ESTUDIOS PENALES Y CRIMINOLÓGICOS

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

Artículos doctrinales

CENTRO NACIONAL DE INTELIGENCIA, DATOS PERSONALES Y PROCESO PENAL: UN TRINOMIO IMPERFECTO[1]

NATIONAL INTELLIGENCE CENTER, PERSONAL DATA AND CRIMINAL PROCEEDINGS: AN IMPERFECT TRINOMIAL

Mª Ángeles Catalina Benavente[1,a]

[1] Profesora Contratada Doctora. Área de Derecho Procesal. Departamento de Derecho Público Especial y de la Empresa. Facultad de Derecho. Avenida Ángel Echeverri s/n. 15782. Universidad de Santiago de Compostela, España

[a]angeles.catalina@usc.es

Resumen

El Centro Nacional de Inteligencia cada vez tiene acceso a más datos personales de los ciudadanos. Al mismo tiempo, los ficheros propiedad del CNI se encuentran expresamente excluidos del ámbito de aplicación de la normativa de protección de datos de carácter personal. La eventual confluencia de las investigaciones de seguridad del CNI y las investigaciones policiales, a través del flujo de datos del primero al segundo, supone una amenaza a los derechos procesales. La única manera de poner fin a esta amenaza es regular esta cesión, estableciendo las limitaciones procedentes y fijando las consecuencias de la incorporación de datos procedentes del CNI a un futuro proceso penal.

Palabras clave: Centro Nacional de Inteligencia; protección de datos; cesión de datos personales; seguridad nacional; proceso penal.

Abstract

The National Intelligence Centre has access to more and more citizens' personal data. At the same time, the files owned by the National Intelligence Center are expressly excluded from the scope of application of personal data protection regulations. The possible confluence of intelligence investigations and police investigations, through the flow of data from the former to the latter, poses a threat to procedural rights. The only way to put an end to this threat is to regulate this transfer, establishing the appropriate limitations and the consequences derived from the incorporation of data from the CNI into a future criminal process.

Keywords: Intelligence National Center; data protection; transmission of personal data; national security; criminal proceedings.

[1] Este trabajo ha sido realizado en el marco del Proyecto PID2022-137826NB-I00, financiado por el Ministerio de Ciencia e Innovación – Agencia Estatal de Investigación, sobre «Datos personales e información en la era digital: desafíos en su obtención y uso en los procesos judiciales y en los procedimientos sancionadores» (DATER).

1. Introducción: delimitación del objeto de estudio

Desde el mes de abril de 2022 el Centro Nacional de Inteligencia, en adelante CNI, ha acaparado la atención mediática como consecuencia de la situación generada tras conocerse el espionaje llevado a cabo a un elevado número de políticos independentistas catalanes, que no solo provocó el cese de la directora del CNI[2] , sino que ha vuelto a traer al debate público la discusión sobre el control judicial previo de las actuaciones del CNI cuando implican, principalmente, la posible vulneración del derecho al secreto de las comunicaciones (art. 18.3 CE). A lo largo de estos meses hemos leído y escuchado opiniones de diverso signo en relación con las facultades del CNI en el marco de la realización de investigaciones de seguridad que impliquen restricción de derechos fundamentales y se ha reabierto la cuestión de cómo se están gestionando en nuestros días los riesgos y amenazas a la seguridad nacional, y si las técnicas y medidas de lucha contra esos riesgos son proporcionadas.

Al hilo de estas discusiones creemos que es importante extender el debate sobre las actuaciones y facultades del CNI y reflexionar sobre un aspecto muy concreto, a la vez que preocupante, relacionado con el ejercicio de las funciones encomendadas a uno de los órganos que forman parte de los servicios de inteligencia del Estado: la creciente acumulación de datos personales por el CNI, avalada por el propio legislador, que, sin embargo, no va acompañada de un adecuado régimen de protección de los datos personales cuando se encuentran en poder de este organismo[3] . Esta preocupación se convierte en inquietud, o incluso en temor, cuando, como tendremos oportunidad de analizar en este trabajo, a la ausencia de un régimen específico de protección de los datos personales en poder del CNI hay que unir la posibilidad, reconocida por la Sala de lo Penal del Tribunal Supremo[4] , de que material procedente del CNI se pueda incorporar a un proceso penal. La posible confluencia de las investigaciones de seguridad llevadas a cabo por el CNI y las investigaciones criminales llevadas a cabo por las Fuerzas y Cuerpos de Seguridad del Estado puede estar generando un espacio de impunidad y posible restricción de derechos fundamentales al que no podemos permanecer indiferentes. El foco de atención, por tanto, hay que ponerlo en las garantías que rodean la obtención del dato personal por el CNI, para luego analizar las que rodean su tratamiento entendido en sentido amplio: conservación, supresión y cesión de los datos personales en poder del CNI a las autoridades con competencias como policía judicial.

El legislador español ha realizado un esfuerzo importante en los últimos años, a instancia esencialmente del legislador europeo, en orden a garantizar la creación de diferentes tipos de ficheros destinados a la conservación generalizada de datos personales de muy diferente tipo

---

[2] El 11 de mayo de 2022 se publicó el Real Decreto 351/2022, de 10 de mayo, por el que se dispone el cese de doña Paz Esteban López como Secretaria de Estado Directora del CNI.

[3] La preocupación por esta acumulación de datos personales por los servicios de inteligencia de los Estados miembros ha sido puesta de manifiesto en diversos foros, en los que se incide en que los avances tecnológicos permiten que los servicios de inteligencia tengan acceso cada vez a más cantidad de datos personales, al tiempo que, en muchas jurisdicciones, los servicios de inteligencia quedan fuera del ámbito de aplicación de las leyes de protección de datos (Ver *Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. El derecho a la privacidad en la era digital*, de 3 de agosto de 2018, versión en castellano, apartado 34, p. 11). Sobre la base de que la defensa de la seguridad nacional constituye una materia que escapa a la regulación del Derecho de la Unión (art. 4.2 del Tratado de la Unión Europea), y de que son los Estados miembros los competentes para adoptar las normas que estimen necesarias en orden a garantizar su seguridad nacional, parece haberse creado un espacio de impunidad para los servicios de inteligencia.

[4] STS núm. 1094/2010, de 10 de diciembre (ECLI:ES:TS:2010:7056).

con finalidades esencialmente preventivas y represivas. A pesar de las críticas que la recogida masiva de datos personales con fines penales ha generado tanto en la opinión pública como en la doctrina científica[5] , así como las limitaciones que a esta recogida están tratando de establecer el Tribunal Europeo de Derechos Humanos (TEDH), el Tribunal de Justicia de la Unión Europea (TJUE), y los propios órganos jurisdiccionales españoles, lo cierto es que en España contamos ya con un significativo cuerpo legislativo que permite la recopilación y conservación con fines penales de un importante y amplio grupo de datos personales: 1) la LO 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN, (en adelante, LOADN), que permite la recogida de los datos relativos al ADN; 2) la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, la recogida de estos datos; 3) la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, que prevé la recogida de los datos financieros; 4) la LO 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, que regula la recogida de los datos relativos al registro de nombre de los pasajeros, los conocidos como datos PNR por su acrónimo en inglés, *Passenger Name Record* (en adelante, LOPNR); y 5) la LO 9/2022, de 28 de julio, por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales, de modificación de la Ley Orgánica 8/1980, de 22 de septiembre, de Financiación de las Comunidades Autónomas y otras disposiciones conexas y de modificación de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Todas estas normas incluyen entre las autoridades competentes para recibir los datos personales recopilados con fines penales al CNI, con el objetivo de que el CNI pueda usar estos datos para el cumplimiento de las funciones que legalmente tiene asignadas en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (en adelante, LCNI)[6] . El artículo 1 de esta ley señala que la función principal del CNI es «facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evaluar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones»[7] .

---

[5] La doctrina ha sido especialmente crítica con la expansión que se ha llevado a cabo de las bases de datos privadas o públicas con la finalidad de servir a la prevención y persecución de delitos, toda vez que imponen la obligación de conservación generalizada e indiscriminada de multitud de datos e información personal, sin que ni siquiera se exija la existencia de indicios o sospechas sobre los interesados cuyos datos se recaban y conservan por largos periodos de tiempo. Ver por todos MONTORO SÁNCHEZ, J.A., *Uso y cesión de datos de carácter personal en el proceso penal*, Thomson Reuters-Aranzadi, 2022, p. 332 y la bibliografía allí citada.

[6] Esta Ley, aprobada casi veinticinco años después de la Constitución, es la primera norma con rango de ley que regula la actuación de los servicios de inteligencia del Estado español, y surge con la vocación de ofrecer a la sociedad española «unos servicios de inteligencia eficaces, especializados y modernos, capaces de afrontar los nuevos retos del actual escenario nacional e internacional, regidos por los principios de control y pleno sometimiento al ordenamiento jurídico», tal y como señala la Exposición de motivos. La disposición adicional segunda de la LCNI suprimió el Centro Superior de Información de la Defensa, que se había creado con anterioridad a la Constitución, por Real Decreto 1558/1977, de 4 de julio, por el que se reestructuran determinados Órganos de la Administración Central del Estado y se incorpora dentro del Ministerio de Defensa.

[7] Los objetivos del CNI son aprobados anualmente por el Gobierno mediante la Directiva de Inteligencia, que tiene carácter secreto (art. 3 LCNI). Para el cumplimiento de sus objetivos el CNI puede llevar a cabo cualesquiera de las funciones enumeradas en el artículo 4 LCNI: «a) Obtener, evaluar e interpretar información y

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

A ello hay que añadir, además, que el artículo 5.5 LCNI parece otorgar vía libre al CNI para acceder a los datos personales que hayan podido ser recopilados por las entidades públicas o privadas para el desarrollo de sus funciones: «Para el cumplimiento de sus funciones, el Centro Nacional de Inteligencia podrá llevar a cabo investigaciones de seguridad sobre personas o entidades en la forma prevista en esta Ley y en la Ley Orgánica reguladora del control judicial previo del Centro Nacional de Inteligencia. Para la realización de estas investigaciones podrá recabar de organismos e instituciones públicas y privadas la colaboración precisa».

Sin embargo, ni la inclusión del CNI entre las autoridades competentes para recibir datos personales recopilados con fines penales, ni el deber general de colaboración con el CNI que se impone a las entidades públicas o privadas, van acompañados de un régimen jurídico de protección aplicable a los datos personales en poder del CNI. La LO 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, y la LO 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, excluyen expresamente de su ámbito de aplicación el tratamiento de datos personales sometidos a la normativa sobre materias clasificadas (arts. 2.2.c) y 2.3.d, respectivamente). La Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, en adelante LOCNI, y a pesar del desarrollo que ha tenido en los últimos años la protección de los derechos a la intimidad y a la protección de datos personales como consecuencia del incremento exponencial que los avances tecnológicos han supuesto para la afectación de esos derechos fundamentales, también ha permanecido ajena a cualquier actualización, renovación, o incluso podría hasta decirse que preocupación, por el tratamiento de datos personales efectuados por el CNI. Su interés se sigue centrando exclusivamente en el derecho a la inviolabilidad del domicilio (art. 18.2 CE) y el derecho al secreto de las comunicaciones (art. 18.3 CE).

El análisis que vamos a llevar a cabo en las páginas siguientes sobre la recopilación y tratamiento de datos personales por el CNI, y la posible incorporación de estos datos a un proceso penal, parte de tres puntos sobre los que no vamos a entrar en discusión, sin perjuicio de que puntualmente remitamos al lector a referencias bibliográficas que cuestionen algunas de las afirmaciones planteadas. En primer lugar, la legitimación de la existencia en nuestro ordenamiento jurídico del CNI cuya función es, como ya hemos señalado, «facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del

---

difundir la inteligencia necesaria para proteger y promover los intereses políticos, económicos, industriales y comerciales y estratégicos de España, pudiendo actuar dentro o fuera del territorio nacional. b) Prevenir, detectar y posibilitar la neutralización de aquellas actividades de servicios extranjeros, grupos o personas que pongan en riesgo, amenacen o atenten contra el ordenamiento constitucional, los derechos y libertades de los ciudadanos españoles, la soberanía, integridad y seguridad del Estado, la estabilidad de sus instituciones, los intereses económicos y nacionales y el bienestar de la población. c) Promover las relaciones de cooperación y colaboración con servicios de inteligencia de otros países o de Organismos internacionales, para el mejor cumplimiento de sus objetivos. d) Obtener, evaluar e interpretar el tráfico de señales de carácter estratégico, para el cumplimiento de los objetivos de inteligencia señalados al Centro. e) Coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada de material criptológico y formar al personal, propio o de otros servicios de la Administración, especialista en este campo para asegurar el adecuado cumplimiento de las misiones del Centro. f) Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada. g) Garantizar la seguridad y protección de sus propias instalaciones, información y medios materiales y personales».

Estado de derecho y sus instituciones» (art. 1 LCNI)[8] . En segundo lugar, el carácter secreto de las actividades del CNI, «así como su organización y estructura interna, medios y procedimientos, personal, instalaciones, bases y centros de datos, fuentes de información y las informaciones o datos que puedan conducir al conocimiento de las anteriores materias» (art. 5.1 LCNI)[9] . En tercer lugar, que, en el cumplimiento de las funciones legalmente asignadas, el CNI debe respetar tanto los derechos fundamentales como los principios esenciales de nuestro Estado social y democrático de Derecho (art. 2.1 LCNI)[10] .

2. El CNI como autoridad competente para recibir datos de carácter personal recopilados con fines penales

La recogida de datos personales con fines penales que, de manera tímida inicia la LOADN, se ha ido consolidando y extendiendo con el paso de los años, al hilo de los avances tecnológicos producidos y de las obligaciones impuestas por la Unión Europea. Esta extensión de la recogida de datos personales con fines penales se articula esencialmente sobre tres pilares. En primer lugar, la ampliación de los fines para los que se pueden utilizar los datos personales: los datos personales ya no se recogen solo para la investigación y averiguación de delitos, y su posterior enjuiciamiento, sino que se recogen también con fines preventivos. En segundo lugar, la ampliación del ámbito subjetivo de quienes se ven sometidos a la recogida de sus datos personales con fines penales. No solo se van a recoger los datos personales de quienes tienen algún tipo de relación o vinculación con los hechos cometidos y que están siendo investigados, sino que se empiezan a recoger y conservar datos personales de sujetos sobre los que no existe ninguna sospecha de haber delinquido, tal y como ocurre en los casos de los datos relativos a las comunicaciones electrónicas, los datos financieros y los datos PNR. El tercer pilar es la ampliación del ámbito de sujetos obligados a recoger y conservar datos personales, con el objetivo de que estén disponibles para que puedan ser utilizados por las autoridades competentes para la prevención, detección, investigación o enjuiciamiento de hechos delictivos. Así, las operadoras de telefonía, las entidades de crédito y las compañías aéreas se ven obligadas a recoger y conservar los datos personales de sus clientes, para que, en su caso, puedan ser cedidos a las autoridades competentes.

Esta evolución no ha dejado indiferente a quienes propugnan las limitaciones que los derechos fundamentales a la intimidad y a la protección de datos personales imponen a la recogida masiva de datos personales con fines penales. Sin embargo, mucha menos atención ha generado la posibilidad de que todos estos datos puedan llegar a manos del CNI, que ha

---

[8] RUIZ MIGUEL, C., *Servicios de inteligencia y seguridad del Estado constitucional*, Tecnos, 2002, pp. 174 y ss., analiza el fundamento jurídico-constitucional de los servicios de inteligencia en nuestro ordenamiento jurídico.

[9] En este sentido, y como resalta BACHMAIER WINTER, L., «Información de inteligencia y proceso penal», en BACHMAIER WINTER, L., (Coord.), *Terrorismo, proceso penal y derechos fundamentales*, Madrid, Marcial Pons, 2012, p. 53, todo servicio de inteligencia actúa, por definición, sin publicidad y sin transparencia. Por ello, «(e)l Estado de derecho, en la medida en que admite la necesidad de este tipo de actuaciones secretas, renuncia a la transparencia y a un detallado control».

[10] Todos podemos imaginarnos el riesgo que supondría la existencia de servicios de inteligencia sin fiscalización en el cumplimiento de los fines que tiene encomendados, y especialmente en el respeto a los derechos fundamentales. Sin perjuicio de que, como afirma ABA CATOIRA, A., «El secreto de Estado y los servicios de inteligencia», en *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol*, nº 38/39, Valencia, 2002, p. 143, una de las características de los servicios de inteligencia es su invisibilidad y la falta de información que la ciudadanía tiene sobre ellos, lo que dificulta su control y lleva inevitablemente a que surjan dudas sobre la conformidad de su actuación con el ordenamiento democrático.

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

encontrado acomodo entre las autoridades competentes para recibir, y solicitar, datos personales recogidos con fines penales. Así, es una de las autoridades competentes para recibir datos relativos al ADN en el artículo 7.3.c) de la LOADN; para recibir los datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación en el artículo 6.2.c) de la Ley 25/2007; para recibir y solicitar los datos PNR, o el resultado de su tratamiento, en el artículo 14.1.c) de la LOPNR; y, por último, para acceder a los datos financieros incorporados en el Fichero de Titularidades Financieras (en adelante, FTF), así como para solicitar y recibir información financiera del Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, en el artículo 43.3, párrafo quinto, de la Ley 10/2010, y en la disposición adicional primera de la LO 9/2022.

Con esta regulación el legislador español comete, en nuestra opinión, dos errores y tiene un acierto. En lo que se refiere al acierto, es inevitable poner de manifiesto que el carácter secreto de las actuaciones llevadas a cabo por los servicios de inteligencia suele ser aprovechado por los Estados para no regular esta materia y dejarla en una situación de vacío o indefinición jurídica, que solo adquiere notoriedad cuando salta a la prensa algún escándalo[11] , o cuando los abusos de los servicios de inteligencia son sometidos a control judicial. Por ello, hay que valorar de manera positiva que el legislador español prevea expresamente que el CNI tiene acceso a estos datos personales. Si es cierto, como señala la doctrina, que «la cantidad y calidad de las informaciones que obtienen los Estados, así como el saber quién o quiénes son los encargados de obtenerla, los métodos empleados para ello, y la protección de los derechos fundamentales afectados, son indicadores del nivel democrático de dichos Estados»[12] , al menos podemos afirmar que en España ha existido interés en fijar legalmente algunos de los datos que pueden acabar en manos del CNI.

Sin embargo, no es aceptable que el acopio de datos personales por el CNI se regule en las normas que autorizan la utilización de estos datos por las Fuerzas y Cuerpos de Seguridad del Estado, por los fiscales y por los órganos judiciales. El legislador no solo no regula esta materia dentro de la normativa específica del CNI, sino que parece confundir las funciones encomendadas al CNI y las que corresponden a la policía en su función de prevención e investigación de delitos. Primer error. La Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, (en adelante, LOCNI), resulta más adecuada para hacer frente al desarrollo de esta cuestión esencial en unos tiempos en los que los avances tecnológicos permiten un acceso sin precedentes, y casi sin límites, a datos de carácter personal. Esta última afirmación no impide, sin embargo, que aboguemos por la necesaria actualización y reforma de la normativa reguladora del CNI, tanto la de la ley ordinaria, que se ocupa del régimen general de organización y funcionamiento de este organismo, como la ley orgánica que regula las posibles limitaciones de derechos fundamentales por el CNI en el cumplimiento de las funciones legalmente asignadas. Veinte años son muchos para unas leyes que regulan cuestiones tan cruciales como la organización,

[11] Como señala SÁNCHEZ BARRILAO, J.F., «Servicios de inteligencia, secreto y garantía judicial de los derechos», en *UNED. Teoría y Realidad Constitucional*, núm. 44, 2019, p. 309, el caso Villarejo trajo a la palestra constitucional las dificultades del control judicial sobre ámbitos propios de la inteligencia, la seguridad y el secreto.

[12] Cfr. ABA CATOIRA, A., «El secreto de Estado y los servicios de inteligencia», cit., p. 134. Como señala SERRA CRISTÓBAL, R., «El control de datos de circulación de personas en la UE como mecanismo de salvaguarda de la seguridad nacional», *UNED. Revista de Derecho Político*, nº. 102, mayo-agosto 2018, p. 310, «el primer paso en inteligencia reside en la obtención de información, que luego será analizada y tratada para convertir esa información en conocimiento».

funcionamiento y límites de los servicios de inteligencia en una sociedad cada vez más tecnológica y que se enfrenta a riesgos que hace veinte años no existían[13] .

El segundo error es considerar, como ya hemos apuntado anteriormente, que, si los datos personales se recogen para luchar contra el terrorismo, el blanqueo de capitales y otras formas de delincuencia grave, queda justificada su utilización en la defensa de la seguridad nacional. El derecho a la protección de datos personales, reconocido en el artículo 18.4 CE y en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea (en adelante, CDFUE), exige que la norma que prevé la recogida de datos personales especifique claramente el fin o fines que motivan su recogida.

La inclusión del CNI entre las autoridades competentes para acceder a estos datos personales supone una clara extralimitación de los fines que motivan la recogida de datos personales en cada una de estas normas, lo que debe colocarnos en situación de alerta, teniendo en cuenta que uno de los pilares esenciales del derecho a la protección de datos de carácter personal es el respeto a la finalidad que motivó la recogida del dato. Entre las funciones del CNI no se encuentran la prevención, detección o investigación de delitos, sin perjuicio de que, si en el curso de sus labores averiguan o tienen indicios de acciones delictivas, deban ponerlo en conocimiento de los órganos policiales y judiciales competentes; pero, como ha señalado claramente la Sala de lo Penal del Tribunal Supremo, la actividad del CNI «no va encaminada directamente al descubrimiento de delitos, ni tiene como condicionante la previa comisión de alguno» (STS núm. 1094/2010, de 10 de diciembre).

Por ello, no podemos dejar de plantearnos si el legislador español ha considerado que el principio de la «jerarquía de los fines» para los que se van a utilizar los datos personales deja abierta la puerta a la inclusión del CNI entre las autoridades competentes. Si la lucha contra el terrorismo, el blanqueo de capitales y otras formas de delincuencia grave justifica la recogida y conservación de datos personales, el acopio de estos datos por el CNI no sería contrario a la jerarquía de objetivos, puesto que se puede entender que la lucha contra la delincuencia grave es de una importancia menor, en la jerarquía de objetivos de interés general, que la defensa de la seguridad nacional. A la jerarquía de fines se refiere la STJUE (Gran Sala), de 20 de septiembre de 2022, al hilo del acceso a los datos de tráfico y de localización conservados por los proveedores de servicios de comunicaciones electrónicas. La Gran Sala, tras afirmar que el acceso a estos datos solo puede estar justificado, en principio, por el objetivo de interés general para el que dicha conservación se impuso a los proveedores, añade que solo cabría una solución diferente «si la importancia del objetivo perseguido por el acceso fuera mayor que la del objetivo que justificó la conservación»[14] .

---

[13] El 29 de agosto de 2023, el Grupo Parlamentario Vasco (EAJ-PNV) presentó una Proposición de Ley de Modificación de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y de la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia (122/000002), que fue calificada el 5 de septiembre, y publicada en el Boletín Oficial de las Cortes Generales, Serie B. Proposiciones de Ley, de 8 de septiembre de 2023. En esta Proposición de Ley se propone una nueva regulación del control judicial del CNI, que ya no se limita al control previo, pero no se hace ninguna referencia a la extensión del control a otros derechos fundamentales, y se centra exclusivamente en los derechos a la inviolabilidad del domicilio y al secreto de las comunicaciones.

[14] STJUE (Gran Sala), de 20 de septiembre de 2022 (texto rectificado mediante auto de 27 de octubre de 2022), ECLI:EU:C:2022:702, párrafo 128. Aunque en este caso se planteaba la situación inversa, ya que el Gobierno danés alude a una situación «en la que el objetivo de la solicitud de acceso en cuestión, a saber, la lucha contra la delincuencia grave, es de una importancia menor, en la jerarquía de los objetivos de interés general, que la del que justificó la conservación, a saber, la protección de la seguridad nacional» (párrafo 129). Ver también los párrafos 99 y 100 de la sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, ECLI:EU:C:2022:258.

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

2.1 El CNI y los datos ADN

La LOADN fue la primera norma que incluyó al CNI entre las autoridades competentes para recibir datos personales recopilados con fines penales, en este caso, los datos contenidos en la base de datos policial de identificadores obtenidos a partir del ADN (art. 7.3.c LOADN). Esta base de datos, dependiente del Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, fue creada por la LOADN con el objetivo de que, en el curso de las investigaciones criminales, la policía pudiera disponer de esta información que podía resultar esencial para la identificación del culpable y el esclarecimiento de los hechos delictivos. En este caso, el acopio y conservación del dato personal corresponde a los cuerpos policiales, y la finalidad de su análisis es permitir la identificación de autores de delitos graves[15] .

Los datos que se incorporan a la base de datos policial son los datos identificativos extraídos a partir del ADN de muestras o fluidos obtenidos en el marco de una investigación criminal[16] , lo que incluye tanto los datos del sospechoso, detenido o imputado por alguno de los delitos enumerados en el apartado a) del artículo 3.1 LOADN[17] , como los datos de cualquier afectado que hubiera prestado expresamente su consentimiento, y los que se hayan podido obtener a partir de muestras abandonadas en el lugar de los hechos. Estos datos solo podrán utilizarse por las Fuerzas y Cuerpos de Seguridad del Estado en el ejercicio de las funciones de policía judicial, por las autoridades judiciales y por el Ministerio Fiscal (art. 7.1 LOADN[18]).

La cesión de datos relativos al ADN al CNI no es, por tanto, compatible con la finalidad expresamente declarada en el artículo 1 LOADN, y, por ello, no podemos dejarnos engañar por la redacción, totalmente incorrecta en nuestra opinión, del apartado 3.c) del artículo 7, que señala que el CNI podrá utilizar los datos «para el cumplimiento de sus funciones relativas a la prevención de tales delitos, en la forma prevista en la Ley 11/2002, de 6 de mayo, reguladora

---

[15] Además de para la investigación de delitos, los datos de ADN se recogen también para la identificación de cadáveres y la averiguación de personas desconocidas. En estos casos, la LOADN deja claro que cuando el tratamiento se realice para la identificación de cadáveres o para la averiguación de personas desaparecidas, los datos incluidos en la base de datos solo podrán ser utilizados en la investigación para la que fueron obtenidos (art. 7.3 LOADN). Sobre estos datos es recomendable la lectura de ALCOCEBA GIL, J.M., «Adquisición y tratamiento procesal de los datos genéticos de terceros en el marco de la investigación penal», en COLOMER HERNÁNDEZ, I. (Dir.), *Uso y cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios*, Cizur Menor, Thomson Reuters-Aranzadi, 2017, pp. 553-580.

[16] Solo pueden incorporarse a la base de datos policial «los identificadores obtenidos a partir del ADN, en el marco de una investigación criminal, que proporcionen, exclusivamente, información genética reveladora de la identidad de la persona y de su sexo» (art. 4 LOADN). La policía judicial es la encargada de remitir estos datos para su correspondiente incorporación en la base de datos policial, debiendo adoptar para ello «todas las garantías legales que aseguren su traslado, conservación y custodia» (art. 6 LOADN).

[17] Los delitos en el marco de cuya investigación se podrán utilizar los datos ADN vienen enumerados en el artículo 3.1.a) LOADN: «delitos graves y, en todo caso, los que afecten a la vida, la libertad, la indemnidad o la libertad sexual, la integridad de las personas, el patrimonio siempre que fuesen realizados con fuerza en las cosas, o violencia o intimidación en las personas, así como en los casos de la delincuencia organizada, debiendo entenderse incluida, en todo caso, en el término delincuencia organizada la recogida en el artículo 282 bis, apartado 4, de la Ley de Enjuiciamiento Criminal en relación con los delitos enumerados».

[18] Sin perjuicio de que los datos incluidos en la base de datos puedan ser cedidos a las autoridades judiciales, fiscales o policiales de terceros países, de acuerdo con lo previsto en los convenios internacionales ratificados por España y que estén vigentes (art. 7.3.a LOADN).

del Centro Nacional de Inteligencia»[19] . Aún a riesgo de ser reiterativos, no queremos dejar de resaltar que la función del CNI no es la prevención ni la investigación de hechos delictivos.

2.2 El CNI y los datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

La Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, es la segunda norma en la que se incluye al CNI entre las autoridades competentes para recibir datos personales[20] . Esta Ley impone a los operadores que prestan servicios de comunicaciones electrónicas disponibles al público, o que explotan redes públicas de comunicaciones, la obligación de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como la de ceder estos datos a los agentes facultados, siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos contemplados en el Código Penal o en las leyes penales especiales (art. 1.1 Ley 25/2007 y art. 61 de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones). Esta Ley se aplica a los datos de tráfico y localización de personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado (art. 1.2 Ley 25/2007), pero no se podrá conservar ni ceder el contenido de las comunicaciones, incluida la información consultada utilizando una red de comunicaciones electrónicas (art. 1.3 Ley 25/2007).

A pesar de la polémica que viene suscitando esta norma desde que la STJUE de 8 de abril de 2014, *Digital Rights Ireland Ltd* (asunto C-293/12), declaró contraria al Derecho de la Unión la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE[21] , lo cierto es que en España

---

[19] Por ello, coincidimos con RAMALLO MACHÍN, A.C., *ADN: Huellas genéticas en el proceso penal*, Tesis doctoral disponible en el repositorio de la Universidade da Coruñahttps://ruc.udc.es/dspace/handle/2183/16126, p. 341, cuando señala que la cesión al CNI es demasiado amplia, en cuanto que otorga un amplio reconocimiento de acceso y uso de este tipo de información y una desviación de los fines de esta base de datos. Sin embargo, a VALEIJE ÁLVAREZ, I., «La consecuencia accesoria de cesión de muestras biológicas y registro de identificadores de ADN en las bases policiales (art. 129 bis del CP)», en ORTS BERENGUER, E., ALONSO RIMO, A., ROIG TORRES, M., (Dirs.), *Peligrosidad criminal y Estado de Derecho*, Valencia, Tirant lo Blanch, 2017, p. 157, le llama la atención que se cedan datos ADN al CNI pero que «no se especifique si es para un delito concreto o una investigación detallada por lo que no se establecen garantías procedimentales contra el uso abusivo e impropio de tal información».

[20] La Ley 25/2007 no habla de «autoridades competentes», sino de «sujetos facultados». Terminología que el CGPJ, en su *Informe al Anteproyecto de Ley de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*, de 18 de octubre de 2006, p. 12, considera «inapropiada», puesto que «(s)iendo el objetivo de la conservación de datos su eventual cesión a las autoridades o agentes encargados de la investigación de delitos o de la preservación de la seguridad nacional, quizá sería más apropiado que el artículo se refiriese directamente a los agentes de policía judicial y al personal del Centro Nacional de Inteligencia, únicos destinatarios posibles de la información». Informe disponible en: www.poderjudicial.es/cgpj

[21] Por ello, y como señala PÉREZ GIL, J., «Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal», en BELLIDO PENADÉS, R., DE LUIS GARCÍA, E., JIMÉNEZ CONDE, F., LLOPIS NADAL, P. (Coord.), *Justicia: ¿Garantías versus Eficiencia?*, Valencia, Tirant lo Blanch, 2020, *tol. 7.855.589*, no deja de llamar la atención que el legislador siga sin encontrar incentivos suficientes para afrontar la necesidad urgente de esta Ley. Ver también OUBIÑA BARBOLLA, S., «Cambio de enfoque en la cooperación judicial penal y

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

se mantiene la obligación de recoger y conservar de forma masiva todos los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación[22] , con la finalidad de que puedan ser utilizados por distintas autoridades, entre ellas el CNI, con fines de detección, investigación y enjuiciamiento de delitos graves.

La previsión legal de que el personal del CNI podrá solicitar estos datos en el curso de las investigaciones de seguridad sobre personas o entidades que lleve a cabo en cumplimiento de las funciones que corresponden a este organismo (art. 6.2.c Ley 25/2007)[23] , supone también una extensión de los fines que motivan la recogida masiva de los datos relativos a las comunicaciones electrónicas y redes públicas de comunicaciones estos datos. Estos datos personales se recogen para la detección, investigación y enjuiciamiento de delitos, pero pueden ser cedidos a una autoridad que no está legitimada para la investigación de delitos.

2.3 El CNI y los datos PNR

El CNI es también una de las autoridades competentes para recibir y solicitar los datos PNR, tal y como señala el artículo 14.1.c LOPNR[24] . Desde la aprobación de la LO 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y otros delitos graves, las compañías aéreas y las entidades de gestión de reservas de vuelos tienen la obligación de recoger los datos PNR de las personas que viajen en los vuelos internacionales, tanto interiores como exteriores de la UE, ya sean comerciales o privados, con salida o llegada en territorio español, o que hagan escala en él (art. 2.1 LOPNR). Además, y de manera extraordinaria, podrá aplicarse esta obligación a concretas rutas o vuelos nacionales, que son aquellos que tienen como punto de salida y llegada el territorio español, y no han hecho escala en ningún otro Estado (art. 2.3 LOPNR).

Los datos PNR se recogen con fines de prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y un amplio elenco de delitos graves enumerados en

---

policial en la UE en relación con la transmisión de datos personales: las nuevas propuestas normativas y la STJUE de 8 de abril de 2014», en COLOMER HERNÁNDEZ, I., (Dir.), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Cizur Menor, Aranzadi, 2015, pp. 111-121; RODRÍGUEZ LAINZ, J.L., «La evolución de la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de conservación indiscriminada de datos de comunicaciones electrónicas en la STJUE del Caso G.D. y Comissioner an Garda Síochána», en *Diario La Ley*, nº. 10058, 28 de abril de 2022.

[22] Los datos de que se trata son, en particular, los datos necesarios para rastrear e identificar el origen de una comunicación y su destino, para identificar la fecha, hora y duración de una comunicación y el equipo de comunicación de los usuarios y para identificar la localización del equipo de comunicación móvil, datos entre los que figuran el nombre y la dirección del abonado o usuario registrado, los números de teléfono de origen y destino y una dirección IP para los servicios de Internet. Estos datos permiten, en particular, saber con qué persona se ha comunicado un abonado o un usuario registrado y de qué modo, así como determinar el momento de la comunicación y el lugar desde la que esta se ha producido. Además, permiten conocer la frecuencia de las comunicaciones del abonado o del usuario registrado con determinadas personas durante un período concreto.

[23] Como podemos observar, y a diferencia del artículo 7.3.c) LOADN, este precepto sí que se refiere con precisión a la función que le corresponde al CNI.

[24] España no es el único país que ha incluido a los servicios de inteligencia entre las autoridades competentes para recibir estos datos. En relación con esta cuestión, OLSEN, H.P., WIESENER, C., «Beyond data protection concerns- The European Passenger Name Record System», en *I Courts Working Paper Series*, no. 207, 2020, p. 14, señalan que muchos de los Estados miembros, entre ellos Alemania y Dinamarca, han dado a sus servicios de inteligencia acceso a los datos PNR.

el artículo 4 de la Ley. Una vez recogidos estos datos, las compañías aéreas deberán enviarlos al Centro de Inteligencia contra el Terrorismo (en adelante, CITCO), en su condición de Unidad de Información de Pasajeros española (en adelante, UIP). El CITCO será el encargado de la conservación, tratamiento, cesión y posterior supresión de este conjunto de datos personales.

2.4 El CNI y los datos financieros

En último lugar, el CNI es también una de las autoridades competentes para acceder y consultar el FTF y para solicitar y recibir información financiera o análisis financieros del Servicio Ejecutivo de la Comisión (arts. 43.3 y 46.1 de la Ley 10/2010 y disposición adicional primera de la LO 9/2022[25]). Los datos financieros se han convertido en los últimos años en un elemento fundamental para luchar contra cualquier forma de delincuencia grave, en particular, contra el fraude financiero, el blanqueo de capitales y la financiación del terrorismo. De ahí, el esfuerzo llevado a cabo por el legislador europeo en los últimos años para mantener totalmente actualizada la normativa de lucha contra estos delitos implicando, evidentemente, a todos los Estados miembros. La necesidad de garantizar y facilitar el intercambio y el acceso a los datos financieros por parte de las autoridades competentes de los Estados miembros es imprescindible para prevenir, detectar, investigar o enjuiciar estos delitos.

El FTF es un fichero de titularidad pública, del que es responsable la Secretaría de Estado de Economía y Apoyo a la Empresa, a través del SEPBLAC (Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias), en el que se conserva la información suministrada por las entidades de crédito, las entidades de dinero electrónico y las entidades de pago al Servicio Ejecutivo de la Comisión, sobre la «apertura o cancelación de cuentas corrientes, cuentas de ahorro, depósitos y de cualquier otro tipo de cuentas de pago, así como los contratos de alquiler de cajas de seguridad y su periodo de arrendamiento, con independencia de su denominación comercial» (art. 43 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo)[26] .

La obligación de conservar de forma masiva todo este conjunto de datos financieros tiene como finalidad, prevenir, impedir y detectar el blanqueo de capitales y la financiación del terrorismo, así como, contribuir a la prevención, detección, investigación o enjuiciamiento de delitos graves. La información suministrada por las entidades mencionadas contendrá, en todo caso, «los datos identificativos de los titulares y de sus titulares reales y los datos identificativos de los representantes o autorizados y cualesquiera otras personas con poderes de disposición. La información de los productos a declarar incluirá en todo caso la numeración que los identifique, el tipo de producto declarado y las fechas de apertura y de cancelación. En el caso de las cajas de seguridad se incluirá la duración del periodo de

[25] Disposición adicional primera LO 9/2022: «Centro Nacional de Inteligencia. El Centro Nacional de Inteligencia podrá acceder y consultar el Fichero de Titularidades Financieras, así como solicitar y recibir información financiera o análisis financieros del Servicio Ejecutivo de la Comisión, para el ejercicio de las funciones que le encomienda la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia».

[26] El Fichero de Titularidades Financieras fue creado por la Orden ECC/2503/2014, de 29 de diciembre (BOE núm. 316 de 31 de diciembre de 2014). Conforme a lo dispuesto en el artículo 2 de esta Orden, el responsable del Fichero es la Secretaría de Estado de Economía y Apoyo a la Empresa, actuando como encargado del tratamiento por cuenta de éste el Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias, conforme a lo dispuesto en el artículo 43 de la Ley 10/2010, y en el artículo 50.2 del Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010.

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

arrendamiento. Reglamentariamente se podrán determinar otros datos de identificación que deban ser declarados» (art. 43.1 Ley 10/2010).

La inclusión del CNI entre las autoridades competentes para acceder al FTF tuvo lugar con la aprobación del Real Decreto-ley 7/2021, de modificación del artículo 43.3 de la Ley 10/2010[27] , y consolida la política legislativa que opta por garantizar la llegada al CNI de todos los datos personales recopilados de forma masiva con fines de prevención y persecución de delitos. La condición del CNI como autoridad competente para acceder al FTF y para recibir los informes elaborados por el SEPBLAC fue objeto de análisis por los distintos órganos competentes para emitir informe al Anteproyecto de Ley de utilización de información financiera para la prevención, detección, investigación o enjuiciamiento de infracciones penales[28] , como consecuencia de que el artículo 3 del Anteproyecto no incluía al CNI entre las autoridades competentes. El Ministerio de Defensa solicitó la inclusión del CNI entre las autoridades competentes, mientras que el Ministerio del Interior y el Consejo de Estado se opusieron a ella.

En este punto resulta de lo más interesante la justificación que ofrece el Consejo de Estado para oponerse a la inclusión del CNI entre las autoridades competentes. Para el Consejo de Estado[29] , «el papel del CNI respecto a la seguridad nacional no justifica que deba figurar como autoridad competente en este anteproyecto, más vinculado a finalidades policiales y judiciales penales», y recuerda que el artículo 3 de la Directiva (UE) 2019/1153 se refiere a las autoridades competentes en cada Estado miembro para la prevención, detección, investigación o enjuiciamiento de infracciones penales lo que, en su opinión, «necesariamente supone un muy reducido elenco de habilitados para tales cometidos, no pudiendo en ningún caso hacerse una interpretación amplia de dicha prevención, forzosamente restrictiva». A pesar de que, desde el año 2007 el CNI está incluido entre las autoridades competentes para obtener datos personales recopilados con fines penales, no es hasta este Dictamen cuando el Consejo de Estado pone de manifiesto que la inclusión del CNI excede de las finalidades que justifican la recogida de los datos personales en estas leyes.

El CNI accederá al FTF a través del punto único de acceso (PUA) existente en el propio CNI, tal y como señala el artículo 52 del Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo[30].

---

[27] Por ello nos ocupamos de estos datos en cuarto lugar, después de los datos PNR, puesto que, aunque la recogida de datos financieros ya se incluyó en la redacción originaria de la Ley 10/2010, y de que el FTF entró en vigor el 1 de enero de 2015, no fue hasta el año 2021 cuando el CNI se incluyó entre las autoridades competentes para acceder a estos datos. En todo caso, el Preámbulo del Real Decreto nada dice sobre el fundamento de dicha inclusión.

[28] La finalidad de este anteproyecto era la transposición al ordenamiento español de la Directiva (UE) 2019/1153, que extiende la posibilidad de utilizar la información financiera con fines penales en la lucha contra la delincuencia grave, y no limitándola a la financiación del terrorismo y al blanqueo de capitales.

[29] *Dictamen del Consejo de Estado al Anteproyecto de Ley Orgánica por la que establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales*, de 24 de febrero de 2022, (Ref: 1159/2021), p. 28.

3. La obligación de colaborar con el CNI en el desarrollo de sus investigaciones de seguridad

El deber general de colaboración en el desarrollo de las investigaciones de seguridad del CNI que la ley impone a las entidades públicas y privadas (art. 5.5 LCNI), exige plantearnos si este precepto tan parco ha de considerase la norma que habilita la cesión al CNI de los datos personales que las entidades públicas o privadas hayan recopilado para el normal desempeño de sus funciones. Es decir, si esta norma puede considerarse el antecedente, o el equivalente, de la previsión contenida en el artículo 7 LO 7/2021, que establece el deber general de colaboración con las autoridades competentes para todas las Administraciones públicas, así como cualquier persona física o jurídica, cuando se necesiten datos personales con fines de prevención, detección, investigación o enjuiciamiento de infracciones penales. En el caso del CNI, cuando los datos personales se necesiten con la finalidad de «prevenir y evaluar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los interese nacionales y la estabilidad del Estado de derecho y sus instituciones».

Si entendemos que el artículo 5.5 LCNI incluye una habilitación general de cesión de datos personales al CNI, nos encontramos, por tanto, con que al CNI podrán llegar, «legalmente», más datos personales que aquellos a los que nos hemos referido en el apartado precedente. Esta norma autoriza a que el CNI pueda acceder, entre otros, a los datos relativos a la información padronal[31] , a los datos relativos al hospedaje y alquiler de vehículos a motor[32] , a los datos sanitarios, datos bancarios, datos de pedidos o compras realizados en determinados establecimientos, a las grabaciones realizadas dentro de edificios o lugares públicos o privados por entidades privadas, a las grabaciones de imágenes y sonido realizadas por las Fuerzas y Cuerpos de Seguridad en el ámbito de la videovigilancia, etc.

En definitiva, todo dato personal recopilado y destinado a ser incluido en un fichero, es decir, conservado por la entidad que lo recopila, puede acabar en poder del CNI. Aunque la LCNI no dice nada, el deber general de colaboración debería matizarse en aquellos supuestos en los que la cesión de datos personales está condicionada a la necesidad de previa autorización judicial, tal y como desarrollaremos en el epígrafe siguiente. Por otro lado, la Ley no debe limitarse a establecer este deber de manera tan generalizada, y debería regular los supuestos en los que las entidades públicas o privadas pudieran negarse a la entrega de dichos datos. El TEDH ha venido exigiendo, en definitiva, no solo una habilitación legal que

[31] Disposición adicional cuarta de la LO 7/2021: «Ficheros y Registro de Población de las Administraciones Públicas», que contempla la posibilidad de que las autoridades competentes, sin consentimiento del interesado, soliciten al Instituto Nacional de Estadística y a los órganos estadísticos de ámbito autonómico, «una copia actualizada del fichero formado con los datos del documento nacional de identidad, nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en el padrón municipal de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias. Esta solicitud deberá estar motivada en base a cualquiera de los fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública».

[32] Real Decreto 933/2021, de 26 de octubre, por el que se establecen las obligaciones de registro documental e información de las personas físicas o jurídicas que ejercen actividades de hospedaje y alquiler de vehículos a motor, que prevé la comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad, determinando la aplicación de la LO 7/2021, pero que no hace referencia al CNI.

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

autorice la injerencia en los derechos fundamentales por parte de los servicios de inteligencia, sino una norma que sea precisa y respetuosa con los derechos fundamentales[33] .

4. El control judicial previo de los datos personales que llegan al CNI

La LCNI, con el objetivo de garantizar el adecuado desarrollo de las funciones legalmente encomendadas a este organismo, somete las actividades del CNI a distintos tipos de controles: político[34] , económico[35] , parlamentario[36] y judicial[37] . Esto supone, por tanto, que, aunque el carácter secreto de las actuaciones del CNI limita el acceso a sus actuaciones, en ningún caso excluye el control, puesto que el CNI se rige, en el ejercicio de sus funciones, por el principio del sometimiento al ordenamiento jurídico (art. 2.1 LCNI)[38] .

El control judicial previo del CNI, simplemente mencionado en el artículo 12 LCNI, es desarrollado en la LOCNI que exige autorización judicial previa para que el CNI pueda llevar a cabo aquellas actividades que puedan afectar al derecho fundamental a la inviolabilidad del domicilio (art. 18.2 CE) o al derecho al secreto de las comunicaciones (art. 18.3 CE)[39] , que eran dos de los instrumentos más potentes que contemplaba el ordenamiento para la obtención de información, que es una de las actividades básicas del CNI[40] . La competencia

---

[33] Ver la STEDH *Asunto Big Brother Watch y otros c. Reino Unido* (Demandas núms. 58170/13, 62322/14 y 24960/15), de 13 de septiembre de 2018.

[34] El control político de la actuación del CNI lo lleva a cabo el Gobierno a través de la Comisión Delegada para Asuntos de Inteligencia (art. 6.1 LCNI). Esta Comisión está regulada en el artículo 4 del Real Decreto 399/2020, de 25 de febrero, por el que se establecen las Comisiones Delegadas del Gobierno. Ver LÓPEZ ALFRANCA, M.V., «¿Pero quién vigilará a los vigilantes?», en *ICADE, Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, núm. 92, mayo-agosto 2014, pp. 117-123.

[35] La Ley de Presupuestos Generales del Estado establece las partidas de gastos reservados, entre ellas la de los fondos presupuestarios para el CNI. Se puede considerar que esta asignación es un control previo, ya que estos fondos son los que limitan el desarrollo de las actividades del Centro. Además, el CNI tiene asignado un interventor delegado de la Intervención General de la Administración del Estado, que lleva a cabo un control financiero permanente, comprobando que cumple la normativa y que se ajusta a los principios de buena gestión, estabilidad presupuestaria y equilibrio financiero. Igualmente, deberá auditar y aprobar las cuentas anuales del CNI antes de ponerlas a disposición del Tribunal de Cuentas.

[36] El control parlamentario corresponde al Congreso de los Diputados, en la forma prevista por su Reglamento, a través de la Comisión que controla los créditos destinados a gastos reservados, presidida por el Presidente de la Cámara (art. 11.1 LCNI).

[37] Aunque la doctrina es unánime en afirmar que no se puede hablar de control judicial propiamente dicho, sino de autorización judicial previa. Ver por todos, GONZÁLEZ CUSSAC, J.L., «Intromisión en la intimidad y servicios de inteligencia», en *Revista Penal México*, núm. 3, enero-junio, 2012, pp. 160-161; y de este mismo autor, «Intromisión en la intimidad y CNI. Crítica al modelo español de control judicial previo», en *Inteligencia y Seguridad*, 15 (enero-junio 2014), pp. 154-155.

[38] En este sentido, y como ya apuntaba GARCÍA-TREVIJANO GARNICA, E., «Materias clasificadas y control parlamentario», en *Revista Española de Derecho Constitucional*, núm. 48, 1996, p. 149, no se puede confundir la reserva impuesta en relación con dichas materias y su ilicitud, toda vez que es obvio que la Constitución no podría amparar bajo dicha excepción la realización de actuaciones ilícitas. En todo caso, como afirma ABA CATOIRA, A., «El secreto de Estado y los servicios de inteligencia», p. 143, siempre surgirán dudas sobre la conformidad de su actuación con el ordenamiento democrático.

[39] Para GIMBERNAT ORDEIG, E., «La vida de nosotros», publicado en el periódico El Mundo, el 30 de abril de 2008, esta Ley es inconstitucional,

[40] RUIZ MIGUEL, C., *Servicios de inteligencia y seguridad del Estado constitucional*, cit., p. 212.

para autorizar las medidas de investigación solicitadas por el CNI que impliquen restricción de estos derechos fundamentales corresponde a un Magistrado del Tribunal Supremo, de la Sala Segunda de lo Penal o de la Sala Tercera de lo Contencioso-Administrativo, designado conforme al procedimiento establecido en la LOPJ[41] . Este Magistrado, así como quien deba sustituirle en caso de vacancia, ausencia o imposibilidad, será nombrado por el Pleno del Consejo General del Poder Judicial, a propuesta de su Presidente (arts. 598.9ª y 599.1.4ª LOPJ). El nombramiento se efectuará por un periodo de cinco años[42] , y solo podrán ser elegidos para esta función aquellos Magistrados del Tribunal Supremo que cuenten con tres años de servicio activo en la categoría (art. 342 bis LOPJ)[43] .

En el año 2002, sin embargo, el legislador se olvida de que hay otros derechos fundamentales que pueden ser vulnerados en el desarrollo de las actividades específicas de los servicios de inteligencia del Estado, entre ellos el derecho a la protección de datos personales (art. 18.4 CE)[44] . La inclusión del CNI entre las autoridades competentes para acceder a los datos personales recopilados con fines penales, o la posibilidad de solicitar datos personales en poder de entidades públicas o privadas, no ha generado ninguna reacción del legislador en orden a extender el control judicial previo a los supuestos de cesión de estos datos personales. Aun cuando, como analizaremos de manera más detenida en un epígrafe posterior, las investigaciones de seguridad del CNI no están destinadas a generar actos de prueba, el CNI no tiene carta blanca para la restricción de los derechos fundamentales no mencionados en la LOCNI sobre la base de que la obtención de esta información puede ser esencial para la defensa de la seguridad nacional.

En lo que se refiere al derecho a la protección de datos personales, y a pesar de la ausencia de cualquier referencia expresa al artículo 18.4 en la LOCNI, la llegada al CNI de datos personales recogidos con fines penales ha de estar sometida, al menos, a los mismos requisitos establecidos en cada una de las normas que venimos analizando. Cuando para el cumplimiento de las finalidades enumeradas en el artículo 4 LCNI, y concretadas en la

---

[41] Para PÉREZ VILLALOBOS, M.C., *Derechos fundamentales y servicios de inteligencia*», disponible en: https://digibug.ugr.es/bitstream/handle/10481/27876, p. 128, tal vez se debería haber previsto la creación de un órgano colegiado formado por, al menos tres Magistrados, que hubieran asegurado un mejor control de los derechos en juego. En los debates parlamentarios se llegó a pedir la competencia de la Sala Segunda del Tribunal Supremo en Pleno (Ver BOCG, de 20 de diciembre de 2001, núm. 132).

[42] A finales de 2023, el Magistrado Pablo Lucas Murillo de la Cueva es el Magistrado de la Sala de lo Contencioso-Administrativo del TS encargado, desde 2009, de autorizar las actividades del CNI que requieren autorización judicial previa. Ha sido renovado en el cargo dos veces, la última en 2019. Esta situación es, en nuestra opinión, ciertamente anómala, puesto que parece difícilmente justificable que desde hace más de catorce años sea el mismo Magistrado del TS el competente para las autorizaciones del CNI (Ver Acuerdos del Pleno del Consejo General del Poder Judicial de 19 de noviembre de 2009, de 20 de noviembre de 2014 y de 19 de diciembre de 2019). En lo que se refiere al Magistrado suplente, el 20 de diciembre de 2017 el Pleno del CGPJ acordó designar a Andrés Martínez Arrieta, Magistrado de la Sala de lo Penal del TS, nuevo magistrado para conocer de las actividades del CNI en caso de ausencia del primer designado para esas funciones.

[43] El Grupo Parlamentario Vasco (EAJ-PNV), en la Proposición de Ley a la que ya hemos hecho referencia publicada en el Boletín Oficial de las Cortes Generales, de 8 de septiembre de 2023, propone que sea un órgano colegiado compuesto por tres Magistrados del Tribunal Supremo quien, por unanimidad, acuerde, mediante resolución motivada, la autorización judicial para la medida restrictiva de derechos fundamentales.

[44] Y ello a pesar de que, en el año 2002, cuando se aprueban las dos leyes reguladoras del CNI, el Pleno del Tribunal Constitucional ya había dictado su importante sentencia en relación con el derecho a la autodeterminación informativa, la STC 292/2000, de 30 de noviembre, que continúa siendo un referente en relación con el alcance de este derecho fundamental. En el mismo sentido, SÁNCHEZ BARRILAO, J.F., «Servicios de inteligencia, secreto y garantía judicial de los derechos», cit., pp. 330-331, señala que la exigencia de autorización del Magistrado del Tribunal Supremo se tendría que haber extendido a más derechos.

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

Directiva de Inteligencia aprobada anualmente por el Gobierno[45] , el CNI requiera datos relativos al ADN, datos relativos a comunicaciones electrónicas o de redes públicas de comunicación, datos PNR, o pretenda acceder a los datos contenidos en el FTF, deberá ajustarse a los requisitos previstos en estas normas para la cesión de estos datos al resto de autoridades competentes. Cesión que, como veremos, no en todos los casos requiere autorización judicial. En consecuencia, cuando una norma exija la autorización judicial previa para la cesión de datos personales recopilados con fines penales, para que estos datos personales puedan ser cedidos al CNI será necesaria la pertinente autorización judicial, que solo puede otorgarla el Magistrado del Tribunal Supremo competente para autorizar las actividades del CNI restrictivas de derechos fundamentales.

Este argumento es aplicable, igualmente, a aquellos datos personales que sean requeridos por el CNI a cualesquiera entidades públicas o privadas. En aquellos casos en los que la cesión de estos datos a la policía requiera autorización judicial previa, el CNI solo podrá solicitarlos con la pertinente autorización del Magistrado del Tribunal Supremo competente. Esto no significa, sin embargo, que, *a sensu contrario* y con carácter general, no sea necesaria autorización judicial para la cesión de datos personales mientras no exista una norma que expresamente imponga la autorización judicial previa. La doctrina del Tribunal Constitucional y la jurisprudencia del Tribunal Supremo en relación con la cesión de datos personales reflejan que la cuestión es mucho más compleja, y requiere, en muchas ocasiones, una valoración individualizada atendiendo al concreto dato personal solicitado.

La afectación de un derecho fundamental no es argumento suficiente, por sí sola, para postular como presupuesto imprescindible la previa autorización judicial salvo explícita habilitación legal. El hecho de que los apartados primero y cuarto del artículo 18 CE no exijan que cualquier restricción de los derechos a la intimidad o a la protección de datos personales sea acordada por la autoridad judicial, ha llevado al Tribunal Supremo a entender que «existen espacios de privacidad e intimidad tan socialmente tenues o abiertos que pueden ser invadidos por los Cuerpos y Fuerzas de Seguridad cuando cumplen con el interés constitucionalmente legítimo de salvaguardar la seguridad pública o de auxiliar a la autoridad judicial en determinadas investigaciones criminales, siempre que respeten un deber de proporcionalidad exigible en todo caso» (STS núm. 971/2022, de 16 de diciembre[46]). Los problemas que plantea el acopio de datos personales por la policía cuando la ley no exige expresamente autorización judicial se acentúan cuando el solicitante de los datos es el CNI.

[45] El Gobierno fija cada año los objetivos del CNI. Para ello, la CDGAI propone al presidente del Gobierno los objetivos anuales del CNI, que quedan plasmados en la Directiva de Inteligencia, que es «un documento con carácter secreto que recoge los objetivos o necesidades de Inteligencia del Gobierno». A la CDGAI le corresponde igualmente el seguimiento y evaluación periódica del desarrollo de los objetivos fijados en la Directiva. A partir de la aprobación de la Directiva de Inteligencia, el CNI «realiza un proceso de planificación y organización de los recursos disponibles para obtener la información necesaria y elaborar la Inteligencia que satisfaga esas necesidades planteadas por el Gobierno». Como señala el propio CNI, la información la obtiene de distintas fuentes: a) HUMINT (información procedente de fuentes humanas); b) OSINT (información procedente de fuentes abiertas); c) SIGINT (información procedente de fuentes técnicas); y d) GEOINT (información procedente de la explotación y análisis de imágenes e información geográfica). Ver https://www.cni.es/la-inteligencia/obtencion.

[46] ECLI:ES:TS:2022:4754. Ver también las SSTS núm. 489/2018, de 23 de octubre (ECLI:ES:TS:2018:3754) y 777/2013, de 7 de octubre (ECLI:ES:TS:2013:5677).

4.1 Datos personales que requieren previa autorización judicial

La autorización judicial para la cesión de datos personales con fines penales en las cuatro normas que incluyen al CNI entre las autoridades competentes para recibir los datos personales solo es necesaria para obtener los datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, en cuanto se trate de datos vinculados a procesos de comunicación (art. 7.1 y 2 Ley 25/2007), y para la obtención de datos PNR, siempre y cuando la LOPNR sea interpretada de conformidad con lo dispuesto en la STJUE, de 21 de junio de 2022[47] . Esta última observación necesita ser explicada. La LOPNR solo exige autorización judicial, o de la autoridad administrativa correspondiente, para la cesión de los datos PNR a cualquiera de las autoridades competentes enumeradas en el artículo 14, cuando se trate de la transmisión de datos PNR despersonalizados. Los datos PNR se despersonalizan transcurridos seis meses desde la transmisión de los datos PNR por las compañías aéreas al CITCO, en cuanto UIP española (art. 19.2 LOPNR). Una vez despersonalizados, si alguna de las autoridades competentes, entre ellas el CNI, quisiera acceder a los datos PNR completos habría que proceder a la repersonalización, lo que requiere, tal y como señala la Ley, previa autorización judicial o de la autoridad administrativa correspondiente (art. 19.3.b LOPNR). Esta regulación de la cesión de datos personales en la norma española es una transcripción literal de lo previsto en la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril, relativa a la utilización de datos del Registro de Nombres de los Pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave (art. 12.3.b)[48] . La STJUE, de 21 de junio de 2022, ha modificado sustancialmente esta situación al considerar que la autorización judicial, o de la correspondiente autoridad administrativa, debe exigirse en toda transmisión de datos PNR por parte de la Unidad de Información de Pasajeros a las autoridades competentes. En consecuencia, y a pesar de que no se ha producido ninguna reforma en la LOPNR, el CNI y el CITCO están afectados por dicha sentencia, y la transmisión de datos PNR requerirá que el CNI solicite la autorización judicial correspondiente al Magistrado del Tribunal Supremo competente[49] . Sin dicha autorización, el CITCO no podrá proceder al envío de los datos PNR que le haya podido requerir el CNI.

En lo que se refiere a la cesión de datos personales en poder de entidades públicas o privadas, que tienen un deber general de colaboración con el CNI, la autorización previa del Magistrado del Tribunal Supremo va a ser necesaria en aquellos supuestos en los que las leyes indiquen expresamente que la cesión de datos personales a la policía para la investigación de hechos delictivos requiere autorización judicial, por ejemplo, los datos sanitarios[50] .

---

[47] La STJUE, de 21 de junio de 2022, da respuesta a la cuestión prejudicial planteada por la *Cour Costitutionelle (Bélgica), el 31 de octubre de 2019 –Ligue des droits humains/Conseil des ministres* [Asunto C-817/19) (2020/C 36/21)].

[48] La disponibilidad de los datos PNR para las autoridades competentes en la Unión Europea para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y otros delitos graves es la base del sistema PNR diseñado por la Unión Europea, por lo que la Directiva (UE) 2016/681 no condiciona la transmisión de los datos PNR durante los seis primeros meses a la previa autorización judicial o administrativa.

[49] Ver sobre esta cuestión nuestro trabajo, CATALINA BENAVENTE, M.A., *El uso de los datos PNR en el proceso penal*, Cizur Menor, Thomson Reuters-Aranzadi, 2022, pp. 185-188.

[50] El Tribunal Supremo entiende que el artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, impone la autorización judicial expresa «cuando se trata de recoger y tratar datos no anonimizados que pertenezcan a la Administración sanitaria o a los prestadores de servicios de salud, esto es, cuando se reclamen

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

Sin embargo, y debido a la gran heterogeneidad de datos de carácter personal recogidos por entidades públicas o privadas y conservados en ficheros o bases de datos, es imposible que exista para todos ellos una norma que especifique si ese concreto dato personal puede ser recabado directamente por la policía o, por el contrario, requiere de autorización judicial. En estos casos se hace necesario examinar los criterios fijados por el Tribunal Supremo, el Tribunal Constitucional, pero también el TJUE y el TEDH, para determinar de qué depende que su obtención competa a una u otra autoridad. En este sentido, conviene precisar desde este primer momento que la regla general proclamada por el Tribunal Supremo siguiendo la doctrina constitucional se articula sobre el derecho fundamental a la intimidad (art. 18.1 CE), pero que puede ser aplicada por extensión al derecho a la protección de datos personales (art. 18.4 CE). Los funcionarios policiales se encuentran constitucionalmente habilitados para realizar investigaciones de las que se derive una injerencia de carácter no grave o leve en el derecho fundamental a la intimidad, siempre y cuando, además, cuenten con suficiente habilitación legal; su práctica se ajuste a las exigencias del principio de proporcionalidad y se ponga a disposición posterior de la autoridad judicial la totalidad de los datos personales obtenidos con la finalidad de que se efectúe el oportuno control jurisdiccional de adecuación. Esto es, «si de la cesión resulta una injerencia grave en el derecho a la protección de datos del titular -o en la intimidad como consecuencia directa de aquella-, la legitimidad de obtención del dato residiría en manos del órgano judicial, en cambio, si la injerencia que se produce en tales derechos es de carácter leve, la Policía se encontraría habilitada para recabar el dato a través de sus agentes. Y es que, como ya advirtió el TJUE, la posibilidad de que los Estados miembros justifiquen una limitación de los derechos a la protección de datos e intimidad personal, debe determinarse atendiendo a la gravedad de la injerencia que supone esa limitación y comprobando que la importancia del objetivo de interés general perseguida por dicha limitación guarde relación con tal gravedad»[51] .

El juicio de idoneidad, necesidad y proporcionalidad de la petición de datos recae en una ingente cantidad de supuestos, por tanto, en los agentes de policía que están llevando a cabo la investigación; pero este juicio es sometido posteriormente, incluso en diferentes ocasiones, al control judicial: en la instrucción a la hora de aceptar la incorporación de estos datos en este momento procesal, en el momento de decidir sobre su admisión como medios de prueba, o, en fase de recurso, para determinar si su utilización en el proceso penal ha traído consigo la vulneración de derechos fundamentales del condenado.

El principio general reiterado por el Tribunal Supremo en distintas resoluciones de que «la jurisdiccionalidad es exigible en algunos casos; en otros no» es válido para la obtención de datos personales por la policía, cuya finalidad es la generación de actos de prueba. Sin

---

datos identificativos y clinicoasistenciales unificados» (STS núm. 971/2022, de 16 de diciembre, ECLI:ES:TS:2022:4754). La Sala II acaba estimando la vulneración del derecho a la intimidad del recurrente como consecuencia de que los agentes policiales, sin autorización del titular del derecho y sin autorización judicial, accedieron a los datos recogidos en el historial médico hospitalario, obteniendo la identidad y los datos de incriminación que finalmente llevaron a dictar sentencia condenatoria. En consecuencia, declara la nulidad de la investigación llevada a cabo y acuerda la absolución del recurrente. Sobre esta sentencia ver LOMAS HERNÁNDEZ, V., «La cesión de datos sanitarios a las Fuerzas y Cuerpos de Seguridad: STS (Sala de lo Penal) de 16 de diciembre, y Agencias de Protección de Datos Personales», en *Diario La Ley*, núm. 10220, 2 de febrero de 2023. En todo caso, es importante poner de manifiesto que el artículo 16 de la Ley 41/2002 no menciona expresamente a las Fuerzas y Cuerpos de Seguridad del Estado. Sobre la cesión de datos relativos a la salud al proceso penal ver GÓMEZ ÁLVAREZ, J., «La cesión de datos de carácter personal al proceso penal. En especial los datos relativos a la salud», en COLOMER HERNÁNDEZ, I. (Dir.), *Uso y cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios*, Cizur Menor, Thomson Reuters-Aranzadi, 2017, pp. 607-646.

[51] Cfr. MONTORO SÁNCHEZ, J.A., *Uso y cesión de datos de carácter personal en el proceso penal*, cit., p. 651.

embargo, no creemos que sea de traslación automática a la obtención de datos personales por el CNI en aquellos supuestos en los que no exista una norma que expresamente requiera la autorización judicial para la cesión de datos. La inexistencia de previsión legal de necesaria autorización judicial no puede ser suplida por una supuesta obligación del CNI de someter el ejercicio de sus actuaciones a los criterios establecidos por Tribunal Supremo y Tribunal Constitucional.

En definitiva, la ausencia de una normativa específica que regule la cesión de datos personales al CNI por parte de las entidades públicas o privadas deja en manos del CNI la decisión de si procede recabar o no previamente la autorización judicial previa del Magistrado del Tribunal Supremo competente, en aquellos casos en que una norma no lo exige. Lo ideal sería que el CNI efectuara previamente el juicio de idoneidad, necesidad y proporcionalidad de los datos personales que solicita a las entidades públicas o privadas, y acudiera al Magistrado del Tribunal Supremo competente cuando considere que los datos solicitados pueden suponer una injerencia grave en el derecho a la intimidad o en el derecho a la protección de datos personales. Lo normal será que no la solicite, porque no hay ninguna norma que le obligue a ello.

4.1.1 Procedimiento para la obtención de la autorización judicial

El procedimiento regulado en la LOCNI para obtener la autorización judicial en los casos de entrada o registro e intervención de las comunicaciones por el CNI se tiene que aplicar por extensión a la solicitud de datos personales que requieren autorización judicial previa. Se trata de un procedimiento relativamente sencillo, en el que la persona que ocupa la dirección del CNI asume un papel relevante[52] . Cuando para la realización de las investigaciones de seguridad que le son propias, el CNI necesite datos personales que requieren previa autorización judicial, la persona que ocupa la dirección del CNI deberá solicitar por escrito al Magistrado competente del Tribunal Supremo la autorización judicial previa que le habilita a reclamar estos datos a la entidad que los tiene en su poder. Esta solicitud deberá incluir, al menos, la siguiente información: los concretos datos que se solicitan, los hechos en los que se apoya la solicitud, los fines que la motivan y las razones que aconsejan la cesión de los datos de carácter personal[53] . Además, y en el caso de que se conocieren, se deberán incluir los titulares de los datos personales que se van a ver afectados por la cesión.

En todo caso, resulta interesante poner de manifiesto que la LOCNI no prevé la posibilidad de que la persona que ocupa la dirección del CNI pueda, en casos de urgencia, acordar la medida restrictiva de derechos fundamentales, y someterla a la confirmación *a posteriori* del Magistrado del Tribunal Supremo competente. A pesar de que la LECrim prevé la posibilidad de que, en casos excepcionales, la policía pueda realizar una medida restrictiva de derechos fundamentales sin previa autorización judicial[54] , el hecho de que esta posibilidad no esté prevista expresamente en la LOCNI nos lleva a creer que esta excepción no sería admisible en estos casos; es decir, que fuera la persona que ocupa la dirección del CNI la que

[52] Nos referimos «a la persona que ocupa la dirección del CNI» a pesar de que la LOCNI se refiere al «Secretario de Estado. Director del Centro Nacional de Inteligencia» (art. Único 1 LOCNI).

[53] En opinión de PÉREZ VILLALOBOS, M.C., *Derechos fundamentales y servicios de inteligencia*, cit., p. 147, no es seguro que, con la información suministrada por el director del CNI, el Magistrado del Tribunal Supremo competente se encuentre en disposición de ponderar adecuadamente la proporcionalidad de la medida solicitada.

[54] Ver artículos 579.3, 588 ter d.3), 588 quinquies b.4) y 588 sexies c.3 y 4 LECrim.

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

acordara la cesión de datos, y que posteriormente recabara la pertinente autorización judicial que confirmara dicha medida[55] .

Una vez recibida la solicitud, el Magistrado del Tribunal Supremo competente deberá resolver, en el plazo improrrogable de setenta y dos horas, si autoriza o no la cesión de datos de carácter personal solicitada. En casos de urgencia, este plazo podrá reducirse a veinticuatro horas. Para ello será necesario que en la solicitud se justifiquen debidamente los motivos de urgencia (artículo único 3 primer párrafo LOCNI).

La LOCNI, sin embargo, ya no sirve de referencia para conocer cuál ha de ser el contenido del auto acordando, o denegando, la medida solicitada, puesto que nada indica al respecto. Para resolver si procede o no la cesión solicitada, el Magistrado del Tribunal Supremo ha de llevar a cabo una ponderación de bienes jurídicos que no se identifican con los que son valorados en el seno de un proceso penal. La función de este Magistrado no está exenta de dificultades, en cuanto que debe valorar si la cesión de los datos requeridos es necesaria para «prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones» (art. 1 LCNI)[56] .

Una vez dictado el auto acordando la cesión de datos personales, el Magistrado del Tribunal Supremo dispondrá lo procedente para salvaguardar la reserva de sus actuaciones, que tendrán la clasificación de secreto (artículo único 3 segundo párrafo LOCNI). Este auto no es recurrible, como tampoco lo es el auto que acuerda la entrada y registro o la intervención de las comunicaciones[57] .

4.1.2 Ejecución de la orden de cesión de datos al CNI

Una vez obtenida la autorización judicial, y a pesar de la ausencia de cualquier referencia expresa sobre esta cuestión, hay que entender que la persona que ocupa la dirección del CNI deberá reenviarla a la entidad pública o privada que tiene los datos personales que se solicitan, para que procedan a cumplir lo dispuesto en el auto. En este sentido, nos parece relevante poner de manifiesto que la autorización judicial en ningún caso permite al CNI el acceso directo a las bases de datos en las que se encuentran los datos reclamados[58] .

---

[55] En sentido diverso, SÁNCHEZ BARRILAO, J.F., «Servicios de inteligencia, secreto y garantía judicial de los derechos», cit., p. 334, que plantea la posibilidad de que la persona que ocupa el Ministerio de Defensa (que es del que depende el CNI), o quien ocupa la dirección del CNI, pudieran autorizar en casos de urgencia esta medida. Lo deseable sería que en una futura reforma de la LOCNI se incluyera esta posibilidad, así como las actuaciones a realizar para conseguir la autorización ulterior del Magistrado del Tribunal Supremo competente.

[56] Se trata, como señala la SAN núm. 9/2022, de 31 de marzo (ECLI:ES:AN:2022:1855), de una «singular forma de control judicial», que deriva del hecho de que «el Magistrado autorizante ha de verificar una ponderación de bienes jurídicos que no se identifican con los que son valorados en el seno de un proceso penal».

[57] Como recuerda la SAN núm. 9/2022, de 31 de marzo, citando la STS núm. 1094/2010, de 10 de diciembre, «(l)a exclusión de cualquier posibilidad impugnativa de la resolución habilitante y, sobre todo, la ausencia de un seguimiento ulterior de lo actuado a partir de la autorización, añaden mayores dosis de especialidad al régimen jurídico dibujado por el legislador español». En opinión de GONZÁLEZ CUSSAC, J.L., «Intromisión en la intimidad y CNI. Crítica al modelo español de control judicial previo», cit., pp. 157-158, el hecho de que las actuaciones del Magistrado competente tengan el carácter de secretas, va a tener consecuencias en el alcance de la motivación del auto.

[58] Esta posibilidad, tal y como se señala en el *Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. El derecho al a privacidad en la era digital*, cit., apartado 18, se da en algunos Estados, lo que debe ser completamente rechazable, en cuanto que los sistemas que permiten el acceso directo a los flujos de

El auto que acuerda la cesión de datos de carácter personal deberá incluir el plazo de ejecución de la cesión de los datos solicitados. A la hora de fijar dicho plazo, el Magistrado del Tribunal Supremo deberá atender a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación. En relación con esta cuestión, mientras que la LOPNR no hace ninguna referencia al plazo de transmisión, la Ley 25/2007 señala que, salvo que se establezca un plazo distinto, la cesión deberá efectuarse dentro del plazo de siete días naturales contados a partir de las 8:00 horas del día natural siguiente a aquel en que el sujeto obligado reciba la orden (art. 7.3 Ley 25/2007).

4.1.3 Inexistencia de control judicial a posteriori

Una vez que los datos personales han sido cedidos al CNI, no es posible encontrar en la LOCNI ninguna pauta en relación con el control que sobre el tratamiento de dichos datos personales le corresponde al Magistrado del Tribunal Supremo que autorizó la cesión. La doctrina lleva años poniendo de manifiesto que el control judicial de las actuaciones del CNI restrictivas de derechos fundamentales se agota con la emisión del auto autorizando la medida, puesto que la LOCNI no prevé ningún tipo de control judicial sobre el resultado de dichas medidas[59] . La única referencia que hace la Ley al control posterior es que será la persona que ocupe la dirección del CNI quien «ordenará la inmediata destrucción del material relativo a todas aquellas informaciones que, obtenidas mediante la autorización prevista en este artículo, no guarden relación con el objeto o fines de la misma» (artículo único 4 LOCNI). En definitiva, es a la persona que ocupa la dirección del CNI a la que corresponde evaluar y usar la información obtenida de cara a conseguir los objetivos perseguidos, esto es, a quien le corresponde decidir «qué es relevante y qué no lo es, y qué hacer con tales informaciones, antes de su preceptiva destrucción o borrado»[60] , sin que, en ningún caso, se le imponga obligación alguna de rendir cuentas del resultado obtenido a partir de las actividades que se llevaron a cabo tras la autorización judicial[61] . En relación con los datos personales cedidos al CNI se mantiene este mismo planteamiento, puesto que al quedar excluidos del régimen

datos que circulan a través de las redes de los proveedores de servicios de telecomunicaciones e Internet, «son particularmente propicios a los abusos y tienden a eludir las garantías procesales fundamentales», como ya se apuntó en la STEDH *Caso Roman Zakharov c. Rusia*, Demanda núm. 47143/06, de 4 de diciembre de 2015, párr. 270.

[59] Esto lleva a PÉREZ VILLALOBOS, M.C., *Derechos fundamentales y servicios de inteligencia*, p. 130, a ratificarse en la idea de que el control judicial previsto por la LOCNI es «un acto meramente formal», y no «un control judicial real y efectivo». Posteriormente afirma, p. 146, que «en la más extrema de las interpretaciones, podría pensarse que el legislador no ha tenido verdadera intención de someter la actuación de los servicios de inteligencia a un verdadero control». Ver también JIMÉNEZ-PÉREZ, D., «Legitimidad y control del Centro Nacional de Inteligencia», Comunicación presentada en el Congreso Análisis de Inteligencia y Prospectiva. Grupo de Estudios en Seguridad Internacional. Universidad de Granada, 8-9 de abril de 2019, 15p. (disponible en https://www.ugr.es/~gesi/congreso/comunicacion31-14.pdf).

[60] Ver GONZÁLEZ CUSSAC, J.L., «Intromisión en la intimidad y CNI. Crítica al modelo español de control judicial previo», cit., p. 163. El Grupo Parlamentario Vasco (EAJ-PNV), en la Proposición de Ley a la que ya hemos hecho referencia publicada en el Boletín Oficial de las Cortes Generales, de 8 de septiembre de 2023, incluye un control judicial *ex post*, al indicar que los Magistrados del Tribunal Supremo deberán ser informados por el Secretario de Estado director o la secretaria de Estado directora del CNI del grado de ejecución de cada autorización, a fin de que puedan asegurarse de su adecuación al contenido de estas.

[61] GONZÁLEZ CUSSAC, J.L., «Intromisión en la intimidad y CNI. Crítica al modelo español de control judicial previo», cit., p. 155.

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

general de protección de datos, parece que el director del CNI no tiene que dar cuenta a nadie de la situación de estos datos personales.

La cobertura que proporciona la autorización judicial previa no es suficiente si no se controla posteriormente por el propio Magistrado que autorizó la medida. El proceso de inteligencia requiere no solo la obtención de información, sino su evaluación o tratamiento. Por ello, no basta con el control de la forma en que los datos personales llegan al CNI, sino que es necesario asegurar que la actividad del CNI no colisiona con ningún derecho fundamental, entre ellos, el derecho fundamental a la protección de datos personales.

4.2 Datos personales que no requieren autorización judicial previa

Por lo que se refiere a los datos personales expresamente recopilados y conservados con fines penales, ni la LOADN ni la Ley 10/2010 exigen autorización judicial para que las autoridades competentes accedan a estos datos para el cumplimiento de los fines asignados. Al no existir una regulación diferenciada, y más restrictiva, para que el CNI pueda acceder a estos datos personales, hay que entender que el CNI tampoco necesita autorización judicial previa para acceder a los datos relativos al ADN incorporados en las bases de datos policiales, ni para acceder a la información contenida en el FTF. En todo caso, el hecho de que no sea necesaria autorización judicial previa no significa que el CNI pueda acceder directamente a dichos datos, sino que es necesario que el acceso se realice a través del procedimiento establecido. Así, cualquier información o solicitud de datos relativos al ADN ha de realizarse a través del administrador nacional de la base de datos, que es la Secretaría de Estado de Seguridad[62] .

El CNI accederá al FTF a través del PUA, al que ya nos hemos referido. Los accesos y consultas realizadas y los resultados obtenidos se efectuarán por medios telemáticos. Todas las consultas y accesos al FTF se realizan a través de la Red Sara bajo la Plataforma de Intermediación. Para ello, los PUA deberán tener correctamente habilitada y configurada su conexión a dicha red. Cada organismo, a través de su PUA, comprobará la identidad de la autoridad o funcionario solicitante, verificará su habilitación legal para realizar la petición de acceso y velará por la pertinencia de las solicitudes, que deberán estar adecuadamente motivadas y quedarán bajo la responsabilidad de la autoridad o funcionario solicitante[63] . Cada

[62] A diferencia de lo que ocurre con las autoridades con competencia de policía judicial que sí que tienen garantizado el acceso directo. Ver la *Memoria Enero-Diciembre 2021*. *Base de datos policial de identificadores obtenidos a partir de ADN*, elaborada por la Subdirección General de Sistemas de la Información y Comunicaciones para la Seguridad, Secretaría de Estado de Estado de Seguridad, Ministerio del Interior, pp. 13-14, en la que se indica que actualmente solo tres usuarios tienen acceso a la base de datos nacional de ADN, e indica cuáles son dichos usuarios en la Secretaría de Estado de Seguridad, que es el administrador nacional de la base de datos de ADN; en la Dirección General de la Policía; y en la Dirección General de la Guardia Civil. Y concluye señalando: «Incluso aun cuando existan disposiciones legales que autorizaran el acceso a la base de datos y/o registros de ADN como sucede con el miembro nacional de España en Eurojust, o el CNI, el acceso técnicamente no es posible y, por tanto, cualquier información o solicitud ha de realizarse a través del administrador nacional de la base de datos». Memoria disponible en: https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/Base-de-datos-policial-de-identificadores-obtenidos-a-partir-de-ADN.-Memoria/Base_de_datos_policial_identificadores_ADN_Memoria_2021_126200173_web.pdf

[63] En cuanto al contenido de las solicitudes ver la Instrucción de 2 de julio de 2015, de la Secretaría de Estado de Economía y Apoyo a la Empresa, por la que se establecen los requisitos mínimos que deben cumplir las solicitudes de datos al Fichero de Titularidades Financieras, efectuadas a través de los puntos únicos de acceso.

PUA deberá mantener un registro pormenorizado de las peticiones realizadas, en el que figurará en todo caso la autoridad o funcionario solicitante y la justificación de la petición (art. 52 del Real Decreto 304/2014)[64] .

Las solicitudes de datos financieros han de ser concretas, en cuanto que es necesario que la autoridad solicitante identifique a la persona, personas o número de cuenta respecto de las que requiere información, no resultando admisibles búsquedas abiertas, genéricas o por aproximación (artículo 52 del Real Decreto 304/2014)[65] . Esta exigencia es aplicable al CNI, independientemente de que sus actuaciones estén sometidas a secreto. Cualquier acceso al Fichero queda registrado, también los efectuados por el CNI, y estos registros se conservarán por un periodo de cinco años (art. 43.3 in fine Ley 10/2010).

En relación con los datos financieros creemos que es importante hacer referencia al cambio tan importante que introdujo la LO 9/2022. Desde el 29 de agosto de 2022, fecha de entrada en vigor de la LO 9/2022, el CNI puede acceder al FTF, a través de su PUA, sin necesidad de autorización judicial. La LO 9/2022 suprime la exigencia de autorización judicial previa, o del Ministerio Fiscal, para el acceso al FTF por parte de las autoridades competentes, con la consiguiente modificación del artículo 43 de la Ley 10/2010, por lo que el CNI tampoco necesita dicha autorización para acceder a esta información. Desde la creación del FTF, el acceso a la información allí contenida se hacía depender de la autorización previa, que, sin embargo, el legislador ha considerado conveniente suprimir en esta última reforma, con el objetivo de «garantizar un acceso directo e inmediato» a los datos contenidos en el FTF, en los términos expresamente previstos por la Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, que prevé el acceso directo de las autoridades competentes a los registros nacionales centralizados de cuentas bancarias o a los sistemas de recuperación de datos. En relación con esta cuestión, no está de más apuntar que, aunque la Ley 10/2010 se refería indistintamente a autorización judicial o del MF, en el caso de la solicitud por el CNI la autorización correspondía exclusivamente acordarla al Magistrado del Tribunal Supremo competente.

Esta reforma legal transmite la inquietante sensación de que la autorización judicial, o del Ministerio Fiscal, para que las autoridades competentes puedan acceder a los datos contenidos en el FTF, no ha de verse como una garantía para los titulares de dichos productos financieros, sino como un entorpecimiento de la lucha contra la financiación del terrorismo, el blanqueo de capitales, o todo un conjunto de delitos graves[66] . El legislador lo justifica señalando que «el acceso al Fichero proporciona una foto estática, sin información alguna que revele la capacidad económica de las personas afectadas», sin perjuicio de que, al tratarse de

[64] Aunque este precepto exige que en la solicitud conste la identidad de la autoridad judicial o fiscal que ha acordado o autorizado la obtención de datos, la LO 9/2022 ha suprimido la exigencia de autorización previa para que las autoridades competentes puedan acceder a los datos contenidos en el FTF.

[65] Sobre esta cuestión ver las observaciones efectuadas por la AEPD al realizar el informe preceptivo sobre el proyecto de la que finalmente fue la Instrucción de 2 de julio de 2015, disponible en https://www.aepd.es/es/documento/2015-0238.pdf.

[66] A título de ejemplo reproducimos este párrafo del apartado III del Preámbulo: «El acceso a esa información de manera directa e inmediata y en el marco de una cooperación leal y rápida, se entiende como indispensable para alcanzar el éxito de una investigación penal acerca de un delito considerado como grave. En efecto, la dificultad de acceder a determinada información financiera constituye un obstáculo para la investigación de delitos graves, y también entorpece la desarticulación de tramas terroristas o la localización e inmovilización de los ingresos procedentes de actividades delictivas. Interesa poner de relieve que numerosas investigaciones llegan a un punto muerto, precisamente, ante la imposibilidad de acceder de forma oportuna, exacta y completa a los datos financieros relevantes».

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

información sensible sea necesario garantizar «un acceso proporcionado y dentro del concepto de "intimidad económica" que maneja nuestra jurisprudencia» (apartado IV del Preámbulo). Una medida ciertamente muy discutible.

De las autoridades competentes para emitir informes al Anteproyecto de LO 9/2022 solo el CGPJ se opuso a la supresión de la exigencia de la autorización judicial[67] . Ni el Consejo de Estado[68] , ni el Consejo Fiscal[69] , manifestaron ningún tipo de preocupación por la eliminación de esta garantía, entendiendo que resulta proporcionado con la exigencia de garantizar la seguridad pública y respetuoso con el derecho fundamental a la intimidad proclamado en el artículo 18.1 CE[70] .

En conclusión, el CNI solo ha necesitado autorización judicial para acceder al FTF en el periodo comprendido entre el 29 de abril de 2021, fecha de entrada en vigor del Real Decreto-ley 7/2021, que lo incluyó entre las autoridades competentes para acceder a la información contenida en el FTF, y el 28 de agosto de 2022. Durante dichos dieciséis meses, por lo tanto, todo acceso por parte del CNI a través de su PUA tuvo que ir acompañado de la pertinente autorización judicial solicitada por quien en esos momentos ocupaba la dirección del CNI. Solicitud que debía de ajustarse a los requisitos impuestos en el Real Decreto 304/2014 y en la Instrucción de 2 de julio de 2015.

Para el resto de datos personales, y tal y como señalábamos previamente, el hecho de que no exista una norma que expresamente exija la autorización judicial para la cesión de datos personales por parte de las entidades públicas o privadas que los tienen en su poder, ha de entenderse en el sentido de que el CNI no necesitará la autorización judicial previa del Magistrado competente del Tribunal Supremo. Cuestión distinta serán las consecuencias ulteriores que la ausencia de autorización judicial genere en el supuesto de que se cedan estos datos a las autoridades con competencia de policía judicial. Pero de eso nos ocuparemos más adelante.

---

[67] Ver apartados 62 y 63, y conclusión undécima del *Informe del CGPJ sobre el Anteproyecto de Ley Orgánica por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales*, de 23 de septiembre de 2021.

[68] *Informe del Consejo de Estado al Anteproyecto de Ley Orgánica por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales*, de 24 de febrero de 2022. (Referencia 1159/2021). Para el Consejo de Estado: «Sin duda dicha información es sensible pero dicha sensibilidad no supone una información invasiva del concepto de "intimidad económica" antes aludido. No hay un conocimiento exhaustivamente definitorio de la situación económica, sino una mera noticia genérica de la presencia de una titularidad financiera (una cuenta corriente, una posición crediticia), puesto que no se proporciona en momento alguno ninguna información económica».

[69] *Informe del Consejo Fiscal al Anteproyecto de Ley Orgánica por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales*, de 7 de octubre de 2021.

[70] El Preámbulo de la LO 9/2022 señala que se trata de «una de las cuestiones más relevantes» de la nueva ley. En opinión de MONTORO SÁNCHEZ, J.A., «La Ley Orgánica 9/2022, de 28 de julio. Un controvertido instrumento para la investigación de la dimensión económica del delito», *Eunomía. Revista en Cultura de la Legalidad*, 24, 2023, pp. 352-353, esta medida se antoja compatible y respetuosa con los derechos fundamentales a la intimidad personal y la protección de datos personales. Ver también LEÓN ALAPONT, J., «Un comentario de urgencia a la Ley Orgánica 9/2022, de 28 de julio, por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales», en *Diario La Ley*, núm. 10123, de 5 de septiembre de 2022.

5. La exclusión del CNI del régimen general de protección de datos personales

El 27 de abril de 2016 se aprobaron dos normas que cambiaron el marco normativo de protección de los datos de carácter personal en la Unión Europea[71] . La primera, 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 (en adelante, RGPD). La segunda, 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.

Estas dos normas excluyen de su ámbito de protección el tratamiento de datos personales con fines de seguridad nacional[72] , al tratarse de actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión, que deberán regirse por su normativa específica. El RGPD[73] y la Directiva 2016/680[74] recogen la denominada «excepción de seguridad nacional», conforme a la cual, las actividades de los Estados miembros para la defensa de la integridad territorial, el mantenimiento del orden público y la defensa de la seguridad nacional no entran dentro de las competencias de la Unión Europea, tal y como señala el artículo 4.2 del Tratado de la Unión Europea (en adelante, TUE)[75] .

En España, la primera norma que reguló la protección de datos, la LO 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, ya excluyó de su ámbito de protección los ficheros «sometidos a la normativa sobre protección de materias clasificadas», e indicaba que estas materias habían de regirse «por sus disposiciones específicas» (art. 3.2.b). Esta remisión a las disposiciones específicas en materia

---

[71] Ambas se publicaron en el DOUE de 4 de mayo de 2016. El 27 de abril se aprobó también la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, a la que nos referiremos posteriormente (que también se publicó en el DOUE de 4 de mayo de 2016).

[72] El Tribunal de Justicia ya ha declarado que «el objetivo de protección de la seguridad nacional corresponde al interés primordial de proteger las funciones esenciales del Estado y los intereses fundamentales de la sociedad e incluye la prevención y la represión de actividades que puedan desestabilizar gravemente las estructuras constitucionales, políticas, económicas o sociales fundamentales de un país, y, en particular, amenazar directamente a la sociedad, a la población o al propio Estado, tales como las actividades terroristas» [STJUE (Gran Sala), de 20 de septiembre de 2022 (texto rectificado mediante auto de 27 de octubre de 2022), ECLI:EU:C:2022:702, apartado 92; STJUE, de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, ECLI:EU:C:2022:258, apartado 61 y jurisprudencia allí citada].

[73] Ver artículos 2.a) y 23.1.a) del RGPD.

[74] Artículo 2.3.a) de la Directiva (UE) 2016/680, en relación con el Considerando 14.

[75] GUZMÁN FLUJA, V., «Consideraciones sobre el alcance objetivo y subjetivo de la Directiva UE 680/2016», en MORENO CATENA, V., ROMERO PRADAS, M.I., (Coords.), *Nuevos postulados de la cooperación judicial en la Unión Europea. Libro homenaje a la Prof.ª Mª Isabel González Cano*, Valencia, Tirant lo Blanch, 2021, p. 853, habla de «zona fuera de cobertura». También habla de «agujeros negros» citando a CARUANA, M.M., «The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement», en *International Review of Law, Computers & Technology*, volumen, 33, núm. 3, 2019, p. 257, es decir, espacios en los que no existe ninguna protección para los datos personales.

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

de protección de datos sometidos a la normativa sobre materias clasificadas fue considerada por la doctrina como una «remisión *in vacuo*», en cuanto que la Ley 9/1968, de 5 de abril, sobre secretos oficiales, no contenía (tampoco ahora) ningún precepto sobre protección de datos personales[76] . Unos años después, la LO 15/1999, de 13 de diciembre, de protección de datos de carácter personal, también excluyó los ficheros sometidos a la normativa sobre protección de materias clasificadas de su régimen de protección (art. 2.2.b), pero sin incluirlos dentro de aquellos que habían de regirse por sus disposiciones específicas (que eran los enumerados en el apartado 3 del artículo 2)[77]

En la actualidad, y siguiendo tanto nuestra tradición jurídica como las directrices de la Unión Europea, la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantías de los derechos digitales, cuyo objetivo es adaptar el ordenamiento jurídico español al RGPD, y la LO 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, de transposición al ordenamiento español de la Directiva (UE) 2016/680, excluyen expresamente de su ámbito de aplicación los tratamientos de datos personales sometidos a la normativa sobre materias clasificadas (arts. 2.2.c LO 3/2018, y 2.3.d LO 7/2021[78]).

En consonancia con todo ello, el CNI recoge en su «política de privacidad» la cláusula de excepción de seguridad nacional y señala expresamente que «los ficheros propiedad del CNI se encuentran expresamente excluidos del ámbito de aplicación de la normativa de protección de datos de carácter personal»[79] . Esto supone, por tanto, que a pesar de que el CNI es una de las autoridades competentes para recibir datos personales recogidos con fines penales, y de que puede solicitar datos personales a las entidades públicas o privadas en el desarrollo de sus investigaciones de seguridad (art. 5.5 LCNI), el tratamiento de estos datos personales por el CNI no queda cubierto ni por el régimen general de protección de datos establecido en la LO 3/2018, ni por el específico régimen de protección previsto para el tratamiento de datos personales con fines de prevención, detección, investigación o enjuiciamiento de infracciones penales en la LO 7/2021. Esta exclusión, sin embargo, no viene acompañada de una regulación propia aplicable al tratamiento de los datos personales en poder del CNI. Por un lado, ni la LCNI[80] , ni la LOCNI regulan de manera expresa el derecho a la protección de datos personales por el CNI. Por otro lado, la Ley 9/1968, de 5 de abril, sobre secretos oficiales, tampoco contiene ningún precepto sobre esta cuestión.

---

[76] Cfr. RUIZ MIGUEL, C., Servicios de Inteligencia y seguridad del Estado constitucional, cit., p. 232.

[77] Por ello, RUIZ MIGUEL, C., *ídem*, p. 223, entiende que esta redacción era más correcta técnicamente, al no aludir a inexistentes disposiciones específicas sobre la materia.

[78] Un análisis más detallado de este precepto y de su redacción en el anteproyecto y el proyecto de ley orgánica, así como los informes emitidos por el Consejo de Estado y por el CGPJ puede verse en COLMENERO GUERRA, J.A., «La protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales vinculados al "discurso terrorista"», en GALÁN MUÑOZ, A., GÓMEZ RIVERO, M.C., (Dirs.), *La represión y persecución penal del discurso terrorista*, Tirant lo Blanch, 2022, pp. 706-716.

[79] https://www.cni.es/politica-de-privacidad. En todo caso, es necesario poner de manifiesto que el CNI sigue refiriéndose a la LO 15/1999, cuando ya está aprobada y ha entrado en vigor la LO 7/2021, de 26 de mayo, relativa a la protección de datos personales utilizados con fines penales.

[80] GONZÁLEZ CUSSAC, J.L., «Intromisión en la intimidad y servicios de inteligencia», cit., p. 174, se planteaba si del apartado primero del artículo 5 LCNI, y al tratarse los datos obrantes en el CNI de materia clasificada, pudiera derivarse que están «*relativamente exentos*» de todos los controles previstos en la ley de protección de datos.

Por lo que se refiere a las concretas normas que incluyen al CNI entre las autoridades competentes para recibir datos personales con fines penales, solo la LOPNR incluye una referencia al régimen de protección en relación con el CNI. Lo hace en la disposición adicional tercera: «Régimen jurídico del acceso por el Centro Nacional de Inteligencia a datos PNR. El acceso a los datos PNR por parte del Centro Nacional de Inteligencia y su control, se realizarán de acuerdo con lo previsto en esta ley orgánica, salvaguardando, en todo caso, el carácter de materia legalmente clasificada como secreto de sus actividades y objetivos, con el fin de dar cumplimiento a las misiones y funciones establecidas en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia». El régimen de protección de la LOPNR está diseñado para el tratamiento de los datos PNR por el CITCO que, aunque forma parte de la comunidad de inteligencia española[81] , en relación con los datos PNR su carácter esencial deriva de su condición de Unidad de Información sobre Pasajeros española[82] . La disposición adicional tercera garantiza que la cesión de datos PNR por el CITCO al CNI se ajustará a lo establecido con carácter general para la cesión de estos datos al resto de autoridades competentes[83] , pero no alcanza al tratamiento que el CNI haga de los datos PNR una vez que llegan a su poder y son utilizados para el cumplimiento de las funciones legalmente asignadas a este organismo.

La exención de seguridad nacional del artículo 4.2 TUE no puede ser vista en el sentido de que excluye totalmente la aplicación del Derecho de la Unión, tal y como señala la Agencia de la Unión Europea de Derechos Fundamentales (la FRA, conocida así por su acrónimo en inglés, *Fundamental Rights Agency*). El TJUE ha confirmado desde entonces esta conclusión, afirmando que los servicios de inteligencia de los Estados miembros no pueden invocar la seguridad nacional para eludir el Derecho de la Unión, incluidas las limitaciones que se derivan de los derechos fundamentales reconocidos en la CDFUE[84] .

Por ello, el hecho de que en las normas que regulan en la Unión Europea el tratamiento de datos personales con carácter general, y el tratamiento de datos personales con fines penales

---

[81] Tal y como señala FERNÁNDEZ SOLAS, M., «Modelos de inteligencia contra el terrorismo: una comparación entre España e Italia», en LOZANO MIRALLES, J. (Coord.), *La lucha contra el terrorismo en el marco del sistema de seguridad nacional. El papel de las Fuerzas Armadas, las Centrales de Inteligencia y las Fuerzas y Cuerpos de Seguridad del Estado*, Cizur Menor, Thomson Reuters-Aranzadi, 2021, p. 395. Sobre la comunidad de inteligencia española ver también SÁNCHEZ BARRILAO, J.F., «Servicios de inteligencia, secreto y garantía judicial de los derechos», cit., pp. 311-316.

[82] La LOPNR dedica tres preceptos a la protección de los datos PNR en cuanto datos de carácter personal: el artículo 11 («Régimen jurídico aplicable al tratamiento de los datos PNR»), el artículo 15 («Protección de los datos de carácter personal») y, el artículo 20 («Competencias de la Agencia Española de Protección de Datos»).

[83] Esto supone, por ejemplo, que el CITCO no podrá transmitir al CNI datos PNR que revelen información sensible; que el CITCO deberá llevar registros de toda cesión de datos PNR al CNI; o que el CITCO no podrá transmitir al CNI datos completos una vez transcurridos los seis primeros meses desde que fueron enviados por las compañías aéreas, salvo que hayan sido repersonalizados conforme al procedimiento establecido.

[84] Así lo señala expresamente la STJUE de 6 de octubre de 2020, La Quadrature du Net, ECLI:EU:C:2020:791: «En efecto, según reiterada jurisprudencia del Tribunal de Justicia, si bien corresponde a los Estados miembros determinar sus intereses esenciales de seguridad y adoptar las medidas adecuadas para garantizar su seguridad interior y exterior, el mero hecho de que se haya adoptado una medida nacional con el fin de proteger la seguridad nacional no puede dar lugar a la inaplicabilidad del Derecho de la Unión ni dispensar a los Estados miembros de la necesaria observancia de dicho Derecho» (apartado 99). Ver también: STJUE de 4 de junio de 2013, ZZ, C-300/11, EU:C:2013:363, apartado 38; la STJUE de 20 de marzo de 2018, Comisión/Austria (Imprenta del Estado), C-187/16, EU:C:2018:194, apartados 75 y 76; y la STJUE de 2 de abril de 2020, Comisión/Polonia, Hungría y República Checa (Mecanismo temporal de reubicación de solicitantes de protección internacional), C-715/17, C-718/17 y C-719/17, EU:C:2020:257, apartados 143 y 170.

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

en particular, exista una exclusión expresa en relación con el tratamiento de datos personales por los servicios encargados en los distintos Estados miembros de garantizar la seguridad nacional, así como la exclusión expresa en la legislación española del sometimiento del CNI al régimen general y particular de protección de datos personales, no significa que no exista un régimen mínimo de protección de los datos personales que se encuentran en poder de los servicios de inteligencia de los Estados miembros con carácter general, y del CNI en particular. Este nivel mínimo, pero también claro y expreso, viene conformado principalmente por la jurisprudencia del TEDH y del TJUE, así como por declaraciones de principios aprobadas por los Estados miembros, en cuanto Estados pertenecientes a otras organizaciones o instituciones internacionales, que han aprobado principios aplicables al tratamiento de datos personales por los servicios de inteligencia de los Estados miembros.

En nuestra opinión, el análisis del régimen de protección del tratamiento de datos personales por parte de los servicios de inteligencia de los Estados miembros en el cumplimiento de sus funciones de garantizar la seguridad nacional debe hacerse tomando como base las garantías establecidas en la Directiva (UE) 2016/680[85] . A partir de ahí, se trata de analizar en qué medida el singular objetivo de las agencias de inteligencia de los Estados miembros justifica, en el marco de la CDFUE, del CEDH y de su desarrollo jurisprudencial, un régimen jurídico propio, autónomo y más flexible que el establecido para el tratamiento de datos personales recogidos en la Unión Europea con fines de prevención, detección, investigación y enjuiciamiento de delitos graves[86] .

El tratamiento de datos personales con fines penales se articula desde la aprobación de la Directiva (UE) 2016/680 en torno a cuatro elementos clave: 1) El respeto a unos principios básicos relativos al tratamiento de datos personales con fines penales; 2) El reconocimiento de todo un conjunto de derechos a los titulares de los datos personales recopilados con fines penales, que, sin embargo, pueden ser objeto de excepciones en los casos legalmente previstos; 3) La necesidad de garantizar, con carácter general, la existencia de un delegado de protección de datos; y, 4) La existencia de una autoridad nacional de control. Estos elementos clave se han incorporado a nuestro ordenamiento de manera efectiva con la aprobación de la LO 7/2021, de 26 de mayo, que entró en vigor el 27 de julio de 2021[87] . Por ello, en las siguientes páginas pretendemos reflexionar sobre cuáles de las garantías previstas en la LO 7/2021 para la utilización de datos personales con fines penales por las autoridades competentes enumeradas en el artículo 4[88] , son trasladables a la utilización de datos

---

[85] Ver GUZMÁN FLUJA, V., «Consideraciones sobre el alcance objetivo y subjetivo de la Directiva UE 680/2016», cit., p. 854, y la doctrina allí citada.

[86] Objetivo que plantea GONZÁLEZ CUSSAC, J.L., «Intromisión en la intimidad y servicios de inteligencia», cit., p. 167. Como acertadamente señala COLMENERO GUERRA, J.A., «La protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales vinculados al "discurso terrorista"», cit., p. 629, ni la prevención, detección, investigación o enjuiciamiento de delitos, ni la defensa o seguridad nacional, admite el no respeto a los derechos fundamentales, entre ellos el de protección de datos.

[87] A pesar de que la fecha límite de transposición fijada en el artículo 63.1 de la Directiva 2016/680 era el 6 de mayo de 2018. La Comisión Europea interpuso recurso por incumplimiento ante el TJUE contra el Reino de España por no haber transpuesto la Directiva 2016/680. Recurso que se resolvió en la STJUE de 25 de febrero de 2021 (Asunto C-658/19), en la que el Tribunal de Justicia condenó a España a pagar 15.000.000€ y una multa diaria de 89.000€ mientras persistiese en el incumplimiento.

[88] El régimen de protección previsto en la LO 7/2021 se aplica al tratamiento con fines penales de datos personales por parte de quienes, conforme a esta ley orgánica, tienen la consideración de autoridades competentes: las Fuerzas y Cuerpos de Seguridad del Estado, las Administraciones Penitenciarias, la Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria, el Servicio Ejecutivo de la

personales para la realización de actividades «*extraprocesales, preventivas y prospectivas* como son las practicadas por los servicios de inteligencia»[89] . En definitiva, se trata de acomodar el régimen de protección de datos personales utilizados con fines penales a las finalidades constitucionales y legales atribuidas al CNI: prevenir y neutralizar amenazas a la defensa y seguridad nacional[90] . Sin perjuicio de que los Estados miembros gozan de un amplio margen de apreciación para decidir qué tipo de medidas pueden resultar necesarias para proteger la seguridad nacional, esta discrecionalidad no puede traducirse en exención de control y en no respeto a los principios esenciales de funcionamiento de la Unión Europea. De ahí la necesidad de establecer «salvaguardas mínimas» de inevitable cumplimiento para los servicios de inteligencia.

5.1 Principios aplicables al tratamiento de datos personales por el CNI

Los principios vertebradores del tratamiento de datos personales con fines de prevención, detección, investigación o enjuiciamiento de infracciones penales por las autoridades españolas competentes vienen expresamente enumerados en el artículo 6.1 LO 7/2021, conforme al cual, los datos personales han de ser: «a) Tratados de manera lícita y leal. b) Recogidos con fines determinados, explícitos y legítimos, y no serán tratados de forma incompatible con esos fines. c) Adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados. d) Exactos y, si fuera necesario, actualizados. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen, sin dilación indebida, los datos personales que sean inexactos con respecto a los fines para los que son tratados. e) Conservados de forma que permitan identificar al interesado durante un período no superior al necesario para los fines para los que son tratados. f) Tratados de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. Para ello, se utilizarán las medidas técnicas u organizativas adecuadas»[91] .

A ello hay que añadir que los ministros y representantes de todos los Estados miembros de la *Organization for Economic Co-operation and Development* (la OECD) y de la Unión Europea firmaron, en el mes de diciembre de 2022, una declaración en la que fijaron los principios rectores del acceso de los gobiernos a los datos personales en poder de entidades del sector privado[92] , con el objetivo de garantizar el acceso legítimo por parte de los

Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, la Comisión de Vigilancia de Actividades de Financiación del Terrorismo (art. 4.1), así como las autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal (art. 4.2).

[89] Tal y como las define GONZÁLEZ CUSSAC, J.L., «Intromisión en la intimidad y servicios de inteligencia», cit., p. 169.

[90] Como señaló la STEDH en el caso *S. y Marper c. Reino Unido* (GC), núms. 30562/84 y 30566/04, TEDH 2008, no todo lo que sea útil para los servicios de inteligencia es permisible en una sociedad democrática [como recuerda la STEDH *Asunto Big Brother Watch y otros c. Reino Unido* (Demandas núms. 58170/13, 62322/14 y 24960/15), párrafo 277].

[91] Se trata de una reproducción literal de los principios enumerados en el artículo 4.1 de la Directiva (UE) 2016/680 que, a su vez, reproduce de forma prácticamente mimética los principios enumerados en el artículo 6.1 RGPD, excepto el principio relativo a la transparencia y la proactividad.

[92] *Declaración sobre el acceso de los gobiernos a los datos personales en poder de las entidades del sector privado*, Instrumentos jurídicos de la OCDE, de 14-15 de diciembre de 2022, disponible en https://www.oecd.org/newsroom/adopcion-de-un-acuerdo-historico-para-salvaguardar-la-privacidad-en-el-

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

gobiernos a estos datos personales. El acceso de los gobiernos a los datos en poder de las entidades del sector privado se ha convertido en necesario para cumplir con los deberes y responsabilidades que tienen atribuidos en el ejercicio de su soberanía[93] , lo que requiere, en consecuencia, que las autoridades competentes para garantizar la seguridad nacional estén facultadas para acceder legítimamente a dichos datos. Por ello, es fundamental asegurar que el acceso de los gobiernos a los datos personales en poder de las entidades del sector privado no sea «ilimitado, excesivo, arbitrario o desproporcionado», es decir, incompatible con los valores democráticos y el Estado de derecho.

Estos principios son: I) Base legal: los Estados miembros deben tener un marco jurídico que establezca los fines, las condiciones, las limitaciones y las salvaguardias en relación con el acceso gubernamental a los datos personales en poder de las entidades privadas, de modo que los individuos dispongan de garantías suficientes contra el riesgo de uso indebido y abuso; II) Objetivos legítimos: el acceso de los gobiernos a los datos personales en poder de entidades privadas tiene como finalidad la consecución de objetivos específicos y legítimos, y se lleva a cabo conforme a los principios de necesidad, proporcionalidad y racionalidad, para evitar cualquier riesgo de abuso; III) Aprobación previa: el acceso debe efectuarse conforme a las normas, reglas y procedimientos aplicables que, además, deben exigir requisitos más estrictos para los casos de injerencias más graves. En los casos más graves, puede implicar la necesidad de solicitar la aprobación de autoridades judiciales o no judiciales imparciales. Además, las excepciones de emergencia a los requisitos de aprobación deben estar legalmente previstas y claramente definidas, con indicación de sus justificaciones, condiciones y duración; IV) Tratamiento de datos: los datos personales solo podrán ser procesados y tratados por personal autorizado, y se deben establecer reglas que garanticen la privacidad, seguridad, confidencialidad e integridad de los datos. Además, se deben establecer mecanismos para garantizar que los datos se procesen de forma legal, se conserven durante el tiempo necesario para el cumplimiento de la finalidad que persiguen, y se garantice la exactitud y actualización de dichos datos; V) Transparencia: el marco jurídico legal que rige el acceso de los gobiernos a los datos ha de ser claro de fácil acceso para el público. Se prevé incluso que las entidades privadas emitan informes estadísticos sobre las solicitudes de acceso gubernamental de conformidad con el marco jurídico; VI) Supervisión: han de existir mecanismos que permitan una supervisión eficaz e imparcial para garantizar que el acceso de los gobiernos a los datos personales se hace respetando el marco jurídico aplicable. La supervisión, señala el informe, se puede realizar a través de organismos como oficinas de cumplimiento interno, órganos jurisdiccionales, comisiones parlamentarias o legislativas y autoridades administrativas independientes; VII) El marco jurídico debe brindar a los individuos una efectiva reparación judicial y no judicial para identificar y resarcir las infracciones que hayan podido cometer los Estados en el acceso a datos personales en poder de entidades privadas[94] .

---

acceso-a-datos-policiales-y-de-seguridadnacional.htm#:~:text=La%20Declaraci%C3%B3n%20de%20la%20OCDE.que%20los%20organismos%20de%20seguridad

[93] En la propia Declaración se señala: «RECONOCEMOS el deber y la responsabilidad soberanos de todo país de proteger la seguridad de sus ciudadanos mediante la prevención, la detección y la lucha contra las actividades delictivas y las amenazas al orden público y a la seguridad nacional, con arreglo a los valores democráticos, el Estado de derecho y la protección de la privacidad y de otros derechos humanos y libertades».

[94] De los mecanismos de reparación se ocupa el Informe: El derecho a la privacidad en la era digital, 2018, párrafo. 50, p 15: «Las víctimas de vulneraciones o violaciones de la privacidad cometidas por los Estados o las empresas deben tener acceso a mecanismos de reparación eficaces». En relación con esta cuestión nos parece del máximo interés reproducir lo dispuesto en el apartado 56, p. 17: «La naturaleza de los daños causados por las vulneraciones de la privacidad es fuente de nuevos desafíos. Las consecuencias de este tipo de abusos son

5.2 Derechos del titular de los datos personales mientras se encuentran en poder del CNI

Una de las finalidades del RGPD es la de devolver el control de los datos personales a sus titulares mediante el reconocimiento de nuevos derechos que se garantizan a los ciudadanos (arts. 12 a 22 RGPD): derecho de información, acceso, rectificación, supresión, limitación del tratamiento y portabilidad de los datos. El poder de disposición y control sobre los datos personales, que constituye parte del contenido del derecho fundamental a la protección de datos, -y se concretan en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular-, «requiere como complementos indispensables por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos» (STC 292/2000, de 30 de noviembre).

Los derechos reconocidos en el RGPD, coloquialmente conocidos como derechos ARSOPOL[95] , alcanzan al tratamiento de datos personales con fines penales, pero pueden estar sometidos a ciertas restricciones como consecuencia de la finalidad para la que se van a utilizar. En todo caso, el punto de partida es que la Directiva (UE) 2016/680 reconoce específicamente los derechos de acceso, rectificación, supresión y limitación del tratamiento en relación con los datos personales penales en favor de sus titulares cuando sean objeto de tratamiento con fines penales. Este reconocimiento refleja claramente que en el seno de la Unión Europea «la protección de datos personales se ha insertado en la médula del sistema de enjuiciamiento criminal»[96] .

La LO 7/2021 recoge estos derechos de información, acceso, rectificación, supresión y limitación del tratamiento del titular de los datos personales utilizados con fines penales en el capítulo III (arts. 21 a 23), imponiendo la obligación de garantizarlos al organismo o autoridad que, en cada momento, sea responsable del tratamiento de los datos personales con fines penales[97] . Pues bien, todos estos derechos, que no desaparecen cuando los datos personales

difíciles de reparar y pueden tener efectos persistentes y otras consecuencias para los derechos humanos. La facilidad para conservar, intercambiar, reutilizar y fusionar datos y perfiles influye en la perdurabilidad de los datos digitales, lo que significa que las personas pueden enfrentarse a riesgos nuevos o persistentes para sus derechos en el futuro».

[95] Derecho de acceso, rectificación, oposición, supresión, limitación del tratamiento, portabilidad y oposición al tratamiento de decisiones automatizadas.

[96] COLOMER HERNÁNDEZ, I., «A propósito de la compleja trasposición de la Directiva 2016/680 relativa al tratamiento de datos personales para fines penales», *Diario La Ley*, nº 1979, 17 de abril de 2018; COLOMER HERNÁNDEZ, I., «Control y límites en el uso de la información y los datos personales por parte de la Inteligencia Artificial en los procesos penales», en BARONA VILAR, S. (ed.), *Justicia algorítima y neuroderecho. Una mirada multidisciplinar*, Valencia, Tirant lo Blanch, 2021, pp. 288-289. Ver también GUTIÉRREZ ZARZA, A., «La protección de las personas físicas en lo que respecta a su derecho a la intimidad y los datos personales por las autoridades de emisión y ejecución de las Órdenes Europeas de Investigación», en ARANGÜENA FANEGO, C., De HOYOS SANCHO, M., VIDAL FERNÁNDEZ, B., (Coords.), *Garantías procesales de investigados y acusados. Situación actual en el ámbito de la Unión Europea*, Valencia, Tirant lo Blanch, 2018, *tol. 6.958.342*.

[97] El responsable del tratamiento es «la autoridad competente que sola o juntamente con otras determine los fines y medios del tratamiento de datos personales; en caso de que los fines y medios del tratamiento estén determinados por el Derecho de la Unión o del Estado miembro, el responsable del tratamiento o los criterios específicos para su tratamiento podrán ser fijados por el Derecho de la Unión o del Estado miembro» (art. 3.8 Directiva 2016/680). El «encargado del tratamiento» es «la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable» (art. 3.9 Directiva 2016/680).

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

se tratan con fines penales[98] , tampoco desaparecen cuando se encuentran a disposición del CNI para el cumplimiento de las finalidades legalmente asignadas, sin perjuicio de que requieran cierta modulación y de que puedan ser objeto de restricción por parte del responsable del tratamiento. Cualquier otro planteamiento es, en nuestra opinión, erróneo, en cuanto induce a pensar que existe un ámbito exento de control, o «fuera de cobertura», del tratamiento de datos personales vinculado al fin para el cual se pretenden utilizar. Al igual que el CNI no tiene carta blanca para las restricciones al derecho a la inviolabilidad del domicilio o al secreto de las comunicaciones, ni sería admisible que empleara la tortura o restricciones del derecho a la libertad para obtener información, el derecho a la protección de datos también actúa como garantía en el desarrollo de las investigaciones de seguridad del CNI.

El «malentendido» al que, quizá conscientemente, quiere conducir el CNI con la leyenda incorporada en su régimen de privacidad, no puede hacernos olvidar que no hay ningún órgano del Estado que se sitúe al margen de la Constitución. El carácter secreto de las actividades del CNI, así como de las bases de datos que obran en poder de este organismo, no es óbice para la existencia de una regulación de los derechos ARSOPOL compatible con la protección de la seguridad nacional en nuestro Estado de Derecho.

Los ciudadanos necesitan poder emplazar a los gobiernos a informar sobre si efectivamente hicieron acopio masivo de sus datos, por qué lo hicieron y cuál fue el tratamiento al que fueron sometidos dichos datos[99] . El deber general de informar a los ciudadanos de la posibilidad de que sus datos personales sean recopilados por el CNI se garantiza con la existencia de normas que establezcan claramente los datos personales de los que puede hacer acopio el CNI. Esto ocurre en nuestro ordenamiento, como hemos tenido oportunidad de analizar, con los datos relativos al ADN, los datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, los datos PNR y los datos contenidos en el FTF, en los que, de manera expresa, cada una de las normas que regulan la recogida de estos datos normas incluyen al CNI entre las autoridades competentes para solicitar dichos datos.

Sin embargo, y como también hemos apuntado previamente, el deber general de colaboración con el CNI impuesto a todas las entidades públicas o privadas establecido en el artículo 5.5 LCNI, que podemos admitir, aunque bien es cierto que con muchas reticencias, como la norma habilitante para la cesión de datos personales que estas entidades hayan recopilado y conservado en el normal cumplimiento de sus funciones, no cumple, en nuestra opinión, todos los requisitos necesarios. Por ello, creemos que sería conveniente incorporar en la ley reguladora del CNI uno o varios preceptos similares a los contenidos en la LO 7/2021.

Más complicado resulta, sin embargo, que los ciudadanos tengamos la posibilidad de conocer si nuestros datos personales han sido efectivamente cedidos al CNI. El ejercicio del derecho de acceso, entendido en el sentido del derecho del titular de los datos a conocer si sus datos personales han sido efectivamente transmitidos al CNI, está limitado por el hecho de que la cesión de datos personales queda amparada por el carácter secreto de las actuaciones del CNI. Pero no impide que sea necesario establecer una vía a través de la cual los ciudadanos podamos ejercer esta dimensión del derecho a la protección de datos de carácter personal. El

[98] Sin perjuicio de que la propia Ley prevé la restricción de estos derechos cuando resulte necesario y proporcional para la consecución de los fines expresamente mencionados (art. 24.1 LO 7/2021).

[99] Cfr. SERRA CRISTÓBAL, R., «La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional», cit., p. 82. Ver también la bibliografía allí citada.

órgano competente ante el que hacer efectivo este derecho ha de tener en cuenta el carácter de materia clasificada de las bases de datos del CNI.

El derecho a la supresión de los datos personales en poder del CNI, o la limitación del plazo máximo de conservación por el CNI de datos personales de los ciudadanos, es una cuestión que necesariamente debe estar regulada por la Ley. Ni la finalidad de garantizar la seguridad nacional, ni el carácter secreto de las actividades del CNI, pueden ser argumentos para obstaculizar la imposición al CNI de la obligación de suprimir los datos personales transcurrido un determinado periodo de tiempo. Nada impide que se puedan trasladar al CNI los plazos previstos en el artículo 8 LO 7/2021. En primer lugar, el CNI conservará los datos exclusivamente durante el tiempo que sea necesario para el cumplimiento de los fines que motivaron su recogida. La determinación de este tiempo corresponde a la persona que ocupe la dirección del CNI. En segundo lugar, el CNI debe quedar obligado a revisar cada cierto periodo de tiempo la necesidad de conservar, limitar o suprimir el conjunto de datos personales bajo su responsabilidad. El apartado segundo del artículo 8 LO 7/2021 establece que esta revisión de los datos se ha de realizar, como máximo, cada tres años. Nos parece un plazo de tiempo que puede aplicarse sin problema al CNI, que se vería obligado igualmente a ajustarse a estos plazos de revisión. En tercer lugar, la LO 7/2021 establece un plazo máximo de conservación de los datos personales de veinte años, «salvo que concurran factores como la existencia de investigaciones abiertas o delitos que no hayan prescrito, la no conclusión de la ejecución de la pena, reincidencia, necesidad de protección de las víctimas u otras circunstancias motivadas» (art. 8.3 LO 7/2021[100]). La futura ley que debe ser aprobada debería precisar cuáles serían los supuestos en los que hasta el plazo máximo de veinte años podría ser ampliado por la autoridad competente para que el CNI pudiera seguir ejerciendo sus funciones. En todo caso, en la supresión de datos personales por el CNI debería otorgarse un papel relevante al Magistrado del Tribunal Supremo competente para autorizar las medidas restrictivas de derechos fundamentales derivadas de las actuaciones del CNI.

En último lugar, es necesario resaltar la importancia de limitar el tratamiento de los datos personales por el CNI, en un momento en el que los avances tecnológicos avisan claramente de la amenaza que supone la utilización de la inteligencia artificial en el tratamiento automatizado de datos personales. La ley debería establecer con precisión los límites del tratamiento automatizado de datos personales por el CNI[101] . Esta regulación debería incluir, además, la obligación de que cualquier resultado positivo que se derivara del tratamiento

[100] Como acertadamente señala COLMENERO GUERRA, J.A., «La protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales vinculados al "discurso terrorista"», cit., p. 717, no es sólo que la regla general establecida en este precepto sea «desproporcionada y excesiva, y no ajustada al respeto del núcleo esencial del art. 18.4 CE», sino que la salvedad prevista en este precepto hace que sea «posible alargar dicho plazo, en principio sin intervalo exacto». Ver también, de este mismo autor, COLMENERO GUERRA, J.A., «La Ley Orgánica 7/2021, de protección de datos en materia penal: ámbito y principio de proporcionalidad», en COLOMER HERNÁNDEZ, I. (Dir.), *Uso de la información y de los datos personales en los procesos: los cambios en la era digital*, Thomson Reuters-Aranzadi, Cizur Menor, 2022, pp. 475-477. La Enmienda núm. 16 presentada por el Grupo Plural al artículo 8 del Proyecto de ley orgánica, que se publicó en el Boletín Oficial del Congreso de los Diputados el 19 de febrero de 2021, señalaba que no podía establecerse un plazo genérico de hasta veinte años, y que esto se hiciese depender en exclusiva del juicio del responsable del tratamiento.

[101] El TEDH ha señalado que el Convenio 108 admite la posibilidad de excluir parte del régimen protector de los datos personales cuando esta medida resulte necesaria en una sociedad democrática para salvaguardar ciertos fines, como la protección de la seguridad del Estado o la seguridad pública (art. 9.2.a del Convenio 108). En todo caso, el tratamiento de datos personales sin consentimiento del interesado solo resulta compatible con las exigencias del artículo 8 CEDH y del Convenio 108 cuando está sometido a algún tipo de control, que, evidentemente, alcanza a los servicios de inteligencia.

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

automatizado de los datos personales por el CNI, que hubiera dado lugar a la identificación de una persona o grupos de personas, fuera sometida a una verificación por medios no automatizados. Es decir, la norma debería incluir la previsión de que no se puede derivar ninguna consecuencia negativa para el titular de los datos basado exclusivamente en el tratamiento automatizado de sus datos personales. Esta verificación por medios no automatizados correspondería realizarla a alguno de los miembros del CNI.

5.3 La inexistencia de un delegado de protección de datos en el CNI

El RGPD obliga a toda autoridad u organismo del sector público que lleve a cabo un tratamiento de datos personales, salvo los juzgados y tribunales en el ejercicio de la potestad jurisdiccional, a designar un delegado de protección de datos (art. 37 RGPD), que es el responsable de gestionar el cumplimiento del RGPD. Se trata de una de las novedades más relevantes en el paquete normativo que se aprobó en abril de 2016[102] , y su introducción es consecuencia del «giro copernicano que ha sufrido el modelo de responsabilidad al que están sujetos los responsables y encargados del tratamiento en el desarrollo de las actividades que impliquen tratamiento de datos de carácter personal»[103] . La obligación de designar un delegado de protección de datos alcanza a los responsables del tratamiento de datos personales con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, salvo a los órganos jurisdiccionales y al Ministerio Fiscal cuando el tratamiento de datos personales se realice con fines jurisdiccionales (art. 40.1 LO 7/2021). Las funciones del delegado de protección de datos, enumeradas en el artículo 42 LO 7/2021, se concretan esencialmente en la función de información, asesoramiento y supervisión del tratamiento de datos personales con fines penales llevado a cabo por los responsables del tratamiento.

La no aplicación del régimen general de protección de datos personales al tratamiento de datos por el CNI implica que la obligatoriedad de nombrar un delegado de protección de datos no incluye al CNI. Esto no impide, sin embargo, que se considere conveniente o procedente su designación[104] . En este sentido, el CITCO, que depende de la Secretaría de Estado de Seguridad del Ministerio del Interior, y que, al igual que el CNI, forma parte de los servicios de inteligencia del Estado español, y cuyas actividades también tienen el carácter de reservadas, sí que cuenta con un delegado de protección de datos[105] .

---

[102] La Directiva 95/46/CE no establecía la obligación de designar un delegado de protección de datos.

[103] Montoro Sánchez, J.A., *Uso y cesión de datos de carácter personal en el proceso penal*, cit., p. 227.

[104] Por ejemplo, aunque el Ministerio Fiscal no está obligado a designar un delegado de protección de datos, sí que se ha procedido a su designación (Ver la Instrucción 2/2019, de 20 de diciembre, de la Fiscalía General del Estado, sobre la protección de datos en el ámbito del Ministerio Fiscal: el responsable y el Delegado de Protección de Datos). Esto no ha ocurrido, sin embargo, en el caso de los juzgados y tribunales.

[105] El delegado de protección de datos en el CITCO actuará como punto de contacto único, al que cualquier interesado tendrá derecho a dirigirse para todas las cuestiones relativas al tratamiento de sus datos PNR, y velará por que se adopten las medidas oportunas para controlar el tratamiento de los datos PNR y por que se apliquen las garantías en materia de protección de datos (art. 8.1 LOPNR). Este delegado deberá contar con los medios necesarios y tener acceso a todos los datos PNR tratados por el CITCO para poder cumplir eficazmente las funciones legalmente establecidas (art. 8.2 y 3 LOPNR). El CITCO no podrá oponerse a este acceso alegando la existencia de un deber de confidencialidad o secreto (art. 41.3 LO 7/2021). En definitiva, el carácter secreto de las actuaciones llevadas a cabo por el CITCO no afecta al control del tratamiento de los datos personales llevado a cabo por este organismo. Los datos de contacto del delegado de protección de datos son: Oficina Nacional de Información sobre Pasajeros (ONIP) del Centro de Inteligencia Contra el Terrorismo y Crimen Organizado:

El CNI, sin embargo, se integra en el Ministerio de Defensa. Aunque en este Ministerio también hay un delegado de protección de datos[106] , no creemos, sin embargo, que deba ser él quien ejerza las funciones de delegado de protección de datos en los casos de tratamiento de datos por el CNI. En el supuesto de que se optara por designar un delegado de protección de datos, debería nombrarse uno específico para el CNI[107] . En todo caso, en nuestra opinión, puede aceptarse que en el CNI no haya delegado de protección de datos. La cuestión esencial es, como veremos en el epígrafe siguiente, garantizar la existencia de una autoridad de control.

5.4 La Comisión de Secretos Oficiales como Autoridad Nacional de control de datos personales en el CNI: ¿una posible solución?

Desde los orígenes del derecho a la protección de datos personales en Europa, el establecimiento de una autoridad de control independiente ha constituido un elemento esencial inherente a este derecho, tal y como se indicaba expresamente en el Considerando 62 de la Directiva 95/46/UE. El respeto a la protección de datos de carácter personal quedará sujeto al control de una autoridad independiente (art. 8.3 CDFUE), cuya función es la de supervisar el cumplimiento de la normativa de protección de datos en favor de los interesados[108] . En este sentido, mientras que es aceptable que en el CNI no haya un delegado de protección de datos, no lo es la inexistencia de una autoridad de control[109] .

La independencia de la autoridad de control en el desempeño de sus funciones y en el ejercicio de sus poderes es la principal característica que el RGPD exige a esta autoridad (art. 52)[110] . La Agencia Española de Protección de Datos (en adelante, AEPD), y las

Responsable de Protección de Datos. C\Josefa Valcárcel, 28-5ª, Madrid 28071. Correo electrónico: citco.dpd.onip@interior.es

[106] El Ministerio de Defensa, tal y como establece el RGPD, tiene designado un Delegado de Protección de Datos. Los interesados podrán ponerse en contacto con dicho Delegado en la siguiente dirección de correo electrónico: DPD@mde.es (https://www.defensa.gob.es/comun/politica-de-privacidad.html).

[107] Sobre la independencia del responsable de protección de datos, ver Recio Gayo, M., *El estatuto jurídico del Data Protection Officer*, La Ley Wolters Kluwer, 2019, pp. 196-213, que recuerda el valor esencial que esta independencia supone para garantizar de manera adecuada el derecho fundamental a la protección de datos de carácter personal.

[108] Sobre esta autoridad de control ver: Montoro Sánchez, J.A., *Uso y cesión de datos de carácter personal en el proceso penal*, cit., pp. 216-226; Villalba Cano, L. «El derecho a presentar una reclamación ante una autoridad de control (Comentario al artículo 77 RGPD)», en Troncoso Reigada, A., (Dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de protección de datos personales y garantía de los derechos digitales*, Tomo II, Cizur Menor, Civitas-Thomson Reuters, 2021, p. 2968; Frías Martínez, E., «Ficheros jurisdiccionales. Autoridad de control», en *Diario La ley*, núm. 9986, 11 de enero de 2022; Soleto Muñoz, H., Alcoceba Gil, J., «Protección de datos y transmisión de perfiles de ADN», en Cabezudo Bajo, M.J., (Dir.), *Las bases de datos policiales de ADN. ¿Son una herramienta realmente eficaz en la lucha contra la criminalidad grave nacional y transfronteriza?*, Madrid, Dykinson, 2013, p. 335.

[109] González Cussac, J.L., Flores Giménez, F., «Una metodología para el análisis de las amenazas a la seguridad, la evaluación de las respuestas y su impacto sobre los derechos fundamentales», cit., pp. 57-58, recuerdan que «la fiabilidad, consistencia y la propia utilidad de los servicios de inteligencia en una sociedad democrática dependen de la medida en que se atengan a los términos de un mandato capaz de suscitar un amplio consenso y en el que los objetivos, los límites de los métodos de trabajo, así como la rendición de cuentas y el control externo se encuentran claramente perfilados».

[110] Tal y como se indica también en el Considerando 117: «El establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercitar sus competencias con plena

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

correspondientes Agencias de las Comunidades Autónomas, son las autoridades administrativas independientes reguladas en la LO 3/2018. La AEPD «actuará en todo caso cuando sea precisa la investigación de tratamientos que implique un tráfico masivo de datos personales» (art. 67.1.II LO 3/2018)[111] .

La existencia de autoridades que ejerzan sus funciones de control con plena independencia constituye la «columna vertebral» de todo el sistema de garantías de los derechos de los ciudadanos frente al tratamiento de sus datos personales con fines penales[112] , de ahí que la Directiva (UE) 2016/680 imponga a los Estados miembros la obligación de designar una, o varias, autoridades públicas independientes para supervisar el tratamiento de datos personales con fines penales (art. 41.1)[113] . En la designación de esta autoridad de control, los Estados miembros son libres para decidir si confían esta función a la autoridad de control creada al amparo de lo previsto en el RGPD, o si, por el contrario, atribuyen esta competencia a una autoridad creada específicamente para supervisar el tratamiento de los datos personales con fines penales. Esta libertad de elección ha llevado a la doctrina a cuestionarse cuál de las dos opciones debe considerarse más adecuada: si la de configurar una autoridad de control específica para el tratamiento de los datos personales con fines penales, o si, por el contrario, basta con que esta autoridad sea la misma que para los tratamientos de datos personales con fines privados. Si bien lo fundamental es que esta autoridad de control sea independiente, lo cierto es que la opción por uno de estos modelos tiene su relevancia.

El legislador español finalmente ha atribuido la condición de autoridad nacional de control a la AEPD, sin perjuicio de las competencias que les corresponden a las autoridades autonómicas de protección de datos (art. 48 LO 7/2021). Es decir, no ha establecido una autoridad nacional de control específica para el tratamiento de los datos personales con fines penales, a pesar de que eran varias las razones que aconsejaban optar por esta solución, tales como la especialidad de la materia objeto de supervisión y la trascendencia e importancia de esta función de supervisión[114] . En los próximos años veremos si esta decisión fue la correcta, o si es necesario proceder a una revisión de los planteamientos y crear una autoridad específica para la protección de datos personales utilizados con fines penales. En todo caso, la AEPD comparte su condición de autoridad nacional con la Dirección General de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial como autoridad de

independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal».

[111] Este inciso fue consecuencia de la admisión de la Enmienda núm. 20 presentada por el Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea, que pretendía «reforzar las garantías de que la Agencia Española de Protección de Datos podrá velar eficazmente por el ejercicio de los derechos de las personas ante el creciente tráfico de nuestros datos desde empresas hasta otras empresas y hasta el sector público».

[112] Tal y como señala COLOMER HERNÁNDEZ, I., «A propósito de la compleja trasposición de la Directiva 2016/680 relativa al tratamiento de datos personales para fines penales», cit. Ver también el Considerando (75) de la Directiva (UE) 2016/680.

[113] El principio 1 de la Recomendación núm. R(87)15 del Comité de Ministros del Consejo de Europa, de 17 de septiembre de 1987, dirigida a regular la utilización de datos de carácter personal por la policía, ya requería el establecimiento de una autoridad independiente que supervisase el procesamiento de datos personales por la policía, exigiendo al mismo tiempo que los ficheros policiales que contuviesen datos personales fuesen notificados a la autoridad de supervisión.

[114] Ver COLOMER HERNÁNDEZ, I., «Control del tratamiento de datos personales penales y tutela judicial efectiva en la Directiva 2016/680», en GUTIÉRREZ ZARZA, M.A., (Coord.), *Los avances del espacio de libertad, seguridad y justicia en la Unión Europea en 2017*, II Anuario, ReDPE, pp. 117-118; y también en COLOMER HERNÁNDEZ, I., «A propósito de la compleja trasposición de la Directiva 2016/680 relativa al tratamiento de datos personales para fines penales, cit.

control de los tratamientos de datos vinculados al ejercicio de la función jurisdiccional (art. 236 nonies LOPJ), y con la Unidad General de Supervisión y Control de Protección de Datos de la Fiscalía General del Estado (art. 20.4 EOMF).

La AEPD no es, sin embargo, la autoridad nacional de control competente para controlar las actuaciones del CNI. Así lo puso de manifiesto la propia Agencia al inadmitir a trámite la denuncia presentada por la presidenta del Parlamento de Cataluña con motivo del programa Pegasus. En la denuncia presentada ante la AEPD se ponía de manifiesto que, entre los años 2015 y 2020, diversas personalidades de la sociedad civil y política de Cataluña, entre ellas miembros del Parlamento de Cataluña, habían sufrido intromisiones en sus dispositivos electrónicos mediante el programa Pegasus. La AEPD inadmitió a trámite dicha denuncia, al señalar que no es competente para conocer los hechos que se ponen de manifiesto, dado que se refieren a actuaciones supuestamente realizadas por el CNI que constituyen materia clasificada y, por tanto, están excluidas de la aplicación de la LO 3/2018 y de la LO 7/2021[115] .

La cuestión que queda sin respuesta es cuál es la autoridad de control en el caso del tratamiento de datos personales por el CNI, en cuanto que no hay ninguna norma que haga referencia a esta cuestión. A la hora de identificar cuál debe ser dicha autoridad es esencial tomar como punto de partida la especial naturaleza y función del CNI. Por ello, resulta inevitable acudir a la Ley 9/1968 de 5 de abril, sobre secretos oficiales, que excluye del principio de publicidad de las actuaciones de los órganos del Estado las materias «clasificadas», cuyo secreto o limitado conocimiento queda amparado por la presente Ley (art. 1.1 LSO). La declaración de materias clasificadas, en cualquiera de sus dos variedades, secreta o reservada, no afecta ni al Congreso de los Diputados ni al Senado, que tendrán siempre acceso a cuanta información reclamen, en la forma en que determinen sus respectivos Reglamentos y, en su caso, en sesiones secretas[116] .

El control parlamentario sobre el funcionamiento y actividades del CNI corresponde a la Comisión que controla los créditos destinados a gastos reservados del Congreso de los Diputados, coloquialmente conocida como la «Comisión de Secretos Oficiales»[117] . Esta Comisión se crea por la Ley 11/1995, de 11 de mayo, reguladora de la utilización y control de los créditos destinados a gastos reservados, está presidida por la persona que ocupe la presidencia del Congreso de los Diputados, y la integran aquellos Diputados que, de conformidad con la normativa parlamentaria, tienen acceso a secretos oficiales (art. 7.1). No

---

[115] Referencia: IT/04563/2022. Ver *Memoria Anual 2022*, de la AEPD, pp. 103-104, disponible en: https://www.aepd.es/es/documento/memoria-aepd-2022.pdf.

[116] Sobre esta cuestión ver ALONSO DE ANTONIO, A.L., «Conocimiento por los parlamentarios de las materias clasificadas en virtud de la Ley de Secretos Oficiales», en *Foro, Nueva época*, vol. 21, núm. 2, 2018, pp. 19-44; GARCÍA-TREVIJANO GARNICA, E., «Materias clasificadas y control parlamentario», cit., p. 159; WILKINSON MORERA DE LA VALL, H., *Secretos de Estado y Estado de Derecho: régimen jurídico de los secretos oficiales en España*, Atelier, 2007, pp. 125-148. Para MARTÍNEZ VÁZQUEZ, F., «El control parlamentario de los secretos oficiales», en *Revista de las Cortes Generales*, núm. 104, 2018, p. 411, el control parlamentario de los secretos oficiales ha de verse como una prueba de la calidad de la democracia parlamentaria.

[117] Ver DÍAZ FERNÁNDEZ, A.M., «Modelos de control parlamentario de los servicios de inteligencia», en *Estudio/Working Paper*, núm. 139/2012. Bastante crítico con esta Comisión "estrella", se mostró en su momento CANO BUESO, J., «Información parlamentaria y secretos oficiales», en *Revista de las Cortes Generales*, núm. 42, 1997, pp. 30-31, lo que le lleva a proponer (p. 34) la necesidad de «crear una verdadera Comisión parlamentaria, con estructura, funcionamiento y poderes perfectamente definidos», así como la necesidad de definir el acceso a las materias clasificadas tanto por el Parlamento como por la autoridad judicial. Para FERNÁNDEZ RODRÍGUEZ, J.J., «Los límites al acceso a la información en España: A propósito del terrorismo», en *Revista Española de la Transparencia*, núm. 5, 2017, p. 141, esta Comisión «equilibra la necesidad democrática de información de los parlamentarios con las exigencias de secreto».

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

obstante, hay que esperar hasta el año 2002, cuando se aprueba la LCNI, para que se le atribuya el control parlamentario del CNI.

Las sesiones de la Comisión son secretas, y sus miembros no pueden divulgar las informaciones obtenidas (art. 7.3 de la Ley 11/1995, art. 16 del Reglamento el Congreso de los Diputados, y apartado noveno de la Resolución de la Presidencia del Congreso de los Diputados sobre secretos oficiales, de 26 de abril de 2022). La actuación de la Comisión de Secretos Oficiales del Congreso de los Diputados se rige por lo dispuesto en la Resolución de la Presidencia del Congreso de los Diputados sobre secretos oficiales, de 26 de abril de 2022, que derogó a la anterior resolución de 11 de mayo de 2004[118] . Las modificaciones que se han llevado a cabo en el acceso por el Congreso de los Diputados a materias clasificadas, desde que se reguló por primera vez con la Resolución de la Presidencia de 18 de diciembre de 1986 hasta esta última resolución de abril de 2022, han tenido por finalidad posibilitar que el pluralismo político representado en la Cámara tenga acceso a las materias clasificadas a través de un diputado por cada Grupo Parlamentario[119] . En este sentido, y tal y como señala el apartado tercero de la Resolución de la Presidencia, de 26 de abril de 2022, en los supuestos de materias clasificadas como secretas, «el Gobierno facilitará la información recabada a un Diputado por cada Grupo Parlamentario. Los Diputados serán elegidos al efecto por el Pleno de la Cámara por mayoría absoluta». Además, «(m)otivadamente y con carácter excepcional, el Gobierno podrá solicitar de la Mesa de la Cámara que la información sobre una determinada materia declarada secreta sea facilitada exclusivamente a la Presidencia del Congreso, o al de la Comisión, cuando la petición hubiese sido formulada por esta última. Corresponde, en todo caso, a la Mesa del Congreso la resolución definitiva sobre la solicitud del Gobierno» (apartado quinto de la Resolución de 26 de abril de 2022).

En nuestra opinión, la Comisión de Secretos Oficiales podría asumir la condición de autoridad nacional de control en lo relativo al tratamiento de los datos personales por parte del CNI, con la finalidad de garantizar que dicho tratamiento se ajuste a los principios generales derivados del derecho a la protección de datos personales. Entre sus funciones como autoridad nacional destacarían, esencialmente, el control sobre la forma de obtención de datos personales, la proporcionalidad en la obtención de datos personales de los ciudadanos, el periodo de conservación de dichos datos, así como el tratamiento automatizado que, en su caso, el CNI haya llevado a cabo de dichos datos. Todo ello con el objetivo de garantizar que el acopio de datos personales por el CNI ha sido la estrictamente necesaria para la obtención de inteligencia vital para el cumplimiento de las funciones que legalmente tiene asignadas. Esta Comisión garantizaría el carácter independiente exigible a la autoridad de vigilancia, aunque sería necesario, además, garantizar, que dispusiera de los conocimientos técnicos, competencias y recursos pertinentes y adecuados para el adecuado desarrollo de dicha supervisión[120] .

---

[118] Una evolución histórica de la regulación sobre el acceso de los parlamentarios a las materias clasificadas puede verse en ALONSO DE ANTONIO, A.L., «Conocimiento por los parlamentarios de las materias clasificadas en virtud de la Ley de Secretos Oficiales», cit., pp. 30-33.

[119] Esta Resolución ha modificado las mayorías necesarias para nombrar a sus miembros, pasando de los tres quintos que exigía la Resolución de 11 de mayo de 2004, a la mayoría absoluta.

[120] Requisitos exigidos a la autoridad de supervisión en el Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, «El derecho a la privacidad en la era digital», de 3 de agosto de 2010, apartado 40, p. 11 (Ref: A/HRC/39/29).

6. La relación entre las investigaciones de seguridad y las investigaciones criminales

En este último apartado queremos abordar el análisis de una de las consecuencias más preocupantes que trae consigo, por un lado, la facilidad del CNI para hacer acopio de datos personales y, por otro, la falta de un régimen de protección de los datos personales cuando se encuentran en poder del CNI: la posibilidad de que estos datos puedan ser la base o servir de apoyo a las investigaciones preliminares llevadas a cabo por la policía judicial y que, en consecuencia, puedan acabar finalmente incorporados a un proceso penal[121] .

Las investigaciones de seguridad del CNI pueden definirse como investigaciones secretas «de carácter estratégico, exploratorio, táctico, preventivo, general, prospectivo»[122] , cuyo objetivo es recopilar información y transformarla en inteligencia al servicio de la seguridad nacional. Por tanto, la función legal del CNI no es la investigación de delitos, sin perjuicio de que si en el curso de sus labores averiguan o tienen indicios de acciones delictivas lo pongan en conocimiento de los órganos policiales y judiciales competentes; pero, como insiste la Sala II del Tribunal Supremo, la actividad del CNI «no va encaminada directamente al descubrimiento de delitos, ni tiene como condicionante la previa comisión de alguno». El CNI y la policía, incluidos los órganos policiales de inteligencia, trabajan en esferas diferenciadas, especialmente en lo relativo a la represión y neutralización de la actividad criminal. Por ello, los miembros del CNI no tienen la consideración de agentes de la autoridad y, en consecuencia, su misión no está orientada a la investigación preliminar de los procesos penales[123] .

No obstante, y aunque las actividades del CNI no están funcionalmente subordinadas al esclarecimiento de hechos aparentemente constitutivos de delito, la posibilidad de que un órgano de la jurisdicción penal incorpore a la causa de la que está conociendo material procedente del CNI, y clasificado como secreto, está abierta en nuestro sistema (STS núm. 1094/2010, de 10 de diciembre)[124] . La inexistencia de un régimen general de protección de los datos personales cuando están en poder del CNI se completa con la ausencia de cualquier regulación de la cesión de datos personales por parte del CNI a la policía. Es cierto que este no es solo un defecto de regulación en estos casos, pues la doctrina lleva años poniendo de manifiesto los problemas que plantea la falta de regulación de la cesión de datos personales

---

[121] GUZMÁN FLUJA, V., «Consideraciones sobre el alcance objetivo y subjetivo de la Directiva UE 680/2016», cit., p. 852, ya dejaba apuntada la cuestión, al señalar la importancia de configurar un régimen de protección de datos en el marco de la seguridad nacional; «régimen, que por limitado que deba ser, debe existir, debe ser el punto de partida sobre el que apoyarse cuando el tratamiento de datos personales pueda entrecruzarse o ser aplicado tanto a la protección de la seguridad nacional, como a la prevención y protección de la seguridad pública, como a la prevención, detección, investigación o enjuiciamiento de infracciones criminales».

[122] SERRA CRISTÓBAL, R., *La seguridad como amenaza. Los desafíos de la lucha contra el terrorismo para el Estado democrático*, Valencia, Tirant lo Blanch, 2020, p. 103; y también en «La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional», *UNED. Revista de Derecho Político*, nº. 92, enero-abril 2015, p. 81.

[123] Ver SANSÓ-RUBERT PASCUAL, D., «La articulación de la comunidad de inteligencia española: realidad y perspectiva de futuro», en *Boletín de Información. Centro Superior de Estudios de la Defensa Nacional*, núm. 297, 2006, p. 61. PÉREZ VILLALOBOS, M.C., *Derechos fundamentales y servicios de inteligencia*, cit., p. 145, recuerda que los agentes del CNI no pueden detener ni retener a una persona, ni interrogarla, ni, por supuesto, someterla a condiciones o procedimientos que supongan sufrimiento físico o mental.

[124] Ver también STS núm. 1140/2010, de 29 de diciembre (ECLI:ES:TS:2010:7184); SAN núm. 9/2022, de 31 de marzo.

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

entre procesos penales, incluyendo igualmente los peligros de la cesión de datos personales entre procesos penales y procesos administrativos sancionadores[125] . Por ello, es esencial que el legislador afronte la necesaria regulación de la transmisión de datos por parte del CNI a las autoridades competentes para la investigación de los hechos delictivos. De hecho, el Anteproyecto de Ley de Enjuiciamiento Criminal elaborado por el Ministerio de Justicia en 2020, que lamentablemente hoy descansará plácidamente en un cajón, ya incluyó una sección sobre «El acceso y tratamiento de datos personales» (arts. 514-520), en los que se regulaban las principales líneas de actuación en relación con la obtención, adquisición, tratamiento y valor probatorio de los datos personales en las investigaciones penales.

Las investigaciones de seguridad y las investigaciones criminales hace muchos años que no discurren por caminos separados y las posibilidades de confluencia e intercambio de información son una realidad a la que el legislador no puede permanecer por más tiempo indiferente[126] . Es necesario evitar que se incorporen al proceso penal datos que, procediendo del CNI, no se ajusten a los requisitos exigidos por el contenido esencial del derecho a la protección de datos personales.

6.1 La intervención del Magistrado del Tribunal Supremo no judicializa el expediente de seguridad del CNI

La incorporación de datos personales al proceso penal requiere, en primer lugar, que en aquellos casos en que una Ley exija la autorización judicial previa para la cesión de datos a la policía, la policía obtenga dicha autorización. Además, y como tuvimos oportunidad de poner de manifiesto en un epígrafe anterior, aunque no exista una norma que requiera la previa habilitación legal, habrá que estar a los criterios establecidos por el Tribunal Supremo y el Tribunal Constitucional para determinar si la obtención del dato requiere dicha autorización judicial, o si la «levedad» de la injerencia en los derechos fundamentales del titular del dato permite el acceso directo por la policía.

Los actos de investigación desarrollados por el CNI con la previa autorización del Magistrado competente del Tribunal Supremo encargado del control previo de las actividades de los servicios de inteligencia no pueden ser catalogados como actos judiciales de investigación. El auto del Magistrado del Tribunal Supremo habilitante para la adopción de la medida restrictiva de derechos fundamentales, en este caso, acordando la cesión de datos personales al CNI, no judicializa la investigación de seguridad del CNI. La necesaria autorización judicial no transmuta la esencia de la investigación del CNI, que es una investigación llamada a permanecer ajena al proceso, salvo en supuestos muy excepcionales. Por ello, los datos personales que se transmiten al CNI no tienen vía libre para incorporarse al

---

[125] Esta cuestión viene siendo tratada desde hace años por un importante sector doctrinal en diversas publicaciones colectivas: COLOMER HERNÁNDEZ, I. (Dir.), *Uso de la información y de los datos personales en los procesos: los cambios en la era digital*, Cizur Menor, Thomson Reuters-Aranzadi, 2022; COLOMER HERNÁNDEZ, I. (Dir.), *Uso y cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios*, Cizur Menor, Thomson Reuters-Aranzadi, 2019; COLOMER HERNÁNDEZ, I. (Dir.), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la UE*, Cizur Menor, Thomson Reuters-Aranzadi, 2015.

[126] En este sentido, SERRA CRISTÓBAL, R., *La seguridad como amenaza. Los desafíos de la lucha contra el terrorismo para el Estado democrático*, cit, p. 103; y también en «La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional», cit., p. 81, señala que aunque la investigación preliminar de la policía «tradicionalmente no ha respondido al patrón de un programa de vigilancia general e indiscriminado», en este tema «las cosas parecen estar cambiando».

proceso penal. El proceso penal no es una continuación natural del expediente de seguridad tramitado por el CNI, de tal manera que entre ambos «no existe una secuencia cronológica que permita establecer una suerte de tracto sucesivo que enlace la actividad del CNI y la que desarrolla con posterioridad el Juez de instrucción». Los actos generados por el CNI, aunque hayan estado sometidos al control previo del Magistrado autorizante, «no son verdaderos actos de prueba. No fueron concebidos como medios de prueba -ni siquiera como diligencias de investigación- en un proceso penal» (STS núm. 1094/2010)[127] . En definitiva, «la existencia de un ulterior proceso penal en el que la *notitia criminis* no sea ajena al expediente de seguridad tramitado por el CNI, no implica la transmutación de la funcionalidad de ese expediente, que dejaría de ser lo que es, distanciándose de sus principios reguladores, para convertirse en un acto procesal *sine qua non* del verdadero proceso y, por tanto, sometido a las reglas generales que disciplinan el principio de publicidad».

No es posible situar en el mismo plano las consecuencias que la LECrim asocia a la petición de autorización judicial para acordar una medida restrictiva de derechos fundamentales, y las consecuencias que han de derivarse de la autorización acordada por el Magistrado del Tribunal Supremo en el marco de una investigación de seguridad. No solo se trata de que el desarrollo del expediente de seguridad llevado a cabo por el CNI no está inspirado en los principios de contradicción y defensa, sino que el análisis que el Magistrado del Tribunal Supremo realiza sobre la solicitud de cesión de datos personales presentada por la persona que ocupa la dirección del CNI no se puede comparar con el que debe llevar a cabo el juez de instrucción cuando se encuentra con una solicitud de cesión de datos personales procedente de la policía o del Ministerio Fiscal. Es decir, la autorización judicial previa del Magistrado del Tribunal Supremo competente que permite la cesión de datos personales al CNI no es equiparable, ni sustituye, a la necesaria autorización judicial exigida para la obtención de estos mismos datos por la policía judicial.

La autorización del Magistrado del Tribunal Supremo legitima la incorporación de los datos personales a las bases de datos del CNI, y legitima que puedan ser utilizados para la elaboración de inteligencia y, en definitiva, el cumplimiento de los fines asignados al Centro. Pero esta autorización judicial no legitima la utilización de estos datos como fuente de prueba en un proceso penal. Las garantías previstas en la LOCNI para la injerencia en los derechos fundamentales a la inviolabilidad del domicilio y al secreto de las comunicaciones que, como hemos señalado, han de aplicarse a los datos personales solicitados por el CNI cuando una ley exija previa autorización judicial, no son las mismas que las exigidas para la práctica de estas mismas diligencias en el seno de un proceso penal. Las garantías que rodean la obtención del dato con fines de investigación de hechos delictivos no van solo dirigidas a la protección del derecho material en juego (ya sea la inviolabilidad del domicilio, el secreto de las comunicaciones, la intimidad o la protección de datos), sino a la protección de los derechos fundamentales de defensa, del derecho a un proceso con todas las garantías o del derecho a la presunción de inocencia (art. 24.2 CE). Por ello, y en cuanto que «las actuaciones de los servicios de inteligencia no van dirigidas a enervar válidamente la presunción de inocencia en un proceso judicial, esto es, a obtener pruebas incriminatorias, la LO 2/2002 limita sus efectos

[127] La Sala II del TS señala expresamente: «Resulta indudable, pues, que la función del Magistrado llamado al control previo de las actividades del CNI no es la de un anticipado coadyuvante del Juez de instrucción. El expediente incoado con ocasión del ejercicio de las funciones propias de los servicios de inteligencia y las diligencias penales encaminadas a la investigación de un hecho punible, no están necesariamente llamados a converger en un hipotético proceso penal. Responden a principios distintos, su contenido es también diferente y, por tanto, el sacrificio de los derechos fundamentales que se producen en uno y otro ámbito, se justifica por razones no coincidentes».

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

y los acomoda a las finalidades constitucionales y legales atribuidas a las agencias de inteligencia: prevenir y neutralizar amenazas a la defensa y seguridad nacional»[128] . En definitiva, la autorización judicial del Magistrado del Tribunal Supremo no compensa, sustituye o equivale a la del juez competente para autorizar la cesión de datos a la policía judicial.

6.2 La desclasificación del material procedente del CNI

La intervención del Magistrado del Tribunal Supremo autorizando la entrega de datos personales al CNI ni judicializa la investigación de seguridad del CNI, ni altera el carácter reservado de las actuaciones realizadas por el CNI.

La información que recaba el CNI, en cuanto servicio de inteligencia al servicio de la seguridad del Estado, no puede estar al alcance de cualquier persona. La Constitución impone de manera directa que los asuntos que afectan a la seguridad o a la defensa del Estado han de permanecer secretos (art. 105 b CE). Por otro lado, la ley reguladora del CNI señala expresamente que las actividades del CNI, su organización y estructura interna, medios y procedimientos, personal, instituciones, bases y centros de datos, fuentes de información y las informaciones o datos que pueden conducir al conocimiento de las anteriores materias, constituyen información clasificada con el grado de secreto (art. 5.1 LCNI). El carácter secreto de las actividades del CNI alcanza a los órganos jurisdiccionales que también se ven obligados, por tanto, a solicitar previamente la desclasificación de los materiales del CNI si consideran conveniente su incorporación al proceso penal[129]. La información clasificada con el grado de secreto no tiene acceso al proceso penal y no puede ser tenida en cuenta o valorada por el tribunal para formar su convicción sobre la culpabilidad de los acusados, si previamente el Consejo de Ministros no ha acordado su desclasificación[130] .

La decisión sobre la conveniencia de solicitar o no la desclasificación del material procedente del CNI, sobre la base de su necesaria incorporación al proceso penal, corresponde al juez de instrucción o, en su caso, y si estamos en una fase más avanzada del proceso penal, al juez o tribunal competente para el enjuiciamiento. En el momento en que el órgano judicial, de oficio o a instancia de parte[131] , tenga conocimiento o sospeche que parte de los datos que han servido para la investigación preliminar, o que se han incorporado a la instrucción judicial, proceden del CNI debe decidir si solicita o no la desclasificación de la información. Los jueces y tribunales penales no tienen ni la capacidad para obligar al CNI a facilitarles información clasificada, ni competencia para desclasificar material calificado como

---

[128] Como acertadamente señala GONZÁLEZ CUSSAC, J.L., «Intromisión en la intimidad y servicios de inteligencia», cit., p. 167, mientras que «la intromisión en la intimidad practicada por los servicios policiales se inscribe necesariamente en el marco del proceso penal y está orientada al acopio de evidencias destinadas a la represión de hechos delictivos, (…) la intromisión en la intimidad provocada en el desarrollo de las actividades de los servicios de inteligencia -aun cuando comporten el mismo grado de afectación al contenido del derecho fundamental- nunca persigue obtener pruebas susceptibles de trasladarse a un proceso penal, sino exclusivamente obtener información para después analizarla y, finalmente, ser entregada al decisor político dentro de las finalidades atribuidas relativas a la seguridad nacional».

[130] STS núm. 1140/2010, de 29 de diciembre; SAN núm. 9/2022, de 31 de marzo.

[131] Al estar incursos en un proceso penal, la petición de desclasificación tiene que hacerse a través del juez o tribunal que está conociendo del asunto. Así, los investigados o acusados instarán al órgano judicial que solicite la desclasificación del expediente de seguridad del CNI que, en su opinión, constituye la base de la investigación preliminar o judicial. A esta petición debe dar respuesta el órgano judicial a través de una resolución, que ha de adoptar la forma de auto, y que será recurrible conforme al régimen general establecido en la LECrim.

secreto, aunque lo consideren esencial para el desarrollo del proceso penal, por lo que deben iniciar el procedimiento previsto en nuestro ordenamiento, que pasa por solicitar la desclasificación al Consejo de Ministros[132] .

Si el órgano judicial considera necesaria la desclasificación, en orden a conocer la trazabilidad de los datos que pasaron del CNI a la policía judicial, elevará la petición al Consejo de Ministros, que es el órgano competente para resolver sobre la desclasificación del expediente de seguridad del CNI[133] .

A la hora de resolver sobre la desclasificación solicitada, el Consejo de Ministros habrá de tener en cuenta que en el contexto de un proceso jurisdiccional hay que ponderar el derecho a la tutela judicial efectiva, el derecho de defensa, el derecho a un proceso con todas las garantías, la existencia del deber de colaborar con la justicia (art. 118 CE), y el interés público en el descubrimiento de la verdad frente al bien que se trata de proteger por el secreto de Estado, que no es otro que la seguridad y la defensa del Estado[134] . En el caso de que el Consejo de Ministros acuerde la desclasificación de los materiales solicitados, que puede ser total o parcial[135] , tanto el acusado como el resto de partes del proceso podrán tener acceso a estos materiales y utilizarlos en sus respectivas estrategias procesales.

6.3 La inexistencia de un derecho a conocer el contenido íntegro de las investigaciones preprocesales

La negativa a desclasificar material procedente del CNI no impide, sin embargo, que los datos personales del CNI se puedan utilizar en la investigación preliminar de hechos delictivos y que, en consecuencia, puedan acabar incorporados a un proceso penal.

La solicitud de desclasificación de los materiales que, supuestamente, proceden del CNI tiene que superar un trámite previo y esencial: que el juez de instrucción considere procedente la solicitud de desclasificación. Si el órgano judicial no considera procedente la solicitud de desclasificación, rechazará esta petición a través de auto. La negativa del órgano judicial a solicitar la desclasificación de material procedente del CNI deberá estar motivada, y

---

[132] La Sentencia del Tribunal de Conflictos de Jurisdicción de 14 de diciembre de 1995 (RJ 1995/10064), señaló que el juez de instrucción que considere necesarios, a los fines de la investigación sumarial, determinados documentos clasificados como secreto oficial no puede imponer, sin más, al Ministro responsable su entrega y aportación. Puede dirigirse a él, por medio de exposición razonada (art. 187 LECrim), al objeto de que traslade al órgano competente, el Consejo de Ministros, la petición de desclasificación, para que este «pueda valorar, dentro de sus funciones directivas de gobierno, los intereses en juego, principalmente el de la seguridad del Estado, cuya exclusiva interpretación le corresponde en esta materia, y decidir en consecuencia».

[133] En el mes de abril de 2023 se publica en los medios de comunicación la noticia de que el Juzgado de Instrucción número 20 de Barcelona ha pedido al Gobierno la desclasificación de documentos secretos sobre el uso del programa espía Pegasus en la causa del presidente del grupo de ERC en el Parlament, Josep María Jové, y la portavoz del partido en el Parlamento Europeo, Diana Riba. Según estas noticias, la titular del Juzgado de Instrucción núm. 20 de Barcelona ha indicado que, en el caso de obtener la desclasificación, citaría a declarar a la actual directora del CNI, Esperanza Casteleiro (https://www.eldiario.es/catalunya/jueza-barcelona-pide-gobierno-desclasificar-documentos-secretos-pegasus_1_10096084.html).

[134] SÁNCHEZ FERRO, S., *El secreto de Estado*, Madrid, Centro de Estudios Constitucionales, 2006, p. 408.

[135] El problema en ocasiones de la desclasificación parcial es que finalmente no sirva para nada. Esto es lo que alegaron los recurrentes en la SAN núm. 9/2022, de 31 de marzo. En este caso se concedió una desclasificación de los materiales del CNI, que la defensa calificó de «muy limitada, pues sólo se desclasificaron dos autos del Tribunal Supremo que están absolutamente plagados de tachones, y que no sirven absolutamente para nada, porque se hacen tremendamente incomprensibles».

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

permitirá al investigado o acusado interponer los recursos correspondientes, con el objetivo de conseguir una resolución favorable a la petición de desclasificación. El órgano judicial podrá fundamentar su negativa en la inexistencia de indicios o elementos que lleven a la conclusión de que se han incorporado al proceso penal datos personales procedentes del CNI, o, como sucedió en el caso que dio lugar a la STS núm. 1094/2010, de 10 de diciembre, en «la falta de conexión entre el hipotético contenido del expediente de seguridad y el hecho ilícito que estaba siendo objeto de investigación».

Más preocupante es, sin embargo, la posibilidad del órgano judicial de fundamentar su negativa en el hecho de considerar que el investigado está solicitando información que forma parte del contenido de la investigación preprocesal, que no hay derecho a conocer en todo caso. En estos casos, la decisión del órgano judicial de no iniciar el procedimiento correspondiente para lograr la desclasificación del expediente de seguridad del CNI no implica la imposibilidad absoluta de utilizar esta información en el proceso penal, siempre y cuando el órgano judicial considere que su utilización ha sido previa al proceso y que, por tanto, no quedan, en su consideración, afectados los derechos y garantías reconocidos a quienes son investigados o acusados en un proceso penal.

La STS núm. 312/2021, de 13 de abril, recuerda que «el derecho a conocer la información que pueda resultar relevante para el material probatorio no es de configuración absoluta y sin modulación», tal y como se deduce del artículo 7.4 de la Directiva 2012/13/UE, relativa al derecho a la información en los procesos penales[136] . No obstante, la Sala II del Tribunal Supremo deja claro que la ocultación a los encausados de los elementos de la investigación policial con incidencia en el valor o en la fuerza probatoria del material aportado está sometida a dos límites infranqueables: 1) Que esta ocultación no comporte «el vaciamiento del derecho del encausado a un proceso con todas las garantías»; 2) Que sea una autoridad judicial la que pondere la oportunidad de la ocultación, y que esta decisión no se deje a la consideración de la policía judicial o de las acusaciones.

La investigación preliminar llevada a cabo por la policía, que se concreta en el atestado al que la ley reconoce el valor de denuncia o de mero objeto de prueba (art. 297 LECrim), solo sirve para el arranque del proceso penal y se materializa como referencia inaugural para el ejercicio del derecho de defensa en la forma procesalmente prevista, tal y como señala el Tribunal Supremo. Por ello, «(s)ólo cuando una de las partes presente indicios fundados de que la actuación policial o preprocesal puede haber quebrantado sus derechos fundamentales, incurrido en irregularidades, o discurrido de un modo que pueda afectar a la validez de la prueba o del procedimiento penal, así como cuando aporte indicios de coexistir circunstancias en la investigación que puedan afectar a la fuerza incriminatoria del material probatorio, se justifica, por los principios de equilibrio y defensa, autorizar tal prospección, siempre limitada a los estrictamente necesario y bajo control judicial. Es evidente que los mecanismos de investigación proscritos por un sistema de garantías no pueden ser aprovechados en el proceso penal con el insubstancial discurso de que se desplegaron antes de que el proceso penal se iniciara. En modo alguno resulta admisible que el procedimiento penal venga trufado

[136] Según este artículo: «No obstante lo dispuesto en los apartados 2 y 3, siempre y cuando ello no suponga un perjuicio para el derecho a un juicio equitativo, podrá denegarse el acceso a determinados materiales si ello puede dar lugar a una amenaza grave para la vida o los derechos fundamentales de otra persona o si la denegación es estrictamente necesaria para defender un interés público importante, como en los casos en que se corre el riesgo de perjudicar una investigación en curso, o cuando se puede menoscabar gravemente la seguridad nacional del Estado miembro en el que tiene lugar el proceso penal. Los Estados miembros garantizarán que, de conformidad con los procedimientos previstos por la legislación nacional, sea un tribunal quien adopte la decisión de denegar el acceso a determinados materiales con arreglo al presente apartado o, por lo menos, que dicha decisión se someta a control judicial».

de materiales incriminatorios que arranquen de intervenciones ilegales u otros mecanismos técnicos que resulten lesivos a los derechos fundamentales y que no estén debidamente autorizados»[137] .

La incorporación al proceso penal de datos procedentes del CNI por la vía de «diluirlos» en las actividades de investigación llevadas a cabo por la policía en la investigación preliminar no puede admitirse. Una de las garantías que rodean la utilización de datos personales en el proceso penal es la trazabilidad de dichos datos, que permite a la autoridad judicial controlar la forma de adquisición de estos datos, precisar el momento en que se recopilaron y conocer las operaciones de tratamiento a las que han sido sometidos.

La trazabilidad del dato como parte del contenido esencial del derecho a la protección de datos personales obliga a excluir del proceso penal los datos respecto de los cuales no es posible conocer su tratamiento, entendido en sentido amplio, lo que alcanza a los datos personales procedentes del CNI que, a través de cualquier vía, hayan podido acabar incorporados al proceso penal. Si el dato personal que está en poder del CNI termina siendo influyente en la investigación de un delito, debe garantizarse la trazabilidad de las operaciones de tratamiento efectuadas sobre el dato personal en cuestión desde el principio, para que el sistema de protección regulado en la LO 7/2021, a pesar de sus limitaciones, sea efectivo y no presente fallos por este motivo[138] .

Las garantías establecidas en la LO 7/2021 no son aplicables a los datos personales que están en poder del CNI mientras este organismo los utiliza para el desempeño de las funciones que legalmente tiene asignadas, pero sí que van a ser aplicables a esos mismos datos si de alguna manera se incorporan al proceso penal. En la medida en que la ley española, tal y como exige la Directiva (UE) 2016/680, ha extendido el régimen de protección de los datos personales a la utilización de estos datos por la policía en funciones preventivas, el derecho a la protección de datos personales se extiende a la fase anterior a la propia comisión del delito, y requiere conocer cuál es el origen de las pesquisas policiales.

6.4 La necesidad de regular el flujo de datos del CNI a la policía

Lo dicho hasta ahora pone de manifiesto la necesidad de regular el flujo de datos personales del CNI a los órganos encargados de la investigación de los delitos. La «colaboración» entre el CNI y las autoridades policiales es una realidad a la que no podemos permanecer ajenos. Esta colaboración no precisa solamente que se regule de manera adecuada la incorporación al proceso penal de los informes de inteligencia, o de la denominada «pericial de inteligencia»[139] , sino que requiere aclarar cómo se debe articular el mero intercambio de datos entre el CNI y la policía.

---

[137] Y continúa señalando: «No pueden tolerarse pruebas obtenidas en registros domiciliarios ilícitos o en actos de tortura. No es asumible que determinadas actuaciones, como coacciones, sobornos o incluso ingenuos incentivos, puedan minar la credibilidad de la información que a su través se obtenga, pero que se oculte a la defensa la existencia del elemento que erosiona su credibilidad. La autoridad judicial no puede consentir una realidad procesal así, como tampoco puede asumirla sin prestarle una notable atención, pues de otro modo estaría legitimando la actuación misma y coadyuvando al quebrantamiento de la Justicia a partir de la evaporación de un derecho de defensa real y eficaz».

[138] Ver GUZMÁN FLUJA, V., «Consideraciones sobre el alcance objetivo y subjetivo de la Directiva UE 680/2016», cit., pp. 854-855, que da, en nuestra opinión, en el punto clave del problema que plantea la incorporación de datos personales en poder del CNI a una investigación criminal.

[139] Como señala GONZÁLEZ CUSSAC, J.L., «Intromisión en la intimidad y CNI. Crítica al modelo español de control judicial previo», p. 158, aunque la finalidad del CNI no es la obtención de pruebas para incorporar al proceso

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

Como ya hemos apuntado, uno de los muchos problemas que viene planteando la utilización de datos personales con fines penales es la cesión de estos datos entre las autoridades competentes para la prevención, detección, investigación o enjuiciamiento de delitos. El peligro de que datos personales recopilados con una finalidad determinada y transmitidos a una autoridad policial para la investigación de unos concretos hechos delictivos puedan acabar siendo utilizados por otra autoridad policial para investigar unos hechos distintos, o incorporados a un proceso penal distinto, y para el enjuiciamiento de hechos delictivos diferentes de los que motivaron su recogida y cesión inicial, es, hoy en día, un peligro real y tangible. Por ello es esencial perfilar y clarificar los límites a la cesión de datos o información entre las autoridades competentes para recopilar y tratar datos personales con fines penales.

La cesión de datos entre el CNI y las autoridades competentes para las investigaciones criminales se añade a la lista de riesgos que las nuevas tecnologías y la recogida masiva de datos de carácter personal suponen para los ciudadanos[140] , en cuanto titulares de los datos personales[141] . De ahí la importancia de una adecuada regulación. La regulación de la cesión de datos personales es necesaria, por un lado, para que los órganos judiciales sepan cuáles son los datos que pueden aceptar y los que no. Incluso a la hora de determinar el alcance del derecho a conocer lo ocurrido en la investigación preliminar, el órgano judicial tiene que conocer las consecuencias que se derivan de la utilización de datos personales que no deberían haberse utilizado. Por otro lado, la regulación es necesaria para que los investigados sepan cómo articular su estrategia defensiva en orden a conseguir la exclusión de los datos que no deberían haber sido utilizados, y para conseguir que se declare la nulidad de las actuaciones que derivaron de dichos datos. La obligación de excluir del proceso aquellos medios de prueba que, directa o indirectamente, se hayan obtenido vulnerando derechos fundamentales (art. 11.1 LOPJ), reconoce el derecho a todo investigado o acusado a cuestionar la incorporación de datos personales al proceso[142] .

---

penal, surge el problema de si es posible trasladar las informaciones sobrantes a la policía, si ello ha de estar formalizado, así como cuáles serían los efectos que provocaría esta práctica.

[140] Como recuerda VELASCO NÚÑEZ, E., «Investigación penal y protección de datos», en *El Cronista del Estado social y democrático de Derecho*, núms. 88-89, 2021, p. 147: «Vivimos en una sociedad que pretende controlar y conjurar riesgos, para evitar lesiones a bienes jurídicos protegidos prominentes, pero paradójicamente, si para hacerlo, almacenamos y tratamos datos personales prospectiva o predictivamente, generamos otras nuevas lesiones, igualmente denostables, que, al formar parte del problema, deben tenerse en cuenta a la hora de pretender hallar su solución»

[141] Otro problema al que no vamos a hacer referencia es la cesión a la inversa, es decir, la cesión de datos personales por la policía al CNI. Sobre esta cuestión se pronunció la AEPD, cuando aún estaba vigente la LO 15/1999, y señaló que conforme a lo dispuesto en el artículo 21.1 LO 15/1999, relativo a la comunicación de datos entre Administraciones públicas, «los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas». En opinión de la AEPD, esta previsión «no deshabilita a las Fuerzas y Cuerpos de Seguridad del Estado a ceder datos al CNI en el marco de una investigación» (Expediente de la AEPD núm.: E/00096/2010).

[142] Como señala PÉREZ GIL, J., «Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal», cit., p. 15, si no hay garantías adecuadas en el tratamiento de los datos personales con fines penales, la prueba podría considerase ilícita. En el mismo sentido, FRÍAS MARTÍNEZ, E., «Protección y tratamiento de datos por el Ministerio Fiscal», en *La Ley Penal*, núm. 71, mayo 2020, para quien la ilicitud en la obtención de los datos personales tendrá consecuencias directas en la consideración de su valor probatorio, pues indudablemente los datos que se hayan obtenido con quebranto del derecho fundamental a la protección de datos no podrán ser valorados para desvirtuar la presunción de inocencia. Ver también VELASCO NÚÑEZ, E., «Investigación penal y protección de datos», cit., pp. 140-151.

El objetivo sería que la futura regulación permitiese la aplicación inmediata del derecho procesal penal, y de las garantías procesales, cada vez que investigaciones realizadas por el CNI condujesen al conocimiento de una *notitia criminis*. Esta regulación debería hacerse de manera simultánea, y complementaria, tanto en la LOCNI como en la Ley de Enjuiciamiento Criminal.

Si no se articula adecuadamente el flujo de datos personales en poder de los servicios de inteligencia nos encontraremos con que las amplias facultades de las que gozan estos servicios de inteligencia en los Estados miembros, y en concreto en el caso de España el CNI[143], pueden acabar vulnerando las garantías procesales de quienes finalmente se ven sometidos a un proceso penal.

7. Conclusión

La situación de desprotección en la que se encuentran los datos personales en poder del CNI no puede seguir justificándose en la exclusión de seguridad nacional prevista en el artículo 4.2 TUE. En una época en la que la recogida masiva de datos personales, su tratamiento y cesión es tan sencilla como consecuencia de los avances tecnológicos, es inadmisible que el legislador español no se olvide del CNI para garantizar su acceso a los datos personales que se recopilan con fines penales, en muchos casos de manera masiva, o de permitir el libre acceso a los datos en poder de entidades públicas o privadas, pero se olvide de delimitar las restricciones a su uso.

En lo que se refiere al momento del acopio del dato personal, en este trabajo hemos tratado de poner de manifiesto que esta falta de regulación ha de ser suplida aplicando las garantías exigidas en la LOCNI para la restricción del derecho fundamental a la inviolabilidad del domicilio (art. 18.2 CE) y del derecho al secreto de las comunicaciones (art. 18.3 CE). Pero esto no puede aceptarse por mucho más tiempo. Es necesaria una reforma de la LOCNI, o, mejor dicho, una nueva Ley Orgánica reguladora que afronte de manera completa e integral el control judicial de las actividades del CNI. En primer lugar, que supere de una vez, como ya hizo el legislador en la reforma de la LECrim del año 2015, que los únicos derechos que pueden ser vulnerados por las actuaciones de los servicios de inteligencia son el derecho a la inviolabilidad del domicilio y al secreto de las comunicaciones. Los derechos a la intimidad y a la protección de datos cada vez están sometidos a más amenazas y peligros, y el Magistrado del Tribunal Supremo competente debe velar por que, en aras de los principios de necesidad y proporcionalidad, no todo se oculte bajo la necesidad de la seguridad nacional. En segundo lugar, el control judicial no debe limitarse a la autorización judicial previa. Hay que extenderla al momento posterior a la adopción de la medida restrictiva de derechos fundamentales. En el caso que analizamos, a lo que ocurre con los datos personales una vez que llegan al CNI.

La necesidad de una adecuada regulación del régimen de protección de los datos personales en poder del CNI ha sido el eje principal de este trabajo. Hemos querido poner de

[143] Nos parece de interés reproducir aquí esta reflexión de PÉREZ VILLALOBOS, M.C., «El control de los servicios de inteligencia en los Estados democráticos», Ponencia presentada en el I Congreso Nacional de Inteligencia: *La inteligencia como disciplina científica*, Madrid, 22-24 de octubre de 2008, disponible en http://hdl.handle.net/10481/27872, cuando señala que la investigación del CNI «no tiene que estar basada en indicios de delito; en la mayoría de las ocasiones la información que se obtiene no tiene siquiera apariencia delictiva, ni tiene que moverse en el mundo de la delincuencia; por eso, esta actividad, desde el punto de vista constitucional, no se desarrolla en el ámbito natural del principio de intervención indiciaria. Esto hace más difícil la justificación y el control de sus actuaciones que, si no estuvieran amparadas por el interés general, rozarían la inconstitucionalidad».

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

manifiesto las carencias de la regulación en esta materia, y los peligros que de esta situación se derivan. Y también hemos querido rebatir que es una cuestión sobre la que la Unión Europea no tiene mucho que decir. La posibilidad de que el CNI tenga acceso a datos relativos al ADN, datos relativos a comunicaciones electrónicas, datos financieros o datos PNR; así como el procedimiento conforme al cual se produce dicho acceso, afecta directamente, cuando menos, al derecho fundamental a la intimidad (art. 18.1 CE) y al derecho fundamental a la protección de datos personales (art. 18.4 CE). De ahí la importancia de una adecuada regulación del acceso por parte del CNI a estos datos personales que, sin embargo, el legislador español ha querido diluir en la normativa general que regula el acceso de otras autoridades a estos datos de carácter personal.

Esta amenaza, que es real y grave, hemos querido concretarla en el libre flujo de datos en poder del CNI a la policía, y la posibilidad, nada remota, de que datos en poder del CNI pueden acabar incorporados al proceso penal. Las investigaciones de seguridad y las investigaciones criminales hace muchos años que no discurren por caminos separados y las posibilidades de confluencia e intercambio de información son una realidad a la que el legislador no puede permanecer por más tiempo indiferente. Es necesario evitar que se incorporen al proceso penal datos que, procediendo del CNI, no se ajusten a los requisitos exigidos por el contenido esencial del derecho a la protección de datos personales. Esto es posible hacerlo. Es necesario hacerlo, una vez que hemos constatado que nuestro ordenamiento procesal no ofrece garantías para evitar que la incorporación de datos procedentes del CNI implique la vulneración de derechos fundamentales del investigado o acusado, en concreto, a que no se utilicen medios de prueba obtenidos vulnerando derechos fundamentales, en cuanto que se hayan incorporado al proceso penal, y utilizado para dictar sentencia de condena, datos que no respetan el contenido esencial del derecho a la protección de datos personales. Por ello, el legislador tiene que hacer el ejercicio de tratar de adaptar las garantías establecidas en la LO 7/2021 para la utilización de los datos personales con fines de prevención, detección, investigación y enjuiciamiento de delitos, a la utilización de los datos personales por el CNI con fines de seguridad nacional.

Bibliografía

ABA CATOIRA, A, «El secreto de Estado y los servicios de inteligencia», *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol*, nº 38/39, Valencia, 2002, pp. 133-168.

ALCOCEBA GIL, J.M., «Adquisición y tratamiento procesal de los datos genéticos de terceros en el marco de la investigación penal», en COLOMER HERNÁNDEZ, I. (Dir.), *Uso y cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios*, Cizur Menor, Thomson Reuters-Aranzadi, 2017, pp. 553-580.

ALONSO DE ANTONIO, A.L., «Conocimiento por los parlamentarios de las materias clasificadas en virtud de la Ley de Secretos Oficiales», en *Foro, Nueva época*, vol. 21, núm. 2, 2018, pp. 19-44. https://doi.org/10.5209/FORO.64016

BACHMAIER WINTER, L., «Información de inteligencia y proceso penal», en BACHMAIER WINTER, L., (Coord.), *Terrorismo, proceso penal y derechos fundamentales*, Madrid, Marcial Pons, 2012, pp. 45-101.

CANO BUESO, J., «Información parlamentaria y secretos oficiales», en *Revista de las Cortes Generales*, núm. 42, 1997, pp. 7-34.

CATALINA BENAVENTE, M.A., *El uso de los datos PNR en el proceso penal*, Cizur Menor, Thomson Reuters-Aranzadi, 2022.

COLMENERO GUERRA, J.A., «La protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales vinculados al "discurso terrorista"», en GALÁN MUÑOZ, A., GÓMEZ RIVERO, M.C., (Dirs.), *La represión y persecución penal del discurso terrorista*, Valencia, Tirant lo Blanch, 2022, pp. 627-720.

COLMENERO GUERRA, J.A., «La Ley Orgánica 7/2021, de protección de datos en materia penal: ámbito y principio de proporcionalidad», en COLOMER HERNÁNDEZ, I. (dir.); CATALINA BENAVENTE, M.A, OUBIÑA BARBOLLA, S. (coords.), *Uso de la información y de los datos personales en los procesos: los cambios en la era digital*, Thomson Reuters-Aranzadi, Cizur Menor, 2022, pp. 423-477.

COLOMER HERNÁNDEZ, I., «A propósito de la compleja trasposición de la Directiva 2016/680 relativa al tratamiento de datos personales para fines penales», en *Diario La Ley*, nº 1979, 17 de abril de 2018.

COLOMER HERNÁNDEZ, I., «Control del tratamiento de datos personales penales y tutela judicial efectiva en la Directiva 2016/680», en GUTIÉRREZ ZARZA, M.A., (Coord.), *Los avances del espacio de libertad, seguridad y justicia en la Unión Europea en 2017*, II Anuario, ReDPE, pp. 117-118.

COLOMER HERNÁNDEZ, I., «Control y límites en el uso de la información y los datos personales por parte de la Inteligencia Artificial en los procesos penales», en BARONA VILAR, S. (Ed.), *Justicia algorítima y neuroderecho. Una mirada multidisciplinar*, Valencia, Tirant lo Blanch, 2021, pp. 288-289.

DÍAZ FERNÁNDEZ, A.M., «Modelos de control parlamentario de los servicios de inteligencia», *Estudio/Working Paper*, núm. 139/2012.

Dictamen al Anteproyecto de Ley de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, de 22 de febrero de 2007, (Ref: 32/2007).

Dictamen del Consejo de Estado al Anteproyecto de Ley Orgánica por la que establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales, de 24 de febrero de 2022, (Ref: 1159/2021).

FERNÁNDEZ RODRÍGUEZ, J.J., «Los límites al acceso a la información en España: A propósito del terrorismo», *Revista Española de la Transparencia*, núm. 5, 2017, pp. 128-147.

FERNÁNDEZ SOLAS, M., «Modelos de inteligencia contra el terrorismo: una comparación entre España e Italia», en LOZANO MIRALLES, J. (Coord.), *La lucha contra el terrorismo en el marco del sistema de seguridad nacional. El papel de las Fuerzas Armadas, las Centrales de Inteligencia y las Fuerzas y Cuerpos de Seguridad del Estado*, Cizur Menor, Thomson Reuters-Aranzadi, 2021, pp. 393-411.

FRÍAS MARTÍNEZ, E., «Ficheros jurisdiccionales. Autoridad de control», en *Diario La ley*, núm. 9986, 11 de enero de 2022.

FRÍAS MARTÍNEZ, E., «Protección y tratamiento de datos personales por el Ministerio Fiscal", en *La Ley Penal*, núm. 71, mayo 2020.

GARCÍA-TREVIJANO GARNICA, E., «Materias clasificadas y control parlamentario», en *Revista Española de Derecho Constitucional*, núm. 48, 1996, pp. 145-178.

Estudios Penales y Criminológicos., 43 (2023). ISSN-e: 2340-0080
https://doi.org/10.15304/epc.43.9427

GIMBERNAT ORDEIG, E., «La vida de nosotros», publicado en el periódico El Mundo, el 30 de abril de 2008, (disponible en file:///C:/Users/angeles.catalina/Downloads/Iustel_1028760.pdf).

GÓMEZ ÁLVAREZ, J., «La cesión de datos de carácter personal al proceso penal. En especial los datos relativos a la salud», en COLOMER HERNÁNDEZ, I. (Dir.), *Uso y cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios*, Cizur Menor, Thomson Reuters-Aranzadi, 2017, pp. 607-646.

GONZÁLEZ CUSSAC, J.L., «Intromisión en la intimidad y CNI. Crítica al modelo español de control judicial previo», en *Inteligencia y Seguridad*, 15 (enero-junio 2014), pp. 151-186.

GONZÁLEZ CUSSAC, J.L., «Intromisión en la intimidad y servicios de inteligencia», en *Revista Penal México*, núm. 3, enero-junio, 2012, pp. 159-177.

GONZÁLEZ CUSSAC, J.L., FLORES GIMÉNEZ, F., «Una metodología para el análisis de las amenazas a la seguridad, la evaluación de las respuestas y su impacto sobre los derechos fundamentales», en *Cuadernos de Estrategia*, núm. 188, 2017, pp. 15-64.

GUTIÉRREZ ZARZA, A., «La protección de las personas físicas en lo que respecta a su derecho a la intimidad y los datos personales por las autoridades de emisión y ejecución de las Órdenes Europeas de Investigación», en ARANGÜENA FANEGO, C., DE HOYOS SANCHO, M., VIDAL FERNÁNDEZ, B., (Coords.), *Garantías procesales de investigados y acusados. Situación actual en el ámbito de la Unión Europea*, Valencia, Tirant lo Blanch, 2018, *tol. 6.958.342*.

GUZMÁN FLUJA, V., «Consideraciones sobre el alcance objetivo y subjetivo de la Directiva UE 680/2016», en MORENO CATENA, V., ROMERO PRADAS, M.I., (Coords.), *Nuevos postulados de la cooperación judicial en la Unión Europea. Libro homenaje a la Prof.ª Mª Isabel González Cano*, Valencia, Tirant lo Blanch, 2021, pp. 821-893.

Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, «El derecho a la privacidad en la era digital», de 3 de agosto de 2018, (Ref: A/HRC/39/29).

JIMÉNEZ-PÉREZ, D., «Legitimidad y control del Centro Nacional de Inteligencia», Comunicación presentada en el Congreso Análisis de Inteligencia y Prospectiva. Grupo de Estudios en Seguridad Internacional. Universidad de Granada, 8-9 de abril de 2019, 15p. (disponible en https://www.ugr.es/~gesi/congreso/comunicacion31-14.pdf).

LEÓN ALAPONT, J., «Un comentario de urgencia a la Ley Orgánica 9/2022, de 28 de julio, por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales», en *Diario La Ley*, núm. 10123, de 5 de septiembre de 2022.

LOMAS HERNÁNDEZ, V., «La cesión de datos sanitarios a las Fuerzas y Cuerpos de Seguridad: STS (Sala de lo Penal) de 16 de diciembre, y Agencias de Protección de Datos Personales», en *Diario La Ley*, núm. 10220, 2 de febrero de 2023.

LÓPEZ ALFRANCA, M.V., «¿Pero quién vigilará a los vigilantes?», en *ICADE, Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, núm. 92, mayo-agosto 2014, pp. 107-142.

MARTÍNEZ VÁZQUEZ, F., «El control parlamentario de los secretos oficiales», en *Revista de las Cortes Generales*, núm. 104, 2018, pp. 395-420.

MONTORO SÁNCHEZ, J.A., «La Ley Orgánica 9/2022, de 28 de julio. Un controvertido instrumento para la investigación de la dimensión económica del delito», en *Eunomía.*

Revista en Cultura de la Legalidad, 24, 2023, pp. 348-357. https://doi.org/10.20318/eunomia.2023.7675

MONTORO SÁNCHEZ, J.A., *Uso y cesión de datos de carácter personal en el proceso penal*, Cizur Menor, Thomson Reuters-Aranzadi, 2022.

OLSEN, H.P., WIESENER, C., «Beyond data protection concerns- The European Passenger Name Record System», en *I Courts Working Paper Series*, no. 207, 2020.

OUBIÑA BARBOLLA, S., «Cambio de enfoque en la cooperación judicial penal y policial en la UE en relación con la transmisión de datos personales: las nuevas propuestas normativas y la STJUE de 8 de abril de 2014», en COLOMER HERNÁNDEZ, I., (Dir.), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Cizur Menor, Aranzadi, 2015, pp. 71-123.

PÉREZ GIL, J., «Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal», en BELLIDO PENADÉS, R., DE LUIS GARCÍA, E., JIMÉNEZ CONDE, F., LLOPIS NADAL, P. (Coord.), *Justicia: ¿Garantías versus Eficiencia?*, Valencia, Tirant lo Blanch, 2020, *tol. 7.855.589.*

PÉREZ VILLALOBOS, M.C., *Derechos fundamentales y servicios de inteligencia*, disponible en: https://digibug.ugr.es/bitstream/handle/10481/27876

PÉREZ VILLALOBOS, M.C., «El control de los servicios de inteligencia en los Estados democráticos», Ponencia presentada en el I Congreso Nacional de Inteligencia: *La inteligencia como disciplina científica*, Madrid, 22-24 de octubre de 2008, disponible en. http://hdl.handle.net/10481/27872

RAMALLO MACHÍN, A.C., *ADN: Huellas genéticas en el proceso penal*. Tesis doctoral disponible en el repositorio de la Universidade da Coruña https://ruc.udc.es/dspace/handle/2183/16126.

RECIO GAYO, M., *El estatuto jurídico del Data Protection Officer*, Madrid, La Ley Wolters Kluwer, 2019.

SÁNCHEZ FERRO, S., *El secreto de Estado*, Madrid, Centro de Estudios Constitucionales, 2006.

SÁNCHEZ BARRILAO, J.F., «Servicios de inteligencia, secreto y garantía judicial de los derechos», en *UNED. Teoría y Realidad Constitucional*, núm. 44, 2019, pp. 309-340. https://doi.org/10.5944/trc.44.2019.26004

RUIZ MIGUEL, C., *Servicios de inteligencia y seguridad del Estado constitucional*, Madrid, Tecnos, 2002.

SANSÓ-RUBERT PASCUAL, D., «La articulación de la comunidad de inteligencia española: realidad y perspectiva de futuro», en *Boletín de Información. Centro Superior de Estudios de la Defensa Nacional*, núm. 297, 2006, pp. 53-80.

SENDÍN MATEOS, J.A., «El abuso del secreto de Estado en la ocultación de las actuaciones ilegítimas de los poderes públicos», en *Revista Española de la Transparencia*, núm. 13, 2021, pp. 173-191. https://doi.org/10.51915/ret.182

SERRA CRISTÓBAL, R., *La seguridad como amenaza. Los desafíos de la lucha contra el terrorismo para el Estado democrático*, Valencia, Tirant lo Blanch, 2020.

SERRA CRISTÓBAL, R., «El control de datos de circulación de personas en la UE como mecanismo de salvaguarda de la seguridad nacional», en *UNED. Revista de Derecho*

Político, nº. 102, mayo-agosto 2018, pp. 305-332. https://doi.org/10.5944/rdp.102.2018.22395

SERRA CRISTÓBAL, R., «La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional», *UNED. Revista de Derecho Político*, nº. 92, enero-abril 2015, pp. 73-118. https://doi.org/10.5944/rdp.92.2015.14422

SOLETO MUÑOZ, H., ALCOCEBA GIL, J., «Protección de datos y transmisión de perfiles de ADN», en CABEZUDO BAJO, M.J, (Dir.), *Las bases de datos policiales de ADN. ¿Son una herramienta realmente eficaz en la lucha contra la criminalidad grave nacional y transfronteriza?*, Madrid, Dykinson, 2013, pp. 325-344.

VALEIJE ÁLVAREZ, I., «La consecuencia accesoria de cesión de muestras biológicas y registro de identificadores de ADN en las bases policiales (art. 129 bis del CP)», en ORTS BERENGUER, E., ALONSO RIMO, A., ROIG TORRES, M., (Dirs.), *Peligrosidad criminal y Estado de Derecho*, Valencia, Tirant lo Blanch, 2017, pp. 143-226.

VELASCO NÚÑEZ, E., «Investigación penal y protección de datos», en *El Cronista del Estado social y democrático de Derecho*, núms. 88-89, 2021, pp. 136-151.

VILLALBA CANO, L., «El derecho a presentar una reclamación ante una autoridad de control (Comentario al artículo 77 RGPD)», en TRONCOSO REIGADA, A. (dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de protección de datos personales y garantía de los derechos digitales*, Tomo II, Cizur Menor, Civitas-Thomson Reuters, 2021, pp. 2967-2987.

WILKINSON MORERA DE LA VALL, H., *Secretos de Estado y Estado de Derecho: régimen jurídico de los secretos oficiales en España*, Atelier, 2007.