

Estrasburgo, 19 de junio de 2025 T-PD(2021)7rev13

COMITÉ CONSULTIVO DEL CONVENIO PARA LA PROTECCION DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL

Convenio núm. 108

Directrices sobre los principios generales del artículo 11 del Convenio núm. 108 modernizado

www.coe.int/dataprotection

1. Introducción

El Convenio Europeo de Derechos Humanos (CEDH), que entró en vigor el 3 de septiembre de 1953, dispone que: "*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*", y establece las condiciones para restringir esos derechos, en particular en el artículo 8.2, cuando prevé que: "*No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás*." Estas condiciones basadas en principios fueron confirmadas principalmente por el Tribunal Europeo de Derechos Humanos (TEDH), a través de su abundante jurisprudencia sobre el artículo 8, y por otros órganos e instituciones del Consejo de Europa, tales como la Comisión de Venecia. Estos confirmaron el derecho a la privacidad en las jurisdicciones interesadas, como un derecho humano individual y universal que es alienable e imprescriptible. Estos avances también pueden observarse a través de la jurisprudencia de la Corte Interamericana de Derechos Humanos[1].

En lo que respecta al Consejo de Europa, el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE núm. 108, "Convenio núm. 108"), quedó abierto a la firma el 28 de enero de 1981 en Estrasburgo. El objetivo de este Convenio fue fortalecer la protección de datos, es decir, la protección jurídica de las personas con respecto al tratamiento automatizado de la información personal sobre ellas.[2]

Cuando se trata de excepciones, el artículo 9 del Convenio núm. 108 ya contenía disposiciones específicas para la aplicación legal de excepciones en virtud del Convenio, en consonancia con el artículo 8.2 del CEDH y la evolución de la jurisprudencia.[3]

En 2011 comenzó un avance importante en este ámbito, a saber, el proceso de modernización del Convenio núm. 108, que ha tenido al menos tres objetivos: a) garantizar la dignidad humana de las personas en la era digital, asegurando una protección adecuada de su privacidad, y otros derechos humanos, en particular a través de la protección de sus datos personales; b) facilitar el flujo transfronterizo de datos personales, y c) establecer un régimen común para la aplicación de excepciones a los principios y normas de protección de datos para sus Partes. De este modo, el Protocolo CSTE núm. 223 de enmienda al Convenio núm. 108 (al que se hace referencia en el presente documento como "el

[1] Caso de Tristán Donoso contra Panamá, caso de Nadega Dorzema et al. contra la República Dominicana, y caso de García Rodríguez et al. contra México.

[2] El Informe explicativo especifica que en aquel momento hubo un amplio consenso acerca de que se necesitaban dichas normas jurídicas, habida cuenta de la creciente utilización de ordenadores con fines administrativos con una capacidad de almacenamiento muy superior y posibilidades para realizar transacciones mucho más diversas, que pueden llevar a cabo a gran velocidad. Por otra parte, se acordó en la década de 1970 que "el poder de información" debería conllevar una responsabilidad social correspondiente de los usuarios de los datos en el sector público y privado. También se consideró esencial que las personas responsables de estos ficheros se aseguraran de que las ventajas innegables que pueden obtener del tratamiento automatizado de datos no conduzcan al mismo tiempo al debilitamiento de la posición de las personas sobre las que se almacenan datos.

[3] Indicó que: "*Las excepciones a los principios básicos para la protección de datos se limitan a aquellas que son necesarias para la protección de los valores fundamentales en una sociedad democrática. El texto del segundo párrafo del artículo 9 se ha inspirado en el del segundo párrafo de los artículos 6, 8, 10 y 11 del Convenio Europeo de Derechos Humanos*."

Convenio" o "el Convenio núm. 108+") en forma de derecho internacional público pretendía proporcionar una base jurídica para los requisitos básicos del artículo 8.2 del CEDH de una manera más moderna y concreta, involucrando así indirectamente la jurisprudencia cambiante sobre dicha disposición.

Históricamente, durante el proceso de evolución de la jurisprudencia del TEDH, surgió otro aspecto importante: los Estados no solo tienen la obligación negativa de no interferir en los derechos humanos y las libertades fundamentales, sino también la obligación positiva de garantizarlos y de velar por que puedan ejercerse plenamente,[4] lo que, una vez más, es un elemento importante que debe considerarse al transponer los principios generales sobre la aplicación de excepciones.

Las Partes que ya han ratificado el Protocolo CSTE núm. 223 o que están en pleno proceso de ratificación tal vez se hayan enfrentado a dificultades al incorporar esos elementos a su marco jurídico nacional, lo que muy a menudo también ha conllevado enmiendas a otros instrumentos legislativos en otros ámbitos. Consciente de estas dificultades a nivel nacional y deseoso de ofrecer una interpretación armonizada que pudiera contribuir asimismo a una rápida entrada en vigor y a más adhesiones al Convenio núm. 108+, pero también de sentar unas bases sólidas para proporcionar orientación más específica, el Comité del Convenio núm. 108, de conformidad con el artículo 19 del Convenio núm. 108 y en consonancia con el artículo 23 del Convenio núm. 108+, decidió formular directrices sobre la posible transposición y aplicación de los principios generales establecidos en el artículo 11.1, teniendo en cuenta las mejores prácticas ya existentes de las Partes[5].

2. Finalidad y ámbito de aplicación de las Directrices

- Finalidad del documento

Las presentes Directrices son de carácter interpretativo y no crean nuevos derechos u obligaciones. Tienen por objeto facilitar y apoyar la ratificación del Protocolo CSTE núm. 223 de enmienda al Convenio núm. 108+, tal como prevé el artículo 37 del Protocolo de enmienda. Las Directrices también pueden ayudar a las futuras Partes a interpretar los principios generales establecidos en el artículo 11.1 e incorporarlos oportunamente a la legislación nacional durante un proceso de adhesión al Convenio núm. 108+, tal como se establece en el artículo 33. Además, podrían proporcionar un modelo para cualquier futura orientación que requieran otras disposiciones de este Convenio.

Estas Directrices ofrecen una explicación general de los principios y normas contenidos en el artículo 11.1 del Convenio núm. 108+, cuando es posible, proporcionando ejemplos de una manera abstracta a fin de contribuir a una interpretación y aplicación más armonizadas de las disposiciones del Convenio núm. 108+. De este modo, pretenden facilitar la aplicación de este Convenio y aumentar la confianza entre las Partes.

---

[4] KU contra Finlandia; Soderman contra Suecia; A y B contra Croacia; X y otros contra Bulgaria; Silva Monteiro Martins Ribeiro contra Portugal, etc.

[5] Las Directrices se apoyan en principios que reflejan la jurisprudencia a nivel internacional, regional y nacional, en particular del Tribunal Europeo de Derechos Humanos, la Corte Interamericana de Derechos Humanos, y la Corte Africana de Derechos Humanos y de los Pueblos.

- Ámbito de aplicación

La versión actual del Convenio núm. 108 prevé, mediante declaración unilateral dirigida al Secretario General del Consejo de Europa, la posibilidad de excluir categorías específicas de ficheros o actividades de tratamiento de datos de su ámbito de aplicación. El artículo 3 del Convenio núm. 108+ introdujo un cambio importante en este ámbito. Tras la entrada en vigor del Convenio núm. 108+, ya no podrá contemplarse la posibilidad de eliminar ámbitos o sectores específicos (tales como la seguridad nacional, la defensa, la aplicación de la ley, etc.) de la aplicación de los principios y normas de protección de datos mediante declaración unilateral de las Partes. En su lugar, será posible establecer restricciones limitadas a las disposiciones del Convenio núm. 108+.

Por consiguiente, el ámbito de aplicación de estas Directrices se atiene al amplio ámbito de aplicación del Convenio núm. 108+, que se aplica al tratamiento de datos personales en el sector tanto público como privado. Las Partes no pueden prever unilateralmente excepciones a su ámbito de aplicación; las condiciones para la aplicación de excepciones se regulan en el artículo 11.

También hay otros cambios importantes: el artículo 11.1 del Convenio núm. 108+, si bien sigue la lógica y la estructura del artículo 9 del Convenio núm. 108, contiene más condiciones para la legitimidad de la aplicación de excepciones específicas. Al mismo tiempo, prevé otros objetivos esenciales muy diversos de interés público general relacionados con las excepciones con respecto al fin legítimo del tratamiento de datos. Cabe señalar que contiene asimismo un régimen muy específico que prevé excepciones más amplias en el caso del tratamiento de datos con fines de seguridad nacional y de defensa. Sin embargo, cuando eso se aplica, una nueva disposición del artículo 11.3 exige que las Partes garanticen "*una supervisión y un control independientes y efectivos de conformidad con la legislación nacional*".

La lista de condiciones está complementada por el criterio "*respeta la esencia de los derechos y libertades fundamentales*", que es aplicable a todo el tratamiento que está sujeto a una excepción. Sus modalidades se explican con más detalle en el presente documento.

Como conclusión, el artículo 11 establece, en comparación con los artículos 3 y 9 del Convenio núm. 108, condiciones concretas para que el legislador las incorpore al marco jurídico nacional, lo que solo permitiría a los responsables del tratamiento de datos aplicar excepciones a una disposición determinada del Convenio para una lista de fines legítimos.

Cabe señalar que toda posible excepción prevista en el artículo 11 debería estar vinculada con un tratamiento de datos específico y cumplir los requisitos establecidos en el artículo 11.1. Esto significa que deben sopesarse y justificarse los intereses en juego entre la necesidad de prever excepciones a ciertas disposiciones del Convenio y el respeto de los derechos humanos y las libertades fundamentales de las personas, para lo cual estas Directrices pretenden prestar apoyo y proporcionar una metodología sencilla.

En relación con esto, debería observarse en primer lugar que el artículo 1 del Convenio núm. 108+ indica que debe brindarse protección a las personas durante el proceso de tratamiento de sus datos personales, independientemente de su nacionalidad y de dónde tengan su residencia, lo que puede repercutir en cierta medida en la transposición de estas

disposiciones. La lógica subyacente es que la protección de la vida privada es un derecho humano universal reconocido en el artículo 8 del CEDH y otros instrumentos internacionales de derechos humanos,[6] así como en las constituciones de la mayoría de las Partes en el Convenio. Por consiguiente, las Directrices se concentrarán en los principios generales de la protección de datos, pero, cuando proceda, sensibilizarán a las Partes acerca del impacto del tratamiento de datos personales en el derecho a la privacidad y en otros derechos humanos y libertades fundamentales.

Las definiciones contenidas en el artículo 2 del Convenio núm. 108+ revisten particular importancia para el ámbito de aplicación de las presentes Directrices, y debería hacerse referencia a ellas.

3. Estructura del artículo 11

El artículo 11 establece los límites para cualquier posible excepción a determinadas disposiciones del Convenio. En el marco de aplicación del Convenio, otras disposiciones siguen siendo aplicables en el caso de que se aplique una de las excepciones previstas en el artículo 11.

El artículo 11 establece tres regímenes de excepciones, dependiendo de la finalidad del tratamiento de datos, que están sujetos a algunas condiciones objetivas y que contienen, respectivamente, una lista de disposiciones del Convenio que pueden verse afectadas por excepciones y restricciones.

- Los tres regímenes de excepciones

Los regímenes que figuran a continuación se describen sobre la base de la medida en que permiten excepciones a las disposiciones del Convenio para las tres principales categorías de fines legítimos: interés público general, archivo, investigaciones y estadísticas, y seguridad nacional y defensa:

1) Excepciones en lo que respecta al interés público general:
    a. Fines legítimos para los que pueden aplicarse:
        i. La protección de la seguridad nacional, la defensa, la seguridad pública, intereses económicos y financieros importantes del Estado, la imparcialidad y la independencia del poder judicial, o la prevención, la investigación y el enjuiciamiento de infracciones penales y la ejecución de sanciones penales, y otros objetivos esenciales de interés público general;
        ii. La protección de la persona concernida, o de los derechos y libertades fundamentales de terceros, en particular la libertad de expresión.

[6] Tales como el artículo 12 de la Declaración Universal de Derechos Humanos, el artículo 7 del Pacto Internacional de Derechos Civiles y Políticos, el artículo 11.2 de la Convención Americana de Derechos Humanos, el artículo 4 de la Carta Africana sobre los Derechos Humanos y de los Pueblos, y los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea.

b. Condiciones generales para la aplicación de una excepción:
    i. Prevista por la ley;
    ii. Respeta la esencia de los derechos y libertades fundamentales;
    iii. Constituye una medida necesaria y proporcionada en una sociedad democrática.

c. Disposiciones que pueden estar sujetas a una restricción o excepción:
    i. Principios generales como la justicia, la transparencia, la limitación de la finalidad, y los requisitos sobre la calidad de los datos: adecuados, pertinentes y no excesivos, precisos, actualizados, que permitan la identificación solamente durante el tiempo necesario (artículo 5, párrafo 4);
    ii. Notificación de la violación de datos a la autoridad de control (artículo 7, párrafo 2);
    iii. Obligación de los responsables del tratamiento de datos de informar a la persona concernida (artículo 8, párrafo 1);
    iv. Derechos de la persona concernida (artículo 9).

2) Excepciones en lo que respecta al archivo, las investigaciones y las estadísticas:
    a. Fines legítimos para los que pueden aplicarse:
        i. Fines de archivo en interés público;
        ii. Fines de investigación científica o histórica;
        iii. Fines estadísticos.
    b. Condiciones generales para la aplicación de una excepción:
        i. Prevista por la ley;
        ii. Cuando no exista un riesgo reconocible de vulneración de los derechos y libertades fundamentales de las personas concernidas.
    c. Disposiciones que pueden estar sujetas a una restricción o excepción:
        i. Obligación del responsable del tratamiento de datos de informar a la persona concernida (artículo 8);
        ii. Derechos de la persona concernida (artículo 9).

3) Excepciones adicionales en lo que respecta a la seguridad nacional y la defensa:
    a. Fines legítimos para los que pueden aplicarse:
        i. Seguridad nacional;
        ii. Defensa.
    b. Condiciones adicionales para la aplicación de una excepción:
        i. Prevista por la ley;
        ii. En la medida en que constituye una medida necesaria y proporcionada en una sociedad democrática para lograr el objetivo.
    c. Disposiciones que pueden estar sujetas a una restricción o excepción:
        i. Competencia del Comité Convencional para evaluar la eficacia de las medidas adoptadas a fin de aplicar las disposiciones del Convenio (artículo 4, párrafo 3);
        ii. Para proporcionar información a la autoridad de control sobre la transferencia internacional de datos (artículo 14, párrafo 5);
        iii. Para que la autoridad de control exija que se demuestren las condiciones legítimas para la transferencia internacional de datos y su capacidad para intervenir (artículo 14, párrafo 6);
        iv. Poder de la autoridad de control para investigar e intervenir, funciones relativas a la transferencia internacional de datos, poder

para tomar decisiones regulatorias e imponer sanciones, y para recurrir al poder judicial (artículo 15, párrafo 2, apartados a, b, c y d).

Las siguientes disposiciones son aplicables en cualquier régimen de excepciones:

- Artículo 4 (párrafos 1 y 2): Las Partes tomarán las medidas necesarias en su legislación para aplicar las disposiciones de este Convenio y garantizar su aplicación efectiva.

- Artículo 5 (párrafos 1 a 3): No es aplicable ninguna excepción en lo que respecta a la proporcionalidad, la legitimidad del tratamiento de datos, y la legitimidad de la finalidad de los principios del tratamiento de datos. Esto significa que debe garantizarse la proporcionalidad del tratamiento de datos, así como los requisitos para el tratamiento de datos personales, sobre una base jurídica válida y con un fin legítimo.

- Artículo 6 (párrafo 1): Algunas categorías particulares de datos gozan de protección especial, lo cual requiere garantías que complementen las ya establecidas para las actividades de tratamiento de datos. Dichas garantías deben prevenir los riesgos de menoscabo de los intereses, los derechos y las libertades fundamentales de las personas concernidas, en particular el riesgo de discriminación.

- Artículo 7 (párrafo 1): Seguridad de los datos: La obligación de tomar medidas para garantizar la seguridad de los datos se aplica sin excepción.

- Artículo 10: Deben preverse medidas de rendición de cuentas: En el marco jurídico nacional aún debe garantizarse la obligación de los responsables del tratamiento de datos de demostrar que se han adoptado medidas adecuadas para cumplir las disposiciones del Convenio, de examinar el posible impacto del tratamiento de datos previsto y de adoptar el enfoque de “privacidad desde el diseño”, así como otras medidas recomendadas para mitigar el/los riesgo(s) de injerencia ilícita;

- Artículo 12: No se contemplarán excepciones en lo que respecta a la aplicabilidad de las sanciones judiciales y no judiciales, ni a los recursos, por la violación de las disposiciones del Convenio;

- Artículo 13: Una Parte puede brindar una protección más amplia a la persona concernida;

- Artículo 14 (párrafos 1 a 4): Se aplican las normas sobre la transferencia fronteriza de datos;

- Artículo 15 (párrafo 2, apartado e) a párrafo 10): la autoridad de control i) realiza actividades de sensibilización, ii) es consultada sobre las medidas legislativas o administrativas, ii) tramita las solicitudes y las quejas presentadas por la persona concernida, y la mantiene informada, iv) actúa con total independencia e imparcialidad, v) dispone de suficientes recursos, vi) prepara un informe anual, vii) tiene obligaciones de confidencialidad con los miembros del personal, viii) sus decisiones pueden ser objeto de un recurso, examinado por un tribunal, ix) el poder judicial no realizará un examen.

4. Principios generales del artículo 11

4.1. Prevista por la ley

El criterio "prevista por la ley" significa que la excepción de que se trate debe estar consagrada en la ley en el sentido más amplio.[7] Cuando las presentes Directrices se refieren a una ley, esta no debe ser necesariamente una ley adoptada por un parlamento, sin perjuicio de los requisitos conformes al orden constitucional de las Partes concernidas. En consonancia con el ordenamiento jurídico interno de la Parte, la ley se entiende de una manera general y puede significar varias leyes o disposiciones legales, ya sean de la legislación escrita o de la jurisprudencia, incluidas, pero no exclusivamente, todas las leyes escritas de las autoridades legislativas (leyes en el sentido formal), así como todas las medidas regulatorias (decretos, reglamentos, órdenes y directivas administrativas) basadas en dicha ley, a condición de que estén en vigor y sean plenamente aplicables, y respeten el principio del Estado de derecho. El párrafo 91 del Informe explicativo del Convenio núm. 108+ ("Informe explicativo") especifica asimismo que: *"dicha medida debe estar prescrita por una ley accesible y previsible, que debe ser suficientemente detallada".*

Esto puede significar, entre otras cosas, que la ley de un país debería ser suficientemente detallada en vista de su fin legítimo y sus objetivos establecidos, sus condiciones, sus limitaciones y sus garantías, para que se proteja de manera adecuada a las personas frente al uso indebido y al abuso. La ley también debe ser clara y estar a disposición del público, a fin de que las personas puedan considerar el posible impacto de la aplicación de excepciones en determinadas circunstancias en su derecho a la privacidad, en otros derechos humanos y en las libertades fundamentales.

Sin embargo, el grado de detalle de la ley podría variar dependiendo del nivel de injerencia en los derechos humanos y las libertades fundamentales que permitan las disposiciones. El informe titulado "*Digital solution to fight Covid 19"*[8] recomienda que los países presten particular atención al plazo de las medidas extraordinarias, las cláusulas de extinción legal, la limitación de finalidad, la necesidad y proporcionalidad de la medida, y la participación

[7] Este criterio debería interpretarse en consonancia con el artículo 4.1 del Convenio núm. 108+, como se especifica con más detalle en el párrafo 32 del Informe explicativo (la expresión "ley de las Partes") y con la jurisprudencia aplicable del TEDH sobre el artículo 8.2 del CEDH ("prevista por la ley"), y no debería conllevar otros requisitos. Otra referencia importante a la interpretación de "el sentido más amplio de la ley" sería el párrafo 50 del Memorando explicativo de la Recomendación núm. R (97) 18 del Comité de Ministros a los Estados Miembros sobre la protección de datos personales recopilados y tratados con fines estadísticos.

[8] Véase: https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c (en inglés).

de las autoridades encargadas de la protección de datos a lo largo de todo el proceso.[9] El párrafo 56 del Informe explicativo indica que, en caso de tratamiento de datos sensibles con fines legítimos, deben establecerse las garantías adecuadas que complementen las que ya se aplican. Dichos requisitos también pueden tener repercusiones en el grado de detalle de la ley, es decir, para referirse explícitamente a las garantías adicionales cuando esos datos vayan a tratarse[10]. De lo anterior y del párrafo 32 del Informe explicativo se desprende que "*la ley debería ser suficientemente clara para que las personas y otras entidades puedan regular su propio comportamiento a la luz de las consecuencias jurídicas previstas de sus actos, y que las personas que probablemente se vean afectadas por esta ley deberían tener acceso a ella*."

En términos de accesibilidad como criterio de la ley, cabe señalar que, dado que es muy probable que la aplicación de excepciones conduzca a la injerencia en el derecho a la vida privada de las personas, el hecho de que esto debería basarse en las leyes nacionales y ser de acceso público representa la primera garantía importante contra la injerencia arbitraria de las autoridades públicas. Además, estas leyes deberían incluir garantías, que pueden ser de carácter jurídico, procesal, operacional o técnico, a fin de garantizar que las excepciones se apliquen legalmente, en relación con la finalidad del tratamiento de datos y de conformidad con el Estado de derecho específico y con las condiciones y requisitos en materia de protección de datos mencionados anteriormente. Sin embargo, el requisito "*suficientemente detallada*" no significa que una Parte tenga la obligación de hacer pública toda garantía disponible o todo elemento de la misma que se aplica a nivel operacional a una actividad de tratamiento de datos encubierta o secreta, a fin de aplicar una excepción con respecto a la seguridad nacional.

Estos principios también se aplican *a fortiori* cuando las excepciones se aplican a una actividad de tratamiento de datos encubierta o secreta, por ejemplo, cuando una persona concernida tal vez desconozca la actividad de tratamiento de datos que está teniendo lugar. Por consiguiente, la ley debería contener normas claras para la aplicación de dichas excepciones, a fin de cumplir los requisitos cualitativos de accesibilidad y previsibilidad.

4.2. Respeto de la esencia de los derechos y libertades fundamentales

Los derechos humanos y las libertades fundamentales garantizan valores particulares que se consideran universales. La esencia de esos derechos y libertades son las principales características y los valores esenciales que deben proteger los Estados; por ejemplo, el derecho a la dignidad humana y el derecho a que ningún procedimiento conduzca a que las personas sean objeto de tratos inhumanos o gravemente degradantes. En otras palabras, una medida adoptada por las autoridades públicas, aunque se haya tomado por un motivo legítimo en interés público, no puede conducir a la supresión de la protección por los Estados de los derechos garantizados a las personas.

[9] Inclusive al decidir los detalles que van a publicarse o el nivel de transparencia general de las medidas legislativas adoptadas.

[10] Dichas garantías comprenden, por ejemplo, garantías a título individual o por acumulación; el consentimiento explícito de la persona concernida; una ley que cubre el objetivo previsto y los medios del tratamiento de datos o que indica los casos excepcionales en los que se permitiría el tratamiento de dichos datos; una obligación de secreto profesional; medidas tras un análisis de los riesgos; una medida de seguridad técnica u organizativa particular y calificada (por ejemplo, cifrado de datos).

En consonancia con estos criterios, al redactar excepciones de la ley, el legislador debe tener en cuenta sus límites y sus efectos directos e inmediatos. Por consiguiente, una excepción de la ley no podría conducir a la privación de la privacidad de una persona de una manera ilimitada, incondicional o irrevocable, o a una negación total o un rechazo permanente de los derechos de la persona concernida (por ejemplo, cuando se ha denegado o restringido el derecho de acceso en un momento determinado, el acceso puede concederse ulteriormente a condición de que hayan cambiado las circunstancias relacionadas con la denegación o la restricción). Puede haber diferentes maneras de restringir el derecho de acceso; por ejemplo, teniendo en cuenta los diferentes contextos en los que se aplicarán dichas excepciones. Por lo general, se debería mantener informada a la persona concernida de los progresos realizados, a petición suya, y se le debería proporcionar información suficiente, siempre que ello no obstaculice el objetivo subyacente a la aplicación de la excepción.

Ni la introducción ni la aplicación de una excepción de la ley equivale automáticamente a una vulneración de los derechos humanos o de las libertades fundamentales. Sin embargo, al introducir la excepción de la ley y al aplicarla, debería prestarse particular atención al efecto que dicha restricción podría tener en la persona concernida, que no debería conducir a la privación absoluta e indefinida de los derechos humanos y las libertades fundamentales, como se ha explicado más arriba.

4.3. Necesarias y proporcionadas en una sociedad democrática

La obligación de garantizar que las excepciones son necesarias y proporcionadas a menudo está relacionada con la manera en que el Estado desempeña sus funciones esenciales: proteger a las personas, y garantizar el orden público, la seguridad y el buen funcionamiento de las instituciones democráticas. Sin embargo, el cumplimiento de las obligaciones de las instituciones estatales no puede lograrse por todos los medios disponibles, de manera arbitraria o al margen de las funciones de interés público. Una amenaza real y significativa para dichas obligaciones o funciones esenciales del Estado debería justificar la aplicación de las excepciones previstas. En tales casos, los Estados estarían obligados/autorizados, en consonancia con la legislación nacional y con su mandato relacionado con el interés público, a, por ejemplo, proteger a la población, las instituciones estatales, las propiedades, y los intereses monetarios y financieros; a restablecer el orden público y la seguridad pública; a garantizar el funcionamiento del poder judicial, etc. Además, los Estados deberían garantizar la protección de otros derechos humanos y libertades fundamentales, en particular la libertad de expresión, en consonancia con el artículo 11.1.b, al actuar en (otro) interés público. De conformidad con el párrafo 96 del Informe explicativo: *“Estas medidas de protección deberían referirse a los derechos y libertades fundamentales de los particulares, tales como los de la propia persona concernida (por ejemplo, cuando se amenazan los intereses vitales de la persona concernida porque faltan) o de terceros, tales como la libertad de expresión, incluida la libertad de expresión periodística, académica, artística o literaria, y el derecho a recibir y proporcionar información, a la confidencialidad de la correspondencia y de las comunicaciones, o al secreto profesional o comercial y otros secretos protegidos legalmente.”*

Por consiguiente, a fin de cumplir el criterio de “necesarias y proporcionadas” en una sociedad democrática, el legislador debería evaluar si el ejercicio del poder y/o la capacidad subyacente a la aplicación de la excepción de la protección de datos está

contemplado en la ley, si tiene un fin legítimo y si, por consiguiente, atiende una necesidad social apremiante que no puede satisfacerse por otros medios menos invasivos (párrafo 91 del Informe explicativo). La evaluación debería concluir que no existen alternativas disponibles para "medios menos intrusivos o menos gravosos" a fin de lograrlo, y que las propias medidas deben justificarse como necesarias y proporcionadas habida cuenta de los intereses en juego en una situación y contexto particulares. Tal como prevé el artículo 5.1, "*el tratamiento de datos (…) reflejará en todas las etapas del tratamiento un justo equilibrio entre todos los intereses en juego, ya sean públicos o privados, y los derechos y libertades en juego*". Por consiguiente, siempre se recomienda verificar si la aplicación de una excepción es eficiente y eficaz en respuesta a la necesidad social apremiante específica, y si dicha eficacia y eficiencia no se lograrían por medios menos intrusivos. También parece sumamente importante garantizar, en virtud del Derecho derivado u otros medios adecuados, que sólo se practica la injerencia necesaria y proporcionada en los derechos a la protección de la privacidad y de los datos personales. Esta limitación del impacto podría establecerse describiendo el tratamiento de datos previsto con el mayor detalle posible, así como el impacto potencial o que cabría esperar razonablemente en los intereses, derechos y libertades que están en juego.

El interés de los Estados en tomar ciertas medidas debe sopesarse frente a la gravedad de la injerencia en el derecho de las personas al respeto de su vida privada.

Por consiguiente, el legislador debería practicar una prueba de tres pasos en relación con las excepciones, a fin de garantizar que el marco jurídico nacional subyacente asegure estas condiciones generales para la aplicación de una excepción, es decir: la excepción es a) con un fin legítimo; b) necesaria para lograr ese fin y c) proporcionada para lograr ese fin. La manera en que los responsables del tratamiento de datos deben aplicar esas condiciones, una vez definidas por la ley, probablemente se examine en otras directrices y orientaciones. Sin embargo, sigue siendo muy recomendable que el legislador verifique si la ley establece, permite o hace posible, explícita o implícitamente, acciones y operaciones que permitirían la aplicación de una excepción a las disposiciones del Convenio núm. 108+, y si éstas están en consonancia con la prueba de tres pasos.

Verificar la primera condición parece ser lo más directo, ya que las tareas y funciones de las autoridades nacionales están bien reguladas, a menudo al nivel más alto (en las Constituciones nacionales). Por lo tanto, es lógico que, a fin de evaluar si el tratamiento de datos se lleva a cabo con un fin legítimo, como se define en el artículo 11.1, se invite al legislador a verificar si los fines para los que puede aplicarse la excepción están definidos por la ley y en consonancia con ella.

La segunda condición requiere lo que se conoce como "evaluación de la necesidad", que se propone que sea llevada a cabo para demostrar que la aplicación de una excepción es adecuada en lo que respecta al fin legítimo del tratamiento de datos. En otras palabras, la aplicación de una excepción debe ser necesaria para lograr el fin legítimo definido, debe ser esencial para ello o para evitar daños o perjuicios a dicho objetivo o fin jurídico, y no solo debe representar una mera ventaja. Esto último puede verificarse fácilmente evaluando si no existen alternativas menos gravosas disponibles. Se recomienda que la evaluación incorpore un conjunto de fuentes de información independientes y de prácticas comparativas.

La tercera condición propone una evaluación de la proporcionalidad, que debe realizarse en un sentido estricto y durante la cual debería sopesarse el interés público en lograr un

fin legítimo (incluida la protección de otros derechos humanos y libertades fundamentales) frente a la gravedad de una injerencia en el derecho de las personas al respeto de su vida privada. Dicha evaluación debería llevarse a cabo a fin de tener en cuenta todos los efectos adversos de una medida en el derecho a la privacidad y a la protección de datos (incluidos terceros no previstos), y que la injerencia no sea excesiva en relación con las ventajas obtenidas. En otras palabras, el objetivo de la evaluación es demostrar que los efectos adversos no son excesivos en relación con el impacto positivo, que es esencial (como lo justifica el criterio anterior) para responder a una necesidad social apremiante. El legislador debería elegir medidas menos intrusivas con miras a lograr el fin legítimo, para que puedan considerarse proporcionadas.

Por último, es importante tener en cuenta que, según la jurisprudencia del TEDH, los Estados tienen un margen de apreciación para decidir las medidas y los medios más adecuados para lograr los fines legítimos predefinidos. El legislador en la legislación nacional podría apoyarse en el margen de apreciación dentro de los parámetros detallados más arriba, y se le invita a considerar que la excepción aplicada se mantenga dentro de dicho margen. Es aconsejable evaluar la necesidad y la proporcionalidad de la medida concreta adoptada, utilizando la metodología propuesta más arriba.