

El anteproyecto remitido tiene por objeto regular el régimen jurídico aplicable a la información clasificada, que se define como aquella información cuya revelación no autorizada o utilización indebida pueda ocasionar un daño o poner en peligro la seguridad o defensa nacional. Asimismo, regula los procesos de clasificación, desclasificación y reclasificación de dicha información, derogando la Ley 9/1968, de 5 de abril, sobre Secretos Oficiales.

I

En el ámbito europeo, la Carta de los Derechos Fundamentales de la Unión Europea, proclamada en Niza en diciembre de 2000 por el Parlamento Europeo, el Consejo y la Comisión, incluyó entre los mismos el derecho a la protección de datos personales en su artículo 8, regulándolo de manera independiente al derecho a la vida privada y familiar (artículo 7).

Artículo 8

Protección de datos de carácter personal

- 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*
- 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.*
- 3. El respeto de estas normas estará sujeto al control de una autoridad independiente.*

La Carta, que en un primer momento tuvo un valor meramente político, adquirió carácter vinculante tras la entrada en vigor del Tratado de Lisboa, en diciembre de 2009.

Actualmente, el derecho fundamental a la protección de datos se recoge en el artículo 16 del Tratado de Funcionamiento de la Unión Europea que, partiendo de dicha naturaleza y como novedad atribuye, en su apartado 2, a las Instituciones Europeas la competencia para establecer, a través del procedimiento legislativo ordinario, las normas sobre la protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito

de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos:

Artículo 16

(antiguo artículo 286 TCE)

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea.

En desarrollo de dicho precepto, se ha aprobado el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD).

Tal y como señala en su Considerando 1, *“La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental [...]”*.

En el ámbito penal, dicha normativa debe completarse con las previsiones específicas contenidas en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. El Considerando 1 de la Directiva parte igualmente de que *“La protección de las personas físicas en relación con el tratamiento de los datos de carácter personal es un derecho fundamental”*.

Partiendo de lo anterior y a los efectos del presente informe, interesa determinar con precisión el ámbito de aplicación de la citada normativa europea, en la medida en la que los tratamientos de los datos personales que puedan incluirse en la información clasificada, cuyo fundamento se encuentra en las necesidades de la seguridad o defensa nacional, van a quedar excluidos de su aplicación.

En este sentido, el ámbito de aplicación de la normativa europea queda circunscrito a las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, tal y como recuerda el Considerando 16 del RGPD:

(16) El presente Reglamento no se aplica a cuestiones de protección de los derechos y las libertades fundamentales o la libre circulación de datos personales relacionadas con actividades excluidas del ámbito de del Derecho de la Unión, como las actividades relativas a la seguridad nacional. Tampoco se aplica al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión.

Consecuentemente, el artículo 2 del RGPD regula su ámbito de aplicación material:

Artículo 2 Ámbito de aplicación material.

1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. El presente Reglamento no se aplica al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;

b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;

c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;

d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

3. El Reglamento (CE) n.º 45/2001 es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.º 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su artículo 98.

4. El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15.

En cuanto a la Directiva 2016/680, viene a configurar un régimen especial, al que se someterían únicamente los tratamientos que la misma regula, frente al régimen general de protección de datos que se recoge en el Reglamento general de protección de datos. Por este motivo, las disposiciones del mismo serán de aplicación a todos los tratamientos llevados a cabo dentro del ámbito de aplicación del derecho de la Unión y que no estén regulados específicamente por la Directiva, tal y como se desprende del ámbito de aplicación establecido en el artículo 2 del Reglamento.

Y, al igual que el RGPD, la misma no resulta de aplicación a las actividades relacionadas con la seguridad nacional, tal y como recuerda en su Considerando 14:

Puesto que la presente Directiva no debe aplicarse al tratamiento de datos personales en el marco de una actividad que no esté comprendida en el ámbito de aplicación del Derecho de la Unión, no deben considerarse comprendidas en el ámbito de aplicación de la presente Directiva las actividades relacionadas con la seguridad nacional, las actividades de los servicios o unidades que traten cuestiones de seguridad nacional y las actividades de tratamiento de datos personales que lleven a cabo los Estados miembros en el ejercicio de las actividades incluidas en el ámbito de aplicación del título V, capítulo 2, del Tratado de la Unión Europea (TUE).

Consecuentemente, la Directiva contiene la correspondiente exclusión de su ámbito de aplicación material en el apartado 3 de su artículo 2:

3. La presente Directiva no se aplica al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;

b) por parte de las instituciones, órganos u organismos de la Unión.

Por consiguiente, atendiendo al objeto del presente informe, quedan excluidos del ámbito de aplicación material de la normativa europea los tratamientos de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relativas a la seguridad nacional, ya que la seguridad nacional es una competencia exclusiva que corresponde a los Estados miembros, tal y como establece claramente el apartado 2 del artículo 4 del Tratado de la Unión Europea (TUE):

2. La Unión respetará la igualdad de los Estados miembros ante los Tratados, así como su identidad nacional, inherente a las estructuras fundamentales políticas y constitucionales de éstos, también en lo referente a la autonomía local y regional. Respetará las funciones

esenciales del Estado, especialmente las que tienen por objeto garantizar su integridad territorial, mantener el orden público y salvaguardar la seguridad nacional. En particular, la seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro.

Asimismo, el TFUE contiene previsiones específicas dirigidas a proteger la información en dichos ámbitos, si bien con diferentes alcances según se trate de seguridad nacional o seguridad pública, como ocurre en el artículo 346 del TFUE:

Artículo 346

(antiguo artículo 296 TCE)

1. Las disposiciones de los Tratados no obstarán a las normas siguientes:

a) ningún Estado miembro estará obligado a facilitar información cuya divulgación considere contraria a los intereses esenciales de su seguridad;

b) todo Estado miembro podrá adoptar las medidas que estime necesarias para la protección de los intereses esenciales de su seguridad y que se refieran a la producción o al comercio de armas, municiones y material de guerra; estas medidas no deberán alterar las condiciones de competencia en el mercado interior respecto de los productos que no estén destinados a fines específicamente militares.

2. El Consejo, por unanimidad y a propuesta de la Comisión, podrá introducir modificaciones en la lista, que estableció el 15 de abril de 1958, de los productos sujetos a las disposiciones de la letra b) del apartado 1.

Por consiguiente, los tratamientos de datos personales en aquellas actividades vinculadas a la seguridad nacional quedan excluidos del ámbito de aplicación de la normativa europea.

El concepto de seguridad nacional es de cuño reciente, empezándose a utilizar doctrinalmente en la década de los 80 del siglo pasado, derivado de la aparición de amenazas híbridas que impiden mantener la tradicional diferenciación entre defensa (para hacer frente a las amenazas procedentes del exterior y a las amenazas interiores más graves para la supervivencia del propio Estado) y seguridad pública (para hacer frente a las amenazas de orden público interiores). La aparición de dichas amenazas obligan a una concepción integral de la Seguridad que garantice la acción coordinada de los distintos actores implicados superando la anterior distinción. En el ámbito europeo el concepto de Seguridad Nacional no se ha recogido normativamente hasta el Tratado de Lisboa (en vigor desde el 1 de diciembre de 2009). Así, actualmente el término solo se recoge en el artículo 4 de la versión consolidada del Tratado de la Unión Europea que señala que la seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro y en el artículo 73 de la

versión consolidada del Tratado de Funcionamiento de la Unión Europea relativo a la cooperación y coordinación en materia de seguridad nacional.

Por el contrario, son muchos los preceptos del tratado que mantienen la tradicional diferenciación entre seguridad pública (artículos 36, 45, 52, 66), o seguridad interior (artículo 72) y defensa (artículos 2, 222 y 333), sin perjuicio de las disposiciones correspondientes a la política común de seguridad y defensa.

Este concepto también ha sido igualmente utilizado por las normas europeas coetáneas y posteriores al Tratado de Lisboa, como la Directiva 2009/81/CE del Parlamento Europeo y del Consejo de 13 de julio de 2009 sobre coordinación de los procedimientos de adjudicación de determinados contratos de obras, de suministro y de servicios por las entidades o poderes adjudicadores en los ámbitos de la defensa y la seguridad, y por la que se modifican las Directivas 2004/17/CE y 2004/18/CE que comienza señalando que “La seguridad nacional sigue siendo responsabilidad exclusiva de cada Estado miembro, tanto en el ámbito de la defensa como de la seguridad”.

En todo caso, tratándose la seguridad nacional de una excepción a la aplicación de los Tratados, y según reiterada jurisprudencia del Tribunal de Justicia, ha de ser objeto de interpretación restrictiva. A estos efectos, puede citarse la extensa doctrina jurisprudencial existente en relación al concepto de “intereses esenciales de la seguridad” que contiene el vigente artículo 346 del TFUE (Sentencia TJUE de 4 de octubre de 1991, Asunto C-367/89, Caso Rickardt y Les Accessoires Scientifiques, Sentencia TJUE de 3 de mayo de 1994, Asunto C-328/92 Caso Comisión contra España, Sentencias TJUE 11 de enero de 2000, Asunto C-285/98, Caso Tanja Kreril contra Bundesrepublik, Sentencia de 28 de marzo de 1995 Asunto C-234/93, Caso Evans Medical, Sentencia 11 de septiembre de 2008, Asunto C-141/07 Caso Comisión contra Alemania, Sentencia de 2 de octubre de 2008, Asunto C-157/06, Caso comisión contra Italia, Sentencia de 16 de septiembre de 1999, Asunto C-414/97, Caso Comisión contra España, Sentencia de 15 de diciembre de 2009, Asunto C-372/05, Caso Comisión contra Alemania, Sentencia de 4 de septiembre de 2014, Caso Schiebel, Sentencia 15 de mayo de 1986, Asunto 222/84, Johnston, entre otras muchas) y que puede sintetizarse en los siguientes criterios:

- 1) Las excepciones que se establecen en dicho artículo, al igual que todos aquellos artículos que permiten no aplicar los principios y normas del tratado, han de ser objeto de interpretación estricta.
- 2) La carga de la prueba de que existen realmente las circunstancias excepcionales que justifican la excepción incumbe a quien pretenda beneficiarse de ellas.
- 3) Las autoridades nacionales disponen de cierto margen de apreciación al adoptar las medidas que consideran necesarias para garantizar la seguridad pública de un Estado miembro.

4) El concepto de seguridad pública se refiere tanto a la seguridad interior de un Estado miembro como a su seguridad exterior.

5) No se puede deducir la existencia de una reserva general, inherente al Tratado, que excluya del ámbito de aplicación del Derecho comunitario cualquier medida adoptada por motivos de seguridad pública.

6) Corresponde a las autoridades nacionales demostrar que esas disposiciones son necesarias para alcanzar el objetivo invocado, y que éste no puede alcanzarse mediante prohibiciones o limitaciones de menor amplitud o que afecten en menor medida al comercio intracomunitario (principio de proporcionalidad).

En el ámbito de la protección de datos, avala igualmente el criterio restrictivo el propio RGPD, que después de excluir su aplicación en los supuestos de seguridad nacional, según lo visto, establece la sujeción al mismo de otros tratamientos de datos personales, si bien pueden establecerse limitaciones en los supuestos de seguridad del Estado, defensa y seguridad pública en su artículo 23:

Artículo 23

Limitaciones

1. El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

- a) la seguridad del Estado;*
- b) la defensa;*
- c) la seguridad pública;*
- d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;*
- e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;*
- f) la protección de la independencia judicial y de los procedimientos judiciales;*
- g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;*
- h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g); i) la protección del interesado o de los derechos y libertades de otros; j) la ejecución de demandas civiles.*

2. En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:

- a) la finalidad del tratamiento o de las categorías de tratamiento;*
- b) las categorías de datos personales de que se trate;*
- c) el alcance de las limitaciones establecidas;*
- d) las garantías para evitar accesos o transferencias ilícitos o abusivos;*
- e) la determinación del responsable o de categorías de responsables;*
- f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento;*
- g) los riesgos para los derechos y libertades de los interesados, y*
- h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.*

Asimismo, dichas circunstancias pueden legitimar el tratamiento de datos personales para finalidades distintas de la inicial para la cual se recogieron los datos personales, tal y como prevé expresamente el apartado 4 del Artículo 6 del RGPD:

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el 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, 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:

- a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;*
- b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;*
- c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;*
- d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;*
- e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.*

Partiendo de los criterios anteriormente señalados, el legislador español ha excluido expresamente de la aplicación de la normativa sobre protección de datos personales a “los tratamientos sometidos a la normativa sobre protección de materias clasificadas” (artículo 2.2.c) del RGPD) y a “los sometidos a la

normativa sobre materias clasificadas, entre los que se encuentran los tratamientos relativos a la Defensa Nacional” (artículo 2.3.d) de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Por consiguiente, en los supuestos en que la información clasificada contenga datos personales (entendidos como toda información sobre una persona física identificada o identificable, conforme a la amplia definición del artículo 4.1) del RGPD y nuestra doctrina constitucional), el tratamiento de dichos datos personales no queda sujeto a la normativa sobre protección de datos personales ni al ámbito de supervisión de las autoridades de protección de datos, sino que se regirá por su normativa específica.

Por lo tanto, y partiendo de la citada exclusión, debe modificarse la redacción del artículo 24.4. del anteproyecto, al referirse al deber de confidencialidad establecido por la normativa sobre protección de datos personales, que como se ha indicado no resulta de aplicación en el presente caso, pese a lo cual señala lo siguiente:

4. Los responsables de la clasificación de la información en cualquiera de las cuatro categorías, así como todas las personas que intervengan en cualquier fase del procedimiento de clasificación, reclasificación o desclasificación, estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679 y el art. 5 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Por ello, debe suprimirse la referencia a dichas normas, pudiendo sustituirse por la referencia al deber de secreto aplicable a todos los empleados públicos previsto en el artículo 53.12 del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público o introducir un deber de secreto o confidencialidad específico.

II

Tal y como se ha indicado en el apartado anterior, el tratamiento de los datos personales incluidos en la información clasificada no entra dentro del ámbito de aplicación de la normativa sobre protección de datos personales ni dentro del ámbito competencial de esta Agencia.

No obstante, la normativa específica que regula la información clasificada, en cuanto que supone una limitación del derecho fundamental a la protección de datos personales, debe respetar los requisitos que han venido

perfilando para dichos límites tanto el Tribunal Europeo de Derechos Humanos como el Tribunal Constitucional.

El TEDH viene considerando, partiendo de una interpretación amplia del derecho a la vida privada que siempre ha realizado y especialmente, desde el Convenio 108, que la protección de datos personales «tiene una importancia fundamental para el disfrute por una persona de su derecho al respeto de la vida privada y familiar garantizado en el artículo 8 del Convenio» (sentencia Gaskin v. Reino Unido, de 7 de julio de 1989). Un resumen de su doctrina se contiene en la Sentencia del Caso S. y Marper contra Reino Unido, de 4 de diciembre de 2008:

66

El Tribunal recuerda que la noción de «vida privada» es una noción amplia, sin una definición exhaustiva que cubre la integridad física y moral de la persona (Sentencias Pretty contra el Reino Unido , núm. 2346/2002, ap. 61, TEDH 2002-III e Y.F. contra Turquía, núm. 24209/1994, ap. 33, TEDH 2003-IX). Engloba, por tanto, numerosos aspectos de la identidad física y social de una persona (Sentencia Mikulic contra Croacia, núm. 53176/1999, ap. 53, TEDH 2002-I). Algunos elementos como, por ejemplo, la identificación sexual, el nombre, la orientación sexual y la vida sexual pertenecen a la esfera personal que protege el artículo 8 (ver, entre otras, Sentencias Bensaid contra Reino Unido, núm. 44599/1998, ap. 47, TEDH 2001-I y las referencias citadas en la misma y Peck contra Reino Unido, núm. 44647/1998, ap. 57, TEDH 2003-I). Además del nombre, la vida privada y familiar puede englobar otros medios de identificación personal y vinculación a una familia (ver, mutatis mutandis , Sentencias Burghartz contra Suiza, 22 febrero 1994, ap. 24, serie A núm. 280-B y Ünal Tekeli contra Turquía, núm. 29865/1996, ap. 42, TEDH 2004-X (extractos). La información relativa a la salud de una persona constituye un elemento importante de su vida privada (Sentencia Z contra Finlandia, 25 febrero 1997, ap. 71, Repertorio de sentencias y resoluciones 1997-I). El Tribunal estima, además, que la identidad étnica de una persona se debe también considerar un elemento importante de su vida privada (ver, concretamente, el artículo 6 de la Convención sobre protección de datos, citado en el párrafo 41, que incluye los datos de carácter personal que revelan el origen racial, junto a otra información sensible sobre la persona, entre las categorías particulares de datos que no pueden ser conservados sin las garantías apropiadas). Además, el artículo 8 protege el derecho al pleno desarrollo personal y el de entablar y desarrollar relaciones con sus semejantes y el mundo exterior (ver, por ejemplo, Sentencias Burghartz , previamente citada, opinión de la Comisión, pg. 37, ap. 47 y Friedl contra Austria de 31 enero 1995, serie A no 305-B, opinión de la Comisión, pg. 20, ap. 45). La noción de vida privada comprende asimismo elementos relacionados con el derecho a la

imagen (Sentencia Sciacca contra Italia, núm. 50774/1999, ap. 29, TEDH 2005-I).

67

El mero hecho de memorizar datos relativos a la vida privada de una persona constituye una injerencia en el sentido del artículo 8 (Sentencia Leander contra Suecia de 26 marzo 1987, ap. 48, serie A núm. 116). Poco importa que la información memorizada se utilice o no posteriormente (Sentencia Amann contra Suiza [GS], núm. 27798/1995, ap. 69, TEDH 2000-II). Sin embargo, para determinar si la información de carácter personal conservada por las autoridades hace que entre en juego uno de los citados aspectos de la vida privada, el Tribunal tendrá debidamente en cuenta el contexto particular en el que ha sido recogida y conservada la información, el carácter de los datos consignados, la manera en la que son utilizados y tratados y los resultados que pueden extraerse de ellos (ver, mutatis mutandis , Friedl, previamente citada, opinión de la Comisión, aps. 49-51, y Peck contra el Reino Unido, anteriormente citada, ap. 59).

Asimismo, al amparo del artículo 8.2. del Convenio Europeo de Derechos Humanos, el TEDH tiene declarado que dicho derecho puede ser limitado, siempre que se cumplan los requisitos establecidos en el mismo:

2. 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 del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

Para determinar si una injerencia en el derecho fundamental a la protección de datos personales está justificada en virtud del apartado 2 del artículo 8 del Convenio, el Tribunal debe examinar si estaba «prevista por la Ley», si perseguía un fin legítimo en virtud del apartado 2 y si era «necesaria en una sociedad democrática» para conseguir dicho fin (véase Sentencia Gillow contra el Reino Unido de 24 noviembre 1986, serie A núm. 124-C. pg. 20, ap. 48, citada por la Sentencia del Caso Blečić contra Croacia de 29 de julio de 2004, pg. 14 ap. 55):

A) Prevista por la ley.

El Tribunal recuerda su constante jurisprudencia según la cual los términos «prevista por la Ley» significan que la medida litigiosa ha de tener una base en derecho interno y ser compatible con la preeminencia del derecho,

expresamente mencionada en el preámbulo del Convenio e inherente al objeto y fin del artículo 8. La Ley ha de ser así suficientemente accesible y previsible, es decir, ha de estar enunciada con la suficiente precisión para permitir que la persona –asistida en su caso por un abogado– regule su conducta. Para que se la pueda juzgar conforme a estas exigencias, debe ofrecer una protección adecuada contra lo arbitrario y, en consecuencia, definir con suficiente claridad el alcance y las modalidades de ejercicio de la facultad que se confiere a las autoridades competentes (Sentencias Malone contra el Reino Unido de 2 agosto 1984, aps. 66-68, serie A núm. 82, Sentencia Kruslin contra Francia de 24 abril 1990, serie A núm. 176-A, ap. 27; Huvig contra Francia de 24 abril 1990, serie A núm. 176-B, ap. 26; Rotaru contra Rumanía [GS], núm. 28341/1995, ap. 55, TEDH 2000-V, Amann, ap. 56, Lambert contra Francia de 24 agosto 1998, Repertorio de sentencias y resoluciones 1998-V, ap. 23; Perry contra Reino Unido núm. 63737/2000, ap. 45, TEDH 2003-IX; Dumitru Popescu contra Rumania, núm. 71525/2001, ap. 61, 26 abril 2007, Sentencia (G.S.) Caso S. y Marper contra Reino Unido de 4 de diciembre de 2008, pg.39 ap. 95 y 96).

El nivel de precisión que requiere la legislación interna –la cual, por lo demás, no puede hacer frente a cualquier eventualidad– depende en gran medida del contenido del texto considerado, del ámbito que supuestamente cubre y del número y la calidad de sus destinatarios (Sentencia Hassan y Tchaouch contra Bulgaria, núm. 30985/1996, ap. 84, TEDH 2000-XI, y las referencias que se citan).

No obstante, una ley que otorga una facultad discrecional no desconoce, por esta mera característica, el requisito de la posible previsión, con tal que se precise con suficiente claridad el alcance de la discrecionalidad y el modo de ejercitarla, teniendo en cuenta la legítima finalidad perseguida, para proporcionar a la persona la adecuada protección contra una actuación arbitraria (Sentencia en el caso Malone de 2 agosto 1984, serie A, núm. 82, pág. 33, ap. 68).

El requisito de la previsibilidad de la Ley se refuerza por el Tribunal en los supuestos de tratamientos de datos personales de forma secreta por los servicios de información, siendo objeto de un análisis detallado en la Sentencia (G.S.) Caso Rotaru contra Rumanía de 4 de mayo de 2000:

*El Tribunal recuerda **que el almacenamiento en un registro secreto y la comunicación de datos relativos a la «vida privada» de un individuo entran en el campo de aplicación del artículo 8.1** (Sentencia Leander contra Suecia de 26 de marzo de 1987, serie A núm. 116, pg. 22, ap. 48).*

El Tribunal recuerda que tanto el almacenamiento por parte de una autoridad pública de datos relativos a la vida privada de un individuo como su utilización y la negativa de conceder la facultad de refutarlos,

constituyen una injerencia en el derecho al respeto de su vida privada garantizado por el artículo 8.1 del Convenio (Sentencias Leander contra Suecia anteriormente citada, pg. 22, ap. 48, Kopp contra Suiza de 25 de marzo de 1998, Repertorio 1998-II, pg. 540, ap. 53 y Amann contra Suiza anteriormente citada, aps. 69 y 80).

47

La principal cuestión que se plantea es la de saber si la injerencia así constatada puede justificarse con respecto al apartado 2 del artículo 8. Al facilitar una excepción a un derecho garantizado por el Convenio, este párrafo apela a una interpretación estricta. **Si el Tribunal reconoce que en una sociedad democrática, la existencia de servicios de información puede considerarse legítima, recuerda que el poder de vigilar en secreto a los ciudadanos únicamente es tolerable según el Convenio en la medida estrictamente necesaria para la protección de las instituciones democráticas** (Sentencia Klass y otros contra Alemania anteriormente citada, pg. 21, ap. 42).

52

El Tribunal recuerda su reiterada jurisprudencia según la **cual la expresión «prevista por la Ley» imponen no solamente que la medida incriminada tenga una base en el derecho interno, sino que se dirija también a la calidad de la Ley en causa: así, debe ser accesible al justiciable y previsible** (véase, en último lugar, Amann contra Suiza anteriormente citada, ap. 50).

53

En este caso, el Tribunal constata que el artículo 6 del Decreto-ley núm. 118/1990 invocado por el Gobierno como fundamento de la medida incriminada permite a todo individuo probar que reúne las condiciones requeridas para que se le reconozcan ciertos derechos, por medio de documentos oficiales emitidos por las autoridades competentes o de cualquier elemento que tenga valor de prueba. Sin embargo, esta disposición no define de qué manera pueden obtenerse las pruebas y no confiere al SRI ningún poder en materia de recogida, almacenamiento y comunicación de datos sobre la vida privada de una persona.

El Tribunal debe por lo tanto indagar si la Ley núm. 14/1992 sobre la organización y el funcionamiento del SRI, invocada igualmente por el Gobierno, puede constituir el fundamento legal de estas medidas. A este respecto, indica que dicha ley autoriza al SRI a recoger, almacenar y utilizar informaciones relativas a la seguridad nacional. El Tribunal expresa sus dudas en cuanto a la pertinencia para la seguridad nacional de las informaciones guardadas con respecto al demandante. Sin embargo, recuerda que incumbe en primer lugar a las autoridades nacionales, y sobre todo a los tribunales, el interpretar y aplicar el derecho interno (Sentencia Kopp contra Suiza anteriormente citada pg. 541, ap. 59) y señala, a este respecto, que en su Sentencia de 25 de noviembre de 1997, el Tribunal de Apelación de Bucarest confirmó la legalidad de la posesión por parte del SRI de esos datos como depositario de los archivos de los antiguos servicios de seguridad.

Así, el Tribunal puede concluir que **el almacenamiento de datos sobre la vida privada del demandante tenía una base en el derecho rumano**.

55

En cuanto a la exigencia de previsibilidad, el Tribunal recuerda que **una norma es «previsible» cuando está redactada con la suficiente precisión como para permitir a toda persona, con ayuda, dado el caso, de asesores, regular su conducta**. El Tribunal ha indicado la importancia de este concepto en materia de vigilancia secreta en estos términos (Sentencia Malone contra el Reino Unido de 2 de agosto de 1984, retomada en Amann contra Suiza anteriormente citada, ap. 56).

«El Tribunal recuerda que en su opinión, la parte de la frase “prevista por la Ley” no se limita a remitir al derecho interno, sino que concierne también a la calidad de la “ley”; la quiere compatible con la preeminencia del derecho mencionada en el preámbulo del Convenio (...). Implica así – y eso se desprende del objeto y de la finalidad del artículo 8 – que el derecho interno debe ofrecer una cierta protección contra los atentados arbitrarios de los poderes públicos a los derechos garantizados por el apartado 1 (...). Ahora bien, el peligro de arbitrariedad aparece con una nitidez especial allí donde el poder del ejecutivo se ejerce en secreto (...).

(...) Ya que la aplicación de medidas de intervención de las comunicaciones escapa tanto al control de los interesados como al del público, la “ley” iría contra la preeminencia del derecho si el poder de apreciación concedido al ejecutivo no conociera límites. En consecuencia, debe definir la extensión y las modalidades de ejercicio de tal poder con una nitidez suficiente –teniendo en cuenta el fin legítimo perseguido– como para suministrar al individuo una protección adecuada contra la arbitrariedad».

56

Conviene, por lo tanto, examinar la «calidad» de las normas jurídicas invocadas en este caso, buscando en particular si el derecho interno fijaba con una precisión suficiente las condiciones en las que el SRI podía almacenar y utilizar las informaciones relativas a la vida privada del demandante.

57

El Tribunal señala a este respecto, que la Ley núm. 14/1992 prevé, en su artículo 8, que puedan ser recogidas, consignadas y archivadas en expedientes secretos informaciones relativas a la seguridad nacional.

Ahora bien, ninguna disposición del derecho interno fija los límites que hay que respetar en el ejercicio de estas prerrogativas. Así, la legislación interna no define ni el tipo de informaciones que pueden ser registradas, ni las categorías de personas susceptibles de ser objeto de medidas de vigilancia tales como la recogida y la conservación de datos,

ni las circunstancias en las que se pueden tomar dichas medidas, ni el procedimiento a seguir. Asimismo, la ley no fija límites en cuanto a la antigüedad de las informaciones que se poseen ni a la duración de su conservación.

En cuanto al artículo 45, éste habilita al SRI a tomar, para cualquier fin de conservación y de utilización, los archivos que pertenecieron a los antiguos órganos de información competentes en el territorio de Rumania, y autoriza la consulta de los documentos del SRI con la aprobación del director.

El Tribunal señala que este artículo no incluye ninguna disposición explícita y detallada de las personas autorizadas a consultar los expedientes, la naturaleza de estos últimos, el procedimiento a seguir y el uso que se puede dar a las informaciones así obtenidas.

58

También indica que, aunque el artículo 2 de la Ley habilita a las autoridades competentes a autorizar las injerencias necesarias a fin de prevenir y contrarrestar las amenazas para la seguridad nacional, el motivo de tales injerencias no está definido con suficiente precisión.

59

El Tribunal debe también constatar la existencia de garantías adecuadas y suficientes contra los abusos, ya que un sistema de vigilancia secreto destinado a proteger la seguridad nacional supone el riesgo de minar o de destruir la democracia con la excusa de defenderla (Sentencia Klass y otros contra Alemania anteriormente citada, aps. 49-50).

En efecto, para que los sistemas de vigilancia secreta sean compatibles con el artículo 8 del Convenio, deben contener las garantías establecidas por la ley y ser aplicables al control de las actividades de los servicios implicados . Los procedimientos de control deben respetar tan fielmente como sea posible los valores de una sociedad democrática, en especial la preeminencia del derecho, a la que se refiere expresamente el preámbulo del Convenio. Ella implica, entre otras cosas, que una injerencia del Ejecutivo en los derechos del individuo esté sometida a un control eficaz que debe normalmente garantizar, por lo menos en última instancia, el poder judicial, ya que ofrece las mejores garantías de independencia, de imparcialidad y de procedimiento regular (Sentencia Klass y otros anteriormente citada, pgs. 25-26, ap. 55).

60

En este caso, el Tribunal señala que el sistema rumano de recogida y archivo de informaciones no aporta tales garantías, ya que la Ley núm. 14/1992 no prevé ningún procedimiento de control, ya sea mientras la medida ordenada esté en vigor, ya sea posteriormente .

61

Así, el Tribunal estima que el derecho interno no indica con suficiente claridad la extensión y las modalidades de ejercicio del poder de apreciación de las autoridades en el campo considerado.

62

El Tribunal concluye de ello, que **la posesión y la utilización por parte del SRI de informaciones sobre la vida privada del demandante no estaban «previstas por la Ley», lo que basta para constituir un desconocimiento del artículo 8**. Además, en este caso, esta circunstancia impide al Tribunal controlar la legitimidad del fin legítimo perseguido por las medidas ordenadas y, suponiendo que existiera un fin legítimo, si dichas medidas eran «necesarias en una sociedad democrática».

Posteriormente, dicha doctrina, referida en un primer momento a las medidas de vigilancia dirigidas a personas o domicilios concretos, se extiende a los supuestos de vigilancia generalizada, tal y como recuerda la Sentencia Liberty y otros contra Reino Unido de 1 de julio de 2008, pg.31 ap. 62 y 63:

62

Más recientemente, en su decisión de admisibilidad en el asunto Weber y Saravia , anteriormente citado, apartados 93-95, el Tribunal resumió su jurisprudencia sobre la exigencia de la «previsibilidad» de la Ley en este campo como sigue (ver también Sentencia Asociación para la Integración Europea y los Derechos Humanos y Ekimzhiev , anteriormente citada, aps. 75-77):

«93. (...) la previsibilidad en el contexto particular de las medidas secretas de vigilancia, como la intervención de las comunicaciones, no significa que una persona pueda prever cuándo es probable que las autoridades intercepten sus comunicaciones para adaptar su comportamiento en consecuencia –ver, entre otras, Leander [contra Suecia de 26 agosto 1987, serie A núm. 116], pg. 23, ap. 51–. Sin embargo, especialmente cuando la facultad conferida al Ejecutivo se ejerce en secreto, el riesgo de actos arbitrarios es evidente (ver, inter alia , Sentencias Malone, anteriormente citada, pg. 32, ap. 67; Huvig, previamente citada, pgs. 54-55, ap. 29; y Rotaru [contra Rumanía [GS], núm. 28341/1995, ap. 55, TEDH 2000-V]). Por tanto, es esencial tener unas normas claras y detalladas para la interceptación de conversaciones telefónicas, tanto más cuanto que los procedimientos técnicos no cesan de perfeccionarse (ver Sentencias Kopp contra Suiza de 25 marzo 1998, Repertorio 1998-II, pgs. 542-43, ap. 72, y Valenzuela Contreras contra España de 30 julio 1998, Repertorio 1998-V, pgs. 1924-25, ap. 46). El Derecho interno ha de emplear términos suficientemente claros para indicar a todos de manera suficiente en qué circunstancias y bajo qué condiciones habilita a los poderes públicos a tomar tales medidas (Sentencias Malone , ibid.; Kopp , previamente

citada, pg. 541, ap. 64; Huvig , previamente citada, pgs. 54-55, ap. 29; y Valenzuela Contreras , *ibid.*).

94. Además, como la aplicación de las medidas de vigilancia secreta de las comunicaciones escapa tanto al control de los interesados como del público en general, la «Ley» pugnaría con la supremacía del derecho de que se trata si la facultad discrecional concedida a la Administración no tuviera límites. Por tanto, la Ley ha de indicar el alcance y las modalidades de ejercicio de dicha facultad con suficiente claridad –teniendo en cuenta la legítima finalidad que se persigue– para facilitar así al individuo la adecuada protección contra las injerencias arbitrarias (ver, entre otras, Sentencias previamente citadas Malone, pgs. 32-33, ap. 68; Leander, pg. 23, ap. 51; y Huvig , pp. 54-55, ap. 29).

95. En su jurisprudencia sobre medidas secretas de vigilancia, el Tribunal ha desarrollado unas garantías mínimas, necesarias para evitar los abusos, que deben figurar en la Ley: la naturaleza de las infracciones que puedan dar lugar a una orden de interceptación, la definición de las categorías de personas susceptibles de ser sometidas a vigilancia telefónica judicial; la fijación de un límite a la duración de la ejecución de la medida; el procedimiento a seguir para el examen, uso y conservación de los datos obtenidos; las precauciones que se han de tomar al comunicar los datos a otras partes; y las circunstancias en las que se puede o se debe realizar el borrado o la destrucción de las cintas (ver, *inter alia* , Sentencias, anteriormente citadas, Huvig , pg. 56, ap. 34; Amann , ap. 76; Valenzuela Contreras, pgs. 1924-25, ap. 46; y Sentencia Prado Bugallo contra España , núm. 58496/2000, ap. 30, 18 febrero 2003)».

63

Es cierto que los anteriores requisitos fueron desarrollados primeramente por el Tribunal en relación con unas medidas de vigilancia dirigidas a unas personas o domicilios específicos [el equivalente, en el Reino Unido, al régimen del artículo 3(1)]. Sin embargo, el asunto Weber y Saravia trata de la «vigilancia estratégica» generalizada en lugar del control de las personas (citado anteriormente, apartado 18 *supra*). El Tribunal no considera que exista ninguna razón para aplicar unos principios diferentes respecto a la accesibilidad y claridad de las normas que rigen la intervención de las comunicaciones individuales, de un lado, y a programas de vigilancia más generales, de otro. El enfoque del Tribunal en cuanto a la exigencia de la previsibilidad en este ámbito ha evolucionado, por tanto, desde que la Comisión entró a considerar el esquema de vigilancia del Reino Unido en la citada Decisión Christie contra Reino Unido.

Recientemente, en la Sentencia del caso Bou Hassoun contra Bulgaria. Sentencia de 6 octubre 2020, referida a un supuesto de expulsión de un ciudadano extranjero por presuntos motivos de seguridad nacional y la

separación de su familia, basada en información clasificada y sometida a un control judicial meramente formal, el TEDH señala lo siguiente:

30

El Tribunal señala, en primer lugar, que la presente demanda es similar a una serie de asuntos anteriores contra Bulgaria relativos a la expulsión de extranjeros por presuntos motivos de seguridad nacional (véanse, por ejemplo, C.G. y otros contra Bulgaria (TEDH 2008, 27) , núm. 1365/07, 24 de abril de 2008; Kaushal y otros contra Bulgaria (JUR 2010, 301157) , núm. 1537/08, 2 de septiembre de 2010; Raza contra Bulgaria (JUR 2010, 41195) , núm. 31465/08, 11 de febrero de 2010; así como Grabchak contra Bulgaria (JUR 2017, 142996) [Comité], núm. 55950/09, 1 de junio de 2017; Kurilovich y otros contra Bulgaria (JUR 2017, 142990) [Comité], núm. 45158/09, 1 de junio de 2017; y Gapaev y otros contra Bulgaria (JUR 2017, 142995) [Comité], núm. 41887/09, 1 de junio de 2017).

(a) Artículo 8 del Convenio

31

El Tribunal señala que las partes discrepan en cuanto a si se había producido una injerencia en el derecho del demandante al respeto de su vida familiar (véanse apds. 26 y 27). Señala también, en primer lugar, que el Gobierno presentó una carta de la Dirección de Migración en la que se indicaba que las autoridades habían acompañado al demandante al puesto de control fronterizo para garantizar su regreso a Turquía como parte de la ejecución de la orden de expulsión (véase ap. 10). El Tribunal considera que esto representa un reconocimiento expreso de las autoridades de la injerencia del Estado en la ejecución de la orden de expulsión del demandante. El Tribunal observa que las afirmaciones del Gobierno de que el demandante había firmado un formulario para su retorno voluntario y había cooperado en la ejecución de la orden de expulsión no están respaldadas por las copias de los documentos correspondientes (véase ap. 10). Incluso aceptando que el demandante había cooperado efectivamente y había elegido un tercer país seguro de retorno, esa circunstancia no cambia el hecho de que, según la documentación aportada al expediente y el virtud de la legislación interna (véase ap. 12), la orden de expulsión en cuestión era de ejecución inmediata, confirmada por la resolución firme del Tribunal Supremo Administrativo de 30 de mayo de 2016 y ejecutada por las autoridades competentes (véanse apds. 7 y 9). Además, la prohibición de volver a entrar en Bulgaria en cinco años sigue vigente (véase ap. 7). En tales circunstancias, el Tribunal considera que las medidas establecidas en la orden de expulsión ejecutoria, de 22 de octubre de

2015, así como el retorno del demandante a la República de Turquía el 24 de noviembre de 2015, debe ser considerado como una injerencia en su vida familiar (véanse, *mutatis mutandis*, *Al Nashif contra Bulgaria* (JUR 2002, 169254) , núm. 50963/99, ap. 115, 20 de junio de 2002; y *Lupsa contra Rumania* (JUR 2006, 177060) , núm. 10337/04, apds. 26-27, TEDH 2006-VII).

32

Queda por determinar si dicha injerencia cumplía los requisitos del párrafo 2 del artículo 8. Por lo tanto, es necesario determinar si era “conforme a la ley”, motivada por uno o más de los objetivos legítimos establecidos en ese párrafo, y “necesaria en una sociedad democrática” (véase la sentencia *Al-Nashif* (JUR 2002, 169254) , precitada, ap. 116).

33

En cuanto al primero de estos requisitos, es decir, que la injerencia debe ser “conforme a la ley”, el Tribunal señala que, en asuntos anteriores similares contra Bulgaria (véase ap. 30), constató que las expulsiones en cuestión ordenadas en virtud de presuntos motivos de seguridad nacional no cumplían con las normas del Convenio debido a que la legislación, los procedimientos y la práctica pertinentes no ofrecían siquiera un mínimo grado de protección contra el carácter arbitrario. En concreto, en *C.G. y otros contra Bulgaria* (TEDH 2008, 27) (precitada, apds. 42-50), el Tribunal declaró, en concreto, que los órganos jurisdiccionales nacionales no habían examinado si el ejecutivo había podido demostrar la existencia de hechos concretos que sirvieran de base para su apreciación de que el demandante suponía una amenaza para la seguridad nacional. El Tribunal declaró, además, que los tribunales nacionales habían aplicado un enfoque formalista y habían dejado a un organismo gubernamental una facultad plena e incontrolada para certificar, basándose poco más que en sus propias declaraciones generales, que un extranjero suponía una amenaza para la seguridad nacional y tenía que ser expulsado. Dado que tales “certificaciones” se consideraron más allá de cualquier control judicial significativo, se consideró, por tanto, que no había ninguna garantía contra el carácter arbitrario (véanse también *Kaushal y otros* (JUR 2010, 301157) , apds. 28-34; y *Grabchak* (JUR 2017, 142996) , apds. 35-40, ambos precitados).

34

El presente asunto es muy similar. La orden de expulsión del demandante se basó en declaraciones que le implicaban en actividades relacionadas con el transporte ilegal de extranjeros y, que por lo tanto,

representaba una amenaza para la seguridad nacional (véase ap. 9). La orden de expulsión parece ser el resultado de una evaluación puramente interna por parte del Servicio Nacional de Seguridad, realizada en base a pruebas no divulgadas, contenidas en una propuesta clasificada. Además, el Tribunal Supremo Administrativo desestimó la solicitud del demandante de una revisión judicial de la orden de expulsión, sin llevar a cabo ningún control significativo de las alegaciones del ejecutivo, afirmando simplemente que la orden en cuestión no vulneraba la ley, ya que los datos recogidos en el procedimiento administrativo, en concreto los mencionados en la propuesta (véase ap. 7), eran suficientes para justificar la conclusión de que representaba una amenaza para la seguridad nacional (véase ap. 9). Su enfoque demasiado formal significaba que no proporcionaba ningún control independiente con sentido de las alegaciones del ejecutivo.

35

En consecuencia, como en los casos precedentes mencionados anteriormente, a pesar de disponer de la posibilidad formal de solicitar la revisión judicial de las medidas en cuestión, el demandante no dispuso de un mínimo grado de protección contra el carácter arbitrario inherente al concepto de legalidad del Convenio. Esto significa que la injerencia en su derecho al respeto de su vida familiar y privada no fue “conforme a la ley”, como requiere el artículo 8.2.

36

Vista esta conclusión, no es necesario que el Tribunal examine el resto de cuestiones, en especial si se perseguían uno o más legítimos objetivos o si la medida denunciada era necesaria en una Sociedad democrática (véase C.G. y otros contra Bulgaria (TEDH 2008, 27) , ap. 49; y Kaushal y otros (JUR 2010, 301157) , ap. 33, ambos precitados).

37

En consecuencia, ha habido una violación del artículo 8 del Convenio.

B) Fin Legítimo

Dentro de los fines legítimos se encuentra, sin duda alguna, la seguridad nacional, prevista específicamente en el artículo 8.2. del Convenio. Consecuentemente, el Tribunal, en la Sentencia del Caso DEP contra Turquía, de 10 de diciembre de 2002 (pg. 14 ap.36) considera como uno de los fines

legítimos que legitiman la injerencia la protección de la integridad territorial y, de esta forma, la «seguridad nacional».

En este mismo sentido, en la Sentencia (G.S.) Caso Kuric y otros contra Eslovenia de 26 de junio de 2012 (pg. 83 ap. 353) el Tribunal considera que con la promulgación de la legislación de independencia, que contenía una opción para todos los ciudadanos de otras repúblicas de la antigua República Federativa Socialista de Yugoslavia residentes en Eslovenia, para adquirir la nacionalidad eslovena en un corto período de tiempo, las autoridades eslovenas trataron de crear un "conjunto de ciudadanos eslovenos" y por tanto, proteger los intereses de la seguridad nacional del país (véase, *mutatis mutandis*, Slivenko, op.cit. , apartados 110 y 111), siendo por tanto, un objetivo legítimo de conformidad con el artículo 8.2 del Convenio.

C) Necesaria en una sociedad democrática.

Para determinar si una limitación es «necesaria en una sociedad democrática», el Tribunal ha de considerar si, a la vista del caso en su conjunto, las razones aducidas para justificar esta medida fueron relevantes y suficientes a efectos del apartado 2 del artículo 8 del Convenio (véase Hoppe contra Alemania núm. 28422/1995, ap. 48, de 5 diciembre 2002). La noción de necesidad implica una necesidad social imperiosa; en concreto, la medida empleada debe ser proporcionada al fin legítimo perseguido. Además, el alcance del margen de apreciación de que gocen las autoridades nacionales dependerá no solamente de la naturaleza del fin o de la restricción, sino también de la naturaleza del derecho afectado.

Por consiguiente, se requiere un análisis del caso en su conjunto, atendiendo a todas las circunstancias concurrentes. Como recuerda la Sentencia Caso DEP contra Turquía, de 10 de diciembre de 2002 (pg. 18 ap.48): el Tribunal no debe limitarse a examinar si el Estado demandado ha usado dicho poder de buena fe, con cuidado y de forma razonable: deberá considerar la injerencia enjuiciada a la luz del conjunto del caso para determinar si era «proporcional al fin legítimo perseguido» y si los motivos invocados por las autoridades nacionales para justificarla eran «pertinentes y suficientes». Al hacerlo, el Tribunal deberá convencerse de que las autoridades han aplicado normas conformes a los principios consagrados en el Convenio y ello, también, basándose en una apreciación aceptable de los hechos pertinentes (ver, «mutatis mutandis», Sentencias Ahmed y otros contra Reino Unido de 2 septiembre 1998, Repertorio 1998-VI, pg. 2377-2378, ap. 55 y Goodwin contra Reino Unido de 27 marzo 1996, Repertorio 1996-II, pg. 500-501, ap. 40).

A este respecto, el Tribunal ha considerado que la disponibilidad de soluciones alternativas, en sí misma, no convierte en injustificada la injerencia en el derecho sino que constituye un factor, entre otros, que es pertinente para

determinar si los medios elegidos pueden ser considerados razonables y apropiados para conseguir el fin legítimo perseguido. Siempre que la injerencia se mantenga dentro de estos límites no es obligación del Tribunal decir si la medida impugnada representa la mejor solución para tratar el problema o si la discrecionalidad del Estado debería haberse ejercido de otra manera (véase, *mutatis mutandis*, James y otros contra el Reino Unido, pg. 35, ap. 51).

Asimismo, la importancia de tal derecho para la persona debe ser tenida en cuenta en el momento de determinar el alcance del margen de apreciación permitido al Gobierno (véase Gillow contra el Reino Unido anteriormente citada [TEDH 1986, 15], pg. 22, ap. 55).

A este respecto, la Sentencia (G.S.) del Caso S. y Marper contra Reino Unido de 4 de diciembre de 2008 (pg.41 ap.101 a 104) analiza esta cuestión refiriéndose expresamente a la importancia del derecho a la protección de datos de carácter personal:

101

Una injerencia se considera «necesaria en una sociedad democrática» para alcanzar un fin legítimo si responde a una «necesidad social imperiosa» y en particular, si es proporcionada al fin legítimo perseguido y si los motivos invocados por las autoridades nacionales para justificarla parecen «pertinentes y suficientes». Si bien corresponde en primer lugar a las autoridades internas juzgar si se cumplen todas estas condiciones, es el Tribunal quien tiene que resolver definitivamente la cuestión de la necesidad de la injerencia respecto a las exigencias del Convenio (Sentencia Coster contra el Reino Unido [TEDH 2001, 44] [GS], núm. 24876/1994, ap. 104, 18 enero 2001, y referencias citadas).

102

Se ha de reconocer al respecto cierto margen de apreciación a las autoridades internas competentes. El alcance de este margen es variable y depende de algunos factores, como el carácter del derecho en cuestión garantizado por el Convenio (RCL 1999, 1190, 1572), su importancia para la persona afectada, el carácter de la injerencia y su finalidad. Este margen es más restringido cuanto mayor es la importancia del derecho de que se trata para garantizar al individuo el goce efectivo de los derechos fundamentales o de orden «íntimo» que le son reconocidos (Sentencia Connors contra el Reino Unido, núm. 66746/2001, ap. 82, 27 mayo 2004, y referencias citadas). Cuando se trata de un aspecto particularmente importante de la existencia o identidad de una persona, el margen de que dispone el Estado es restringido (Sentencia Evans contra el Reino Unido [GS], núm. 6339/2005, ap. 77, TEDH 2007–...). Por el contrario, cuando no hay consenso en el seno de los Estados miembros del Consejo de Europa, ya sea sobre la importancia relativa del interés en juego o sobre los mejores medios de protegerlo, el margen de apreciación es

mayor (Sentencia Dickson contra el Reino Unido [GS], núm. 44362/2004, ap. 78, TEDH 2007–...).

103

La protección de los datos de carácter personal juega un papel fundamental en el ejercicio del derecho al respeto de la vida privada y familiar consagrado por el artículo 8 del Convenio. Por tanto, la legislación interna debe ofrecer unas garantías apropiadas que impidan toda utilización de datos de carácter personal que no sea conforme a las garantías previstas en dicho artículo (ver, *mutatis mutandis*, Sentencia Z contra Finlandia, previamente citada, ap. 95). La necesidad de disponer de tales garantías se hace sentir aún más cuando se trata de proteger los datos de carácter personal sometidos a un tratamiento automático, en particular cuando estos datos son utilizados con fines policiales. El derecho interno ha de asegurar, concretamente, que estos datos sean pertinentes y no excesivos en relación a las finalidades para las que son registrados y que se conserven bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado (preámbulo y artículo 5 del Convenio sobre la protección de datos y principio 7 de la Recomendación R[87]15 del Comité de Ministros destinada a reglamentar el uso de los datos de carácter personal en el sector de la policía). El derecho interno ha de contener también garantías que protejan eficazmente los datos de carácter personal registrados contra los usos impropios y abusivos (ver, en particular, el artículo 7 del Convenio sobre la protección de datos). Las consideraciones que preceden sirven muy especialmente cuando se trata de proteger unas categorías particulares de datos más sensibles (artículo 6 del Convenio sobre la protección de datos), concretamente los datos de ADN que, en la medida en que contienen el patrimonio genético de la persona, son de gran importancia tanto para ella misma como para su familia (Recomendación núm. R [92] 1 del Comité de Ministros sobre la utilización de los análisis de ADN en el marco del sistema judicial penal).

104

El interés de las personas afectadas y del conjunto de la comunidad de que se protejan los datos de carácter personal y, concretamente, los relativos a las huellas dactilares y genéticas, puede desaparecer ante el interés legítimo que constituye la prevención del delito (artículo 9 del Convenio sobre la protección de datos). Sin embargo, habida cuenta del carácter intrínsecamente privado de esta información, el Tribunal debe proceder a un examen riguroso de cualquier medida adoptada por un Estado para autorizar su conservación y utilización por las autoridades sin el consentimiento de la persona afectada (ver, *mutatis mutandis*, Sentencia Z contra Finlandia, previamente citada, ap. 96).

Por otro lado, nuestro Tribunal Constitucional tiene declarado que el derecho fundamental a la protección de datos personales recogido en el artículo 18.4 de la Constitución, como todos los derechos fundamentales, es un derecho limitado.

En este sentido, la STC 292/2000, de 30 de noviembre, después de configurar el derecho fundamental a la protección de datos personales como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso, analiza los límites del mismo, señalando lo siguiente:

“Más concretamente, en las Sentencias mencionadas relativas a la protección de datos, este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, F. 7; 196/1987, de 11 de diciembre [RTC 1987, 196] , F. 6; y respecto del art. 18, la STC 110/1984, F. 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE. La primera constatación que debe hacerse, que no por evidente es menos capital, es que la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental. Los derechos fundamentales pueden ceder, desde luego, ante bienes, e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero [RTC 1994, 57] , F. 6; 18/1999, de 22 de febrero [RTC 1999, 18] , F. 2).

Justamente, si la Ley es la única habilitada por la Constitución para fijar los límites a los derechos fundamentales y, en el caso presente, al derecho fundamental a la protección de datos, y esos límites no pueden ser distintos a los constitucionalmente previstos, que para el caso no son otros que los derivados de la coexistencia de este derecho fundamental con otros derechos y bienes jurídicos de rango

constitucional, el apoderamiento legal que permita a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, sólo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos. Por tanto, si aquellas operaciones con los datos personales de una persona no se realizan con estricta observancia de las normas que lo regulan, se vulnera el derecho a la protección de datos, pues se le imponen límites constitucionalmente ilegítimos, ya sea a su contenido o al ejercicio del haz de facultades que lo componen. Como lo conculcará también esa Ley limitativa si regula los límites de forma tal que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que la Constitución le otorga. Y así será cuando la Ley, que debe regular los límites a los derechos fundamentales con escrupuloso respeto a su contenido esencial, se limita a apoderar a otro Poder Público para fijar en cada caso las restricciones que pueden imponerse a los derechos fundamentales, cuya singular determinación y aplicación estará al albur de las decisiones que adopte ese Poder Público, quien podrá decidir, en lo que ahora nos interesa, sobre la obtención, almacenamiento, tratamiento, uso y cesión de datos personales en los casos que estime convenientes y esgrimiendo, incluso, intereses o bienes que no son protegidos con rango constitucional [...]". (Fundamento Jurídico 11)

"De un lado, porque 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 [RTC 2000, 104] , F. 8 y las allí citadas) y, además, han de ser proporcionadas al fin perseguido con ellas (SSTC 11/1981, F. 5, y 196/1987, F. 6). Pues en otro caso incurrirían en la arbitrariedad proscrita por el art. 9.3 CE.

De otro lado, aun teniendo un fundamento constitucional y resultando proporcionadas las limitaciones del derecho fundamental establecidas por una Ley (STC 178/1985 [RTC 1985, 178]), éstas pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad en los propios límites que imponen y su modo de aplicación. Conclusión que se corrobora en la jurisprudencia del Tribunal Europeo de Derechos Humanos que ha sido citada en el F. 8 y que aquí ha de darse por reproducida. Y ha de señalarse, asimismo, que no sólo lesionaría el principio de seguridad jurídica (art. 9.3 CE), concebida como certeza sobre el ordenamiento aplicable y expectativa razonablemente fundada de la persona sobre cuál ha de ser la actuación del poder aplicando el Derecho (STC 104/2000, F. 7, por todas), sino que al mismo tiempo dicha Ley estaría lesionando el contenido esencial del derecho fundamental así restringido, dado que la forma en que se

han fijado sus límites lo hacen irreconocible e imposibilitan, en la práctica, su ejercicio (SSTC 11/1981, F. 15; 142/1993, de 22 de abril [RTC 1993, 142] , F. 4, y 341/1993, de 18 de noviembre [RTC 1993, 341] , F. 7). De suerte que la falta de precisión de la Ley en los presupuestos materiales de la limitación de un derecho fundamental es susceptible de generar una indeterminación sobre los casos a los que se aplica tal restricción. Y al producirse este resultado, más allá de toda interpretación razonable, la Ley ya no cumple su función de garantía del propio derecho fundamental que restringe, pues deja que en su lugar opere simplemente la voluntad de quien ha de aplicarla, menoscabando así tanto la eficacia del derecho fundamental como la seguridad jurídica [...]”. (Fundamento Jurídico 15).

“Más concretamente, en relación con el derecho fundamental a la intimidad hemos puesto de relieve no sólo la necesidad de que sus posibles limitaciones estén fundadas en una previsión legal que tenga justificación constitucional y que sean proporcionadas (SSTC 110/1984, F. 3, y 254/1993, F. 7) sino que la Ley que restrinja este derecho debe expresar con precisión todos y cada uno de los presupuestos materiales de la medida limitadora. De no ser así, mal cabe entender que la resolución judicial o el acto administrativo que la aplique estén fundados en la Ley, ya que lo que ésta ha hecho, haciendo dejación de sus funciones, es apoderar a otros Poderes Públicos para que sean ellos quienes fijen los límites al derecho fundamental (SSTC 37/1989, de 15 de febrero [RTC 1989, 37], y 49/1999, de 5 de abril [RTC 1999, 49]).

De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido. Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación. [...] (Fundamento Jurídico 16)”.

Más recientemente, analizando igualmente los límites al derecho fundamental a la protección de datos personales, la sentencia núm. 76/2019 de 22 mayo después de recordar que “A la vista de los potenciales efectos intrusivos en el derecho fundamental afectado que resultan del tratamiento de

datos personales, la jurisprudencia de este Tribunal le exige al legislador que, además de cumplir los requisitos anteriormente mencionados, también establezca 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. En este fundamento jurídico precisaremos la naturaleza y el alcance de este específico requisito constitucional”, analiza cuál es la norma que debe contener las citadas garantías:

“Por tanto, la resolución de la presente impugnación exige que aclaremos una duda suscitada con respecto al alcance de nuestra doctrina sobre las garantías adecuadas, que consiste en determinar si las garantías adecuadas frente al uso de la informática deben contenerse en la propia ley que autoriza y regula ese uso o pueden encontrarse también en otras fuentes normativas.

La cuestión solo puede tener una respuesta constitucional. 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 art. 53.1 CE (RCL 1978, 2836) para el legislador de los derechos fundamentales: la reserva de ley para la regulación del ejercicio de los derechos fundamentales reconocidos en el capítulo segundo del título primero de la Constitución y el respeto del contenido esencial de dichos derechos fundamentales.

Según reiterada doctrina constitucional, la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de derechos fundamentales, sino que también es preciso, conforme tanto a exigencias denominadas -unas veces- de predeterminación normativa y -otras- de calidad de la ley como al respeto al contenido esencial del derecho, que en esa regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de medidas restrictivas de derechos fundamentales. Ese mandato de predeterminación respecto de elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares” (Fundamento Jurídico 8).

Por otro lado, y en lo que se refiere al principio de proporcionalidad la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero, recuerda lo siguiente:

“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).”

De acuerdo con la citada doctrina constitucional, los límites al derecho fundamental a la protección de datos personales deben establecerse por una norma con rango de ley, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, definiendo todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas.

Por consiguiente, cumpliéndose tanto los requisitos de previsión en una norma con rango de ley como el de la legítima finalidad derivada de las necesidades de la seguridad nacional, la cuestión principal radica en establecer la proporcionalidad de la injerencia en el derecho fundamental, para lo que es imprescindible introducir en la regulación legal las garantías oportunas, lo que debe valorarse adecuadamente por el legislador.

A este respecto, partiendo de que el sujeto al que se refieran los datos de carácter personal se va a ver privado de los derechos específicos que establece la normativa sobre protección de datos personales, como son, por ejemplo, el derecho de información o el derecho de acceso, una primera garantía es la aplicación estricta de los supuestos en los que procede la clasificación en alguno de los grados que la norma contempla, a la que se refiere expresamente la Exposición de motivos: *“la defensa y seguridad nacional no deben servir como elemento legitimador de la ocultación de cualquier información, sino que ha de ponderarse caso por caso la necesidad de llevar adelante su clasificación de acuerdo con los fines que persigue la Ley, haciendo de este proceso la excepción y no la regla”*.

Asimismo, y sin ánimo exhaustivo, además de las tradicionales garantías para la adecuada protección de la información clasificada derivadas de las limitaciones en el acceso a la misma basado en la “necesidad de conocer”, la previa obtención de las habilitaciones de seguridad correspondientes o la existencia de un deber de reserva, el texto del anteproyecto incluye nuevas garantías, como es el control jurisdiccional de la clasificación regulado en el artículo 37 del anteproyecto, la regulación del acceso a la información clasificada en el marco de un proceso jurisdiccional contenida en su artículo 38 o el establecimiento de un régimen sancionador específico.

III

Para concluir, debe resaltarse que en los supuestos en los que se proceda a la desclasificación de la información y a su archivo o digitalización, previsto en el artículo 31 del anteproyecto, la misma dejará de estar sometida a la normativa sobre materias clasificadas, por lo que el correspondiente tratamiento de datos personales quedará sometido a la normativa de protección de datos personales y, en su caso, a la normativa sobre transparencia y acceso a la información pública, así como a la normativa archivística correspondiente.