo), mientras se asegura la protección adecuada de los individuos con respecto al tratamiento de datos personales. La transferencia transfronteriza de datos sucede cuando se divulgan datos personales o cuando estos se encuentran disponibles para un destinatario sujeto a la jurisdicción de otro Estado u organización internacional.

103. El propósito del régimen del flujo transfronterizo es asegurar que los datos personales tratados originalmente en la jurisdicción de una Parte (datos recopilados o archivados allí, por ejemplo), que luego se encuentran sujetos a una jurisdicción de un Estado que no es Parte del Convenio, continúen siendo tratados con las garantías adecuadas. Lo importante es que los datos tratados en la jurisdicción de una Parte siempre permanezcan protegidos por los principios pertinentes de protección de datos del Convenio. A pesar de que existe una gran variedad de sistemas de protección, la protección otorgada debe presentar una calidad tal que asegure que los derechos humanos no se vean afectados por la globalización y los flujos transfronterizos de datos.

104. El Artículo 14 abarca únicamente la salida de datos, no la entrada, ya que esta última se encuentra cubierta por el régimen de protección de datos de la Parte destinataria.

105. El *párrafo 1* abarca los flujos de datos entre Partes del Convenio. No se pueden prohibir los flujos de datos ni requerir autorización especial "con el solo propósito de proteger los datos personales". Sin embargo, el Convenio no restringe la libertad de una Parte a limitar la transferencia de datos personales a otra Parte en base a otros propósitos, incluyendo, por ejemplo, la seguridad nacional, defensa, seguridad pública u otro interés público importante (incluyendo la protección de los secretos de estado).

106. El razonamiento subyacente a lo dispuesto en el *párrafo 1* es el de esperar que todas las Partes que han suscrito al núcleo común de las disposiciones de protección de datos establecidas en el Convenio, ofrezcan un nivel de protección considerado adecuado y, entonces, en principio, ello permita que los datos circulen libremente. Sin embargo, pueden existir casos excepcionales en los que existe un riesgo serio real de que la libre circulación de datos personales lleve a evadir las disposiciones del Convenio. Al tener carácter excepcional, la presente disposición se interpretará de manera restrictiva y las Partes no podrán basarse en ella cuando el riesgo sea hipotético o menor. Por lo tanto, una Parte solamente podrá utilizar esta excepción en casos específicos en los que exista una evidencia clara y confiable de que la transferencia de datos a otra Parte podría perjudicar las protecciones otorgadas a esos datos de acuerdo con el Convenio y cuando la posibilidad de que ello suceda es alta. Este puede ser el caso, por ejemplo, cuando determinadas protecciones otorgadas por el Convenio ya no se encuentran garantizadas por la otra Parte (por ejemplo, porque su autoridad de control no puede ejercer efectivamente sus funciones) o cuando es probable que los datos transferidos a otra Parte se transfieran (transferencia posterior) sin que se asegure el nivel de protección adecuado. Otra excepción reconocida por las leyes internacionales se da cuando las Partes están obligadas por normas de protección armonizadas compartidas por los Estados que pertenecen a organizaciones (económicas) regionales que buscan un mayor nivel de integración.

107. Esto abarca, entre otros, los Estados miembros de la UE. Sin embargo, como se establece de manera explícita en el Reglamento General de Protección de Datos (UE) 2016/679, la adhesión de un tercer país al Convenio 108 y su aplicación serán factores importantes al momento de emplear el régimen de transferencias internacionales en la UE, especialmente al evaluarse si el tercer país ofrece un nivel de protección adecuado (que permite a su vez el libre flujo de datos personales).

108. El *párrafo 2* contempla la obligación, en principio, de que "se asegurare un nivel de protección apropiado basándose en las disposiciones del presente Convenio". Al mismo tiempo, de acuerdo con el párrafo 4, las Partes pueden transferir datos aun cuando no se cuente con los niveles de protección adecuados si se justifica que existen, entre otros, "intereses legítimos predominantes, en particular, intereses públicos" en tanto lo establezca la ley y cuando dichas transferencias constituyan una medida necesaria y proporcionada en una sociedad democrática (*literal c.*). Los datos personales podrán entonces ser transferidos por razones que son similares a las establecidas en el Artículo 11, párrafos 1 y 3. En todos los casos, las Partes tienen completa libertad según el Convenio de restringir las transferencias de datos a países que no forman parte de este, ya sea con el fin de proteger los datos o por otras razones.

109. El *párrafo 2* menciona los flujos transfronterizos de datos personales hacia un destinatario que no se encuentra sujeto a la jurisdicción de una de las Partes. Se debe garantizar un nivel de protección adecuado para los datos personales que fluyan fuera de las fronteras nacionales. Para los casos en que el destinatario no es Parte del Convenio, este Convenio establece dos medidas para asegurar que el nivel de protección de datos sea verdaderamente adecuado; ya sea mediante la ley, o por garantías *ad hoc* o garantías estandarizadas aprobadas legalmente vinculantes y ejecutables, así como debidamente implementadas.

110. Los *párrafos 2 y 3* mencionan todas las formas adecuadas de protección, ya sean previstas por la ley o mediante garantías estandarizadas. La ley debe incluir los elementos pertinentes para la protección de datos según lo establecido en el presente Convenio. El nivel de protección se deberá evaluar para cada transferencia o categoría de transferencias. Se deberán estudiar varios elementos de la transferencia, por ejemplo: los tipos de datos; el propósito y la duración del tratamiento para el cual se transfieren los datos; el respeto del país destinatario al Estado de Derecho; las normas legales generales y sectoriales que se aplican en el Estado u organización en cuestión; y las normas profesionales y de seguridad que allí se aplican.

111. Las garantías *ad hoc* o estandarizadas deben incluir los elementos relevantes para la protección de los datos. Además, las condiciones contractuales pueden ser tales que, por ejemplo, al titular de datos se le otorgue una persona de contacto perteneciente al personal del individuo responsable de la transferencia de datos, cuya responsabilidad es asegurar el complimiento de los estándares sustanciales de protección. El titular de datos podrá contactar a esta persona en cualquier momento y de forma gratuita con respecto al tratamiento de datos o transferencias y, si correspondiere, obtener asistencia para ejercer sus derechos.

112. Para evaluar si el nivel de protección es adecuado, se deben considerar los principios del Convenio, hasta qué punto el Estado u organización destinataria cumple con dichos principios, siempre y cuando sean pertinentes para el caso específico de transferencia, y cómo el titular de datos es capaz de defender sus intereses en caso de incumplimiento. Para dicha evaluación, se deberán tomar en cuenta la posibilidad de hacer cumplir los derechos del titular de datos y de solicitar amparo administrativo y judicial por parte de los titulares cuyos datos estén siendo transferidos. De forma similar, la evaluación puede realizarse para un Estado u organización entera, permitiendo de esta manera todas las transferencias de datos a estos destinatarios.

113. El *párrafo 4* permite a las Partes desviarse del principio que las obliga a contar con un nivel adecuado de protección y les permite la transferencia a un destinatario que no asegura dicha protección. Dichas desviaciones están permitidas solamente en circunstancias específicas: mediando el consentimiento o interés específico del titular de datos y/o cuando existan intereses legítimos predominantes previstos por la ley y/o cuando la transferencia constituya una medida necesaria y proporcionada en una sociedad democrática para la libertad de expresión. Dichas desviaciones deberán respetar los principios de necesidad y proporcionalidad.

114. El *párrafo 5* contempla las garantías complementarias: especialmente la entrega a la autoridad de control competente de toda la información pertinente relacionada a la transferencia de datos establecida en los párrafos 3.b, y, a solicitud, lo establecido en los párrafos 4.b y 4.c. La autoridad deberá tener derecho a solicitar la información pertinente sobre las circunstancias y la justificación de dichas transferencias. De acuerdo con las condiciones estipuladas en el Artículo 11, párrafo 3, pueden existir excepciones al Artículo 14, párrafo 5.

115. De acuerdo con el *párrafo 6*, las autoridades de control deberán tener derecho a solicitar que se pruebe la efectividad de las medidas tomadas o de los intereses legítimos predominantes y a prohibir, suspender o imponer condiciones para la transferencia si ello fuera necesario para proteger los derechos y libertades fundamentales de los titulares de datos. De acuerdo con las condiciones estipuladas en el Artículo 11, párrafo 3, pueden existir excepciones al artículo 14, párrafo 6.

116. El crecimiento del flujo de datos y la necesidad relacionada de aumentar la protección de los datos personales, llevan a la necesidad de aumentar la cooperación internacional entre las autoridades de control competentes.

**Capítulo IV – Autoridades de control /sigue nota al pie de página n° 16./**

**Artículo 15 – Autoridades de control**

117. El objetivo de este artículo es asegurar la protección eficaz de los individuos. Ell se logra solicitándole a las Partes que designen a una o más autoridades de control públicas, independientes e imparciales que ayuden a proteger los derechos de los individuos y sus libertades en relación con el tratamiento de sus datos personales. Dichas autoridades podrán estar compuestas por una única persona o por un órgano colegiado. Para que las autoridades de control de protección de datos puedan ofrecer soluciones jurídicas necesitan tener facultades y funciones efectivas y deben gozar de una independencia real para llevar a cabo sus obligaciones. Son un componente esencial del sistema de control de protección de datos en una sociedad democrática. En lo que concierne al Artículo 11, párrafo 3, las Partes podrán establecer otras medidas apropiadas para la evaluación y supervisión independiente y eficaz de las actividades de tratamiento a los efectos de la seguridad y defensa nacional.

118. El *párrafo 1* clarifica que es posible que sea necesario contar con más de una autoridad según las circunstancias particulares de los diferentes sistemas legales (por ejemplo, Estados federales). También es posible establecer autoridades de control específicas con actividad limitada a un sector específico (sector de comunicación electrónica, sector de salud, sector público, etc.). Esto también se aplica al tratamiento de datos personales con fines periodísticos si se necesita reconciliar el derecho a la protección de datos personales con el derecho a la libertad de expresión. Las autoridades de control deberán tener la infraestructura y los recursos financieros, técnicos y humanos necesarios (abogados, especialistas en informática) para tomar acciones rápidas y eficaces. La suficiencia de los recursos deberá evaluarse regularmente. El artículo 11, párrafo 3, admite excepciones en relación con las facultades de las autoridades de control con respecto a actividades de tratamiento a los efectos de la seguridad y defensa nacional (cuando se apliquen dichas excepciones es posible que otros párrafos de este artículo no sean aplicables o pertinentes). Sin embargo, esto es así sin perjuicio de los requisitos aplicables relacionados a la independencia y efectividad de las medidas de evaluación y de supervisión /sigue nota al pie de página n° 17/.

119. Las Partes gozan de cierto grado de discreción con respecto a cómo organizar dichas autoridades para que lleven a cabo sus deberes. De acuerdo con el *párrafo 2*, sin embargo, estos deberán contar por lo menos con la facultad de investigación, intervención y emisión de decisiones con respecto a las violaciones a las disposiciones del Convenio, siempre con sujeción a la posibilidad de existencia de excepciones de acuerdo con el Artículo 11, párrafo 3. Esta última facultad de emitir decisiones puede implicar la imposición de sanciones administrativas, incluyendo multas. Si el sistema legal de una Parte no contempla sanciones administrativas, se aplicará el párrafo 2 de tal manera que la sanción se propondrá por la autoridad de control competente y se aplicará por los juzgados nacionales competentes. En todas las circunstancias, las sanciones deberán ser eficaces, proporcionadas y disuasivas.

120. La autoridad estará dotada de facultades de investigación, con sujeción a la posibilidad de existencia de excepciones de acuerdo con el Artículo 11, párrafo 3, como, por ejemplo, la posibilidad de solicitarle al responsable y al encargado del tratamiento información relacionada al tratamiento de datos personales y obtener la misma. En virtud del Artículo 15, dicha información deberá estar disponible, especialmente cuando un titular de datos se comunica con la autoridad de control para ejercer los derechos establecidos en el Artículo 9. Todo ello con sujeción a las excepciones del Artículo 11, párrafo 1.

121. La facultad de intervención de la autoridad de control establecida en el párrafo 1 podrá adoptar diversas variantes en las leyes de cada Parte. Por ejemplo, la autoridad podría estar facultada a ordenarle al responsable del tratamiento la rectificación, eliminación o destrucción de datos incorrectos o tratados ilegalmente por su cuenta o en el caso de que el titular de datos no pudiera ejercitar estos derechos personalmente. La facultad de iniciar acciones contra los responsables del tratamiento que no estén dispuestos a comunicar la información requerida dentro un plazo razonable sería otra demostración particularmente eficaz de la facultad de intervención. Esta facultad podría también incluir la posibilidad de emitir opiniones antes de la implementación de operaciones de tratamiento de datos (si el tratamiento presenta ries-

gos particulares a los derechos y libertades fundamentales, se debería consultar a la autoridad de control desde la primera etapa del diseño de los procesos) o someter casos, cuando fuere apropiado, a la autoridad competente pertinente.

122. Asimismo, de acuerdo con el *párrafo 4*, todo titular de datos deberá tener la posibilidad de solicitarle a la autoridad de control que investigue un reclamo relacionado a sus derechos y libertades con respecto al tratamiento de datos personales. Esto permite garantizar el derecho a una solución jurídica adecuada, conforme a los Artículos 9 y 12. Se deberían otorgar los recursos necesarios para llevar a cabo este deber. Según los recursos disponibles, las autoridades de control deberían poder definir prioridades para cumplir con las solicitudes y quejas presentadas por los titulares de datos.

123. Las Partes deberían otorgar a la autoridad de control la facultad de iniciar procesos judiciales o de denunciar las violaciones las normas de protección de datos a las autoridades judiciales, con sujeción a la existencia de excepciones según el Artículo 11, párrafo 3. Esta facultad deriva de la facultad de llevar a cabo investigaciones, las que podrán llevar a que la autoridad descubra una violación al derecho de un individuo a la protección. Las Partes podrán cumplir con esta obligación de otorgar esta facultad a la autoridad al autorizarla a tomar decisiones.

124. Cuando una decisión administrativa produzca efectos legales, toda persona afectada tiene derecho a una solución jurídica eficaz de acuerdo con las leyes nacionales aplicables.

125. El *párrafo 2,e.* menciona el rol de concientización de las autoridades de control. En este contexto, parece especialmente importante que las autoridades de control busquen proactivamente la visibilidad de sus actividades, funciones y facultades. A estos efectos, la autoridad de control deberá informar al público mediante informes periódicos (ver párrafo 131). Podrá también publicar opiniones, emitir recomendaciones generales con respecto a la aplicación correcta de las reglas de protección de datos o utilizar cualquier otro medio de comunicación. Además, deberá comunicar a los individuos y a los responsables y encargados del tratamiento de datos sus derechos y obligaciones con respecto a la protección de datos. Al concientizar sobre los problemas de protección de datos, las autoridades deben dirigirse específicamente a los niños y categorías vulnerables de personas a través de medios y lenguaje adaptados.

126. Según lo establecido en el *párrafo 3*, las autoridades de control están facultadas para dar su opinión sobre toda medida legislativa o administrativa que establezca tratamiento de datos personales, de acuerdo con las leyes nacionales aplicables. Esta facultad de consulta solamente cubrirá las medidas generales, no las individuales.

127. Además de las consultas estipuladas en el párrafo 3, puede que se le solicite a la autoridad que dé su opinión cuando se están preparando otras medidas de tratamiento de datos personales, por ejemplo, códigos de conducta o normas técnicas.

128. El Artículo 15 no impide que se les adjudiquen otras facultades a las autoridades de control.

129. El *párrafo 5* establece que las autoridades de control no podrían garantizar efectivamente los derechos y libertades individuales si no cuentan con completa independencia. La independencia de la autoridad de control en el ejercicio de sus funciones se garantiza mediante diversos elementos, incluyendo la composición de la autoridad; el método de designación de sus miembros; el plazo de ejercicio y términos de cese de sus funciones; la posibilidad de su participación en asambleas pertinentes sin restricciones indebidas; la opción de consultar expertos técnicos u otros o de realizar consultas externas; contar con recursos suficientes; la posibilidad de contratar su propio personal; o la toma de decisiones sin estar con sujeción a interferencias externas, ya sean directas o indirectas.

130. La prohibición de solicitar o aceptar instrucciones cubre el cumplimiento de sus obligaciones como autoridad de control. Esto no impide que las autoridades de control soliciten asesoramiento especializado cuando ello sea necesario siempre que la autoridad de control ejerza su propia libertad de decisión.

131. El *párrafo 7* establece la transparencia en el trabajo y actividades de la autoridad de control a través de, por ejemplo, la publicación de informes de actividad anuales que contengan información relacionada con el cumplimiento de sus actividades, entre otros.

132. A pesar de esta independencia, deberá ser posible apelar las decisiones de las autoridades de control en el juzgado o corte pertinente de acuerdo con los principios del Estado de Derecho, según lo establecido en el *párrafo 9*.





133. Por otra parte, a pesar de que las autoridades de control deberían tener la capacidad legal de actuar judicialmente y de solicitar el cumplimiento, la intervención (o falta de intervención) de una autoridad de control no debería impedir que un individuo afectado busque una solución jurídica (ver párrafo 124).

134. El *párrafo 10* del Artículo 15 establece que las autoridades de control no tendrán competencia respecto a los tratamientos llevados a cabo por órganos independientes actuando en su calidad de órganos judiciales. Esta excepción a las facultades de control debería limitarse a actividades verdaderamente judiciales, de acuerdo con las leyes nacionales.

**Capítulo V – Cooperación y asistencia mutua**

**Artículo 16 – Designación de autoridades de control**

135. El capítulo V (Artículos 16 al 21) establece varias disposiciones referidas a la cooperación y la asistencia mutua entre las Partes, a través de sus diferentes autoridades, para la aplicación de las leyes de protección de datos establecidas en el Convenio. Estas disposiciones son obligatorias, excepto para los casos establecidos en el Artículo 20. De acuerdo con el Artículo 16, las Partes designarán una o más autoridades e informarán al Secretario General del Consejo de Europa su información de contacto, además de sus competencias materiales y territoriales, si correspondiere. Los siguientes artículos prevén un marco detallado para la cooperación y la asistencia mutua.

136. A pesar de que la cooperación entre las Partes se llevará a cabo generalmente por las autoridades de control establecidas en el Artículo 15, no se deberá excluir la posibilidad de que una Parte designe a otra autoridad a los efectos de cumplir con lo estipulado en el Artículo 16.

137. La cooperación y la asistencia mutua son pertinentes para los controles *a priori y a posteriori* (por ejemplo, para corroborar las actividades de un responsable del tratamiento de datos específico). La información intercambiada podrá tener carácter legal o referirse a hechos.

**Artículo 17 – Formas de cooperación**

138. De acuerdo con el Artículo 17, las autoridades de control en el significado del Artículo 15 deberán cooperar entre sí en la medida necesaria para cumplir con sus obligaciones y ejercer sus facultades. Dado que el Artículo 17 limita la cooperación entre autoridades de control a lo que sea necesario "para cumplir con sus obligaciones y ejercer sus facultades" y dado que la capacidad de una autoridad de control de cooperar depende del alcance de sus facultades, la disposición no se aplicará si la Parte hace uso del Artículo 11, párrafo 3, estableciendo una limitación a las facultades de las autoridades de control de acuerdo con el Artículo 15, párrafo 2, *literales a. al d.*

139. La cooperación podrá tomar varias formas, algunas "duras", como, por ejemplo, hacer cumplir las leyes de protección de datos a través de la asistencia mutua, en las cuales la legalidad de la actuación de las autoridades de control es indispensable, y otras "laxas", como, por ejemplo, concientización, capacitación, intercambio de personal.

140. El catálogo de posibles actividades de cooperación no es exhaustivo. En primer lugar, las autoridades de control deberán proporcionarse asistencia mutua, especialmente compartiendo información pertinente y útil. Esta información puede tener una doble naturaleza: "información y documentación acerca de sus leyes y prácticas administrativas relacionadas con la protección de datos" (lo que normalmente no trae consigo ningún tipo de problema, dicha información podrá intercambiarse libremente y se podrá divulgar públicamente) e información confidencial, incluyendo los datos personales.

141. En lo que concierne a los datos personales, estos solamente podrán intercambiarse cuando ello sea esencial para la cooperación, es decir, cuando la cooperación se vuelva ineficaz en caso de no hacerlo, o si el "titular de datos hubiere prestado su consentimiento explícito, específico, libre e informado". La transferencia de datos personales deberá cumplir en todos los casos con las disposiciones del Convenio y en particular con el Capítulo II (ver también el Artículo 20 que trata sobre los motivos de rechazo).

142. Además del suministro de información pertinente y útil, el objetivo de la cooperación se podría lograr a través de investigaciones o intervenciones coordinadas y acciones conjuntas. Las autoridades de control deberán consultar la legislación doméstica correspondiente, por ejemplo códigos de procesos administrativos, civiles o penales o compromisos supra o internacionales que los vincule, por ejemplo, tratados de asistencia legal mutua, determinando su capacidad legal de proporcionar una cooperación de ese tipo.

143. El *párrafo 3* menciona una red de autoridades de control como una medida para contribuir a la racionalización del proceso de cooperación y, por ende, a la eficacia de la protección de datos personales. Cabe mencionar que el Convenio menciona "una red" en la forma singular. Esto no impide que las autoridades de control de las Partes formen parte de otras redes pertinentes.

**Artículo 18 – Asistencia a los titulares de datos**

144. El *párrafo 1* asegura que los titulares de datos de las Partes del Convenio y de terceros países podrán ejercitar sus derechos reconocidos en el Artículo 9, sin importar su lugar de residencia o su nacionalidad.

145. De acuerdo con el *párrafo 2*, cuando el titular de datos reside en otra de las Partes, la persona tendrá la opción de ejercitar sus derechos tanto directamente en el país donde se trata la información relacionada con el titular de datos como indirectamente mediante un delegado de la autoridad designada.

146. Además, los titulares de datos que viven en el exterior tendrán la oportunidad de ejercitar sus derechos con la ayuda de representantes diplomáticos o consulares de su propio país.

147. El *párrafo 3* establece que las solicitudes deberán ser lo más específicas posibles para facilitar el procedimiento.

**Artículo 19 – Garantías**

148. Este artículo establece que las autoridades de control deberán tener las mismas obligaciones de discreción y confidencialidad con las autoridades de protección de datos de las otras Partes y los titulares de datos que residen en el exterior.

149. La autoridad de control solo podrá otorgar asistencia en nombre de un titular de datos cuando este último la solicite. La autoridad debe haber recibido un mandato del titular de datos y no podrá actuar de manera autónoma en su nombre. Esta disposición es de esencial importancia para la confianza mutua, que es la base de la asistencia mutua.

**Artículo 20 – Rechazo de solicitudes**

150. Este artículo establece que las Partes están obligadas a cumplir con las solicitudes de cooperación y asistencia mutua. Los motivos para rechazar una solicitud se encuentran enumerados de manera exhaustiva.

151. El término "cumplir" utilizado en el *literal c.* se deberá entender en el sentido amplio de la palabra, cubriendo no solo la respuesta a la solicitud, sino también la acción previa. Por ejemplo, la autoridad solicitada podrá rechazar la acción no solo si la transferencia a la autoridad que le solicitó la información puede dañar los derechos y libertades fundamentales de un individuo, sino también cuando el simple hecho de buscar la información puede perjudicar sus derechos o libertades fundamentales. Además, la ley puede establecer que la autoridad solicitada debe asegurarse de que otros intereses de orden público estén siendo protegidos (por ejemplo, asegurar la confidencialidad en una investigación policial). En estos casos, la autoridad de control podrá estar obligada a omitir cierta información o documentos al responder las solicitudes.

**Artículo 21 – Costos y procedimientos**

152. Las disposiciones de este artículo son análogas a las que se encuentran en otros instrumentos internacionales.

153. Para no sobrecargar el Convenio con una gran cantidad de detalles de implementación, el *párrafo 3* de este artículo prevé que los procedimientos, las formas y el idioma a utilizar se acordarán entre las Partes. El texto de este artículo no especifica ningún procedimiento formal y permite acuerdos administrativos, que pueden incluso estar confinados a casos específicos. Por otra parte, se recomienda a las Partes que otorguen la facultad de celebrar dichos acuerdos a las autoridades de control. Las formas de cooperación y de asistencia podrán variar también dependiendo del caso. Es claro que la transmisión de una solicitud de acceso a información médica confidencial deberá cumplir con requisitos diferentes a los necesarios para consultas rutinarias sobre un registro de habitantes.





**Capítulo VI – Comité del Convenio**

154. El objetivo de los Artículos 22, 23 y 24 es facilitar la efectiva aplicación del Convenio y, cuando fuere necesario, perfeccionarlo. El Comité del Convenio constituye otro medio de cooperación entre las Partes para efectivizar las leyes de protección de datos adoptadas de acuerdo con el Convenio.

155. El Comité del Convenio estará compuesto por representantes de todas las Partes, seleccionado de las autoridades de control nacionales o del gobierno.

156. La naturaleza del Comité del Convenio y del probable procedimiento utilizado podrá ser similar a los establecidos en las condiciones de otros convenios pactados en el marco del Consejo de Europa.

157. Dado que el Convenio trata un tema que está en continuo desarrollo, puede esperarse que surjan preguntas relacionadas con la aplicación práctica del Convenio (Artículo 23, *literal a.*) y su significado (mismo artículo, *literal d.*).

158. Las Normas de Procedimiento del Comité del Convenio establecen disposiciones con respecto al derecho de voto de las Partes y las modalidades del ejercicio de este derecho y se encuentran adjuntos al Protocolo de enmienda.

159. Toda enmienda a las Normas de Procedimiento deberá aprobarse por mayoría de dos tercios, excepto en el caso de enmiendas a las disposiciones referidas al derecho de voto y sus correspondientes modalidades, para las cuales se aplicará el Artículo 25 del Convenio.

160. Luego de la adhesión, la UE realizará una declaración para clarificar la distribución de competencias entre la UE y sus Estados miembros con respecto a la protección de datos personales según lo establecido en el Convenio. Posteriormente, la UE informará toda modificación sustancial de la distribución de competencias al Secretario General.

161. De acuerdo con el Artículo 25, el Comité del Convenio podrá proponer enmiendas al Convenio y evaluar otras propuestas de enmienda planteadas por una Parte o por el Comité de Ministros (Artículo 23, *literal b. y c.*).

162. A efectos de garantizar la aplicación de los principios de protección de datos establecidos en el Convenio, el Comité del Convenio tendrá un papel fundamental para evaluar el cumplimiento del Convenio, ya sea al evaluar el nivel de protección de datos de uno de los candidatos a la adhesión (Artículo 23, *literal e.*) o al evaluar periódicamente la implementación del Convenio por las Partes (Artículo 23, *literal h.*). El Comité del Convenio también podrá evaluar el cumplimiento con el sistema de protección de datos del Convenio por un Estado u organización internacional si así lo requiriera el Estado u organización internacional (Artículo 23, *literal f.*).

163. El Comité del Convenio actuará de acuerdo con un procedimiento justo, transparente y público según se establece en las Normas de Procedimiento para emitir su opinión sobre el cumplimiento con el Convenio.

164. Además, el Comité del Convenio podrá aprobar modelos de garantías estandarizadas para transferencias de datos (Artículo 23, *literal g.*).

165. Finalmente, el Comité del Convenio podrá ayudar a resolver las dificultades entre las Partes (Artículo 23, *literal i.*). En el caso de controversias, el Comité del Convenio buscará llegar a un acuerdo entre las Partes a través de negociaciones u otras medidas amistosas.

**Capítulo VII – Enmiendas**

**Artículo 25 – Enmiendas**

166. El Comité de Ministros, quien adoptó el texto original de este Convenio, también tendrá competencia para aprobar toda enmienda al mismo.

167. De acuerdo con el *párrafo 1*, la iniciativa para realizar enmiendas podrá ser tomada por el Comité de Ministros, el Comité del Convenio o una Parte (ya sea Estado miembro del Consejo de Europa o no).

168. De acuerdo con el *párrafo 3*, toda propuesta de enmienda que no provenga del Comité del Convenio deberá enviarse al mismo para ser evaluada.

169. En principio, toda enmienda entrará en vigor treinta días después de que todas las Partes informaran al Secretario General del Consejo Europeo que aceptaron la misma. Sin embargo, el Comité de Ministros

puede decidir en ciertas circunstancias mediante decisión unánime y luego de haber consultado al Comité del Convenio que dichas enmiendas entren en vigor luego de expirado un plazo de 3 años, salvo que una Parte comunique al Secretario General su oposición. Este procedimiento tiene como objetivo acelerar la entrada en vigor de las enmiendas, respetando a su vez el principio del consentimiento de todas las Partes. El mismo solo podrá utilizarse para enmiendas menores y técnicas.

**Capítulo VIII – Cláusulas finales**

**Artículos 26 – Entrada en vigor**

170. El *párrafo 2* establece que el número de ratificaciones por los Estados miembros del Consejo de Europa para la entrada en vigor es de cinco, dado que se considera que para que el Convenio sea eficaz el mismo debe tener un alcance geográfico amplio.

171. El Convenio se encuentra abierto a suscripción por la Unión Europea /sigue nota al pie de página n° 18/.

**Artículo 27 – Adhesión de Estados no miembros y organizaciones internacionales**

172. El Convenio, el cual se desarrolló originalmente en cooperación con la OCDE y varios Estados no europeos, se encuentra abierto para cualquier Estado del mundo que cumpla con sus disposiciones. El Comité del Convenio está a cargo de evaluar dicho cumplimiento y preparar un dictamen referido al nivel de protección de datos del candidato a la adhesión para el Comité de Ministros.

173. Dada la naturaleza sin fronteras del flujo de datos, se busca la adhesión de países y organizaciones internacionales de todo el mundo. Las organizaciones internacionales que pueden adherir al Convenio son solamente aquellas que están definidas como organizaciones regidas por el derecho internacional púbico.

**Artículo 28 – Cláusula territorial**

174. Es de suma importancia que se implemente el Convenio en territorios remotos sujetos la jurisdicción de las Partes o en cuya representación las Partes pueden asumir compromisos dada la manera en que se están utilizando los países lejanos para llevar a cabo las operaciones de tratamiento de datos, ya sea por razones de costos y de mano de obra o de la utilización de capacidad de tratamiento de datos que alternen día y noche.

**Artículo 29 – Reservas**

175. Las normas contenidas en este Convenio constituyen los elementos más básicos y esenciales para la protección eficaz de datos. Por esta razón, el Convenio no permite la reserva de ninguna de sus disposiciones, las cuales son además razonablemente flexibles pues enumeran las excepciones y restricciones permitidas en ciertos artículos.

**Artículo 30 – Denuncia**

176. Toda Parte tiene derecho a denunciar el Convenio en cualquier momento.

**Artículo 31 – Notificaciones**

177. Estas disposiciones cumplen con las cláusulas finales habituales contenidas en otros convenios del Consejo de Europa.

/A fojas 18:/

A pesar de que los principios básicos del Convenio 108 de 1981 se han mantenido a lo largo del tiempo y de que su abordaje generalista y tecnológicamente neutro es de una fortaleza innegable, el Consejo de Europa ha considerado necesario modernizar este instrumento trascendental.

La modernización del Convenio 108 ha tenido dos objetivos principales: abordar los desafíos provenientes del uso de nuevas tecnologías de información y comunicación y reforzar la aplicación eficaz del Convenio.

ENG. PREMS 085218

www.coe.int





El Consejo de Europa es la organización de derechos humanos líder en el continente. Está compuesto por 47 estados miembros, de los cuales 28 son miembros de la Unión Europea. Todos los estados miembros del Consejo de Europa firmaron el Convenio Europeo de Derechos Humanos, un tratado destinado a proteger los derechos humanos, la democracia, y el estado de derecho. El Tribunal Europeo de Derechos Humanos supervisa la implementación del Convenio en los estados miembros.

/Obra bandera del Consejo de Europa./

Consejo de Europa

/A continuación, se traducen las notas al pie de página desde la nota número 1 a la nota número 18./

/Nota al pie de página n°1:/ Reglamento General de Protección de Datos (UE) 2016/679 (/del inglés/ "GDPR") y Directiva de Protección de los Datos para Autoridades Policiales y de Justicia Penal (UE) 2016/680 ("Directiva policial").

/Nota al pie de página n° 2:/ Aceptada por la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en Madrid del 4 al 6 de noviembre de 2009.

/Nota al pie de página n° 3:/ Ver en especial Antecedente 105 del GDPR.

/Nota al pie de página n° 4:/ Ver Convenio del Consejo de Europa sobre Acceso a los Documentos Públicos (CETS n° 205).

/Nota al pie de página n° 5:/ "la protección de los datos personales tiene importancia fundamental para que una persona pueda disfrutar de su derecho al respeto de su vida personal o familiar según lo garantiza el Artículo 8" – EctHR MS *c/ Suecia*, (Solicitud n° 20837/92), 1997, párrafo 41.

/Nota al pie de página n° 6:/ Ver Comisionado de Derechos Humanos del Consejo de Europa. La primacía del derecho en Internet y en el resto del Mundo Digital, Publicación, CommDH/IssuePaper(2014)1, 8 de diciembre 2014, p. 48, punto 3.3 "Todos" sin discriminación.

/Nota al pie de página n° 7:/ Ver Tribunal de Justicia de la UE, *František Ryneš c/ Úřad*, 11 de diciembre de 2014, C212/13k.

/Nota al pie de página n° 8:/ Las organizaciones internacionales se definen como organizaciones reguladas por el derecho internacional público.

/Nota al pie de página n° 9:/ Donde apliquen los cuatro Convenios de Ginebra de 1949, los Protocolos Adicionales de los mismos de 1977, y los Estatutos del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja.

/Nota al pie de página n° 10:/ Recomendación N° R (97) 18 del Comité de Ministros a los Estados miembros, relacionada con la protección de datos personales recolectados y tratados con propósitos estadísticos, Apéndice, punto 1, 30 de setiembre de 1997.

/Nota al pie de página n° 11:/ Memorándum Explicativo de la Recomendación N° R (97) 18 del Comité de Ministros a los Estados miembros, relacionada con la protección de datos personales recolectados y tratados con propósitos estadísticos, párrafos 11 y 14.

/Nota al pie de página n° 12:/ Ver Recomendación Rec. N° R (97) 18 del Comité de Ministros, obra citada

/Nota al pie de página n° 13:/ La jurisprudencia pertinente incluye en particular la protección de la seguridad del estado y democracia constitucional de, entre otros, el espionaje, terrorismo, apoyo al terrorismo y separatismo. Cuando la seguridad nacional se encontrare en juego, se deberán proporcionar garantías contra el poder irrestricto. Las decisiones pertinentes del Tribunal Europeo de Derechos Humanos pueden encontrarse en la página web del Tribunal (hudoc.echr.coe.int).

/Nota al pie de página n° 14:/ Para las Partes que son Estados miembros del Consejo de Europa, la jurisprudencia del Tribunal Europeo de Derechos Humano según el Artículo 8 del Convenio Europeo de los Derechos Humanos ha desarrollado dichos requisitos (ver en particular ECtHR, *Roman Zakharov c/ Rusia* [Solicitud n° 47143/06], 4 de diciembre de 2015, párrafo 233; *Szabó y Vissy c/ Hungría* [Solicitud n° 37138/14], 12 de enero de 2016, párrafos 75 y siguientes).

/Nota al pie de página n° 15:/ Desde la entrada en vigor del Protocolo de Enmienda, el Protocolo Adicional que trata sobre las autoridades de control y los flujos transfronterizos (ETS n° 181) será considerado parte integral del Convenio y sus modificaciones.

/Nota al pie de página n° 16:/ Desde la entrada en vigor del Protocolo de Enmienda, el Protocolo Adicional que trata sobre las autoridades de control y los flujos transfronterizos (ETS n° 181) será considerado parte integral del Convenio y sus modificaciones.

/Nota al pie de página n° 17:/ Ver nota al pie 14.

/Nota al pie de página n° 18:/ Las enmiendas al Convenio aprobadas por el Comité de Ministros el 15 de junio de 1999 perdieron sus propósitos desde la entrada en vigor del Protocolo.

La suscrita Traductora Pública declara que lo que antecede es traducción fiel del documento adjunto, **Informe Explicativo de Convenio**, redactado en idioma inglés, de cuya versión al español guarda copia en su archivo con el número 058/2019. Montevideo, 06 de mayo de 2019.

*Traducción Pública realizada*
*por la Traductora Inés Payssé Terra*

# DICTÁMENES



**Dictamen Nº 01/018, de 12 de marzo de 2018.** Consulta presentada por la Intendencia de Montevideo en el marco del proyecto de Cercanía Digital sobre la legitimidad del tratamiento de datos provenientes de fuentes propias, de terceros y de redes sociales, entre otras.

## CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

| Dictamen Nº | Expediente Nº |
|---|---|
| 01/2018 | 2018-2-10-0000111 |

Montevideo, 12 de marzo de 2018

**VISTO:** La consulta presentada por la Intendencia de Montevideo en el marco del proyecto de Cercanía Digital.

**RESULTANDO:**

I) Que en la mencionada consulta se plantean cuestiones relativas a la legitimidad del tratamiento masivo de datos provenientes de diversas fuentes, tales como bases propias, de terceros y redes sociales.

II) Que en concreto se solicita el pronunciamiento de esta Unidad en referencia a: 1) el rol de la empresa contratada por la Intendencia de Montevideo frente al tratamiento de datos de dicho organismo; 2) el empleo de información proveniente de internet y de redes sociales; 3) el empleo de teléfono y correo electrónico de personas físicas existentes en bases de la propia Intendencia, así como la incorporada de "nuevas estructuras de datos basadas en datos públicos disponibles en la red" –en los términos expuestos por la consultante-; 4) el empleo de información obtenida de otros organismos públicos.

**CONSIDERANDO:**

I) Que las preguntas planteadas por la Intendencia de Montevideo abarcan distintos aspectos vinculados a la protección de datos personales, siendo de aplicación los artículos 4°, 9°, 9° bis y 17° de la Ley N° 18.331, de 11 de agosto de 2008.

II) Que valorados los extremos consultados, se respondieron cada una de las preguntas formuladas en Informe N° 127 que obra de fojas 7 a 9 de estos obrados.

**ATENTO:** A lo expuesto e informado, y a lo previsto en las normas aplicables,

**EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES**

**DICTAMINA:**

1.- El rol del Consorcio contratado para el tratamiento de los datos personales por cuenta y orden de la Intendencia de Montevideo, según la consulta mencionada en el "Visto", es el de encargado de tratamiento -en los términos del artículo 4° de la Ley N° 18.331-, siendo recomendable la suscripción de un contrato en que se detallen las obligaciones de ambas partes. En el caso de otras empresas, deberán analizarse las condiciones específicas de la contratación para determinar el rol que cumplen frente a los citados datos.

2.- Internet no es fuente pública de información conforme lo dispuesto por el artículo 9° bis de la Ley N° 18.331, por lo que deberá estarse a los términos de cada servicio o producto ofrecido para determinar si lo publicado es o no de libre utilización. En el caso de redes sociales, ello debe surgir de los documentos vinculados que regulen la relación entre cada red y sus usuarios.

3.- El empleo de teléfono y correo electrónico de bases de la propia Intendencia como mecanismo de contacto es correcto, siempre que se trate de actividades de la consultante en el marco de sus competencias. No obstante, para la incorporación de "nuevas estructuras de datos basadas en datos públicos disponibles en la red" debe cumplirse con lo indicado en el numeral anterior y darle a la persona la posibilidad de no recibir más comunicaciones.

4.- Con respecto al empleo de información de bases de datos de otros responsables, deberá considerarse en el caso concreto la aplicación de los artículos 9° y 17° de la Ley N° 18.331. En el caso de organismos públicos es pasible de aplicación, la excepción prevista en el literal B) del artículo 9°, más no así en el caso de entidades privadas como las señaladas en la consulta, por no poseer éstas vínculo funcional ni legal con la consultante. En todo caso deberá de analizarse el caso concreto.

5.- Notifíquese, publíquese y oportunamente archívese.

Mag. Federico Monteverde
Consejo Ejecutivo
URCDP





**Dictamen Nº 02/018, de 19 de marzo de 2018.** Consulta remitida por la Administración Nacional de Usinas y Transmisiones Eléctricas (UTE) en el marco del proyecto de redes y medidores inteligentes.

# CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

| Dictamen Nº | Expediente Nº |
|---|---|
| 02/2018 | 2017-2-10-0000519 |

Montevideo, 19 de marzo de 2018

**VISTO:** La consulta de la Administración Nacional de Usinas y Trasmisiones Eléctricas (UTE) en el marco del proyecto de redes y medidores inteligentes.

**RESULTANDO:**

I) Que los medidores inteligentes tienen un comportamiento diferente a los tradicionales ya que permiten conocer los hábitos de consumo de los clientes.

II) Que en función de lo expuesto, UTE consulta si es necesario recabar el previo consentimiento informado de los clientes al momento de instalar los nuevos medidores inteligentes.

**CONSIDERANDO:**

I) Que la relación de la consultante con sus usuarios es de origen contractual, por lo que lo que el cliente prestó su consentimiento expreso para la instalación del medidor y el abastecimiento de energía, además de tratarse de una tarea desarrollada por UTE en ejercicio de funciones propias y en virtud de una obligación legal.

II) Que en su mérito, el cambio de medidores tradicionales por medidores inteligentes no requiere nuevo consentimiento del titular (usuario) con contrato vigente, siempre que el tratamiento de datos realizado obedezca a una finalidad igual o compatible a la realizada por el medidor tradicional conectado originalmente, de acuerdo con lo dispuesto en los artículos 8 y 9 literales B) y D) de la Ley N° 18.331. A tales efectos, corresponderá analizar si el medidor inteligente incorpora nuevos tratamientos y, en caso afirmativo, determinar su compatibilidad con los originalmente pautados.

III) Que aun en caso de no requerirse un nuevo consentimiento en función de que el tratamiento obedece a una finalidad igual o compatible, UTE será responsable del cumplimiento del resto de los principios de legalidad, veracidad, seguridad, reserva y responsabilidad, así como de informar a los usuarios y de garantizar el efectivo ejercicio de los derechos de acceso, rectificación, actualización, inclusión, supresión e impugnación de valoraciones personales, en cuanto correspondan.

IV) Que a los efectos del despliegue de contadores y redes inteligentes, se sugiere nutrir el proceso de implantación con las experiencias y buenas prácticas relevadas por la Comisión Europea en la Recomendación 2012/48/CE, considerando especialmente las acciones de: a) implementar y aplicar un modelo de evaluación de impacto sobre la protección de los datos personales a ser tratados, b) incorporar la protección de datos desde el diseño y por defecto, c) garantizar la seguridad de los datos desde el diseño, d) adoptar medidas de protección de datos tales como anonimizar y aplicar los principios de minimización y transparencia.

**ATENTO:** A lo expuesto e informado, y a lo previsto en las normas aplicables,

**EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES**

**DICTAMINA:**

1.- Estar a lo dispuesto en los Considerandos I a IV.

2.- Notifíquese, publíquese y oportunamente archívese.

Mag. Federico Monteverde
Consejo Ejecutivo
URCDP





**Dictamen Nº 09/018, de 23 de julio de 2018.** Consulta realizada por la Universidad de la República (UDELAR) respecto de la posibilidad de establecer un Registro de Títulos de Grado y Posgrado de consulta abierta, de conformidad con la Ley N° 18.331, de 11 de agosto de 2008.

# CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

| Dictamen Nº | Expediente Nº |
|---|---|
| 09/2018 | 2017-2-10-0000394 |

Montevideo, 23 de julio de 2018

**VISTO:** La consulta formulada por la UNIVERSIDAD DE LA REPÚBLICA (UDELAR).

**RESULTANDO:**

I) Que la UDELAR se presenta ante esta Unidad a los efectos de obtener opinión con respecto a la posibilidad de establecer un Registro de Títulos de Grado y Posgrado de consulta abierta, de conformidad con la Ley N° 18.331, de 11 de agosto de 2008.

II) Que la consultante adelanta opinión en el sentido de que entiende que no existe ley habilitante para ello, y que contiene información personal, sin perjuicio de que entiende que existen dudas atento a distintos dictámenes –que individualiza- de esta Unidad y de la Unidad de Acceso a la Información Pública (UAIP).

**CONSIDERANDO:**

I) Que la información contenida en el Registro de Libros y Sistemas de Gestión de Títulos y Egresados que lleva la Bedelía General contiene información personal de los egresados de la UDELAR, en el sentido establecido en el artículo 4° literal d) de la Ley N° 18.331. Por ello, toda revelación a persona distinta de su titular será una comunicación de datos conforme lo establecido en el literal b del mismo artículo, resultando aplicable además el artículo 17 del citado cuerpo normativo.

II) Que en el literal A del artículo 9 y literal D del artículo 9 Bis de la Ley N° 18.331 se hace referencia a las fuentes públicas de información, incluyendo entre ellas a los registros públicos, especificando que estos son, entre otros, aquellos en los que "prevalezca el interés general en cuanto a que los datos personales en ellos contenidos puedan ser consultados, difundidos o utilizados por parte de terceros". Que en el caso no se aprecia un interés general.

III) Que por otra parte, todo tratamiento de datos debe efectuarse de conformidad con lo establecido en el artículo 7° de la Ley N° 18.331 – relacionado con los principios de proporcionalidad y calidad de los datos-. Este último edicta que los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido.

**ATENTO:** A lo expuesto,

**EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES**

**DICTAMINA:**

1.- Que el tratamiento de la información del registro llevado adelante por la UDELAR debe efectuarse de conformidad con lo establecido en el artículo 17° de la Ley N° 18.331, y teniendo en cuenta lo establecido por su artículo 7°.

2.- Que la publicación abierta de la información en internet de los datos de egresados de carreras de la UDELAR o de universidades extranjeras reconocidos por ésta no se encuentra abarcada en el concepto de interés general, por lo que no es pública, y puede además considerarse excesiva.

3.- Que no obstante ello, cabe admitir la comunicación siempre que se cumplan con los extremos indicados en el artículo 17 de la Ley N° 18.331, a través de procedimientos que permitan determinar la existencia de un interés específico por parte de destinatarios puntuales.

4.- Notifíquese, publíquese y oportunamente archívese.

Dr. Felipe Rotondo Tornaría

Consejo Ejecutivo

URCDP





**Dictamen Nº 12/018, de 21 de agosto de 2018.** Consulta sobre la implementación del Sistema de Historia Clínica Electrónica Nacional.

# CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

| Dictamen | Acta Nº |
|---|---|
| 12/2018 | 21/2018 |

Montevideo, 21 de agosto de 2018

**VISTO:** La implementación del Sistema de Historia Clínica Electrónica Nacional,

**RESULTANDO:**

I) Que esta Unidad se ha pronunciado en múltiples dictámenes acerca de distintos aspectos vinculados a la recolección y comunicación de datos de salud, la Historia Clínica Electrónica, el acceso a la información de salud por parte de médicos y de instituciones subcontratadas, el Sistema y la Plataforma de Historia Clínica Electrónica Nacional, entre otros. A estos efectos, corresponde destacar los Dictámenes Nos. 18/010, de 20 de agosto de 2010, 5/014, de 30 de abril de 2014, 4/016, de 2 de marzo de 2016, 14/016, de 8 de setiembre de 2016, 5/2018 y N° 6/018, ambos de 7 de mayo de 2018.

II) Que en cuanto a la normativa vigente en la materia, las Leyes Nos. 9.202, de 12 de enero de 1934 (Ley Orgánica de Salud Pública), 18.211, de 5 de diciembre de 2007 (Sistema Nacional Integrado de Salud), 18.335, de 15 de agosto de 2008, artículo 20 (sobre Derechos y Obligaciones de Pacientes y Usuarios de los servicios de salud), 19.286, de 25 de setiembre de 2014, 19.355, de 19 de diciembre de 2015, artículo 466 y el Decreto N° 242/017, de 31 de agosto de 2017.

III) Que en lo que refiere específicamente a la protección de datos personales y el tratamiento de datos de salud, resultan de aplicación los artículos 4° lit. E), 17, 18 y 19 de la Ley N° 18.331, de 11 de agosto de 2008, y el Decreto Nº 414/009, de 31 de agosto de 2009.

**CONSIDERANDO:**

I) Que esta Unidad tiene como cometido el realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la Ley N° 18.331, incluyendo el asesoramiento y asistencia con respecto a los alcances de la Ley citada (artículo 34°).

II) Que los dictámenes referidos hacen a distintos aspectos del tratamiento de los datos de salud, los que deben considerarse como complementarios.

III) Que en ese marco, con el fin de facilitar su cumplimiento por parte de los sujetos obligados, y el conocimiento cabal de los derechos en materia de protección de datos personales por parte de los usuarios del Sistema Nacional Integrado de Salud, se estima pertinente clarificar la orientación general de la Unidad en algunos aspectos puntuales.

**ATENTO:** A lo expuesto y lo dispuesto por los artículos mencionados,

**EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES**

**DICTAMINA:**

1.- La Historia Clínica es propiedad del paciente y usuario de los servicios de salud y se encuentra bajo la custodia del prestador de salud, quien reviste la calidad de responsable de tratamiento (artículos 4°, literal K), de la Ley N° 18.331 y 18, de la Ley N° 18.335). El tratamiento de la información contenida en ella, realizado en el marco de la relación contractual con un prestador determinado, deriva del consentimiento otorgado al contratar sus servicios (artículo 18, de la Ley Nº 18.331); en el caso de servicios subcontratados, se funda en la excepción establecida en el artículo 17, literal C), de la Ley N° 18.331.

2.- El uso del Sistema y la Plataforma de Historia Clínica Electrónica Nacional es obligatorio para los prestadores incorporados al Sistema Nacional Integrado de Salud, por lo que el registro de la información necesaria para habilitar los accesos en la Plataforma referida se encuentra autorizado, debiendo cumplirse con los principios y demás disposiciones de la Ley N° 18.331.

3.- El acceso a la información clínica por parte de los responsables de la atención médica y el personal administrativo vinculado (artículo 18 literal D) de la Ley N° 18.335), a través de la Plataforma de Historia Clínica Electrónica Nacional, implica una comunicación de datos personales y requiere del previo consentimiento expreso y escrito del titular de los datos, salvo las siguientes excepciones: a) las referidas en el numeral 1 del presente Dictamen; b) la realizada durante una instancia asistencial, sin que resulte relevante en esta situación el prestador ante el que se encuentre el paciente y usuario de los servicios de salud (artículo 19, de la Ley N° 18.331, refrendado por el artículo 19, del Decreto N° 242/017); c) en situaciones de emergencia (artículo 17, literal C), de la Ley N° 18.331); d) cuando la información se proporcione disociada (artículo 17, literal D); e) en otras situaciones amparadas en lo dispuesto por el artículo 18, de la Ley N° 18.331.

4.- En el tratamiento de los datos de salud deberá cumplirse con los principios en materia de protección de datos, y con el secreto profesional, conforme lo establecido en los artículos 6° a 12, de la Ley N° 18.331, el artículo 20, de la Ley N° 18.335 y en la Ley N° 19.286.

Dr. Felipe Rotondo Tornaría

Consejo Ejecutivo

URCDP





**Dictamen Nº 16/018, de 11 de setiembre de 2018.** Consulta formulada por el Instituto de Regulación y Control del Cannabis (IRCCA) sobre las respuestas que corresponde brindar ante solicitudes remitidas desde las Fiscalías del país, en las que se procura conocer la existencia de autocultivos en determinados domicilios.

# CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

| Dictamen | Expediente Nº |
|---|---|
| 16/2018 | 2018-2-10-0000297 |

Montevideo, 11 de setiembre de 2018

**VISTO:** La consulta formulada por el Instituto de Regulación y Control del Cannabis (IRCCA).

**RESULTANDO:**

I) Que la consultante manifiesta que posee a su cargo el Registro del Cannabis, organizado en varias secciones conforme el artículo 52 del Decreto Nº 120/014, de 6 de mayo de 2014. La identidad de quienes se inscriban posee el carácter de dato sensible de conformidad con lo establecido en el artículo 8º de la Ley Nº 19.172, de 20 de diciembre de 2013.

II) Que atento a lo indicado en el resultando anterior, se consulta con respecto a las respuestas que corresponde brindar ante solicitudes remitidas desde las distintas Fiscalías del país, en las que se procura conocer la existencia de autocultivos en determinados domicilios.

**CONSIDERANDO:**

I) Que el presente se enmarca en lo establecido en los artículos 17 y 18 de la Ley Nº 18.331, de 11 de agosto de 2008, por tratarse de una comunicación de datos personales, algunos de los cuáles son definidos como sensibles. La comunicación de datos requiere del consentimiento previo del titular de los datos, o encontrarse abarcada en alguna de las excepciones previstas en el artículo 17.

II) Que el artículo 45 del Código del Proceso Penal habilita al Ministerio Público a requerir información a todas las entidades públicas estatales, dentro de los límites previstos en el citado artículo -en el marco de una investigación en proceso, y cuando no se afecten garantías o derechos fundamentales-. En el caso del IRCCA, el artículo 17 de la Ley Nº 19.172 establece que se trata de una persona pública no estatal, por lo que no resulta aplicable a su respecto las excepciones de los literales A y B del artículo 17 de la Ley Nº 18.331.

**ATENTO:** A lo expuesto y a lo previsto en las normas legales citadas,

**EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES**

**DICTAMINA:**

1.- La información de la existencia o no de un club cannábico o de un autocultivo en determinado domicilio puede brindarse ante un requerimiento del Ministerio Público, siempre que lo sea en forma anonimizada.

2.- En caso de procurarse información de identidad, esta puede proveerse al Ministerio Público con la intervención del Poder Judicial, en el marco de lo dispuesto en el artículo 177 del Código del Proceso Penal.

3.- Notifíquese, publíquese

Dr. Felipe Rotondo Tornaría

Consejo Ejecutivo

URCDP





**Dictamen Nº 17/018, de 11 de setiembre de 2018.** Consulta realizada por la Intendencia de Florida en relación con el alcance de la información a proveer a un edil departamental que requiere conocer la documentación de más de setecientos postulantes a un llamado público a concurso.

# CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

| Dictamen | Expediente Nº |
|---|---|
| 17/2018 | 2018-2-10-0000323 |

Montevideo, 11 de setiembre de 2018

**VISTO:** La consulta formulada por la Intendencia Departamental de Florida.

**RESULTANDO:**

I) Que la consultante manifiesta algunas dudas vinculadas al alcance de la información a proveer ante el requerimiento de un edil departamental en el marco de lo dispuesto en el artículo 284 de la Constitución. En concreto, se solicitó información relacionada con un llamado público a concurso, generando duda a la consultante las solicitudes de curriculums de postulantes y méritos, copia de cada prueba y puntaje final y listado resultante, detallado por prueba, todo de los más de 700 postulantes participantes.

**CONSIDERANDO:**

I) Que en el presente caso, la solicitud de informes se encuadra en las facultades otorgadas por la Constitución a los miembros de las Juntas Departamentales, a efectos de que puedan dar cumplimiento a su cometido (Art. 284). En particular el artículo 273 de la Constitución establece que dichas Juntas ejercerán las funciones legislativas y de contralor en el Gobierno Departamental.

II) Que fuera de los casos de excepción como el antes indicado, la información requerida deberá publicarse una vez culminadas todas las etapas del respectivo concurso, salvaguardando los datos personales sensibles u otros que no hagan a su objeto (Ley Nº 18.381, de 17 de octubre de 2008).

**ATENTO:** A lo expuesto,

**EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES**

**DICTAMINA:**

1.- Hacer saber a la Intendencia Departamental de Florida que en relación a la consulta señalada en la parte expositiva del presente, corresponde la entrega de la información solicitada al amparo del artículo 284 de la Constitución.

2.- Toda comunicación de información posterior, ya sea por parte de la Intendencia o de la Junta Departamental, incluyendo su publicación, deberá realizarse según lo expuesto por esta Unidad en Dictamen Nº 2/010, de 12 de enero de 2010.

3.- Notifíquese, publíquese

Dr. Felipe Rotondo Tornaría

Consejo Ejecutivo

URCD

**Dictamen Nº 20/018, de 4 de diciembre de 2018.** Consulta realizada por la Intendencia de Durazno en relación con la información pasible de ser exhibida en los recibos de pago emitidos desde su sistema de cobranzas.

# CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

| Dictamen | Expediente Nº |
|---|---|
| 20/2018 | 2017-2-10-0000394 |

Montevideo, 4 de diciembre de 2018

**VISTO:** La consulta formulada por la Intendencia de Durazno.

**RESULTANDO:**

I) Que por la presente se consulta en relación con la información pasible de ser mostrada en los recibos de pagos emitidos desde su sistema de cobranza.

II) Que actualmente el sistema permite mostrar el número de contribuyente, nombres y apellidos, número de padrón, detalle del tributo, y en cada tipo de tributo, la información referente a éste.

**CONSIDERANDO:**

I) Que la presente consulta versa sobre la información que debe figurar en los recibos de pagos de tributos. Atento a que éstos contienen en su mayoría, datos personales, resulta de aplicación lo dispuesto en la Ley N° 18.331, de 11 de agosto de 2008.

II) Que se debe tener presente lo expresado por Dictamen de esta Unidad N° 8/015, de 6 de mayo de 2015, por el cual se establece que los datos personales relativos a nombres, apellidos, domicilio y número de cédula de identidad, pueden figurar en las facturas cuando éstas se entregan a sus titulares. Que, además, establece que las decisiones de gestión en cuanto a las tecnologías a emplear, corresponden a la propia Entidad.

III) Que en forma complementaria, cabe indicar que si la información es proporcionada al propio titular, no existe comunicación de datos. Fuera de esos casos, deberá contarse con consentimiento informado y previo de los titulares, o realizarse la comunicación de datos a través de los mecanismos previstos en el artículo 17 literal D de la Ley N° 18.331.

**ATENTO:** A lo expuesto y lo dispuesto por los artículos 9 y 17 de la Ley N° 18.331,

**EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES**

**DICTAMINA:**

1.- Indicar que los recibos referidos en la consulta pueden contener información del padrón y otra relacionada con el tributo correspondiente, en forma disociada de sus titulares, cuando sean exhibidos a personas distintas de éstos.

2.- La información completa debe ser accesible por los titulares de los datos, con la debida acreditación de su identidad o representación, no siendo necesario recabar su consentimiento, teniendo presente que en este caso no existe comunicación de datos personales.

3.- Notifíquese al interesado.

4.- Publíquese y oportunamente archívese.

Dr. Felipe Rotondo Tornaría

Consejo Ejecutivo

URCD

**Dictamen Nº 21/018, de 4 de diciembre de 2018.** Consulta formulada por el Banco de Previsión Social (BPS), respecto de la posibilidad de informar a la Dirección Nacional de Identificación Civil del Ministerio del Interior, - en el marco de un convenio en proceso de suscripción - la fecha de fallecimiento de las personas.

# CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

| Dictamen | Expediente Nº |
|---|---|
| 21/2018 | 2018-2-10-0000527 |

Montevideo, 4 de diciembre de 2018

**VISTO:** La consulta formulada por el Banco de Previsión Social (BPS).

**RESULTANDO:**

I) Que se consulta con relación a la posibilidad de que BPS informe el dato fecha de fallecimiento a otras entidades que lo soliciten, y en concreto a la Dirección Nacional de Identificación Civil del Ministerio del Interior, en el marco de un Convenio que se procura suscribir entre ambas entidades.

**CONSIDERANDO:**

I) Que el presente caso trata de información de personas fallecidas, respecto de las cuales no resulta de aplicación la Ley N° 18.331, de 11 de agosto de 2008, salvo las excepciones previstas en la propia norma (artículos 14 y 39).

II) Que sin perjuicio de lo establecido, en aplicación de los principios de finalidad y veracidad consagrados en los artículos 7° y 8° de la Ley, y en el artículo 4° del Decreto N° 414/009, de 31 de agosto de 2009, los datos que no cumplan con las finalidades previstas para su recolección deben ser suprimidos o bloqueados, y no deben ser tratados salvo cuando deban ser puestos a disposición de los Poderes del Estado o instituciones legalmente habilitadas, a efectos de atender posibles responsabilidades surgidas del tratamiento.

III) Que asimismo, existen entidades públicas encargadas expresamente de comunicar el dato referido a otras entidades y al público en general, en concreto el Registro de Estado Civil dependiente del Ministerio de Educación y Cultura y los registros existentes en cada Intendencia Departamental.





**ATENTO:** A lo expuesto,

**EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES**

**DICTAMINA:**

1.- Indicar que la comunicación del dato "fecha de fallecimiento" en la forma planteada en la consulta no se ajusta a las disposiciones de la Ley N° 18.331, de 11 de agosto de 2008. En su caso, dicha información podrá ser solicitada directamente a las entidades legalmente habilitadas a proveerlo.

2.- Notifíquese al interesado.

3.- Publíquese y oportunamente archívese.

Dr. Felipe Rotondo Tornaría

Consejo Ejecutivo

URCD

# NOTA de INTERÉS


## ACTUALIZACION DE LA NORMATIVA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

**ANTECEDENTES**

La normativa uruguaya en materia de protección de datos personales fue modificada sustancialmente en el año 2008 con la sanción de la Ley N° 18.331, de 11 de agosto de 2008.

Esta Ley creó un régimen de carácter nacional y general de protección de datos personales, sustentado en el concepto de la protección de datos como derecho fundamental, incluido en lo dispuesto por el artículo 72 de la Constitución.[1] [2]

La concepción de la protección de datos personales como un derecho fundamental no resulta inocua, desde que centra la perspectiva de la protección que brindan las normas legales en la persona humana. No son jurídica ni éticamente viables renuncia particulares sobre datos personales, a cambio de compensaciones - económicas o no-. Ello debido a que si se concibe a la protección de datos personales como un derecho fundamental, inherente a la personalidad humana, no pueden aceptarse transacciones económicas sobre los datos, y su tratamiento depende única y exclusivamente, de las bases establecidas en la Ley.

Por otra parte, el derecho a la protección de datos personales por sí solo no resulta suficiente para la debida protección de las personas, sino que debe encontrarse acompañado por un marco general tuitivo de los derechos humanos. Resulta imprescindible la aplicación efectiva de normas nacionales e internacionales que protejan los derechos de las personas.[3]

Esta concepción del derecho a la protección de datos personales parte de una formulación que tiene como primer hito de relevancia el Convenio N° 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Auto-

1 *El artículo 72 de la Constitución uruguaya indica que: "La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno."*

2 *La Ley N° 18.331 derogó expresamente la anterior Ley N° 17.838, de 24 de setiembre de 2004, que poseía un alcance restringido a la protección de datos destinados a brindar informes objetivos de carácter comercial. No obstante su alcance restringido, los principios incluidos en esta última vinculados al tratamiento de los datos sirvieron de base para la nueva formulación incluida en la Ley N° 18.331.*

3 *Nuestro país se ha caracterizado por el respeto a los Convenios Internacionales y a las normas regionales y globales en materia de Derechos Humanos, como puede observarse en el documento "Estudio sobre armonización legislativa conforme a los TRATADOS DE DERECHOS HUMANOS RATIFICADOS POR URUGUAY u otras normas legales con fuerza vinculante" disponible en http://archivo.presidencia.gub.uy/_web/noticias/2006/09/ARMONIZACION.pdf*

matizado de Datos de Carácter Personal de fecha 28 de enero de 1981. Este Convenio reconoce la necesidad de brindar protección a toda persona en el respeto de sus derechos y libertades fundamentales, y en concreto su derecho a la vida privada, con respecto al tratamiento automatizado de datos de carácter personal (Artículo 1°).[4]

La evolución del derecho a nivel europeo continuó en el año 1995 con la aprobación de la Directiva N° 95/46/CE, que establecía grandes líneas en la materia que debían ser objeto de inclusión en las distintas legislaciones nacionales de los países miembros de la Unión Europea.

El tratamiento en el Convenio y la Directiva, de la protección de datos personales, resultó finalmente un antecedente para legislaciones más allá de Europa.[5]

En particular el artículo 25 de la Directiva -hoy sustituida por el Reglamento General de Protección de Datos N° 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y aplicable desde el 25 de mayo de 2018- preveía la posibilidad de declarar que un país poseía un nivel adecuado de protección en tanto su legislación cumpliera con incluir determinados principios generales (asociados a la finalidad, calidad, proporcionalidad y seguridad del tratamiento), derechos (acceso, rectificación, cancelación, información), previsiones especiales para algunos tipos de datos (sensibles, mercadotecnia, decisiones automatizadas), una autoridad independiente, y acceso a vías para obtener compensación en caso de incumplimientos. Ello debía ser valorado por el Grupo de Trabajo previsto en el artículo 29 de la Directiva, previa realización de un informe externo, elevando posteriormente de ser favorable, una propuesta de adecuación a la Comisión.

Uruguay cumplió con los pasos citados en el año 2012, y el 21 de agosto de 2012 fue declarado país adecuado por Decisión 2012/484/EU.[6]

El poseer estatus de "país adecuado" importa que la UE reconoce en Uruguay, un régimen de protección de los derechos y libertades de las personas, equivalente al que se brinda en Europa, lo que habilita la transferencia libre de datos hacia nuestro país.[7]

## EL CONTENIDO DE LA LEY Y SUS ALCANCES

En lo que respecta al contenido de nuestra Ley de Protección de Datos Personales, ésta se sustenta en un conjunto de principios que brindan coherencia al sistema y resultan aplicables a todo tipo de tratamientos de datos realizados en el país, ya sea por responsables o encargados públicos y privados.

Así, la ley prevé los principios de legalidad, veracidad, finalidad, previo consentimiento informado, seguridad de los datos, reserva y responsabilidad. El artículo 5º establece que estos principios servirán como criterio interpretativo para resolver cuestiones que puedan suscitarse en aplicación de las disposiciones pertinentes.

Parece relevante hacer énfasis en dos cuestiones vinculadas a los principios. En lo que refiere al principio del previo consentimiento informado, éste se erigía en la base principal de legitimidad en el tratamiento de datos personales al momento de la sanción de la Ley. No obstante, el principio plantea un conjunto de excepciones que deberían de considerarse bases tan legítimas como aquel, máxime ante la aplicación de nuevas tecnologías potencialmente lesivas de los derechos de las personas y las nuevas obligaciones que deben asumir responsables y encargados. Todo tratamiento debe evaluarse en forma previa con respecto a las bases que lo sustentan, ya que no siempre el consentimiento servirá como base legitimadora, ni debe operar como una especie de "saneador" de tipos de tratamientos que no corresponde sean realizados por otras cuestiones que pueden ser reñidas con estándares éticos o de otra naturaleza.

4 *El Convenio fue posteriormente ampliado por un Protocolo Adicional de fecha 8 de noviembre de 2001 incluyendo disposiciones respecto a autoridades de control y flujos transfronterizos de datos. Ambos documentos fueron aprobados por la legislación nacional por Ley N° 19.030, de 27 de diciembre de 2012. Uruguay participó además del proceso de modernización del Convenio que culminó en el año 2018 y dio surgimiento al Protocolo de Modernización llamado Convenio 108+, siendo nuestro país el primer país no europeo en firmar dicho Protocolo.*

5 *Puede verse un listado de los países que han sancionado leyes en la materia a nivel global en el trabajo realizado por Greenleaf, Graham, "Global Tables of Data Privacy Laws and Bills (6th Ed January 2019) (February 9, 2019)". (2019) Suplemento de "157 Privacy Laws & Business International Report (PLBIR)", 16 págs. Disponible en SSRN: https://ssrn.com/abstract=3380794*

6 *El Considerando 6 de la Decisión indica expresamente que "Las normas jurídicas de protección de datos personales en la República Oriental del Uruguay se basan en gran medida en las normas establecidas en la Directiva 95/46/CE y figuran en la Ley No 18.331 de Protección de Datos Personales y de Acción de Habeas Data) de 11 de agosto de 2008. Esta Ley se refiere tanto a las personas físicas como a las jurídicas.".*

7 *El Considerando 74 de la Sentencia de la Corte Europea de Justicia de fecha 6 de octubre de 2015 en el Caso C-362/14 (más conocido como caso Schrems) indica que: "De la redacción misma del artículo 25, apartado 6, de la Directiva 95/46 resulta que es el ordenamiento jurídico del tercer país al que se refiere la decisión de la Comisión el que debe garantizar un nivel de protección adecuado. Aunque los medios de los que se sirva ese tercer país para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la Unión para garantizar el cumplimiento de las exigencias derivadas de esa Directiva entendida a la luz de la Carta, deben ser eficaces en la práctica para garantizar una protección sustancialmente equivalente a la garantizada en la Unión."*





Existen determinados tratamientos que están excluidos de la normativa por encontrarse fuera de su alcance objetivo (artículo 3º), o que poseen un régimen particular por la naturaleza de los datos (artículos 18 a 22, 25 a 27).

Los artículos 18 a 22 prevén condiciones especiales en el tratamiento de datos sensibles, salud, telecomunicaciones, publicidad y relativos a información comercial y crediticia. Por su parte, los artículos 25 y 27 establecen ciertas condiciones especiales de tratamiento de algunas bases mantenidas por entidades públicas.

No obstante, aún en los casos en que la ley excluye determinados tipos de tratamiento, existe un criterio definido y constante del Consejo Ejecutivo de la Unidad respecto a la aplicación -en lo pertinente- de los principios precitados.[8]

Los derechos de los titulares de los datos se detallan en el Capítulo III (artículos 13 a 17), consagrándose el derecho a la información frente a la recolección de datos, el derecho de acceso, el derecho de rectificación, actualización, inclusión o supresión, el derecho a la impugnación de valoraciones personales, y derechos referentes a la comunicación de datos.

La evolución del derecho a la protección de datos personales ha generado la formulación de nuevos derechos en el ámbito europeo, con mayor o menor reconocimiento en el resto de las legislaciones. En nuestro país, determinados derechos como el llamado "derecho al olvido" que no es reconocido directamente en la ley -como si ocurre en el RGPD-, sin perjuicio de lo cual el Consejo Ejecutivo ha reiterado que la protección de los titulares de los datos que pretende incorporar este derecho puede obtenerse a través del ejercicio de otros derechos consagrados en nuestra legislación.

Se distinguen en nuestro derecho como obligados principales en el cumplimiento de las normas a los responsables y encargados de tratamiento. Los primeros vinculados a su carácter de propietario de la base o decisor respecto de la finalidad, contenido y uso del tratamiento y los segundos como aquellos que traten datos personales por cuenta del responsable (artículo 4º de la Ley). Si bien la Ley establece una mayor responsabilidad por el cumplimiento de las normas, existen además obligaciones propias del encargado y la posibilidad de ser responsabilizado por cuenta propia, conforme lo indicado en el acápite del artículo 35.

Las obligaciones de los responsables y encargados se orientan al cumplimiento de los principios mencionados, al correcto aseguramiento del ejercicio de los derechos consagrados y al cumplimiento de determinados deberes formales, que se vieron sustancialmente modificados por la Ley Nº 19.670, de 15 de octubre de 2018. Nuestra Ley originalmente preveía en carácter de obligación formal, la inscripción de sus bases de datos por parte de entidades públicas y personas físicas y jurídicas privadas conforme lo establecido en los artículos 24 (para los primeros) y 28 (para los segundos). Este mecanismo, también consagrado en la Directiva Nº 95/46/CE y en otras legislaciones europeas que sirvieron de inspiración a la norma uruguaya, con el tiempo se observó como insuficiente para asegurar el cumplimiento con la normativa.

También se imponen por parte de la Ley determinadas condiciones para la contratación de servicios por cuenta de terceros (artículo 30), destinados a regular la utilización de la información y las condiciones para la conservación o destrucción de la información, una vez finalizada la relación contractual.

Corresponde señalar además la prohibición general para transferencias internacionales de datos, salvo que estas se realicen en el marco de alguna de las excepciones previstas en el artículo 23.

Uno de los aspectos más trascendentes vinculados a la Ley es la creación de la figura del órgano de un control, con plena autonomía técnica, denominada Unidad Reguladora y de Control de Datos Personales. La integración de su órgano de dirección (el Consejo Ejecutivo), en el que participan además del Director Ejecutivo de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (Agesic), dos miembros designados por el Poder Ejecutivo, procura asegurar la independencia, objetividad e imparcialidad de criterio en el desempeño del cargo. Este Consejo Ejecutivo es asesorado además por un Consejo Consultivo con representación del Poder Legislativo, el Poder Judicial, el Ministerio Público, la Academia y el sector privado.

Las atribuciones del Consejo Ejecutivo son amplias, y van desde la asistencia y asesoramiento a las personas, al control de la observancia del régimen legal, y cuenta además con importantes potestades que incluyen la exhibición de documentación, intervención e incautación de documentos, inspecciones, asesoramiento preceptivo e imposición de sanciones (artículos 34 y 35 de la Ley). Con

8 *Ya en el Dictamen Nº 17/012 de 16 de agosto de 2012 se entendía pertinente la aplicación de los principios generales de la protección de datos, aún en caso de bases no alcanzadas por la Ley Nº 18.331. También en los dictámenes Nº 29/013, de 24 de octubre de 2013 sobre bases de datos de seguridad pública y 6/015, de 25 de marzo de 2015, en todos los casos fundado en la necesaria tutela de un derecho fundamental.*

respecto a estas últimas, el rango sancionatorio va desde la observación hasta la clausura de la base de datos, incluyendo la posibilidad de imponer multas pecuniarias de hasta 500.000 unidades indexadas.

La Ley crea además en sus artículos 37 a 45 una acción judicial sumaria de "Habeas Data" a fin de que pueda plantear cuestiones vinculadas al ejercicio de sus derechos a nivel judicial.

Estas normas, desde la sanción de la Ley Nº 18.331 hasta el año 2018 proveyeron el régimen especial de la materia de protección de datos para todo el territorio nacional.

El RGPD y la modernización del Convenio Nº 108 surgieron como respuesta a una nueva realidad, asociada al uso masivo de los datos personales y sus implicancias en los derechos de las personas, y marcaron un nuevo estándar en la materia que rápidamente se extendió a nivel global.

A nivel latinoamericano, la Red Iberoamericana de Protección de Datos Personales[9] -que es presidida actualmente por nuestro país- se hizo eco de esta nueva realidad, elaborando un documento de consulta esencial para la elaboración de leyes o modificación de las existentes en la materia: los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.[10]

Estos antecedentes, y la necesidad de mantener un nivel adecuado de protección para las personas, hicieron que la Unidad Reguladora y de Control de Datos Personales promoviera una actualización de la normativa, la que finalmente se consagró en los artículos 37 a 40 de la Ley Nº 19.670.

## LAS NUEVAS DISPOSICIONES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

La Ley Nº 19.670 establece cuatro nuevas disposiciones que modernizan la normativa uruguaya, generan nuevas obligaciones para responsables y encargados e incrementa las potestades de la autoridad de control en la materia.

## LA AMPLIACIÓN DEL AMBITO TERRITORIAL

El artículo 37 de la Ley citada eleva a rango legal la determinación del ámbito territorial aplicable, que había sido objeto de reglamentación en el decreto reglamentario Nº 414/009, de 31 de agosto de 2009 (artículo 3º). Pero además, extiende el alcance de las normas uruguayas y por ende de las competencias de la autoridad de control.

*"Artículo 37 – El tratamiento de datos personales estará sometido a la Ley N° 18.331, de 11 de agosto de 2008 y sus modificativas y concordantes, cuando se efectúe por un responsable o encargado de tratamiento establecido en territorio uruguayo, lugar donde ejerce su actividad.*

*En caso de que no esté establecido en ese territorio, dicha ley regirá:*

A. *Si las actividades del tratamiento están relacionadas con la oferta de bienes o servicios dirigidos a habitantes de la República o con el análisis de su comportamiento.*

B. *Si lo disponen normas de derecho internacional público o un contrato.*

C. *Si en el tratamiento se utilizan medios situados en el país.*

*Exceptúanse los casos en que los medios se utilicen exclusivamente con fines de tránsito, siempre que el responsable del tratamiento designe un representante, con domicilio en territorio nacional, ante la Unidad Reguladora y de Control de Datos Personales, a fin de cumplir con las obligaciones previstas por la Ley N° 18.331, de 11 de agosto de 2008".*

La Ley no sólo reconoce la vigencia y aplicación de la Ley uruguaya en casos de responsables y encargados situados en territorio nacional, sino que además incluye actividades de tratamiento relacionadas con oferta de bienes o servicios dirigidos a habitantes de la República o con el análisis de su comportamiento, aún cuando estos responsables o encargados estén fuera de nuestro territorio.

Corresponde puntualizar que la norma procura proteger a todos los habitantes de nuestro país, sin entrar en consideraciones con respecto a su nacionalidad. En lo que respecta a la hipótesis en que así lo disponen normas de derecho internacional público (Convenios o Tratados) o un contrato, evidentemente en este último caso la ley no permite la exclusión de la normativa uruguaya por acuerdo entre particulares, sino la posibilidad de que estos hagan aplicable la Ley, aún cuando esta no lo sea.

La hipótesis prevista en el literal C) ya se encontraba regulada en el Decreto Nº 414/009, por lo que no se ha innovado al respecto.

## LAS VULNERACIONES DE SEGURIDAD

El artículo 38 impone a responsables y encargados la notificación de vulneraciones de seguridad en forma inmediata a los titulares de los datos y al órgano de control. También prevé una actuación conjunta de este último con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (Cert-uy).

*"Artículo 38 - Cuando el responsable o encargado de una base de datos o de tratamiento, tome conocimiento de la ocurrencia de la vulneración de seguridad, deberá informar inmediata y pormenorizadamente de ello y de las medidas que adopte, a los titulares de los datos y a la Unidad Reguladora y de Control de Datos Personales, la que coordinará el curso de acción que corresponda, con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay (CERTuy).*

*La reglamentación determinará el contenido de la información correspondiente a la vulneración de seguridad".*

La disposición normativa, en línea con las tendencias internacionales en la materia, impone una obligación tanto a responsables como encargados, de realizar un informe inmediato o pormenorizado de vulneraciones de seguridad y medidas adoptadas, a titulares y a la URCDP.

Corresponde señalar que esta notificación se enmarca dentro del denominado principio de seguridad de los datos, previsto en el artículo 10 de la Ley Nº 18.331, que impone a los responsables la adopción de medidas necesarias para garantizar la seguridad y confidencialidad de los datos personales.

A nivel reglamentario, además, el nuevo artículo se distancia de la reglamentación contenida en el artículo 8º del Decreto Nº 414/009, de 31 de agosto de 2009, en algunas cuestiones sustanciales:

a. La información debe tener las notas de pormenorizada, con inclusión de las medidas que se adopten.

b. La información debe proveerse en forma inmediata.

c. La notificación ya no es solo a los "interesados" sino a los titulares de los datos y a la URCDP.

d. No se requiere que la vulneración de seguridad provoque una afectación "significativa de los derechos de los interesados".

## ALCANCE DEL PRINCIPIO DE RESPONSABLIDAD

El artículo 12 de la Ley Nº 18.331 establecía el denominado principio de responsabilidad, limitándose a explicitar que el responsable de la base de datos será responsable de las violaciones de la ley.

Esta formulación se visualizó como insuficiente, como ya se mencionó, a la luz de la evolución en las estrategias y medios para el tratamiento de los datos. Resultaba necesario virar hacia un régimen que impusiera un conjunto mayor de obligaciones en cabeza no sólo de responsables sino además de encargados, de modo de asegurar que todo tratamiento de datos incluyera, desde su concepción, los principios y normas en la materia.

*"Artículo 12 - (Principio de responsabilidad). El responsable de la base de datos o tratamiento y el encargado, en su caso, serán responsables de la violación de las disposiciones de la presente ley.*

*En ejercicio de una responsabilidad proactiva, deberán adoptar las medidas técnicas y organizativas apropiadas: privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, entre otras, a fin de garantizar un tratamiento adecuado de los datos personales y demostrar su efectiva implementación.*

*La reglamentación determinará las medidas que correspondan según los tipos de datos, tratamientos y responsables, así como la oportunidad para su revisión y actualización."*

Se hace una explícita referencia a la responsabilidad proactiva, dentro de la que se incluyen la privacidad por diseño, privacidad por defecto, evaluación de impacto, entre otras, con el objetivo de garantizar un tratamiento adecuado de los datos personales, y demostrar su efectiva implementación.

Estas medidas deberán documentarse a efectos de demostrar, cuando sea requerido por la URCDP, el cumplimiento efectivo de las normas en la materia. Obligación que no corresponde sólo a los responsables, sino además, en determinados casos, a los encargados.

9 *La Red Iberoamericana de Protección de Datos Personales fue creada en el año 2003 y se constituye en un foro de distintos actores del sector público y privado con el fin de promover el derecho a la protección de datos personales en Iberoamérica. Puede accederse a más información en: http://www.redipd.org/index-ides-idphp.php*

10 *El texto completo de los Estándares está disponible en: http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf*

## EL DELEGADO DE PROTECCIÓN DE DATOS

En función de la naturaleza de determinados tipos de tratamientos o de datos que pueden generar una situación de mayor vulnerabilidad de las personas, puede ser necesaria la adopción de medidas adicionales que aseguren un tratamiento adecuado. En estas situaciones, se impone la existencia de una figura que dentro de la organización asesore, proponga medidas, controle su cumplimiento y sea un nexo directo con la autoridad de control.

La Ley Nº 19.670 crea así la figura del Delegado de Protección de Datos, con las funciones antedichas.

*"Artículo 40 - Las entidades públicas, estatales o no estatales, las privadas total o parcialmente de propiedad estatal, así como las entidades privadas que traten datos sensibles como negocio principal y las que realicen el tratamiento de grandes volúmenes de datos deberán designar un delegado de protección de datos.*

*Sus funciones principales serán:*

A. *Asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales.*

B. *Supervisar el cumplimiento de la normativa sobre dicha protección en su entidad.*

C. *Proponer todas las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales en materia de protección de datos personales.*

D. *Actuar como nexo entre su entidad y la Unidad Reguladora y de Control de Datos Personales.*

*El delegado deberá poseer las condiciones necesarias para el correcto desempeño de sus funciones y actuará con autonomía técnica".*

El volumen de los datos tratados y su naturaleza de datos sensibles hacen necesario contar con esta figura, que deberá contar con condiciones personales y una posición institucional que le permita el correcto desarrollo de las funciones principales referidas en la Ley.

Si bien resta determinar algunos aspectos vinculados a las condiciones, funciones y atribuciones de los delegados de protección de datos por la vía reglamentaria, la obligación de su designación se encuentra vigente desde el 1º de enero de 2019.

## A MODO DE COROLARIO

Cabe señalar que si bien la normativa uruguaya ya otorgaba un alto nivel de protección a las personas en la materia, los cambios producidos en la última década hacía necesaria una actualización que brindara mayores garantías y otorgara nuevas herramientas de control a la URCDP.

La reglamentación complementará algunas de estas disposiciones en lo relativo a su alcance e instrumentos para asegurar el derecho a la protección de datos personales en el actual entorno de la sociedad de la información y del conocimiento.

# EN TRE VIS TA

## Consejo Ejecutivo **URCDP**

*El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales es el órgano encargado de la dirección técnica y administrativa de la Unidad, creado por la Ley N° 18.331, de 11 de agosto de 2008. Cuenta con la misma integración desde su constitución formal en el año 2009. Son miembros del Consejo el Dr. Felipe Rotondo, el Mag. Federico Monteverde y el Director Ejecutivo de la Agesic Ing. José Clastornik. Lo integra además en carácter de miembro alterno de este último, la Ing. Virginia Pardo.*

### AGESIC fue uno de los impulsores de la ley de protección de datos personales en el año 2008. ¿Qué motivó dicho impulso?

**JC:** Ya desde la concepción de la estrategia de Gobierno Digital sabíamos que la sustentabilidad del modelo que estábamos diseñando dependía de una estructura sólida, basada en el reconocimiento de determinados derechos fundamentales, entre los que se encuentra la protección de datos personales. Este reconocimiento debía, además, estar acompañado de un marco de principios y obligaciones que permitieran una puesta en práctica efectiva, y de una autoridad con autonomía técnica y potestades de control y asesoramiento.

Estos objetivos cumplían además con las líneas estratégicas marcadas por la primera Agenda Digital Uruguay 2008-2010, especialmente las vinculadas al fortalecimiento democrático y la transformación del Estado. En ese marco, se promovió la sanción de la Ley N° 18.331, de 11 de agosto de 2008, y la constitución de la Unidad Reguladora y de Control de Datos Personales.

El reconocimiento de este derecho tuvo otros impactos. Un claro ejemplo es el reconocimiento de nuestro país como "adecuado" a los altos estándares europeos en protección de datos por parte de la Comisión Europea, lo que permite el libre flujo de datos y se convierte en un impulso para la actividad comercial entre Uruguay y todos los países de la Unión Europea.

### ¿Haciendo un análisis retrospectivo de las normas, cree que nuestro país se encuentra preparado en materia de protección de datos personales para los nuevos desafíos que presenta el Gobierno Digital y la Sociedad de la Información?

**JC:** Como ya mencionaba, la política uruguaya en la materia de protección de datos personales forma parte de una estrategia integral para el Gobierno Digital, que incluye la promoción de otros derechos fundamentales como el derecho de Acceso a la Información Pública y una estructura de ciberseguridad, firma y documento electrónico, e intercambio de información entre entidades públicas.

En ese sentido, entiendo que creamos un marco normativo sólido y adaptado a los hechos y circunstancias del momento, lo que no exime de necesarias evoluciones que acompasen los cambios a nivel global. En los últimos años el contexto internacional ha variado sustancialmente, lo que ha hecho necesario replantearnos algunos aspectos de la normativa nacional en protección de datos personales, y motivó el impulso de algunos cambios que se plasmaron en cuatro artículos de la Ley N° 19.670, de 15 de octubre de 2018. Estos refieren al ámbito territorial, la notificación de vulneraciones de seguridad, el delegado de protección de datos y la responsabilidad proactiva.

El hecho de que nuestro régimen haya requerido de pocas adaptaciones para adecuarse a la nueva realidad en la materia muestra que nos encontrábamos en el camino correcto, y esperamos que con ellas podamos seguir avanzando en nuestra estrategia de Gobierno Digital con la misma solidez con la que la iniciamos.

### Se ha hecho referencia en forma reiterada a los datos como un motor de la economía. ¿Cuál es su opinión al respecto?

**FM:** Una década atrás, el ranking de las diez mayores compañías globales estaba dominado por empresas dedicadas al rubro "petróleo y gas" y en la actualidad lo está por empresas de tecnología que tienen como principal foco de su negocio el tratamiento de datos personales. Siete de las diez mayores empresas globales son empresas tecnológicas y los primeros cinco lugares también lo son. Esto ratifica que la frase "los datos son el petróleo del siglo XXI" no es una ingeniosa metáfora, sino una realidad incontestable. Que los datos son un motor de la economía cae de maduro de esta realidad.

### El uso de inteligencia artificial ha sido uno de los temas recurrentes en materia de protección de datos en los últimos años, sobre todo a nivel comercial. ¿Cómo proteger los derechos de las personas ante algoritmos complejos que en ocasiones pueden no ser fácilmente explicados a los afectados?

**FM:** El acento no debe ponerse en los algoritmos, porque sean estos complejos o sencillos, el elemento clave son los datos, siempre han sido los datos. Lo que ha cambiado es la enorme disponibilidad de datos y los avances tecnológicos que permiten que ingentes volúmenes de datos sean almacenados, procesados y comunicados. Ante ello han de primar los principios relativos a la protección de datos personales, como la finalidad, el consentimiento y la responsabilidad.

Toda línea de acción que tienda a que los sistemas sean diseñados e implementados teniendo en cuenta aspectos vinculados a la protección de los datos personales es importante Y lo mismo sucede con la sujeción a principios éticos. Pero en última instancia, la protección efectiva está en la responsabilidad que recae en quien lleva a cabo el tratamiento, conforme a lo dispuesto en la Ley.

### ¿Qué acciones ha adoptado la Unidad para fomentar el conocimiento del derecho a la protección de datos personales?

**VP:** Desde la puesta en funcionamiento de nuestra unidad hemos encaminado dos grandes líneas de trabajo, por un lado de forma general venimos realizando de forma ininterrumpida un conjunto de acciones con el objetivo de posicionar el conocimiento de este derecho en toda la población en general, mediante charlas informativas, generación de consejos y guías prácticas, servicios e información accesible desde la web, así como una estrategia de comunicación general, con el objetivo de informar las generalidades de la ley, los principios fundamentales, así como el rol del órgano de control como los procedimientos para el adecuado ejercicio del derecho.

Todas estas acciones, sumado a la natural incorporación del concepto de privacidad dado por la propia expansión y uso de las nuevas tecnologías por las personas, ha permitido un gran crecimiento del conocimiento del derecho por la población de nuestro país, dando un salto significativo en los últimos años pasando de un 36% al actual 54% de personas mayores de 18 años.

Nuestra segunda línea de acción, y podría afirmar nuestro principal desafío, es lograr incidir en el comportamiento responsable y crítico de las personas en relación al uso de sus datos personales por parte de terceros, especialmente en las poblaciones más vulnerables. Esto nos obliga a trabajar en acciones de sensiblización y formación directa, como ser talleres vivenciales, desarrollo de contenidos educativos y programas de formación permanente, dirigidos tanto a niñas, niños y adolescentes, como a los propios educadores y familias.

### ¿Cómo compatibilizar las normas en materia de protección de datos personales con iniciativas como la de datos abiertos en el Estado?

**VP:** Iniciativas de datos abiertos implican la publicación en formatos abiertos y reutilizables datos públicos en poder de los organismos públicos con la principal finalidad de ser utilizados libremente por los diferentes usuarios en función de sus necesidades y demanda especifica (ej: investigación periodística, desarrollo de nuevas soluciones y servicios, control y auditoria ciudadana, entre otros).

Si bien es necesario disponer de las capacidades e infraestructura técnicas para la apertura y publicación en datos abiertos, sería imposible promover una estrategia nacional consistente y sólida sin contar con los marcos normativos adecuados que den las garantías y la confianza en los procesos de publicación por parte de los organismos, así como la libre utilización por parte de los usuarios en general.

Son pilares fundamentales la Ley 18.381 de Acceso a la Información Pública donde se establece el alcance de la información pública, generando así el marco habilitante para identificar qué información puede ser publicada en formatos abiertos, y en particular la Ley 18.331 de protección de datos personales que delimita claramente el alcance de la información de carácter confidencial, la cual deben aplicarse técnicas de anonimización o disociación, garantizando la no reidentificación al titular del dato personal.

### ¿Cómo mantener vigente la defensa del derecho a la protección de datos consagrado en las normas ante el surgimiento de situaciones complejas y nuevas que no están previstas específicamente en ellas?

**FR:** Las tecnologías producen incesantes cambios, con nuevas oportunidades y a la vez riesgos, también en materia de datos personales.

La defensa del derecho, propio de la dignidad personal, requiere que seamos conscientes de los valores en juego, de los poderes de disposición y control que aquel implica y que contribuyamos, como ciudadanos y como Unidad, a crear una cultura de protección de datos personales.

Suele decirse que entre el derecho y la tecnología existe un cortocircuito, que las normas jurídicas

no logran atender las situaciones nuevas y complejas a que refiere la pregunta. Entiendo que, en todo caso y como sucede en general en las diversas áreas jurídicas, resultan claves los principios, en protección de datos personales los de responsabilidad proactiva, finalidad, veracidad, seguridad, etc.

Ellos son reglas jurídicas directamente aplicables, explicitan los valores esenciales y permiten atender, con su aplicación interrelacionada y adaptación a la realidad en continuo movimiento, las situaciones no previstas.

## ¿Es posible una convergencia internacional en materia de protección de datos? ¿En base a qué fundamentos?

**FR:** Los principios antes citados se han generalizado en la legislación comparada y son base para configurar regímenes adecuados, que sean equivalentes y permitan una convergencia que facilite el intercambio sin necesidad de autorizaciones u otros requisitos. Ello contribuye al desarrollo de los mercados en el ámbito internacional, para lo cual es relevante el flujo transfronterizo de datos personales.

Claro que es bueno tener textos normativos que los desarrollen. En ese sentido es destacable el Convenio Nº 108 del Consejo de Europa como instrumento internacional abierto a los Estados no Miembros de esa organización, caso precisamente de Uruguay. La relevancia de ese Convenio es mayor con su reciente modernización. Asimismo, interesan los Estándares de Protección de Datos aprobados por la Red Iberoamericana de Protección de Datos en el año 2017; ellos son un aporte para la adopción o ajuste de las legislaciones nacionales y un instrumento más para generar una convergencia a que alude la pregunta, a nivel global. Sus principios, derechos y obligaciones están en línea con los promovidos por instrumentos internacionales como el Convenio 108+ y regionales como el Reglamento Europeo aplicable desde el 2018. En ese camino se encuentran los ajustes que rigen desde este año a varias disposiciones de nuestra ley de protección de datos personales y hábeas data, N.º 18.331 de 11-VIII-2008.

# REVISTA PDP

*Revista Uruguaya de Protección de Datos Personales*

# REVISTA PDP

*Revista Uruguaya de Protección de Datos Personales*

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

agesic
DESARROLLANDO EL URUGUAY DIGITAL

PRESIDENCIA
República Oriental del Uruguay