Centro de Estudios de Consumo

PUBLICACIONES JURÍDICAS
http://centrodeestudiosdeconsumo.com

MÁS VALE TARDE QUE NUNCA: EL EJECUTIVO APRUEBA EL PROYECTO DE LEY ORGÁNICA POR LA QUE SE REGULA LA PROTECCIÓN DE LOS DATOS PERSONALES EN LAS TAREAS DE PREVENCIÓN, DETECCIÓN, INVESTIGACIÓN O ENJUICIAMIENTO DE INFRACCIONES PENALES Y DE EJECUCIÓN DE SANCIONES PENALES [*]

Alba García Hernández
Centro de Estudios de Consumo
Universidad de Castilla-La Mancha

Fecha de publicación: 11 de febrero de 2021

1. Introducción

El Consejo de Ministros aprobaba y remitía a las Cortes Generales, el pasado 9 de febrero, el Proyecto de Ley Orgánica por la que se regula la protección de los datos personales utilizados en las labores de prevención, detección, investigación o enjuiciamiento de infracciones penales y de ejecución de sanciones penales, así como en la protección y prevención frente a las amenazas contra la seguridad pública.

Esta norma se ha elaborado con motivo de la transposición de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de

[*] Trabajo realizado en el marco del Contrato con referencia 2020-COB-9996 financiado con cargo a la ayuda para la realización de proyectos de investigación científica y transferencia de tecnología, de la Junta de Comunidades de Castilla-La Mancha cofinanciadas por el Fondo Europeo de Desarrollo Regional (FEDER) para el Proyecto titulado "Protección de consumidores y riesgo de exclusión social en Castilla-La Mancha" (PCRECLM) con Ref.: SBPLY/19/180501/000333 dirigido por Ángel Carrasco Perera y Ana Isabel Mendoza Losana; en el marco del Proyecto de Investigación PGC2018-098683-B-I00, del Ministerio de Ciencia, Innovación y Universidades (MCIU) y la Agencia Estatal de Investigación (AEI) cofinanciado por el Fondo Europeo de Desarrollo Regional (FEDER) titulado "Protección de consumidores y riesgo de exclusión social", dirigido por Ángel Carrasco Perera y Encarna Cordero Lobato; a la Ayuda para la financiación de actividades de investigación dirigidas a grupos de la UCLM Ref.: 2020-GRIN-29156, denominado "Grupo de Investigación del Profesor Ángel Carrasco" (GIPAC) y en el marco del Proyecto Convenio de colaboración entre la UCLM y el Ilustre Colegio Notarial De Castilla-La Mancha (17 enero 2014) (OBSV) con referencia CONV140025, que dirige el Prof. Ángel Carrasco Perera.

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 [en adelante, la Directiva (UE) 2016/680 o la Directiva].

Con la promulgación de esta ley, se pretende impulsar la creación de un marco de regulación nacional en materia de protección de datos, ampliando y especificando el alcance de las normas vigentes: el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Asimismo, destaca la dualidad de objetivos presumible de esta norma, pues, de un lado, se ocupa de la tutela de los derechos y libertades de los ciudadanos en lo que respecta a la protección de datos y, de otro lado, aspira a convertirse en el mecanismo por el que lograr el éxito en materia de cooperación internacional en el ámbito penal y de policía.

Sin embargo, a pesar de los múltiples beneficios que se presumen de la Ley, su tramitación no ha quedado ajena a la polémica por los retrasos en los que se ha incurrido a la hora de adaptar nuestro ordenamiento a las exigencias europeas.

2. Antecedentes normativos: la Directiva (UE) 2016/680

Desde el año 2016, España tiene pendiente la adaptación de la Directiva (UE) 2016/680. Esta norma se circunscribe a la compilación jurídica que la Comisión Europea pretende impulsar para afianzar la protección y defensa de los derechos y libertades de las personas en lo que se refiere a la libre circulación y al tratamiento de datos de naturaleza personal. Se centra en tres pilares básicos: el amparo a los derechos de los interesados, la transferencia de datos en el marco europeo y la creación de mecanismos de cooperación en el ámbito penal y de policía.

La Directiva (UE) 2016/680 parte de la premisa de que la protección de las personas físicas respecto al tratamiento de datos personales ha de ser concebida como un derecho fundamental, por lo que cualquier norma que se contextualice en el marco de esta materia ha de respetar los derechos y libertades de los ciudadanos, independientemente de su nacionalidad o residencia. Además, tal propósito se ha de garantizar en un espacio de libertad, justicia y seguridad, a cuya creación se pretende contribuir con la presente Directiva. Queda fuera del alcance de la norma el tratamiento que tuviera lugar en un

contexto fuera del ámbito de aplicación del Derecho europeo o que se realizara por parte de los órganos e instituciones de la Unión Europea[1].

El legislador europeo, consciente de la complejidad de la realidad actual, reconoce en la Directiva la dinamicidad presente. La norma se desarrolla en un entorno globalizado donde la tecnología cobra cada vez mayor relevancia y la transferencia de información entre multitud de agentes se presenta como un aspecto crucial. En este sentido, los avances tecnológicos han permitido el tratamiento de datos en funciones como la investigación, la prevención, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales.

Todas estas actividades pretenden asegurar y mejorar la cooperación judicial y policial en el marco europeo. No obstante, para alcanzar este objetivo se han de armonizar los métodos de trabajo y las normas que garanticen un nivel de protección reforzado en materia de protección de datos, especialmente, cuando se trata del intercambio de esta información en el ámbito de actuación de los Estados miembros, siendo esta una de las metas que se pretende conseguir con la transposición de la Directiva (UE) 2016/680 por parte de los Estados miembros a sus ordenamientos jurídicos.

Así pues, el legislador reconoce la necesidad de brindar una protección superlativa e igualitaria en el marco de la Unión a aquella información relativa a la esfera más personal de un individuo, particularmente, cuando se trata de actividades de tratamiento que tengan por finalidad las actividades anteriormente mencionadas –la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o de ejecución de sanciones penales incluidas la protección y la prevención frente a las amenazas para la seguridad pública–.

Uno de los objetivos que se han marcado respecto a estas funciones a nivel penal y de policía es el empoderamiento de los derechos de los interesados y, como contrapartida, de aquellas obligaciones y responsabilidades de quienes han de encargarse del tratamiento de datos personales. De esta suerte, la Directiva apunta que los Estados miembros habrán de salvaguardar las libertades individuales a este respecto y garantizar que la cesión e intercambio de datos sea lícito y fluido entre los agentes implicados[2].

Sin embargo, a pesar de los notables avances tecnológicos, la Directiva hace hincapié en la necesidad de que la protección de los datos personales de los interesados no dependa de los medios o técnicas que hubieran sido implementados para asegurar el respeto y cumplimiento de esta cuestión axial en el entorno europeo. Es por esta razón que la Directiva no solamente se aplica a las funciones de tratamiento de datos que se realicen

[1] Art. 2 de la Directiva (UE) 2016/680.
[2] Art. 1 de la Directiva (UE) 2016/680.

de forma automatizada, sino, en la misma medida, es aplicable a aquellas que se llevaran a cabo de forma manual.

Como ya es sabido, la protección de datos tiene como pilar fundamental la defensa de los datos personales de las personas físicas, entendiéndose por tal aquellos que permitieran la identificación directa de una persona o que la hicieran identificable. Así pues, gana gran importancia en el ámbito penal y de policía los procesos de anonimización, es decir, aquellos tendentes a dificultar o a impedir la identificación del interesado. Respecto a esta información, la Directiva (UE) 2016/680 considera que los principios de protección de datos personales no son de aplicación. Sin embargo, la mayor parte del contenido tratado en este ámbito posibilita la identificación, antes o después, de una persona, por lo que se ha de atender a las normas que recoge la normativa, concretamente, en el marco de cooperación para la lucha contra la delincuencia internacional. Así pues, considerando el alto grado de cooperación que se reclama en el entorno europeo en materia de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales incluidas la protección y la prevención frente a las amenazas para la seguridad pública se requiere la creación de mecanismos y técnicas que faciliten la aplicación normativa y la asistencia internacional[3].

Los principios rectores de la protección de datos rigen en este contexto en el mismo sentido. Todo tratamiento de datos debe realizarse en términos de licitud, lealtad, transparencia y exactitud; se ha de llevar a cabo con fines determinados y explícitos y la actividad de tratamiento ha de responder a los principios de pertinencia y adecuación[4]. Con todo, en el ejercicio de las funciones de policía, el ente público podrá desempeñar funciones de videovigilancia o de investigación encubiertas ciñéndose a las condiciones previstas por la Directiva (UE) 2016/680.

Asimismo, si hay una cuestión que ha de ser tenida en cuenta cuando se trata de la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o de ejecución de sanciones penales es que los datos tratados en el campo de la cooperación judicial penal y policíal pertenecen a muy diversas categorías de interesados: individuos sobre los que recaiga de manera fundada la sospecha o la evidencia de la comisión de un ilícito penal, personas condenadas, víctimas, testigos o terceros que dispongan de información relativa a la infracción objeto de la investigación[5].

En este sentido, no solamente la Directiva aprecia la relevancia de las múltiples categorías de datos que han de atender las actividades de tratamiento, sino que la norma apunta la especial sensibilidad de los datos tratados. Muchas de las informaciones con las que se

[3] Art. 40 de la Directiva (UE) 2016/680.
[4] Art. 4 de la Directiva (UE) 2016/680.
[5] Art. 6 de la Directiva (UE) 2016/680.

trabaja se encuentran estrechamente vinculadas con las ideologías, creencias religiosas, estado de salud o raza del interesado. Estos datos solamente podrán ser objeto de tratamiento cuando ello sea estrictamente necesario para defender los intereses de los afectados, lo prevea así la propia legislación europea o tal información sensible haya sido publicada o dada a conocer por el propio interesado[6].

A pesar de todo lo mencionado hasta el momento, si hay un asunto que ha sido cuidadosamente tratado en la Directiva (UE) 2016/680 es la transferencia de datos personales, la cual, como ya se ha anunciado, es una actividad fundamental en el ámbito penal en cuanto a la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o de ejecución de sanciones penales. De este modo, como consecuencia de los elevados riesgos que entraña la actividad de cesión o transferencia de datos en el marco penal europeo, el legislador determina que tales funciones únicamente podrán llevarse a cabo cuando se respete un nivel de adecuación mínimo, se cuente con las garantías apropiadas para ello o nos encontremos ante determinadas excepciones previstas en el ordenamiento.

Respecto al primero de los mecanismos– la adecuación óptima– la transferencia de datos se efectuará cuando[7]:

- La transferencia sea estrictamente necesaria.
- La autoridad a la que se transfiera la información personal fuera competente.
- El Estado miembro responsable de la cesión haya dado su consentimiento.
- […]

Asimismo, para hacer efectiva la transferencia de datos personales, el receptor de la información (ya fuera otro Estado miembros, cualquier otro país o una organización), deberá garantizar un nivel de adecuación óptimo en cuanto a la protección que dicho contenido pueda recibir. En este caso, no se requiere autorización expresa por parte de la Comisión, aunque se habrán de valorar distintos aspectos:

- El destinatario de los datos debe desarrollar sus actividades (o ser) un Estado de Derecho, respetuoso con los derechos y libertades fundamentales.
- Ha de existir o, en caso de que esto no fuera así, articularse la creación de una autoridad de control.

La adecuación de un agente para participar en actividades de transferencia o de intercambio de datos no es una condición que se adquiera de manera absoluta, sino que está sujeta a una revisión periódica por la que, si no se cumplen los requisitos establecidos,

[6] Art. 10 de la Directiva (UE) 2016/680.
[7] Art. 35 de la Directiva (UE) 2016/680.

el país u organización dejará de ostentar la cualidad de garante de una protección adecuada para la transferencia de datos personales[8].

Por otro lado, el segundo mecanismo que ha sido formulado por la Directiva es la creación de garantías jurídicas apropiadas tendentes a garantizar la defensa de los datos recabados[9]. No obstante, es posible que un agente no cumpla con este último requisito ni tampoco lo haga respecto a la salvaguardia de un nivel de protección mínimo. En este caso, habrá de analizarse si concurre alguno de los supuestos excepcionales que prevé el legislador, esto es, que la transferencia sea una medida necesaria para proteger los intereses del afectado o para prevenir acontecimientos que atenten contra la seguridad y el interés públicos de un país[10]. En definitiva, independientemente del mecanismo o técnica empleada para garantizar la seguridad, el punto clave en esta materia es el análisis de la necesidad concurrente y, de manera paralela, la creación de todo un sistema reforzado de protección.

Considerando todo lo anterior, con la transposición de la Directiva (UE) 2016/680 lo que se pretende es la armonización del tratamiento de datos en el ámbito penal. Por medio de la adaptación de esta norma a nuestro ordenamiento jurídico, España se compromete a velar por la protección de los datos personales en la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o de ejecución de sanciones penales incluidas la protección y la prevención frente a las amenazas para la seguridad pública, a formular y articular los mecanismos adecuados que garanticen el efectivo cumplimiento normativo y el respeto a los derechos y libertades de los interesados y a desempeñar un papel protagonista en la colaboración y cooperación con el resto de Estados miembros e instituciones europeas a este respecto.

3. Objetivo doble

El Proyecto de Ley Orgánica que regula la protección de los datos personales empleados en las funciones de prevención, detección, investigación o enjuiciamiento de infracciones penales, así como en la protección y prevención frente a las amenazas contra la seguridad pública tiene dos propósitos esenciales:

- De una parte, aspira a convertirse en mecanismo de defensa y tutela de los derechos fundamentales de las personas en lo que a la protección de datos se refiere. De este modo, se pretende la creación de un nivel de protección superlativo de los derechos de los ciudadanos y de sus datos personales en consonancia con el resto de los Estados miembros.

[8] Art. 36 de la Directiva (UE) 2016/680.
[9] Art. 37 de la Directiva (UE) 2016/680.
[10] Art. 38 de la Directiva (UE) 2016/680.

- Por otro lado, se erige como resorte jurídico para lograr la cooperación y colaboración entre las autoridades europeas en el ámbito penal, sin entrar en contradicción con los derechos de los afectados por el tratamiento de datos.

Es decir, se trata de conjugar la salvaguardia y respeto al derecho a la intimidad de las personas y el derecho a la protección de los datos atinentes a su esfera más privada –en torno a los cuales se construye un blindaje excepcional– con el éxito en la cooperación internacional y la seguridad pública.

Este Proyecto pone especial énfasis en reconocer la sustantividad propia del apartado cuarto 4 del art. 18 de nuestra Constitución, tal y como ya hubieran perfilado en múltiples ocasiones el Tribunal Constitucional (en adelante, el TC) y el propio legislador europeo. Así pues, el TC considera que este precepto supone "una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de las personas (...) un instituto que es, en sí mismo, un derecho o libertad fundamental". Igualmente, marca las diferencias entre este derecho y el derecho a la intimidad, pues con el primero lo que se pretende es "garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado", mientras que, por medio del derecho a la intimidad, lo que se quiere conseguir es la protección "frente a cualquier invasión que pueda realizarse en el ámbito de la vida personal y familiar"[11].

Se estructura en ocho capítulos con 61 artículos, dos disposiciones adicionales y once disposiciones finales. Sus notas esenciales son:

- En su ámbito de aplicación se encuadran tanto las actividades de tratamiento de datos que fueran automatizadas, como aquellas que no.
- Queda circunscrito bajo su alcance el tratamiento recaído sobre datos audiovisuales obtenidos por medio del empleo de cámaras por parte de las Fuerzas y Cuerpos de Seguridad del Estado y de las autoridades competentes en el ejercicio de las funciones de vigilancia, control y regulación.
- La norma prohíbe la utilización de la técnica conocida como *profiling* o elaboración de perfiles criminales, por contravenir este método los principios jurídicos penales, de acuerdo con los cuales se ha de exigir responsabilidad en base a hechos y actos reales que justifiquen la implicación del individuo en la comisión (o el intento) de un ilícito.

[11] GARRIGA DOMÍNGUEZ, A., El derecho a la protección de datos personales en la Jurisprudencia del Tribunal Constitucional, *Nuevos retos para la protección de Datos Personales. En la era del Big Data y la computación ubicua*, 94-101.

- Como ya haría la Directiva, reconoce los derechos generales de los interesados (información, comunicación, acceso, rectificación, supresión, etc.) y las obligaciones presumibles, en términos genéricos, para el responsable de la protección de datos (cooperación con la autoridad de control, registro, realización de evaluaciones de impacto, etc.).
- Hace especial mención a los mecanismos de transferencia internacional de datos de carácter personal.

Este Proyecto de Ley, a pesar de su novedad y precisión, no ha de ser considerado de manera autónoma, sino que ha de entenderse en conjunción con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

4. Régimen sancionador

El Proyecto de Ley asegura un régimen sancionador específico para aquellos que infrinjan las normas de protección de datos en lo que a las investigaciones penales se refiere. En este sentido, la aplicación de sanciones recaerá sobre los responsables y encargados de tratamiento, no así sobre el delegado de protección de datos.

Por otro lado, las infracciones se gradúan en función de la gravedad del ilícito cometido en muy graves (ej. tratamiento de datos con una finalidad distinta a la inicialmente prevista, especialmente cuando tales fines sean incompatibles con los primeros o la transferencia de datos personales no se ajuste al sistema reforzado que ha de cumplirse en tales casos), graves (ej. incumplimiento de los plazos de conservación de los datos personales, la falta de información al interesado o la no cooperación con las instituciones de control) y leves (ej. producción de menoscabos de carácter leve a los interesados como consecuencia de la inobservancia de las medidas técnicas u organizativas que se hubieran llevado a cabo).

La futura Ley Orgánica que regula la protección de los datos personales empleados en las funciones de prevención, detección, investigación o enjuiciamiento de infracciones penales establece un régimen sancionador bastante ambicioso con multas que oscilan entre los 6.000 euros y 240.000 euros. Si bien es cierto que la imposición de tales sanciones se realizará atendiendo a las circunstancias particulares de cada supuesto y valorando factores como la naturaleza, la gravedad y la duración de la infracción; la intencionalidad de la infracción, las medidas practicadas a *posteriori* para disminuir los daños y mermas producidos; la cooperación con la autoridad de control pertinente; etc.

Las infracciones administrativas podrán prescribir, en función de su gravedad, en un plazo de entre seis meses y dos años desde el momento en el que se hubiera cometido el ilícito. Aquellas sanciones interpuestas con motivo de la comisión de una infracción muy grave prescribirán a los tres años, a los dos años para las graves y al año las leves.

5. Tramitación de urgencia

La tramitación de la Ley se ha ido dilatando en el tiempo y, como consecuencia de la acumulación de este retraso, el Ejecutivo ha solicitado su tramitación urgente. Muestra de esta demora es el hecho de que el propio Consejo de Ministros sometió a examen el Anteproyecto de Ley el pasado 10 de marzo de 2020 por primera vez.

El art. 93 de la Resolución de 24 de febrero de 1982 por la que se ordena la publicación en el Boletín Oficial del Estado del nuevo Reglamento del Congreso de los Diputados prevé la posibilidad de que un asunto se tramite por procedimiento de urgencia siempre que así lo solicite el Gobierno, dos Grupos Parlamentarios o una quinta parte de los Diputados. Lo mismo se expone en los arts. 133 a 135 del Reglamento del Senado.

¿Qué supone la tramitación administrativa urgente? Lo que se pretende con esta declaración de urgencia es la reducción de los plazos ordinarios de tramitación parlamentaria con la finalidad exclusiva de acelerar el proceso de elaboración y aprobación, circunstancia necesaria para la transposición inminente y necesaria de la Directiva (UE) 2016/680.

Asimismo, se ha comunicado la aprobación a todos aquellos agentes que quedarían vinculados por la norma: el Consejo General del Poder Judicial, el Consejo Fiscal, la Agencia Española de Protección de Datos, las Direcciones Generales de Policía y Guardia Civil y la Secretaria General de Instituciones Penitenciarias, entre otros.

6. Conclusiones

Como ha quedado patente, la transposición de 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 referido 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 se ha de entender como una prioridad en el momento actual.

La elevada sensibilidad de los datos tratados en materia penal y de policía hace necesaria la creación de un cuerpo jurídico robusto por el que se promueva la construcción de un halo de protección superior que se ha de brindar obligatoriamente a los datos personales. Especial mención merece la transferencia de datos en este contexto donde la cooperación

y colaboración en el entorno de la Unión Europea se hace fundamental para la lucha contra la delincuencia y la salvaguardia de la seguridad pública.

De este modo, la promulgación de la Ley Orgánica por la que se adapta la Directiva europea a nuestro ordenamiento jurídico supone la implementación de una novedosa norma por la que se regulan unas actividades especialmente concretas y específicas como son la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

Con la elaboración de esta nueva ley, el legislador garantiza el ajuste Derecho-realidad práctica, pues asegura que el desarrollo normativo vaya de la mano del rápido avance tecnológico. Asimismo, no solamente hace hincapié el legislador español en la necesidad de adaptar el ordenamiento vigente a los avances técnicos, sino que considera el alto grado de cooperación y globalización del entorno actual, donde la transmisión de información personal es cada vez más frecuente y para la que urge una regulación tendente a la protección de los agentes más débiles involucrados: los ciudadanos.

No obstante, a pesar de las bondades de esta nueva ley, se requiere una participación más activa, si cabe, de los entes públicos, particularmente, de los poderes Ejecutivo y Legislativo. Se ha demostrado y así lo ha hecho patente el propio Gobierno que, a pesar de las ansias por crear un marco regulador nacional en materia de protección de datos y desarrollado en consonancia con la legislación propia de la Unión Europea, los esfuerzos realizados por las autoridades competentes han sido insuficientes y, de nuevo, las dilaciones en el procedimiento cobran mayor importancia que la necesidad acuciante de proteger a las personas.