

0029/2022**I**

La consulta a esta AEPD se solicita sobre la base del art. 5.3.b) del Estatuto de esta AEPD aprobado por Real Decreto 389/2021, de 1 de junio. Sin embargo, examinado dicho precepto, se observa que este hace referencia exclusivamente a la competencia de la AEPD para informar de “anteproyectos de ley o proyectos de reglamento que incidan en la materia propia del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y de la Ley Orgánica 3/2018, de 5 de diciembre”. Tratando la consulta sobre un Decreto Ley 3/2022, de 29 de marzo, de la Generalitat de Catalunya, de acceso a datos de los entes locales y del Departamento de Educación para la aplicación de medidas destinadas a la detección y distribución equilibrada del alumnado con necesidades educativas específicas, publicado en el DOGC nº 8638, de 31 de marzo de 2022, parece que dicha norma no se halla entre las mencionadas en el art. 5.3.b) citado del Estatuto de la AEPD. Se trata por tanto de una norma ya publicada y plenamente vigente desde el mismo día de su publicación oficial (Disposición Final de la misma).

Podría ser de aplicación el art. 5.1 de dicho Estatuto, que menciona que la AEPD tendrá la función de supervisar la aplicación de la normativa vigente en materia de protección de datos personales con el fin de proteger los derechos y libertades de las personas físicas. Ahora bien, conforme al art. 57.1.a) de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), corresponde a las autoridades autonómicas de protección de datos, de acuerdo con la normativa autonómica, las funciones y potestades correspondientes cuando se trate de tratamientos de los que sean responsables las entidades integrantes del sector público de la correspondiente Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial. En el presente caso existe normativa autonómica y una autoridad autonómica específica (art. 31 y 156.d) del Estatuto de Autonomía de Cataluña), siendo por lo demás competencia ejecutiva de la Generalitat de Catalunya -y de dicha autoridad de protección de datos autonómica- “los tratamientos de datos de carácter personal creados o gestionados por las instituciones públicas de Cataluña, la Administración de la

Generalitat, las administraciones locales de Cataluña, las entidades autónomas y las demás entidades de derecho público o privado que dependen de las administraciones autonómica o locales (...). En definitiva, la competencia para la protección de dicho derecho correspondería a la Autoridad Catalana de Protección de Dades (ACPD).

II

Sentado lo anterior, y ante la falta de concreción de la consulta, esta AEPD examinará los aspectos del contenido de la norma que puedan ser relevantes para proceder, en su caso, a la determinación de si dicha norma puede ser objeto de un recurso de inconstitucionalidad, pues poco más puede hacerse desde esta AEPD.

En primer lugar, se trata de un Decreto Ley, por lo que podría plantearse si los tratamientos de datos personales que establecen tienen una base legal adecuada. Dicha cuestión ya fue respondida por el Tribunal Constitucional en su, entre otras, STC 139/2016, de 21 de julio, FJ 6 d).

d) El recurso denuncia que el derecho fundamental a la protección de datos de carácter personal ex art. 18.4 CE ha sido afectado por el art. 4.14, aunque no se aprecia en la demanda la mínima argumentación al respecto. Esta se limita a señalar que esta regulación le está vedada al Decreto-ley por requerir Ley Orgánica. Para contestar a tan genérica queja basta recordar la doctrina de este Tribunal según la cual «la prohibición de ‘afectar’ a los derechos, deberes y libertades de los ciudadanos por Decretos-leyes (art. 86.1 de la Constitución) no coincide en su objeto con la necesidad de disciplinar por Ley Orgánica el ‘desarrollo’ de los derechos fundamentales y libertades públicas» [STC 127/1994, de 5 de mayo, FJ 3 B)], pues este último ámbito es por fuerza más restringido, ya que tan sólo cubre el desarrollo general de un derecho o, en todo caso, la regulación de aspectos esenciales de dicho desarrollo. Por tanto, en la medida en que no se regula con carácter general el derecho fundamental a la protección de datos de carácter personal, debe desestimarse este motivo de inconstitucionalidad.

III

En segundo lugar, el TC, en su STC 76/2019, de 22 de mayo, ha recogido que

(...) el derecho fundamental a la protección de datos personales no tiene carácter absoluto. Puede ser restringido por medio de la ley, siempre que ello responda a un fin de interés general, y los requisitos y el alcance de la restricción estén suficientemente precisados en la ley y respeten el principio de proporcionalidad. A los efectos del presente proceso deben destacarse dos requisitos de esos límites:

– En primer lugar, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas debe responder a un fin constitucionalmente legítimo o encaminarse a la protección o la salvaguarda de un bien constitucionalmente relevante, pues «si bien este Tribunal ha declarado que la Constitución no impide al Estado proteger derechos o bienes jurídicos a costa del sacrificio de otros igualmente reconocidos y, por tanto, que el legislador pueda imponer limitaciones al contenido de los derechos fundamentales o a su ejercicio, también hemos precisado que, en tales supuestos, esas limitaciones han de estar justificadas en la protección de otros derechos o bienes constitucionales (SSTC 104/2000, de 13 de abril, FJ 8 y las allí citadas) y, además, han de ser proporcionadas al fin perseguido con ellas (SSTC 11/1981, FJ 5, y 196/1987, FJ 6)» (STC 292/2000, FJ 15).

– En segundo lugar, por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, ora incida directamente sobre su desarrollo (artículo 81.1 CE), ora limite o condicione su ejercicio (artículo 53.1 CE), precisa una habilitación legal (por todas, STC 49/1999, de 5 de abril, FJ 4). En la STC 49/1999, FJ 4, definimos la función constitucional de esa reserva de ley en los siguientes términos:

En el presente caso, y del texto del Decreto Ley presentado resulta la existencia de una norma con rango de ley que habilita los tratamientos de datos personales, lo que supondría una injerencia en dicho derecho fundamental justificada, en principio, por el fin perseguido, que sería, de acuerdo con dicha norma, evitar la segregación escolar y detectar las necesidades educativas específicas derivadas de la situación socioeconómica y socio cultural de

determinadas personas, lo que justificaría, desde la perspectiva de la finalidad, la injerencia en el derecho fundamental a la protección de datos personales.

Ya la STC 17/2013, de 31 de enero, señaló que los mecanismos de policía administrativa a través del control de flujos migratorios responden a una finalidad legítima expresada en el evidente interés público que subyace en el adecuado control de los antes citados flujos migratorios y de la seguridad pública asegurando, al tiempo, el cumplimiento de lo dispuesto en las leyes, expresión de un interés general que, en cuanto predicable del conjunto de la comunidad, puede no siempre resultar compatible con los que corresponden a las personas singulares, pues es evidente que el respeto a las decisiones del legislador y su adecuada puesta en práctica redundan en beneficio de la comunidad.

En definitiva, y en el caso concreto, existe una finalidad explícita, de interés público, establecido en una norma de rango legal.

Y conforme a la misma sentencia citada 17/2013 (si bien refiriéndose a la LOPD de 1999) decía: *De esta forma, de acuerdo con la Ley Orgánica de protección de datos, la finalidad inicial que justificó la recogida de los datos por parte de una Administración pública no impide el destino posterior de los datos para su uso en finalidades diferentes de aquellas que motivaron su recogida respetando, en todo caso, el principio de reserva de ley para establecer dicho cambio, en cuanto que se trata de un límite al derecho a consentir la cesión de datos personales entre Administraciones públicas para fines distintos a los que motivaron originariamente su recogida, y a los que alcanza únicamente el consentimiento inicialmente prestado por el afectado. Por lo expuesto, desde esa perspectiva, la Ley de bases de régimen local en su condición, además, de norma reguladora de un fichero como el padrón municipal puede prever cesiones de datos entre Administraciones públicas.*

IV

Tal y como resulta del Reglamento General de Protección de Datos, todo tratamiento de datos personales debe ser conforme, por una parte, con los principios relativos a la calidad de los datos, enunciados hoy en el art. 5 del RGPD, y, por otra, con alguno de los principios relativos a la legitimación del tratamiento de datos, enumerados en su artículo 6 (veáse, por ejemplo, sentencias Smaranda Bara y otros C-201/14; Österreichischer Rundfunk y

otros, C-465/00, C-138/01 y C-139/01, EU:C:2003:294, apartado 65; Huber, C-524/06, EU:C:2008:724, apartado 48, y ASNEF y FECEMD, C-468/10 y C-469/10, EU:C:2011:777, apartado 26).

Del propio tenor del Decreto Ley sometido a informe, la base jurídica de los tratamientos que contiene sería bien la establecida en el art. 6.1.c) o 6.1.e), RGPD, esto es, el cumplimiento de una obligación legal por las Administraciones Públicas, o el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Esta AEPD considera que dicha base legal es, preferentemente, la establecida en la letra e), esto, el ejercicio de la competencias -poderes públicos- establecidas en el ordenamiento jurídico. Es de observar que dicha norma, el Decreto Ley, no establece nuevas competencias ni a los órganos de la Administración autonómica ni a los de la Administración Local, sino que tan sólo, para un mejor ejercicio de dichas competencias, la norma establece la posibilidad de ceder datos entre dichas administraciones para fines, en principio, pero no del todo, diferentes del fin inicial para el que se tomaron los datos. Las finalidades previstas para las cuales se tratarán los datos son, para la Generalitat, “orientar la detección de los alumnos con necesidades educativas específicas derivadas de situaciones socioeconómicas y socioculturales”, y para las entidades locales “el ejercicio de las competencias en materia de planificación y prevención de la segregación escolar”. En definitiva, competencias en el ámbito de la educación, en combinación con los servicios sociales.

No se expone en el texto de la norma cuáles fueron las finalidades iniciales de recogida de los datos personales, si bien los datos de la Generalitat que se traspasarán a los entes locales se contienen en un denominado “Registros de Alumnos de Catalunya” (Exposición de Motivos), con lo cual el tratamiento inicial de esos datos responderá, en principio a finalidades educativas; mientras que los datos a ceder por los entes locales a la Administración autonómica son de naturaleza en principio diferente, pues hacen referencia a circunstancias socioeconómicas (art. 2). Ahora bien, dichas circunstancias no están alejadas de la finalidad de la equidad en la educación que menciona el párrafo primero de la Exposición de Motivos, por cuanto recoge que el art. 81 de la ley Orgánica 2/2006, de 3 de mayo, de educación, tiene entre sus objetivos asegurar una actuación preventiva compensatoria y garantizar las condiciones más favorables para la escolarización de todos los

niños, cuyas condiciones personales o sociales supongan una desigualdad inicial para acceder a las diferentes etapas de la educación.

Se tratan pues datos personales para finalidades, en principio diferentes de las iniciales para las que se recogieron los datos. Pero la nueva finalidad está claramente determinada en el Decreto Ley, cumpliendo lo establecido en el art. 6.3 RGPD, siendo, en principio, necesaria para el cumplimiento de la misión de interés público o el ejercicio de las misiones de interés público conferidas a los responsables del tratamiento.

Por otra parte, el art. 6.4 RGPD recoge la posibilidad de que los datos personales puedan ser tratados para fines distintos de aquel para el que se recogieron los datos personales. Dichos tratamientos pueden estar basados en el consentimiento (que no es el caso), en una norma de Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, o, sin concurrir estas causas, si los fines son compatibles. Pero en este último caso el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas las circunstancias previstas en las letras a) a e) de dicho art. 6.4 RGPD. Cabe entender que en el presente caso existe una norma de Derecho de la Unión (el Decreto Ley sometido a informe) que constituye una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1 RGPD. En concreto, el apartado i) de dicho art. 23 se refiere a “la protección del interesado”, -que, conforme al Considerando 73 del RGPD puede incluir la “protección social”- y la norma tiene dicha finalidad, de procurar la prevención de la segregación de la población escolar en función de sus circunstancias socioeconómicas y/o socioculturales. Por lo tanto, se considera que dichos tratamientos son compatibles con la finalidad inicial.

Sin embargo, el principio de limitación de la finalidad (art. 5.1.b) RGPD) aplica de manera idéntica a estos nuevos tratamientos, de manera esos datos personales no podrán utilizarse por los responsables que los han recibido para “otras” finalidades diferentes de la prevista en la norma que habilita el nuevo tratamiento, sin cumplir a su vez con lo dispuesto en el art. 6.4 RGPD. Ello sería constitutivo de una infracción, cuya sanción está prevista en el art. 83.5.a) RGPD.

V

Por otra parte, de la doctrina del Tribunal Constitucional (STC 17/2013, de 31 de enero) resulta que la cesión de datos entre Administraciones Públicas, establecida en una norma de rango legal, para el cumplimiento de finalidades legítimas del órgano cedente y del cesionario, que desde el punto de vista material no resultan incompatibles entre sí, son conformes a la Constitución si se trata de un *“acceso específico en cada caso ajustado a los datos que resulten precisos para la tramitación de un expediente determinado y no de un acceso masivo o indiscriminado”* (...) *“tal acceso solamente puede producirse cuando ese dato resulte necesario o pertinente en relación con la tramitación de un concreto expediente, lo que permite analizar o determinar en cada caso la conformidad del acceso con lo establecido en el régimen legal que le resulta de aplicación”*. En definitiva, rechaza consultas generales y accesos indiscriminados, e impone el acceso individualizado, motivado y para casos concretos. En suma, concluye el TC, la norma impugnada en dicho proceso constitucional (y en el presente caso, el Decreto Ley sometido a informe), no sería contraria a la Constitución interpretada en dicho sentido, esto es, que el art. 18.4 CE no admite consultas generales y accesos indiscriminados, e impone el acceso individualizado, motivado y para casos concretos.

En el presente caso, el Decreto Ley no puede amparar accesos masivos o indiscriminados, sino justificados caso a caso. Si no fuera así, sería inconstitucional. Como observa la Autoridad Catalana de Protecció de Dades, en su *“Informe en relació amb la Proposta presentada pel Departament de Drets Socials sobre l’intercanvi d’informació entre els serveis socials i els serveis de salut, a incloure en l’Avantprojecte de Llei de mesures fiscals i financeres per al 2022 (M-184)”*, a que se hará referencia en el apartado VIII de este Informe, por referirse a un supuesto de establecimiento de tratamientos de datos de carácter similar -intercambio de datos entre administración sanitaria y de servicios sociales- al previsto en el Decreto Ley ahora sometido a Informe de esta AEPD:

Ara bé, això no ha de dur a la pràctica a un accés indiscriminat a la informació que consti als dits sistemes d’informació, sinó només en aquells casos que això sigui justificat i respecte les persones en què sigui necessari.

Esta AEPD estima que podría someterse a la consideración de la correspondiente Comisión Bilateral de Cooperación (art. 33.2 LOTC) para resolver la discrepancia, consistente básicamente en que en el Decreto Ley no se menciona expresamente dicho carácter individualizado caso por caso de la cesión de datos entre las Administraciones concernidas, pudiendo en consecuencia parecer que autoriza una cesión o acceso indiscriminada o masivo a los datos personales a los que se refiere.

VI

En lo relativo a las garantías para los interesados, tanto la doctrina del TC (STC 76/2019), como el propio Tribunal de Justicia de la Unión Europea, TJUE, -véase, entre otras, STJUE de 6 de octubre de 2020, en los casos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, o la STJUE de la misma fecha 6 de octubre de 2020 (C-623/17), Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, establecen que la propia ley habrá de contener las garantías adecuadas frente a la recopilación de datos personales que autoriza. El TC ha sido claro en cuanto a que:

[/]la previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. Solo ese entendimiento es compatible con la doble exigencia que dimana del artículo 53.1 CE (...). Es evidente que, si la norma incluyera una remisión para la integración de la ley con las garantías adecuadas establecidas en normas de rango inferior a la ley, sería considerada como una deslegalización que sacrifica la reserva de ley ex artículo 53.1 CE, y, por este solo motivo, debería ser declarada inconstitucional y nula. (...). Se trata en definitiva, de “garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental”.

Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero:

“En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; SSTC 66/1995, de 8 de mayo [RTC 1995, 66], F. 5; 55/1996, de 28 de marzo [RTC 1996, 55], FF. 7, 8 y 9; 270/1996, de 16 de diciembre [RTC 1996, 270], F. 4.e; 37/1998, de 17 de febrero [RTC 1998, 37], F. 8; 186/2000, de 10 de julio [RTC 2000, 186], F. 6).”

En el caso sometido a consulta, las garantías aplicables se contienen en el propio texto del Decreto Ley (art. 4), y además el tratamiento de datos que contiene la norma parece que cumple con el principio de proporcionalidad, si bien ese juicio de proporcionalidad (juicio de idoneidad, juicio de necesidad y juicio de proporcionalidad en sentido estricto), correspondería hacerlo a los responsables de los tratamientos.

Por otra parte, esos responsables previamente deberían de realizar una Evaluación de Impacto en Protección de Datos (EIPD) en los casos del art. 35.1 RGPD.

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la

protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares,

Concretamente, la Autoridad Catalana de Protección de Datos, a quien corresponde la competencia en el presente caso como autoridad de control, ha establecido, conforme al art. 35.4 RGPD, una lista de los tipos de operaciones de tratamiento que requieren una evaluación de impacto relativa a la protección de datos. Entre ellas se encuentran, el apartado 8. ***Tractaments que impliquin l'associació, combinació o enllaç de registres de bases de dades de dos o més tractaments amb finalitats diferents o per responsables diferents.*** Y el apartado 9 ***Tractaments de dades de subjectes vulnerables o en risc d'exclusió social, incloent dades de menors de 14 anys, majors amb algun grau de discapacitat, discapacitats, persones que accedeixen a serveis socials i víctimes de violència de gènere, així com els seus descendents i persones que estiguin sota la seva guàrdia i custòdia.***

Todo ello supone, en definitiva, que los responsables deberán -si no se hubiera ya realizado de conformidad con el apartado 10 del art. 35 RGPD- realizar dicha EIPD, con el contenido del apartado 7 del art. 35 RGPD, lo que afectará no a la legalidad o licitud del establecimiento del tratamiento en el Decreto ley, sino a su ejecución (a la licitud del propio tratamiento de datos, cuando se realice por el responsable).

VII

Por último, simplemente hay que mencionar que, de conformidad con el art. 14 RGPD, dado que el nuevo responsable del tratamiento, en cada caso, no ha obtenido los datos directamente de los interesados, debe de facilitarles a estos la información a que se refiere dicho precepto (art. 14.1 y 14.2 RGPD), sin que, en opinión de esta AEPD, sean aplicables las excepciones, en el caso concreto de este Decreto Ley, establecidas en el apartado 5 del art. 14 RGPD.

El TJUE, en sentencia de 1 de octubre de 2015, C-201/14, Smaranda Bara y otros, ha examinado este requisito de información a los interesados en caso de tratamientos por responsable distinto del original. Dicha sentencia se refiere a la Directiva 95/46, pero su doctrina es aplicable igualmente al RGPD.

Dicha sentencia dice así:

33 *Como señaló el Abogado General en el punto 74 de sus conclusiones, esa exigencia de información de los interesados resulta especialmente importante en la medida en que es una condición necesaria para el ejercicio por éstos de su derecho de acceso a los datos objeto de tratamiento y de rectificación de los mismos, establecido en el artículo 12 de la Directiva 95/46, y de su derecho de oposición al tratamiento de esos datos, contemplado en el artículo 14 de la propia Directiva.*

34 *Por consiguiente, la exigencia de tratamiento leal de los datos personales prevista en el artículo 6 de la Directiva 95/46 obliga a una administración pública a informar a los interesados de la transmisión de esos datos a otra administración pública para su tratamiento por ésta en su calidad de destinataria de dichos datos.*

(...)

45 *Es preciso añadir que, con arreglo al artículo 11, apartado 2, de la Directiva 95/46, las disposiciones del artículo 11, apartado 1, de la propia Directiva no se aplicarán, en particular, cuando el registro o la comunicación de los datos a un tercero estén expresamente prescritos por ley, debiendo en tales casos los Estados miembros establecer las garantías apropiadas. Por los motivos expuestos en los apartados 40 y 41 de la presente sentencia, las disposiciones de la Ley nº 95/2006 invocadas por el Gobierno rumano y el Protocolo de 2007 no pueden estar amparados ni por el régimen excepcional del artículo 11, apartado 2, ni por el del artículo 13 de la citada Directiva.*

El propio Decreto Ley parece que acoge esta misma interpretación, ya que no sólo en su art. 4 establece que corresponde a los responsables, en cada caso, aplicar las medidas necesarias para garantizar el “*deber de informar a las personas interesadas*”, sino que de los propios tratamientos previstos en el art. 2 y 3 de la norma se desprende, en primer lugar, que los interesados no tienen por qué asumir necesariamente que sus datos personales tratados para una determinada finalidad (servicios sociales, o ayudas al alquiler, por ejemplo) van a ser tratados para una finalidad diferente (educativas), con lo que sufriría el requisito de previsibilidad y certeza exigible a las leyes que supone afectación a derechos fundamentales (STC 76/2019).

VIII

Es necesario señalar que el presente Decreto ley informado no es el único caso de intercambio de datos entre Administraciones Públicas previsto por las normas de Cataluña, sino que recientemente, cuando menos, la ley 2/2021, de 29 de diciembre, de medidas fiscales, financieras, administrativas y del sector público ha introducido en la ley 12/2007, de 11 de octubre, de servicios sociales, una medida similar a la ahora estudiada ¹.

Dicha medida fue objeto de Informe por parte de la Autoridad Catalana de Protección de Dades en su Informe PD 10/2021, ya citado ².

Así, el art. 71 de la ley 2/2021, dice así:

Artículo 71. Modificación de la Ley 12/2007, de servicios sociales

Se añade una disposición adicional, la decimoquinta, a la Ley 12/2007, de 11 de octubre, de servicios sociales, con el siguiente texto:

«Disposición adicional decimoquinta. Comunicación de datos entre servicios sanitarios del sistema público

*»1. A fin de garantizar la atención integral efectiva de las personas atendidas por la Red de Servicios Sociales de Atención Pública y los servicios sanitarios del sistema público, **se habilita la comunicación de datos entre dichos servicios**, sin el consentimiento de las personas interesadas, en los términos previstos en los siguientes apartados:*

»a) Se habilita a los servicios sociales para comunicar a los servicios de salud los datos relacionados con las personas atendidas por ambos sistemas, de carácter identificativo, de contacto, así como las relacionadas con los servicios sociales recibidos que puedan tener repercusión en la salud y sean necesarios para garantizar un proceso de

1 <https://dogc.gencat.cat/es/document-del-dogc/?documentId=917573>

2 <https://apdcat.gencat.cat/es/documentacio/resolucions-dictamens-i-informes/cercadorOn/cercador-detall/PD-10-2021-00001>

atención integral e integrada. Pueden acceder a la información los profesionales sanitarios implicados en el diagnóstico o tratamiento de la persona interesada, debidamente acreditados.

»b) Se habilita a los servicios de salud para comunicar a los servicios sociales los datos relacionados con las personas atendidas por ambos sistemas, de carácter identificativo, de contacto, así como los datos de su historia clínica que puedan tener afectación en la autonomía personal –ya sea por situación de dependencia o de discapacidad–, para detectar e intervenir en situaciones de riesgo social que puedan requerir la activación de prestaciones sociales y que necesiten información sanitaria para hacerse efectivas, y para garantizar un proceso de atención integral e integrada. Pueden acceder a la información los profesionales de los servicios sociales implicados en el seguimiento y evaluación del ciudadano, debidamente acreditados.

»2. Las entidades responsables de las comunicaciones deben aplicar las medidas técnicas y organizativas apropiadas al carácter sensible de la información, a fin de garantizar y verificar periódicamente la confidencialidad, la integridad, la trazabilidad, la disponibilidad y la autenticidad de la información, así como el ejercicio de derechos y del deber de informar a las personas interesadas.

»La trazabilidad debe permitir el control de los accesos al sistema de información por los perfiles de usuarios autorizados, de la identidad y categoría profesional del usuario, la fecha y hora en que tuvo lugar el acceso, la acción realizada, los datos afectados y el motivo del acceso.

»Las entidades responsables deben facilitar a las personas afectadas la consulta de la información sobre la trazabilidad de sus datos.

»3. Los profesionales de los servicios sociales y sanitarios deben mantener el deber de secreto sobre la información a la que tengan acceso, incluso una vez finalizada su vinculación con la entidad para la que prestan servicios.»

A lo que hay que añadir la Disposición Transitoria segunda de la ley 2/2021, a indicación de la ACPD en su Informe citado:

Disposición transitoria segunda. Plazo para establecer mecanismos de trazabilidad de las consultas en la comunicación de datos entre la Red de Servicios Sociales de Atención Pública y los servicios sanitarios del sistema público

*Las entidades responsables, en el ámbito sanitario y de los servicios sociales, de las comunicaciones a que se refiere la disposición adicional decimoquinta de la Ley 12/2007, de 11 de octubre, de servicios sociales, deben **establecer, en el plazo de dos años, mecanismos que permitan a las personas afectadas consultar la trazabilidad de las consultas y acciones realizadas.***

Medida esta última no establecida en el Decreto ley informado.