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 comunicación "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 riesgos 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 posterior*i (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.----------