



Carlos Manuel Fernández González
Delegado de Protección de Datos de la Secretaría de
Estado de Seguridad
Doctorando en la Universidad Católica de Murcia
Master oficial de Criminología y Ciencias
de la Seguridad

**LA SEGURIDAD DE LA INFORMACIÓN DE
LOS TESTIGOS PROTEGIDOS Y VÍCTIMAS
DE DELITOS COMO MEDIDA DE
PROTECCIÓN**

SEGURIDAD DE LA INFORMACIÓN DE LOS TESTIGOS PROTEGIDOS Y VÍCTIMAS DE DELITOS COMO MEDIDA DE PROTECCIÓN.

Sumario: 1. INTRODUCCIÓN. 2. ANÁLISIS DE LA NORMATIVA APLICABLE. 2.1. LA PROTECCIÓN DE TESTIGOS Y VÍCTIMAS EN EL DERECHO NACIONAL. 2.1.1. Normativa de carácter general. 2.1.2. Normativa de carácter específico a testigos y peritos protegidos. 3. TIPO DE MEDIDAS DE PROTECCIÓN DE TESTIGOS PROTEGIDOS Y VÍCTIMAS DE DELITO. 4. PROTECCIÓN DE LA INFORMACIÓN Y DATOS DE CARÁCTER PERSONAL. 4.1. LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL. 4.1.1. Medidas generales de seguridad a aplicar por los responsables del tratamiento. 4.2. REGISTRO DE OPERACIONES. 4.3 RESTRICCIÓN DE DERECHOS, LIMITACIÓN COMO CONSECUENCIA DE INVESTIGACIONES Y PROCESOS PENALES. 4.3.1. Restricción de derechos. 4.3.2. Limitación de derechos como consecuencia de investigaciones y procesos penales. 4.4 GESTIÓN DE BRECHAS DE SEGURIDAD 5. CONCLUSIONES. 6 REFERENCIAS BIBLIOGRÁFICAS.

Resumen: Las personas que resultan víctimas o testigos de delitos, especialmente aquellas a las que es necesario elevar sus niveles de protección en los procesos penales como serían a las que se les otorga la condición de testigos protegidos, las víctimas de delitos de violencia de género o las menores de edad, son sujetos de derecho a los que dichas circunstancias no les deberían derivar perjuicios añadidos. En el curso de las actuaciones, en correspondencia con su condición particular y con el nivel de riesgo que se les atribuya, se les debe proteger eficazmente. Entre las garantías de sus derechos fundamentales, en el mundo totalmente digitalizado en el que vivimos, cobra especial importancia el aseguramiento de sus datos personales y la información que les afecte. Esta medida constituye un elemento básico para poder garantizar el resto de las que se deben adoptar, teniendo en cuenta que la extensión de las Tecnologías de la Información y Comunicación (TIC's), el empleo cotidiano del ciberespacio, de herramientas informáticas y el uso de Inteligencia Artificial (AI) es masivo en el conjunto de las sociedades a nivel mundial y esto tiene como resultado el incremento de la dificultad a la hora de lograr niveles óptimos de seguridad. El insuficiente conocimiento, la falta de concienciación y la dificultad de aplicación efectiva de la legislación, elevan las posibilidades de identificación, seguimiento y localización de las personas, lo que eleva notablemente la dificultad protegerlas.

Abstract: People who become victims or witnesses of crimes, especially those requiring elevated levels of protection in criminal proceedings—such as those granted the status of protected witnesses, victims of gender-based violence, or minors—are subjects of rights to whom such circumstances should not result in additional harm. During legal proceedings, corresponding to their condition and the level of risk attributed to them, they must be effectively protected. Among the guarantees of their fundamental rights, in the fully digitalized world in which we live, the safeguarding of their personal data and information affecting them is of particular importance. This measure constitutes a basic element necessary to guarantee the rest of the measures that need to be adopted, considering that the extensive use of Information and Communication Technologies (ICTs), the everyday use of cyberspace, computer tools, and Artificial Intelligence (AI) is widespread globally. This results in increased difficulty in achieving optimal security levels. Insufficient knowledge, lack of awareness, and difficulty in effectively applying

legislation increase the chances of identification, tracking, and locating individuals, thereby significantly raising the difficulty in protecting them.

Palabras clave: Testigos Protegidos, Víctimas de Violencia de Género, Menores de edad, Protección de Datos Personales. Protección de la Información.

Keywords: Protected Witnesses, Victims of Gender Violence, Minors, Personal Data Protection. Information Protection.

ABREVIATURAS

a.C.: Antes de Cristo.

AI.: Inteligencia Artificial (Artificial Intelligence).

AP.: Audiencia Provincial.

App.: Aplicación Web.

Art.: Artículo.

BOE.: Boletín Oficial del Estado.

CCN.: Centro Criptológico Nacional.

CE.: Constitución Española.

CEDH.: Comité Europeo de Derechos Humanos.

CGPJ.: Consejo General del Poder Judicial.

CP.: Código Penal.

DPD: Delegado de Protección de Datos.

DOEP: Directiva sobre la Orden Europea de Protección.

EOMF: Estatuto Orgánico del Ministerio Fiscal.

ENS.: Esquema Nacional de Seguridad.

FCSE.: Fuerzas y Cuerpos de Seguridad del Estado.

FGE.: Fiscalía General del Estado.

LECRIM.: Ley de Enjuiciamiento Criminal.

LEVD.: Ley del Estatuto de la Víctima del Delito.

LOFCSE.: Ley Orgánica de Fuerzas y Cuerpos de Seguridad.

LOPDGDD: Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

LOPDP.: Ley Orgánica de Protección de Datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

LOPIVI: Ley Orgánica de protección integral a la infancia y la adolescencia frente a la violencia.

LOPIVG. Ley Orgánica de Medidas de Protección Integral contra la Violencia de Género.

LOPJ: Ley Orgánica del Poder Judicial.

LOPSC.: Ley Orgánica de protección de la seguridad ciudadana.

LOPT.: Ley Orgánica de Protección de Testigos.

LOTJ: Ley Orgánica del Tribunal del Jurado.

LRMRP: Ley de Reconocimiento Mutuo de Resoluciones Penales en la Unión Europea.

LSO.: Ley de Secretos Oficiales.

MF.: Ministerio Fiscal.

RDL.: Real Decreto Legislativo.

RDLJTICS: Real Decreto-ley por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo.

RGDP: Reglamento General de Protección de Datos.

STC.: Sentencia del Tribunal Constitucional.

STS.: Sentencia del Tribunal Supremo.

TEDH.: Tribunal Europea de Derechos Humanos.

TIC's.: Tecnologías de la Información y Comunicación.

TJUE.: Tribunal de Justicia de la Unión Europea.

TS.: Tribunal Supremo.

UE.: Unión Europea.

1. INTRODUCCIÓN

En un contexto donde el empleo de los medios de comunicación y las tecnologías de la información se ha construido una sociedad hiperconectada que, a través de un entorno cibernético, facilita enormemente la obtención de información, la comunicación y la localización de las personas mediante un número casi ilimitado de identificadores. Este hábitat, donde la merma de la privacidad es la tónica en todo el espectro de las relaciones sociales, entre otras consecuencias, eleva la dificultad a la hora de proteger determinados bienes jurídicos como son, la intimidad, la imagen, el honor o los datos personales, que son connaturales a la seguridad de la ciudadanía.

En el caso de las víctimas de delitos y testigos en los procesos penales, el análisis detallado de la normativa, la Jurisprudencia y los tratados y convenios internacionales suscritos y refrendados por España revela que, en nuestro país, el conjunto de instrumentos legales específicos para dotar de protección a su información, sobre todo, en procedimientos que se corresponden con conductas ilícitas de terrorismo, delincuencia organizada, ya sea a nivel transnacional o foránea, delitos de violencia de género, contra las mujeres o personas menores de edad, resulta exigua en comparación con lo regulado en los países de nuestro entorno social, político y cultural.

Las herramientas legales para dotar de seguridad a estas personas no poseen aún un grado de desarrollo adecuado, de hecho, aunque se apliquen algunas medidas de protección, principalmente por la labor y el esfuerzo de autoridades judiciales, fiscales y las FCS, se puede afirmar que el sistema no posee el grado de madurez suficiente. Es posible que la actual regulación pueda cumplir sus objetivos en algunos supuestos, pero en la práctica, la realidad nos muestra que las medidas no resultan tan eficientes como sería deseable. En correspondencia con la vulnerabilidad de estas personas, en el año 2012 algunos jueces de la Audiencia Nacional ya mostraban su percepción sobre la LOPT al señalar que *“la ley solo tiene cuatro artículos: no prevé nada, ni trabajo, ni dinero, ni deslocalización” dice el juez Gómez Bermúdez.*” (Irujo, 2012)

Ante el avance de las posibles injerencias de las personas implicadas en todo tipo de actos delictivos que pueden llevarse a cabo, con el objeto de atentar, intimidar o desacreditar a las víctimas o los testigos, las autoridades con competencia en garantizar los derechos fundamentales y la seguridad pública no deberían mantener esta situación. Nuestro sistema democrático incorpora los derechos y obligaciones de las partes en el desarrollo de los procesos penales (como no podía ser de otra manera) lo que debería constituirse en una realidad y no sólo consistir en expresiones programáticas por falta de regulación o medios.

Cabe destacar que las garantías constitucionales y los principios esenciales en estos procesos no deben verse afectados injustificadamente por las medidas de protección a las víctimas o testigos, aunque estas pudieran ser necesarias. Para ello, es crucial que cualquiera de las que se puedan adoptar estén respaldadas por un estricto cumplimiento de la legalidad y una motivación sólida que, ponderados los derechos en juego, establezca la prelación de los intereses de las todas personas involucradas en el sistema de justicia y permita así que puedan alcanzar sus objetivos finales.

Este trabajo por un lado pretende poner de relevancia la importancia de garantizar el derecho fundamental a la protección de datos personales y la seguridad de la

información para lograr la seguridad integral de las personas (Ayllón, 2021). No es posible tener un plan de defensa de un bien jurídico sin que, una vez identificados los agentes dañinos y analizados los riesgos, se implemente un procedimiento organizado y funcional que permita prevenir los peligros desde la fase o estadio más inicial de la amenaza potencial, y el en caso de no poder evitarlo, detectarla y dar una respuesta adecuada. Si el victimario puede fácilmente identificar, localizar y comunicarse con quien pretendemos proteger, las medidas a adoptar, lógicamente, tendrán que ser acordes con dichas previsiones o lo que es lo mismo, deberán adaptarse al hecho de que puede conocer al objetivo y saber dónde, cuándo y con quién estará, resultará mucho más sencillo atentar contra estas personas.

Por otro lado, intenta acentuar que resulta imprescindible conocer las distintas y heterogéneas normas que convergen en estas actuaciones para que la formación y la concienciación se conviertan en elementos clave en la protección de las personas que participan y colaboran en la Administración de Justicia.

No se trataría sólo de que exista una entidad que se encargue singularmente de dotar de protección a quien lo necesite, sino de dejar patente la necesidad de que exista un sistema integral que permita prevenir y combatir los peligros. Esta premisa sólo puede lograrse si, desde el origen de las actuaciones y dentro de todo el marco legal aplicable, se introducen los procesos necesarios para preservar, entre otros factores, la información y los datos de las personas.

Todo ello sin perjuicio de que esa defensa deber ser transversal y completa, de forma que también los derechos fundamentales dispuestos en el artículo 18 de la Constitución (en especial en su apartado 4¹), sean garantizados en toda su extensión tanto para víctimas, victimarios como para todas aquellas personas que participen en los procedimientos del orden penal.

2. ANÁLISIS DE LA NORMATIVA APLICABLE

Es imperativo que las medidas implementadas para proteger a las víctimas y testigos respeten los principios fundamentales de nuestro sistema procesal penal para evitar cualquier infracción significativa que pueda conducir a una indefensión material para las personas acusadas. Esto plantea un delicado equilibrio entre la necesidad de su adopción y los derechos afectados por éstas y, en este contexto, surge la pregunta sobre cuál sería el bien jurídico protegido que debe prevalecer en una posible controversia entre la seguridad de las víctimas, testigos y peritos, y el derecho a una tutela judicial efectiva de las personas a las que se les atribuya la comisión de un ilícito penal (Torras, 2019).

La pregunta en sí no estaría bien formulada, puesto que, desde el origen de los sistemas procesales modernos, la protección de todos los que participan en el mismo debería verse como algo consustancial y principal y no sólo como algo accesorio al objetivo de dictar la resolución o sentencia oportuna². Este grado de seguridad necesario

¹ El artículo 18.4 de la CE dispone que: " 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

² Una vez se consigue el objetivo de sentenciar a la persona acusada la preocupación por las víctimas o las partes colaboradoras de la Justicia no debería decaer por la concurrencia de esa mera circunstancia.

debería ser proporcional al nivel de riesgo que puedan sufrir las personas en su calidad de partícipes en el proceso siempre que también se pueda garantizar la tutela judicial efectiva.

Cuando se pretenden detallar los sistemas de protección de las personas que participan en causas criminales, la primera tesis consiste en discernir si es suficiente la protección general que las leyes de policía y de seguridad ciudadana otorgan al conjunto de la sociedad o no. Éstas facilitan un primer nivel de defensa a todas aquellas personas que se incluyen dentro del ámbito territorial de aplicación de nuestro ordenamiento jurídico y, por ende, también resultarían aplicables cuando dichas personas se encuentren en el papel de víctima, testigo o perito protegidos.

Hay que tener en consideración que la LECRIM obliga a denunciar los delitos de carácter público a cualquier persona y que las que tienen el estatus de testigos tienen el deber de colaborar con la Justicia, cuestiones ambas que exigirían una contraprestación por parte de los estados, es decir, su participación debe quedar incluida en un entorno propicio para que esa cooperación no genere nuevas victimizaciones y no ponga en peligro su bienestar más de lo estrictamente necesario (Ruíz, 2013).

Si la Constitución española garantiza el derecho a que se proteja la vida y la integridad física de cualquier persona, esto incluiría asimismo a las figuras objeto de estudio, si bien, lo que se pretende analizar es qué o cuáles especialidades normativas nacionales se pueden aplicar en estos casos y si éstas resultan suficientes en el campo de asegurar su información y datos (Teatino et al., 2022). Sin olvidar que algunas leyes nacionales recogen contenidos derivados de la aplicación o transposición de la normativa de la UE como puede ser la DOEP y su incorporación al derecho nacional a través de la LMRP.

2.1. LA PROTECCION DE TESTIGOS Y VÍCTIMAS EN EL DERECHO NACIONAL

2.1.1. Normativa de carácter general

Como primer escalón a incluir en este análisis se encontraría el contenido de los artículos 15, 17, 53, 126, 149.29^a de la Constitución española de 1978, la LECRIM, la LOPJ, el EOMF, la LOFCS, el CP, la LOPSC y una larga lista sobre normas de policía y seguridad pública que no se considera conveniente enumerar en su totalidad por cuestiones de oportunidad y extensión.

El derecho a la vida, la libertad, a la tutela judicial efectiva, a la seguridad pública y cómo se constituye el poder y la policía judicial consagrados en nuestra constitución constituirían la base del sistema de protección instrumental de todas las personas que participan en los procesos penales.

Formarían parte igualmente de este apartado las distintas resoluciones y recomendaciones de la ONU, del Consejo de Europa y de la Unión Europea sobre la materia³.

³ Vid. ONU: Resolución de la Asamblea General 39/46, de 10 de diciembre de 1984, Resolución de la Asamblea General 40/34, de 29 de noviembre de 1985, Resolución de la Asamblea General 45/107, de 26 de marzo de 1991, Resolución de la Asamblea General 46/152, de 18 de diciembre de 1991,

En un segundo escalón, las misiones y deberes contenidas en el EOMF, la LOFSC y la LOPSC, que vendrían a establecer qué instituciones son las que más directamente deben garantizar los derechos fundamentales y proteger la seguridad ciudadana y qué actuaciones deben llevar a cabo.

No obstante, existen otras muchas medidas de protección que se derivarían del contenido de otras disposiciones, como ocurre, a modo paradigmático, con en el CP que incluye diversos tipos penales específicos cuyo bien jurídico protegido incluye, no focalizándose exclusivamente en ello, la protección de las víctimas, testigos o peritos derivada de su participación en los procesos penales. Así, podemos citar los artículos 263.2. 1º que recoge un subtipo agravado del delito de daños, el artículo 464 que tipifica las violencias o intimidaciones para influir en los testigos o el artículo 471 bis, que tipifica la corrupción o las represalias de los testigos ante la Corte Penal Internacional.

Igualmente, la LECRIM establece diversas medidas de protección para víctimas y testigos. Estas incluyen la reclamación de indemnizaciones por participación en la causa (artículos 241 y 242), garantías para actuaciones telemáticas en casos específicos como violencia de género (artículo 258 bis), regulación de agentes encubiertos (artículo 282 bis), condición para decretar prisión provisional evitando ocultación o alteración de pruebas relevantes (artículo 503), protección de bienes jurídicos de las víctimas, juicios a puerta cerrada con prohibición absoluta de revelar identidad en casos de menores o discapacitados (artículos 681 y 682), restricciones a medios de comunicación audiovisuales en salas judiciales, y la posibilidad de realizar declaraciones en sala aparte para evitar confrontación con la parte inculpada (artículo 707).

Con la entrada en vigor el 21 de marzo de 2024 del RDLJTICS, se produce un avance cualitativo al regularse:

- la utilización de las tecnologías de la información por parte de ciudadanía y los profesionales en sus relaciones con la Administración de Justicia y en las relaciones de la Administración de Justicia con el resto de las administraciones públicas, y sus organismos públicos y entidades de derecho público vinculadas y dependientes.
- el empleo por la Administración de Justicia de TIC, asegurando la seguridad jurídica digital, el acceso, autenticidad, confidencialidad, integridad, disponibilidad, trazabilidad, conservación, portabilidad e interoperabilidad de los datos, informaciones y servicios que gestione en el ejercicio de sus funciones.

Resolución del Consejo de Seguridad 827/1993, de 25 de mayo, Convención contra la delincuencia transnacional organizada, firmada en Palermo el 15 de noviembre de 2000 y la Convención contra la corrupción, firmada en Mérida el 31 de octubre de 2003 y “Manual de buenas prácticas para la protección de los testigos en las actuaciones penales que guarden relación con la delincuencia organizada” de 2008 la UNODC. Consejo de Europa: Recomendación (97) 13, de 10 de septiembre, sobre la intimidación de los testigos y los derechos de defensa, Recomendación (2005) 9, de 20 de abril, sobre la protección de testigos y colaboradores de la justicia y la Recomendación 2063 (2015), de 30 de enero, sobre la protección de testigos como instrumento indispensable en la lucha contra el crimen organizado y el terrorismo en Europa, por la que se aprueba la Resolución 2038 (2015). UE: Resolución del Consejo de 23 de noviembre de 1995, relativa a la protección de los testigos en el marco de la lucha contra la delincuencia organizada internacional, Resolución del Consejo de 20 de diciembre de 1996, relativa a las personas que colaboran con el proceso judicial en la lucha contra la delincuencia internacional organizada y Manual europeo sobre la protección de testigos: criterios comunes y principios, compuesto por dos documentos: “Principios básicos para la cooperación policial en la Unión Europea en el campo de la protección de testigos”, del año 2000 y “Criterios comunes para la inclusión de un testigo en un programa de protección”, del año 2002.

- el carácter instrumental de soporte y apoyo a la actividad jurisdiccional de las TIC's, con pleno respeto a las garantías procesales y constitucionales.

Muchas de las medidas contenidas en las normas procesales han sido recientemente incorporadas y aplicadas después de la aprobación de la LOPIVI, la cual tiene por objeto garantizar los derechos fundamentales de los niños, niñas y adolescentes a su integridad física, psíquica, psicológica y moral frente a cualquier forma de violencia, asegurando el libre desarrollo de su personalidad y estableciendo medidas de protección integral, que incluyan la sensibilización, la prevención, la detección precoz, la defensa y la reparación del daño en todos los ámbitos en los que se desarrolla su vida. Esta norma define por violencia contra estos colectivos como toda acción, omisión o trato negligente que priva a las personas menores de edad de sus derechos y bienestar, que amenaza o interfiere su desarrollo físico, psíquico o social, con independencia de su forma y medio de comisión, incluida la realizada a través de las tecnologías de la información y la comunicación, especialmente la violencia digital.

Del mismo modo, no se puede soslayar el contenido de la LOPIVG vino a incidir en la protección integral de las víctimas en estos procesos, determinados elevados niveles de defensa de sus bienes jurídicos protegidos, ni el de la LRC, en lo que permite el cambio de apellidos o de identidad mediante expediente a las víctimas de violencia de género y a cualquier persona cuando razones de urgencia o seguridad u otras circunstancias excepcionales lo requieran (que no constituyan violencia de género), podrá autorizarse el cambio de apellidos o el cambio total de identidad, por Orden del Ministerio de Justicia, en los términos fijados reglamentariamente.

Como norma básica, la LEVD establece medidas para garantizar la protección, información, apoyo y participación de las víctimas en el proceso penal, muy especialmente a las personas que necesiten especial protección y menores de edad. Además, contempla medidas de protección que buscan la efectividad frente a represalias, intimidación, victimización secundaria, daños psíquicos o agresiones a la dignidad durante los interrogatorios y declaraciones como testigo, e incluyen desde las medidas de protección física hasta otras, previamente señaladas, como serían el uso de salas separadas en los Tribunales, para evitar contacto de la víctima con el infractor y cualesquiera otras, bajo discrecionalidad judicial, que exijan las circunstancias. En este último caso, dispone que podrán acordarse para la protección de las víctimas, la adopción de alguna o algunas de las medidas de protección a que se refiere el art. 2 de la LOPT.

No se puede olvidar en este marco la aplicación de la normativa de protección de materias clasificadas que, sin perjuicio del contenido de los artículos 301 y 302 de la propia LECRIM, viene específicamente regulada por la LSO y su normativa de desarrollo.

Por último, se debe hacer referencia al contenido de las disposiciones que vienen a cumplir con el mandato del artículo 18.4 de la CE al proteger el derecho fundamental a la protección de datos personales en el marco los tratamientos con finalidad de prevención, detección, investigación y enjuiciamiento de delitos. En concreto, es ineludible citar el capítulo I bis del Título III de la LOPJ, los arts. 12, 14 y 20 LOMF y el contenido completo de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (LOPDP)

2.1.2. Normativa de carácter específico a testigos y peritos protegidos.

Además de la protección abstracta previamente incorporada, en parte derivada del cumplimiento de los acuerdos internacionales ratificados por el Estado español, el legislador promulgó la LOPT. Dicha norma implementó una serie de medidas, con la finalidad de elevar la protección de aquellas personas que actúan como tales en los procesos penales, reconociendo la importancia de su colaboración en el sistema judicial. Sin entrar en profundidad en su análisis, es patente que algunos aspectos han sido completados y mejorados indiscutiblemente por la normativa general posterior, por lo que se podría sintetizar que, actualmente, dicha ley orgánica sólo contiene una serie de medidas con repercusión procesal, policial y personal para unos supuestos muy concretos de especial protección.

La ley se aplica a testigos y peritos en procesos penales, sin definir exhaustivamente dichos conceptos. Dentro de este marco y aplicando subsidiariamente los conceptos y descripciones contenidos en la LEC, la práctica ha ido fijando el contenido de los mismos (por ende, su ámbito subjetivo de aplicación) extendiéndolos, según el caso concreto, a la propia persona definida como testigo (según la definición y obligaciones contenidas en la LECRIM), a las que tengan la condición de peritos (cualquier persona llamada a declarar en un procedimiento en calidad de tal), a las víctimas según el concepto de la LEVD, los coimputados, los agentes de las fuerzas y cuerpos de seguridad y, de modo parcial y de forma práctica, a los familiares de éstas.

Para aplicar estas medidas de seguridad, se requiere que la autoridad judicial aprecie racionalmente un peligro grave para aplicar las disposiciones de la ley. Esta decisión requiere que dicha autoridad aprecie los hechos y determine las acciones pertinentes de forma que las decisiones sean motivadas y condicionadas al presupuesto fáctico y a las circunstancias de las personas a proteger y que se basen en la apreciación de un peligro grave efectivo y de carácter cuanto menos de cierta entidad (Cubillo, 2009)

Estas medidas se deben adoptar diferenciando claramente en esta materia las que se pueden desarrollar en la fase de instrucción y en la fase de enjuiciamiento, siendo según el contenido del artículo 2 de la LOPT, las siguientes:

- No identificar en las diligencias que se practiquen el nombre, apellidos, domicilio, lugar de trabajo y profesión, ni cualquier otro dato que pudiera servir para la identificación de estos, pudiéndose utilizar para ésta un número o cualquier otra clave.
- Comparecencia para la práctica de cualquier diligencia utilizando cualquier procedimiento que imposibilite su identificación visual normal.
- Fijar como domicilio, a efectos de citaciones y notificaciones, la sede del órgano judicial interviniente, el cual las hará llegar reservadamente a la persona destinataria.

Estas medidas son de fácil y rápida aplicación, pero en ocasiones resultaran del todo ineficaces e inoperantes ¿Por qué? Imaginemos por un momento que en un suceso delictivo hay varias personas implicadas (por ejemplo 3). Pues bien, si durante el periodo instructorio se procede a la detención, imputación y posterior acusación (del tipo que sea) de dos de ellas, y si posteriormente se produce la prueba testifical (ya sea la que consideramos *anónima*, *oculta* o resulte modificada la imagen, la voz o la apariencia del

testigo, etc.), en la cual se exponen conocimientos de los cuales sólo podría tener conocimiento el tercer implicado, será fácilmente inferida la identidad. Por todo ello, en esos casos resultaran superfluas dichas primeras medidas de protección, debiendo instaurarse unas más amplias.

En el artículo 3 se incide en las medidas que pueden adoptar por la Autoridad Judicial, el Ministerio Fiscal y las FCS, que se pueden resumir.

- Prohibir la toma de fotografías o imágenes de víctimas, testigos y peritos.
- Traslado en vehículos oficiales y locales reservados en dependencias judiciales
- Establecimiento de protección policial (servicios de escoltas, ya sean dinámicas y/o estáticas, en servicios de contra-vigilancia, instalación de sistemas de alarma, etc.) durante todo el proceso o incluso después de su finalización si persiste el peligro. El Ministerio Fiscal cobra una especial relevancia puesto que puede instar que estas medidas se apliquen durante todo el proceso y, si se mantiene el peligro grave, una vez finalice⁴.
- En casos excepcionales, se puede proporcionar por cada una de las autoridades competentes documentos de nueva identidad (Ministerio del Interior) y medios económicos para cambiar la residencia o lugar de trabajo (Ministerio de Justicia o Comunidades Autónomas)

Una vez adoptadas las medidas anteriores, su artículo 4 dispone que el órgano judicial competente para juzgar podrá revisar las adoptadas por el Juez de Instrucción, ponderando los bienes jurídicos constitucionalmente protegidos y derechos fundamentales en conflicto (Magro, 2010 a). De manera que las decisiones durante el propio proceso se podrían agrupar los siguientes puntos:

- Mantenimiento o supresión de las medidas de seguridad mediante auto motivado que disponga que la persona protegida debe serlo frente al peligro que proviene de la persona u organización, para la que el testimonio pueda considerarse elemento de prueba a efectos de motivar una condena penal (Magro, 2010 b)
- Revelar datos de identidad o no (las partes pueden solicitar conocer la identidad de testigos y peritos propuestos, respetando las garantías de la ley) pero esto puede denegarse por varias causas: negativa judicial motivada, consideración del testigo como no relevante, carecer de relación extraprocesal con la parte acusada, aceptación o inactividad de la defensa, renuncia de la fiscalía al testigo, revelación parcia, etc.
- Apreciación de las pruebas aportadas.

Hay que señalar que las medidas adoptadas son susceptibles de recurso de reforma y apelación.

⁴ La Instrucción de la FGE de 16 de noviembre de 2007, en correspondencia con el Artículo 3.1.10 del EOMF que establece: *“Para el cumplimiento de las misiones establecidas en el artículo 1, corresponde al Ministerio Fiscal: Velar por la protección procesal de las víctimas y por la protección de testigos y peritos, promoviendo los mecanismos previstos para que reciban la ayuda y asistencia efectivas”* establecía que las Fiscalías deberán extremar el cuidado para no dejar de instar en el proceso penal la adopción protectoras que procedieran en virtud del artículo 3.2 de la LOPT.

3. TIPO DE MEDIDAS GENERALES DE PROTECCIÓN DE VÍCTIMAS DE DELITO Y TESTIGOS PROTEGIDOS.

En correspondencia con lo expuesto, el tipo de medidas de protección son abordadas con una combinación de aquellas de tipos legal y práctico que se deben o se pueden adoptar en los supuestos objeto de análisis, pudiendo ser segmentadas en bloques diferenciados por los bienes de estas personas.

De la forma que están incluidas en la normativa, se observa una dispersión de medidas en varias disposiciones legales y la ausencia de una norma específica completa que abarque exhaustivamente la materia en todos o la mayoría de los aspectos. Es reseñable que nuestro país sea el único de la UE que no posee un programa de protección de testigos completo ni de un organismo de composición multidisciplinar que vele por la aplicación y la facilitación efectiva de las medidas y que la norma que estableció el estatuto básico de las víctimas tenga únicamente una vigencia de ocho años.

Los bloques, divididos por temáticas principales, podrían ser:

Determinar la reserva de la identidad:

Como se ha dispuesto, distinta normativa contempla la posibilidad de mantener en secreto la identidad de los testigos y peritos evitando así su revelación pública. Este enfoque busca principalmente prevenir posibles represalias y garantizar su seguridad personal. No obstante, esta reserva puede ser levantada en los procesos penales a resultas de garantizar la tutela judicial efectiva.

Cambio de Identidad:

En situaciones de violencia de género, extrema necesidad o riesgo, el cambio de identidad completa o parcial de la víctima o del testigo puede considerarse como una medida adicional de protección para evitar la localización y minimizar el riesgo de represalias. Sin embargo, existen diferencias significativas entre las normativas relacionadas con el registro civil y las de testigos protegidos en cuanto a la eficacia y la extensión de esta medida. En el primer caso, el cambio de identidad, una vez concedido, tiene efectos legales en el tráfico jurídico. Por otro lado, en el segundo caso, el cambio de identidad no implica un cambio legal o registral de la identidad, sino que únicamente se proporciona a la persona testigo la documentación de una identidad supuesta (normalmente DNI) sin un respaldo normativo expreso para su uso en el tráfico jurídico. Es decir, en una situación se cambia la inscripción registral obteniendo una identidad nueva y en la otra, solamente se facilita un documento para poder operar en vida cotidiana.

Resulta importante señalar que estas medidas no son retroactivas ni afectan a todos los documentos de la persona, lo que significa que los documentos, autorizaciones y certificados (como estudios y permisos), así como otros derechos que se deban ejercer (como hipotecas, propiedades o alquileres), deberán adaptarse a esta nueva realidad. Este proceso puede generar una brecha de seguridad significativa, ya que implica la tramitación de procesos de todo tipo. Si se facilita una nueva identidad definitiva, la persona tendrá que modificar todos sus documentos para adaptarlos a la misma. Es decir, si ya tiene un vehículo a su nombre, debe cambiar el registro en la DGT si tiene un título de grado ocurrirá lo mismo con educación, su puesto de trabajo, etc. Pero más difícil lo

tiene quién sólo posee un documento de identidad supuesta ya que es una situación temporal sin validez jurídica y tendrá que realizar por sí misma todas esas actuaciones igualmente.

Restricciones en captación de imágenes y sonido:

Se prohíbe la captación de imágenes o grabaciones que puedan revelar la identidad de las víctimas (especialmente los menores de edad⁵) y los testigos. Estas restricciones contribuyen a mantener la confidencialidad y proteger especialmente los datos personales de estas personas de manera que dicha actividad puede ser considerada como una medida de seguridad preventiva que tendrá un impacto u otro en virtud del lugar donde se pretenda llevar a cabo. No será igual la posibilidad de su implementación en la vía pública que en la sala de un Juzgado o Tribunal, siendo necesaria en muchas ocasiones y dependiendo del caso concreto la ponderación entre este derecho, el derecho a la publicidad de los procesos penales y el derecho a recibir información veraz por parte de la ciudadanía.

Protección Física:

Con el fin de proteger mejor a las víctimas y testigos, además de resguardar su información, se pueden implementar varias medidas para asegurar su integridad física. Estas medidas incluyen, entre otras, el desarrollo de planes de protección y autoprotección específicos, la geolocalización de los agresores, la asignación de escoltas, la provisión de ubicaciones seguras o reubicaciones, y la autorización de ocultaciones y el establecimiento de dependencias adecuadas para evitar cualquier tipo de amenaza.

Es crucial diferenciar entre la actividad policial y la judicial en estos contextos. La autoridad judicial es responsable de tomar decisiones motivadas basadas en los análisis de riesgos que se le faciliten que indiquen el nivel de peligro para el testigo o sus allegados. Esta decisión debe ser motivada y debería considerar las circunstancias extremas y el alto coste personal, social, moral y económico para quienes van dirigidas. Y, por otro lado, las FCS tienen el cometido de la implementación práctica de estas medidas, como la asignación de escoltas y la vigilancia de ubicaciones seguras

Sin embargo, un hándicap que nos encontramos es que nuestro ordenamiento jurídico no especifica explícitamente las medidas de protección que se pueden aplicar, los órganos administrativos responsables de su ejecución, ni el presupuesto necesario para llevarlas a cabo. Esta falta de regulación detallada dificulta la implementación efectiva de estas medidas y la protección adecuada de las víctimas y testigos.

Medidas Tecnológicas:

Existen recursos tecnológicos que se utilizan para proteger la información del testigo en registros como grabaciones de audio, transcripciones y otros documentos. Las medidas buscan evitar la identificación accidental del testigo a través de medios electrónicos y para ello, se debe garantizar la seguridad de los medios empleados y la de los repositorios por los que transita y se almacena la información y los datos que contiene.

⁵ Conforme al artículo 13.2 de la LOPDP, los datos de las personas menores de edad se pueden tratar, pero siempre garantizando el interés superior de los mismos y con el nivel de seguridad adecuado.

Con ese fin, resulta muy importante que se cumplan las dimensiones de seguridad que recogen en el ENS⁶. Este instrumento dispone que la protección de la información de las administraciones públicas debe garantizar, al menos, las siguientes dimensiones de seguridad: confidencialidad, disponibilidad, integridad, autenticación y trazabilidad de los sistemas y sus usuarios.

Medidas económicas y sociales:

Estas medidas, ya sean directas o indirectas a través de ayudas o prestaciones sociales y económicas, complementan las anteriores y contribuyen a que la colaboración con la justicia y la protección de las víctimas y testigos sean efectivas. Es importante destacar que el sistema aplicable a víctimas, testigos o peritos "ordinarios" es completamente diferente del que se aplica a aquellas personas a las que se les otorga la condición de testigos o peritos protegidos.

La Ley 1/1996, de 10 de enero, de asistencia jurídica gratuita, y las disposiciones contenidas en la LOTJ tienen alcances y ámbitos de aplicación muy diferentes. En el caso de la LOTJ, su aplicación es indeterminada, imprecisa e insuficiente. Dado el reparto constitucional de competencias, y la asunción por las CCAA en la parte de medios de la aplicación de la justicia, son éstas las que ejercen las funciones de facilitar medidas económicas y sociales en cada caso, con la excepción de los casos llevados por la Audiencia Nacional donde dicho órgano aplica directamente algunas medidas de carácter económico en sus procesos.

Derecho a la protección de datos personales:

La legislación reconoce el derecho a la protección de datos de carácter personal de las personas que participen en los procesos penales⁷. Resulta importante apuntar que, en el desarrollo de cada una de estas misiones de las autoridades implicadas, surge un elevado y heterogéneo número de medidas y objetivos a llevar a cabo (protección de víctimas, evaluación de riesgos, seguridad de testigos protegidos, etc.)

De la combinación de las misiones señaladas se deduce indefectiblemente que durante el desarrollo de estas funciones es necesario tratar información y los datos personales que esta contiene, por lo que la actuación de estas instituciones tiene que ir orientada a garantizar los derechos fundamentales tanto como una finalidad en sí misma

⁶ El ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

⁷ El RDLJTICS, dispone en sus artículos 99 y 110 respectivamente: "Artículo 99 Protección de datos en el uso de los medios tecnológicos e informáticos. Los sistemas que se utilicen en la Administración de Justicia y que traten datos personales que vayan a ser incorporados a un proceso judicial o expediente fiscal para fines jurisdiccionales se ajustarán a la normativa prevista en los artículos 236 bis a 236 decies de la Ley Orgánica 6/1985, de 1 de julio; en el artículo 2, párrafos 4 y 5, de la Ley Orgánica 3/2018, de 5 de diciembre, y en el artículo 2.2 de la Ley Orgánica 7/2021, de 26 de mayo. Artículo 100. Protección de datos en los documentos judiciales electrónicos. Las oficinas judiciales y fiscales dispondrán de los medios tecnológicos adecuados para la realización automatizada de la anonimización, seudonimización y disociación de los datos de carácter personal. Con la finalidad de posibilitar lo dispuesto en el párrafo anterior, las resoluciones procesales y judiciales deberán adecuarse a un formato normalizado acordado en el seno del Comité técnico estatal de la Administración judicial electrónica."

como un elemento integrante de cualquiera del resto de sus objetivos. Es decir, se puede señalar que garantizar la protección de los datos personales resulta transversal al desarrollo de todos o de la mayoría de estos cometidos (Fernández, 2023).

El tratamiento de los datos y la información siempre ha sido importante, pero en este momento histórico, esto posee un enorme potencial y resulta un aspecto crucial a la hora de proteger los derechos de las personas y garantizar la seguridad de todas ellas. Si bien, ello no es óbice, más bien al contrario, para que estas acciones se efectúen con un estricto cumplimiento de las normas, la inmediatez, la capacidad, la ética y, por descontado, las garantías y la protección de los derechos necesarias.

4. PROTECCIÓN DE LA INFORMACIÓN Y DATOS DE CARÁCTER PERSONAL.

4.1. LA PROTECCION DE DATOS DE CARÁCTER PERSONAL.

Según el fundamento jurídico 7 de la Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre⁸ el Derecho a la autodeterminación informativa o “*Habeas Data*”, sería el poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. El Tribunal lo define como un derecho independiente, autónomo, diferenciado del derecho a la intimidad, el honor y a la propia imagen. Siendo esta cuestión muy importante puesto que la extensión y alcance de cada derecho, aunque podemos hablar de derechos muy relacionados, tiene unos presupuestos y unas características propias que resulta oportuno conocer ya que se derivan consecuencias y situaciones muy diferentes a la hora de su aplicación, protección o su ejercicio (Teatino, et al, 2022).

En concordancia con este derecho fundamental hay que recordar que, como con casi todos, este no es un derecho absoluto, sino que debe considerarse por función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. Esto cobra especial importancia en los procesos penales, ya que desde las actuaciones pre-procesales más embrionarias del Ministerio Fiscal o las FCS hasta la resolución del proceso se van a analizar las aportaciones y actuaciones de todas las personas y entidades involucradas en ellos de un modo otro.

Para proteger la información y los datos de las personas que colaboran con la justicia se debe analizar en primer lugar qué normativa resulta de aplicación, el RGPD y la LOPGDD u otra de categoría especial. La respuesta es sencilla, la normativa especial, debido a que la propia esencia de los procesos y la finalidad de los tratamientos exigen ciertas diferencias que son difíciles de incorporar a la normativa general.

En la Declaración nº 21 relativa a la protección de datos de carácter personal en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial, aneja al acta final de la Conferencia Intergubernamental que adoptó el Tratado de Lisboa firmado el 13 de diciembre de 2007, de los debates internos de las personas que lo discutían a nivel técnico y del análisis de las circunstancias fácticas que se produjeron a

⁸ Sentencia 290/2000, de 30 de noviembre (BOE núm. 4, de 04 de enero de 2001) ECLI:ES:TC:2000:290

nivel local y mundial en el marco de la seguridad (los atentados de las Torres Gemelas el 11-S, los atentados de Madrid del 11-M, etc.), el legislador europeo vino a descubrir que era necesario desarrollar otras disposiciones que respondieran y se adaptaran a escenarios concretos, como el marco de las misiones de las autoridades competentes para prevenir, detectar, investigar y enjuiciar delitos, así como asegurar el cumplimiento de las penas.

Recordemos que la citada declaración reconocía que podrían requerirse normas específicas sobre protección de datos personales y libre circulación de estos en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial, debido de la naturaleza específica de los mismos (Fernández, 2023).

Derivado de lo anterior, la UE se decantó por establecer un régimen general de tratamiento y uno específico para funciones policiales. Así, en el artículo 2.2.d) del propio RGPD se dispone la exclusión de su ámbito de aplicación al tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

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, cuya trasposición a nuestro ordenamiento se ha producido mediante la LOPDP, que modificó la LOPJ, el EOMF y la LECRIM. Este conjunto supone la base del régimen especial que regula los procedimientos de protección de datos en el marco de la actuación de las autoridades competentes en este marco.

4.1.1. Medidas generales de seguridad a aplicar por los responsables del tratamiento.

En el caso del sistema de justicia, hasta fechas recientes, éste se preocupaba principalmente en garantizar el éxito de la persecución penal y evitar la impunidad de los culpables, sin que la protección de algunas personas que resultaban afectadas por los procesos (como las víctimas y los testigos) se antojara un poco más que instrumentalmente (Turienzo, 2021). Afortunadamente, el enfoque se ha modificado poniendo en el centro de esta protección los derechos de todas las personas, máxime en cuestión de información, datos e identificadores (Fernández, 2023).

La primera medida de carácter general aplicable al colectivo que aplica la LOPDP es la inclusión en la política de las organizaciones de la obligación legal contenida en los estatutos personales del principio general de confidencialidad que exige que las personas que componen las instituciones guarden reserva y secreto de todo lo que conozcan por el desempeño de sus funciones. Esta suele ser una cuestión no demasiado recordada, pero que constituye una de las bases en la que se debería sustentar cualquier sistema de protección de bienes que no pertenecen o que no sólo pertenecen a las organizaciones, como ocurre con las informaciones y los datos personales de terceros o de su personal.

Otra medida principal para lograr este objetivo es tratar los datos de las personas con garantías independientemente de su nacionalidad o lugar de residencia,

distinguiéndose por el responsable, en la medida de lo posible y sin obviar el derecho a la presunción de inocencia, distintas categorías de personas interesadas, en función de su papel o rol, entre:

- Personas respecto de las cuales existan motivos fundados para presumir que hayan cometido, puedan cometer o colaborar en la comisión de una infracción penal.
- Personas condenadas o sancionadas por una infracción penal.
- Víctimas o afectados por una infracción penal o que puedan serlo.
- Terceros involucrados en una infracción penal como son: personas que puedan ser citadas a testificar en investigaciones relacionadas con infracciones o procesos penales ulteriores, personas que puedan facilitar información sobre dichas infracciones, o personas de contacto o asociados de una de las personas mencionadas en los dos primeros apartados.

En estas situaciones, aunque en muchas ocasiones será complejo delimitar la clasificación en un mismo tratamiento (coimputado vs testigo vs codelincuente), el responsable deberá acomodarse a los conceptos y definiciones incluidos en otras normas como sería en los casos de personas condenadas (con o sin sentencia firme, cuestión que no recoge específicamente la norma), las víctimas y testigos protegidos.

Una vez estructurados y fijados estos roles, el responsable debe implementar medidas de seguridad en todo el ciclo de vida del dato, es decir en todas las operaciones llevadas a cabo desde que se obtienen hasta que finalmente se destruyen, sin perjuicio de aplicarlas incluso fuera del perímetro de las propias organizaciones, como, por ejemplo, con sistemas de trazabilidad y control remoto de los datos cuando se trasladan a terceros. Un ejemplo paradigmático de estos sistemas sería el empleo de la herramienta CARLA del CNN-CERT para la protección y trazabilidad del dato (CCN, 2024).

Estas medidas de seguridad se tienen que implantar eficazmente teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, lo que se incrementa exponencialmente en el caso de determinadas víctimas y personas con estatus de testigo protegido. Para ello los responsables o encargados del tratamiento implantarán las medidas técnicas y organizativas apropiadas de las que dispongan para garantizar y estar en condiciones de demostrar que el tratamiento se lleva a cabo de conformidad con la normativa (principio de responsabilidad proactiva: cumplir y poder demostrar que se cumple).

En el caso de las autoridades competentes, además de las medidas de protección que consideren el responsable del tratamiento derivado del análisis de riesgos, deberían adecuarse lo máximo posible al contenido de las incluidas en el anexo II del ENS.

Como sistemas legales implementados, se podrían analizar el nombramiento de las personas designadas como DPD en su función de auditores del sistema, el registro de operaciones, la restricción de derechos, la gestión de brechas de seguridad y la obligación o no de facilitar información sobre los datos que se tratan en fase pre-procesal y procesal.

4.2. REGISTRO DE OPERACIONES.

El Registro de Operaciones constituye una de las bases instrumentales del sistema de autorregulación de los responsables del tratamiento en este marco. Es un sistema de control obligatorio recogido a su vez en el artículo 33 de la LOPDP, conforme al cual los responsables y encargados de tratamiento deben mantener registros que recojan la identificación, autenticación y trazabilidad en los sistemas automatizados de, al menos, las operaciones de recogida, alteración, consulta, comunicación incluidas las posibles transferencias, combinación y supresión de datos personales.

Dentro de estos sistemas automatizados, los registros de consulta y comunicación harán posible igualmente determinar la justificación de la operación, la fecha y la hora de y, en la medida de lo posible, el nombre de la persona que consultó o comunicó datos personales, así como la identidad de los destinatarios de dichos datos personales.

Como puede apreciarse, el incorporar esta herramienta es un indicador de máximo nivel para acreditar las medidas de responsabilidad proactiva y para adecuar el control del acceso, traslado de datos o cesiones al nivel de riesgo de los tratamientos judiciales o policiales lo que redundará directamente en la seguridad de las personas cuyos datos son tratados.

Este registro tiene la finalidad de verificar la legalidad del tratamiento, el autocontrol y garantizar la integridad y la seguridad de los datos personales en el ámbito de los procesos penales. Únicamente será puesto a disposición de la autoridad de control competente (AEPD, CGPJ y la relativa al Ministerio Fiscal), previa solicitud de éstas, y siempre conforme a la legalidad vigente.

4.3 RESTRICCIÓN DE DERECHOS, LIMITACIÓN COMO CONSECUENCIA DE INVESTIGACIONES Y PROCESOS PENALES.

4.3.1. Restricción de derechos

Otro instrumento que pone a disposición de las autoridades competentes la LOPDP, es su artículo 24, que contiene la previsión legal que habilita la restricción del ejercicio de los derechos de las personas interesadas lo que, de facto, constituye en ocasiones otra medida de protección.

El artículo dispone que el responsable del tratamiento pueda aplazar, limitar u omitir la información relacionada con los derechos de la persona interesada, así como denegar total o parcialmente las solicitudes de ejercicio de los derechos, siempre que resulte necesario y proporcional para: impedir que se obstaculicen indagaciones, investigaciones o procedimientos judiciales, evitar que se cause perjuicio a la prevención, detección, investigación y enjuiciamiento de infracciones penales o a la ejecución de sanciones penales o para proteger la seguridad pública, la Seguridad Nacional o los derechos y libertades de otras personas. Debido a lo cual, en ocasiones se evitará facilitar la información en un momento procesal no oportuno y, en otras, las razones de la restricción podrán ser omitidas o ser sustituidas por una redacción neutra cuando su revelación pueda poner en riesgo los fines referidos. Esto es así, porque, la mera comunicación de la restricción (confirmando que se están tratando los datos) ya afectaría a la seguridad de las personas.

4.3.2. Derechos como consecuencia de investigaciones y procesos penales.

El artículo 26 de la LOPDP indica la forma del ejercicio de los derechos de las personas como consecuencia de investigaciones y procesos penales. Éste señala, por un lado, que se efectuará de conformidad con las normas procesales penales cuando los datos personales figuren en una resolución judicial, o en un registro, diligencias o expedientes tramitados en el curso de investigaciones y procesos penales y, por otra parte, informa que el tratamiento de los datos en los procesos penales se llevará a cabo de conformidad con lo dispuesto en la LOPJ, en las normas procesales penales, y, en su caso, en la LOMF. Esto nos indica claramente que sólo en defecto de la regulación de estos ejercicios en dichas normas, se aplicará la LOPDP a la hora de facilitar la información o el acceso a los datos.

El Tribunal Supremo, la Sala Segunda de lo Penal, en su Sentencia 312/2021⁹, cuyo ponente fue Pablo Llanera en la que se analizan estas cuestiones, sobre todo en virtud del contenido de la Directiva 2012/13/UE del Parlamento Europeo y del Consejo, de 22 de mayo de 2012, en su fundamento de derecho primero (1.12), viene a considerar que:

- Las partes personadas, y en particular las encausadas, tienen derecho a conocer el contenido íntegro de las actuaciones procesales, sin más excepción que la derivada de su declaración de secreto (art. 302 LECRIM).
- Este derecho se extiende a conocer actos jurisdiccionales limitativos de derechos fundamentales realizados en otro procedimiento judicial, cuando de su legitimidad dependa la validez del medio probatorio que le afecta y no se hayan ya incorporado al proceso (arts. 579 bis y 588 bis i de la LECRIM).
- El derecho de las partes a conocer y examinar las actuaciones procesales, plasmado en los artículos 118, 627, 780.1 y 784.1 de la LECRIM no faculta conocer la investigación pre-procesal que no se haya reflejado en las actuaciones.
- Excepcionalmente, cuando se presenten indicios fundados de concurrir circunstancias que comprometen la validez de la prueba o que razonablemente pueden condicionar su credibilidad o su capacidad indicativa, afectando con ello al derecho de defensa de las pretensiones de las partes, estas pueden solicitar de la Autoridad Judicial competente que incorpore, únicamente, los extremos concretos de la investigación prejudicial que reflejen tales condicionantes.
- En esos supuestos, la Autoridad judicial realiza un doble análisis de la pertinencia y necesidad de la indagación peticionada (arts. 311, 659, 785 y 786.2 LECRIM).

4.4 GESTIÓN DE BRECHAS DE SEGURIDAD.

Si se produce un incidente de seguridad que afecte a la confidencialidad, como puede ser la filtración de datos a terceros, el responsable debe tener definido e implantado eficientemente un protocolo de contención, comunicación y actuación ante las brechas de seguridad que afecten a sus datos.

No se puede olvidar que una brecha puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos,

⁹ STS 1388/2021, de 13 de abril - ECLI:ES:TS:2021:1388

materiales o inmateriales; por lo que hay que intentar evitarlas y en caso de que sucedan gestionarlas adecuadamente, especialmente en estos casos.

Cuando se haya materializado la brecha, como puede ser por el acceso a datos de víctimas o testigos protegidos, sin perjuicio de otras responsabilidades o actuaciones que se deban llevar a cabo, los responsables tienen la obligación de notificarla a la autoridad de control competente¹⁰ cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas (cuestión que en este caso estaría fuera de toda duda). Dicha comunicación también debe efectuarse a las personas afectadas¹¹, salvo que no sea necesario porque el responsable haya tomado medidas técnicas y organizativas adecuadas que evitan los riesgos anteriores, minimicen los daños a los derechos y libertades y/o los hagan reversibles, que haya tomado, con posterioridad a la brecha de datos personales, las medidas de protección que mitiguen total o parcialmente el posible impacto para los afectados y se garantice que ya no hay posibilidad de que el alto riesgo para sus derechos y libertades se materialice o que suponga un esfuerzo desproporcionado, en cuyo caso, se optará por su publicación en el boletín oficial correspondiente, en la sede electrónica del responsable del tratamiento o en otro canal oficial que permita una comunicación efectiva con las personas afectadas.

No obstante, aunque se pueda inferir que existen niveles de riesgo altos para las personas afectadas, el artículo 39.5 de la LOPDP¹², permite aplazar, limitar u omitir la comunicación con sujeción a las condiciones y en base a las finalidades contenidas en el 24.1¹³.

Estos procedimientos de actuación y comunicación de brechas deben contener instrucciones claras sobre cómo actuar cuando se produzca una filtración de datos de las partes en los procesos penales¹⁴ a los medios de comunicación. Cuestión ésta que no parece que se lleve a efecto con la eficacia necesaria puesto que es una situación recurrente la de encontrar en los medios de comunicación información sobre las personas implicadas (acusadas, víctimas, testigos, etc.) que proviene de fuentes que no son o que no deberían ser abiertas.

¹⁰ A nivel nacional, la autoridad de control sería la Agencia Española de Protección de Datos, salvo que se pueda atribuir al mal funcionamiento de la Administración Autonómica de Andalucía, Cataluña o el País Vasco, en el que correspondería comunicar a la Autoridad de Protección de Datos de dichas comunidades autónomas.

¹¹ Para que puedan ejercer las acciones que consideren oportunas en defensa de sus intereses e implementar las medidas de autoprotección que estimen necesarias.

¹² Artículo 39.5.: “La comunicación al interesado referida en el apartado 1 podrá aplazarse, limitarse u omitirse con sujeción a las condiciones y por los motivos previstos en el artículo 24.”

¹³ Artículo 24.1:” 1. El responsable del tratamiento podrá aplazar, limitar u omitir la información a la que se refiere el artículo 21.2, así como denegar, total o parcialmente, las solicitudes de ejercicio de los derechos contemplados en los artículos 22 y 23, siempre que, teniendo en cuenta los derechos fundamentales y los intereses legítimos de la persona afectada, resulte necesario y proporcional para la consecución de los siguientes fines: a) Impedir que se obstaculicen indagaciones, investigaciones o procedimientos judiciales. b) Evitar que se cause perjuicio a la prevención, detección, investigación y enjuiciamiento de infracciones penales o a la ejecución de sanciones penales. c) Proteger la seguridad pública. d) Proteger la Seguridad Nacional. e) Proteger los derechos y libertades de otras personas.

¹⁴ Es cierto que se debe respetar y proteger el derecho a la información pública, pero habría que analizar si los procesos de obtención de dicha información, por ejemplo, cuando no se obtiene de los gabinetes o unidades de prensa, sino que es “filtrada” por “fuentes” de tal o cual entidad, constituye una brecha de seguridad en las organizaciones que tenían la obligación de mantenerla segura.

5. CONCLUSIONES

El sistema legal de protección de la información y los datos de las personas que participan en los procesos penales está compuesto por varias normas que convergen sobre esta cuestión. En la sociedad de la información y las comunicaciones actual, garantizar esta seguridad resulta fundamental puesto que es muy fácil identificarlas y localizarlas de manera que se las pueda perfilar, coaccionar o amenazar de alguna forma, lo que redundaría en perjuicio de la administración de Justicia.

La LOPJ, el EOMF y la LOPDP, sobre todo desde la entrada en vigor del RDLJTICS, constituyen un hito en los procesos penales al obligar a todas las entidades responsables de las operaciones de tratamiento a adoptar las medidas que aseguren los datos como un elemento principal más de las investigaciones y procesos penales. Estas normas podrían considerarse básicas en este aspecto y sus premisas convergen en otro buen número de normas cuyo contenido desarrolla un sistema sólido y robusto a la hora de lograr sus objetivos desde un punto de vista teórico.

La implementación de los procesos de seguridad conlleva unos plazos y exige una dotación presupuestaria adecuada para que estas acciones se puedan llevar a cabo de manera efectiva y no queden en meras declaraciones de intenciones. Es crucial desarrollar procesos automatizados de seguridad a lo largo de todo el ciclo de vida de los datos, tanto dentro como fuera del perímetro de los órganos implicados, y exigir una mayor responsabilidad ante el incumplimiento de las normas. Es decir, las entidades tienen que instalar procesos técnicos (ciberseguridad) y operativos que, desde las primeras actuaciones hasta que finalicen los procesos y, posteriormente, mientras que sea necesario mantener los datos, asegure la información.

Una filtración de información desde una entidad constituye una brecha de seguridad que debe ser comunicada a las autoridades independientes de control competentes y a las personas interesadas.

Es necesario formar e informar a estas personas sobre los peligros y nivel de riesgo de exponerse o no hacerlo de forma segura en las redes de información, sociales o aplicaciones.

Además de asegurar la información de las víctimas, testigos y peritos, con la misma finalidad, se debe salvaguardar la relativa a las autoridades y funcionarios públicos cuyos datos (más allá de los que legalmente deban ser públicos por el desarrollo de sus funciones) también tienen que quedar también resguardados.

Las normas en este marco todavía no son muy conocidas lo que resalta la necesidad de una mayor inversión, formación y concienciación. Es esencial alinear al personal en la importancia de la información que manejan y hacerles creer que realmente son una parte fundamental del proceso de seguridad. La cadena siempre se rompe por el eslabón más débil, por lo que los cursos y jornadas en un ciclo de mejora continua son un elemento indispensable para conseguir estos objetivos.

En el caso concreto de las personas a las que se les otorga el estatus de testigo o perito protegido, sin entrar en el resto de las medidas adoptadas, se expone que la LOPT tiene lagunas claras en este campo de protección de la información que deben ser

completadas con la aplicación de las normas previamente apuntadas. Este sistema de protección no tiene el necesario respaldo legal ni reglamentario que habilite la creación de un programa de protección de testigos interdepartamental e integral donde se fijen compromisos y obligaciones claras de las partes (testigos vs administración) y facilite soluciones a las graves fallas en la seguridad de la información que posee. Como se recoge en este trabajo, los propios testigos son responsables de realizar las actuaciones necesarias en el tráfico jurídico para adaptar su situación legal derivada de la adopción de una nueva identidad o de la facilitación de documentos de identidad supuesta, por lo que su seguridad se ve permanentemente comprometida en el curso de los expedientes necesarios a tales efectos. Del mismo modo, recae sobre ellas la aplicación de las precauciones de seguridad en el uso de tecnologías de la información y App's.

Analizadas las partes públicas de los proyectos para promulgar una nueva LECRIM de los años 2011, 2013 y 2020 (este último aún publicado en la página de participación pública del Ministerio de Justicia desde el 26 de enero de 2021), ninguno de ellos incluye un programa, sistema o un conjunto de medidas completas y sistematizadas para proteger a estas personas ni un órgano a nivel nacional interadministrativo que posea competencias específicas para ello.

El Tribunal Supremo, en su sentencia de la Sala Segunda de lo Penal nº 468/2020, de 23 de septiembre¹⁵, ponente Vicente Magro Servet, en el fundamento de derecho segundo, 1, indica que la experiencia revela las reticencias de los ciudadanos a auxiliar a la policía judicial y la Administración de Justicia en determinadas causas penales por el temor de sufrir represalias, lo que conlleva, con frecuencia, que no se pueda contar con testimonios y pruebas muy valiosos en estos procesos. Ante esta situación, el legislador debe dictar normas que resulten eficaces en la salvaguarda de quienes, como testigos o peritos, deben cumplir con el deber constitucional de colaboración con la Justicia. Compartiendo dicho criterio, resultaría imprescindible que, si se continua con el último proyecto o en futuros proyectos de reforma de la LECRIM, se incorporaran estas previsiones para cumplir más eficazmente con las exigencias de seguridad y no seguir siendo uno de los pocos países de la Unión Europea que, en el ámbito de las víctimas y los testigos protegidos, no posee un programa nacional que abarque de un modo u otro todos estos extremos.

¹⁵ STS 468/2020, 23 de Septiembre de 2020, ECLI:ES:TS:2020:2987

REFERENCIAS BIBLIOGRÁFICAS

- Ayllón Santiago, H. S. (2021). *Tratamiento de datos de carácter personal en el ámbito policial*. Madrid. Reus.
- CCN, C. C. (10 de marzo de 2024). *CCM-CERT.CNI.ES*. Obtenido de <https://www.ccn-cert.cni.es/es/soluciones-seguridad/carla.html>
- Cubillo López, I. J. (2009). *La protección de testigos en el proceso penal*. Pamplona: Civitas.
- Fernández González, C. (2023). La protección de datos personales en el ámbito policial. Especial referencia a la LO 7/2021, de 26 de mayo. *La administración de justicia y el derecho a la protección de datos personales* (pág. 66). Madrid: Centro de Estudios Jurídicos.
- Gascón Inchausti, F. (2001) "*Prueba sobre la prueba*", *protección de testigos menores, objeto y motivación del veredicto y control del juicio de indicios en el proceso penal*. Recuperado el 16 de 2 de 2024, de <https://eprints.ucm.es/26585>
- Irujo, J.M., (2012) *Testigos desprotegidos. El precio de acusar. El País*.
- Magro Servet, V. (2010) *Régimen legal de los testigos protegidos en el proceso penal*. Recuperado el 16 de 2 de 2024, de <https://dialnet.unirioja.es/servlet/articulo?codigo=3320107>
- Magro Servet, V. (2010). *Régimen legal de los testigos protegidos en el proceso penal*. La Ley Penal -- N. 75 p. 24-35
- Navarrete, E. M., García, J. C., & Muñoz, F. A. (2014). *Protección de Víctimas y Testigos como una garantía Constitucional*. Recuperado el 16 de 2 de 2024, de <http://ri.ues.edu.sv/id/eprint/7504>
- Ruiz Barba, O. (2013). *Diferentes modelos de protección de testigos*. Recuperado el 16 de 2 de 2024, de <https://dialnet.unirioja.es/servlet/articulo?codigo=4548356>
- Teatino Gómez, D. (2022). *Estudio sobre el sistema de protección de datos personales con finalidad de prevención, detección, e investigación policial de infracciones penales*. Madrid: Ministerio del Interior, Secretaría de Estado de Seguridad.
- Torras Coll, J. M. (2019). *Los testigos protegidos y el derecho de defensa*. Recuperado el 16 de 2 de 2024, de <https://dialnet.unirioja.es/servlet/articulo?codigo=7151044>
- Turienzo Fernández, A. (2021). *Sobre el testigo protegido en España: La Ley Orgánica 19/1994, de 23 de diciembre bajo examen*. *Revista General de Derecho Procesal* n° 51, Artículo número 423249.
- Vega Dueñas, L. C. (2015). *La protección de testigos, víctimas y colaboradores con la justicia en la persecución a la criminalidad organizada*. Recuperado el 16 de 2 de 2024, de <https://dialnet.unirioja.es/servlet/tesis?codigo=54332>.

