



#RET

Revista Española de la Transparencia

Nº 5. Segundo Semestre 2017

Elena Gil González

Doctoranda en Big Data y Protección de Datos. Universidad CEU San Pablo

Aproximación al estudio de las decisiones automatizadas en el seno del Reglamento General Europeo de Protección de Datos a la luz de las tecnologías big data y de aprendizaje computacional

Recibido: 06/12/2017
Aceptado: 01/01/2018

RESUMEN

Cada día es más frecuente el uso de medios automatizados para la toma de decisiones gracias al avance de las tecnologías big data o de aprendizaje computacional (*machine learning*). Este hecho ha sido reflejado en el Reglamento General Europeo de Protección de datos, que confiere una gran importancia a la transparencia y a los derechos de los interesados en relación con la toma de decisiones automatizadas.

El foco de este estudio es el análisis de aquellas disposiciones del Reglamento referentes a este tipo de decisiones en el marco de las obligaciones de información a los interesados, su derecho de acceso y el derecho a no ser objeto de decisiones automatizadas, así como la propuesta de medidas para lograr una mayor protección de los derechos e intereses de los individuos.

PALABRAS CLAVE

Big data, transparencia, datos personales, privacidad, derecho de información, algoritmos, reglamento europeo de protección de datos, internet de las cosas, decisiones automatizadas, accountability, principio de responsabilidad proactiva, aprendizaje computacional, machine learning, derecho de acceso.

I. INTRODUCCIÓN

Hasta la actualidad, la protección de datos personales se encontraba regulada en la Unión Europea mediante la Directiva 95/46¹ (en adelante la "Directiva"), que dejará de ser aplicable el 25 de mayo de 2018, día en el que comenzará a aplicarse el nuevo marco normativo del Reglamento General de Protección de Datos² (en adelante el "Reglamento" o "RGDP").

Una de las novedades del Reglamento ha sido reforzar las obligaciones de los responsables del tratamiento, concretamente a través del principio de responsabilidad activa (accountability) (art. 5.2). Este principio, que se ha introducido por primera vez en la

¹ Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

² 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).

Aproximación al estudio de las decisiones automatizadas en el seno del Reglamento General Europeo de Protección de Datos a la luz de las tecnologías big data y de aprendizaje computacional

normativa de protección de datos a nivel comunitario con carácter obligatorio, implica que el responsable o encargado del tratamiento debe garantizar el cumplimiento de lo dispuesto en el Reglamento, y concretamente que los datos sean tratados de manera lícita, leal y transparente con relación al interesado. Además, el Reglamento añade la obligación de ser capaz de demostrar dicho cumplimiento.

Así, el principio de responsabilidad activa debe promover un tratamiento de datos sostenible, asegurando que la carga de valorar la licitud y la lealtad de los tratamientos complejos de datos recae principalmente sobre los responsables y reguladores, y no sobre el individuo. Por este motivo, este principio no debe verse como una alternativa al cumplimiento de las obligaciones legales, sino como una responsabilidad ética (Butarelli, 2016, 78). Con ello, tal y como ha expresado el Grupo de Trabajo del Artículo 29 (en adelante, "GT29"), se pretende lograr una transición de la mera teoría a la práctica en lo referente al cumplimiento de las obligaciones en materia de protección de datos personales, ayudando a las autoridades de control en su función de supervisión y ejecución³.

No obstante, el Reglamento no especifica un sistema cerrado de medidas a través de las cuales los responsables pueden dar cumplimiento a sus obligaciones y probarlo. Por el contrario, se viene a establecer una obligación de resultado: la posibilidad de demostrar el respeto a los principios de protección de datos y la seguridad de los datos personales, sin importar los medios utilizados para conseguirlo, en la medida en que el Reglamento únicamente establece obligaciones genéricas relativas, entre otras, a la implementación del principio de protección de datos desde el diseño, la realización de evaluaciones de impacto, determinadas obligaciones documentales o la designación de un Delegado de Protección de Datos.

Este enfoque requiere una aproximación más madura por parte de los responsables y encargados del tratamiento de datos personales, precisamente en un momento en el que dichos tratamientos son una pieza básica de nuestro sistema económico y social, cuya tendencia es creciente.

Este énfasis en la transparencia evidencia, como ya ha sido adelantado, el objetivo del Reglamento de otorgar un mayor poder de control y disposición a los sujetos sobre el tratamiento de los datos personales que se refieran a ellos. En efecto, otras disposiciones del Reglamento vienen a reiterar este sentimiento, tales como la nueva configuración del consentimiento del interesado, que se vuelve más estricta y adquiere mayor protagonismo.

Existe una tensión entre, por un lado, la transparencia exigida en el cuerpo normativo de la protección de datos personales establecido por el Reglamento y, por otro lado, los nuevos avances tecnológicos, tales como el big data o el aprendizaje computacio-

³ Grupo de Trabajo del Artículo 29, Dictamen 3/2010 sobre el principio de responsabilidad, 00062/10/ES, de 13 de julio de 2010, p.2.

nal (*machine learning*). Estas tecnologías se alimentan de cantidades masivas de datos, provenientes de orígenes cada vez más numerosos en nuestro día a día, como dispositivos inteligentes, nuestra huella digital o el comercio electrónico. Estos datos adquieren nuevas finalidades, que en muchas ocasiones no son previsibles en el momento su recogida, y son tratados de manera automatizada a través del uso de algoritmos, cuyo funcionamiento es opaco para los interesados.

El foco de este estudio es el análisis del concepto de transparencia en relación con la toma de decisiones automatizadas a la luz de lo dispuesto en el Reglamento y del funcionamiento de las tecnologías big data y de aprendizaje computacional. Así, en las próximas páginas analizaremos aquellas disposiciones del Reglamento referentes a este tipo de decisiones en el marco de las obligaciones de información a los interesados, su derecho de acceso y el derecho a no ser objeto de decisiones automatizadas.

II. APROXIMACIÓN A LA REGULACIÓN DEL PRINCIPIO DE TRANSPARENCIA EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

La transparencia ocupa un lugar central en la ordenación de la protección de datos personales en Europa desde su inicio. Sin embargo, el nuevo Reglamento le otorga una importancia aún mayor. Quizás la muestra más visual de ello sea el hecho de que, mientras en la Directiva el término "transparencia" aparece mencionado expresamente una única vez –siendo ésta en un considerando–, en el texto del nuevo Reglamento el término "transparencia" y sus derivados aparecen hasta 24 veces, tanto en los considerandos como en el articulado del mismo. No quiere ello decir que la Directiva no otorgue importancia a la necesidad de transparencia, en la medida en que este concepto se halla de forma implícita incluido, por ejemplo, en lo relativo al derecho a la información (arts. 10 y 11 de la Directiva). No obstante, la evolución de la sociedad de la información y el avance de las tecnologías que permiten recoger, almacenar y tratar datos personales a una escala sin precedentes ha hecho necesaria una revisión que pase por aumentar las garantías de los interesados y su derecho a conocer con claridad los usos que los datos adquieren.

Una de las mayores representaciones de este aumento de la importancia de la transparencia en el Reglamento respecto de la Directiva puede encontrarse en las disposiciones que establecen los principios del tratamiento de datos personales. Así, mientras el art. 6 de la Directiva establecía que los datos deberían ser tratados "de manera leal y lícita", el nuevo art. 5 del RGPD establece que éstos sean tratados "de manera lícita, leal y *transparente*" (cursiva añadida). De este modo, el Reglamento configura la transparencia como un principio básico de la protección de datos, junto con otros principios como el de calidad de los datos. En este sentido, cabe destacar que "los principios generales de protección de datos constituyen el contenido esencial del derecho a la

Aproximación al estudio de las decisiones automatizadas en el seno del Reglamento General Europeo de Protección de Datos a la luz de las tecnologías big data y de aprendizaje computacional

protección de datos, y que, a través de los mismos, se configura un sistema de tutela que garantiza una utilización más racional y razonable de los datos personales" (Puyol Montero, 2016, 136).

Se trata ésta de una de las manifestaciones del espíritu del Reglamento, por la cual se pretende empoderar a los sujetos a los que se refieren los datos personales y otorgarles una mayor capacidad de control sobre el uso que se haga de dichos datos. Otra de estas manifestaciones es la inclusión de la transparencia entre las exigencias que el Reglamento impone a los responsables y encargados del tratamiento de los datos personales en lo relativo a la información que deberá facilitar al interesado (arts. 13 y 14 RGPD).

Podríamos diferenciar en primer lugar un concepto formal de transparencia, referido a la existencia del principio de transparencia (art. 5), así como a la forma de atenderlo (art. 12 y considerandos 39, 58 y 60). En este sentido, en términos sucintos, el Reglamento establece que el principio de transparencia exige que la información dirigida al público o al interesado sea concisa, fácilmente accesible, y utilice un lenguaje sencillo, así como que se oriente a informar de la existencia del tratamiento y sus fines.

En segundo lugar, cabe hablar de un concepto material de transparencia en el Reglamento, que se refiere al contenido mismo de la información que deberá aportarse en relación al tratamiento de datos personales (arts. 13, 14 y 15). Recordemos que este contenido ha sido ampliado por el Reglamento en relación a la Directiva para incluir, entre otros, la obligación de informar al interesado sobre la existencia de decisiones automatizadas, la elaboración de perfiles (art. 13.2.f), art. 14.2.g) y art. 15.1.h)), o la obligación de proporcionar al interesado toda la información pertinente en los casos en los que el responsable del tratamiento "proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron" (art. 13.3 y art. 14.4). Se trata de disposiciones básicas en la sociedad de la información, y concretamente, en entornos de utilización de tecnologías big data que se basan precisamente en la automatización de los procesos a través de un uso intensivo de algoritmos, así como en la dedicación de los datos personales a fines secundarios, diferentes de la finalidad para la que fueron obtenidos en un primer momento.

A pesar de estas previsiones, pudiera parecer que los ciudadanos nos hacemos cada vez más transparentes para aquellos responsables y encargados que recogen y procesan datos personales, al tiempo que las técnicas que se utilizan en dichos tratamientos parecen ser cada vez más oscuras y complejas. Esta idea ya ha sido de hecho recogida por parte de la doctrina (sirvase como ejemplo Moerel y Prins, 2016).

En relación con ello, está siendo ampliamente debatida (entre otros, Veale y Edwards, 2017; Wachter et al, 2016; Hildebrandt, 2016) la existencia o no de un derecho a recibir

una explicación de las decisiones individuales automatizadas a las que se refiere el art. 22 RGPD en relación con el considerando 71, y a las que volveremos a centrarnos más adelante.

III. TRANSPARENCIA Y DECISIONES AUTOMATIZADAS EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

La regulación de las decisiones automatizadas no es nueva en la ordenación de la protección de los datos personales, sino que ya se encontraba en la Directiva de 1995, cuyo art. 15 reconocía el derecho de los individuos a no ser sometidos a decisiones basadas únicamente en un tratamiento automatizado que tuvieran efectos jurídicos sobre estos o les afectase de manera significativa. No obstante, se trataba de una disposición poco conocida y utilizada. Este hecho ha cambiado desde la incorporación de este derecho en el nuevo art. 22 del RGPD, que ha despertado un gran interés en la doctrina debido a los avances de las tecnologías big data, el aprendizaje computacional o la inteligencia artificial, y cuya interpretación en relación con los artículos 13, 14, 15 y el considerando 71 no es uniforme. En las páginas siguientes realizaremos una aproximación a estos conceptos y su interpretación.

A. La información y el derecho de acceso del interesado (artículos 13, 14 y 15 RGPD)

Los artículos 13, 14 y 15, que versan sobre el derecho de los sujetos a la información y acceso, establecen por primera vez que se informe del hecho de la existencia de mecanismos de decisión automatizada en el momento de la recogida de los datos, así como de las posibles consecuencias de dicho tratamiento. En lo referente a este extremo, la redacción en los tres artículos (arts. 13.2 f), 14.2 g) y 15.1 h) del RGPD) es idéntica y establece que debe facilitarse al interesado la información siguiente:

"(...) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado".

No obstante, en contextos de uso de tecnologías complejas como big data o algoritmos de aprendizaje autónomo se torna muy complicado, incluso para el responsable del tratamiento, prever los efectos de dicho tratamiento. Asimismo, para un sujeto medio, una explicación técnica y detallada de la lógica o funcionamiento del algoritmo perdería sentido, ya que sería incomprensible. En este caso, haciendo uso del principio del lenguaje sencillo sin tecnicismos, cabe pensar que el requisito de información en relación con el principio de transparencia podría cumplirse de manera más efectiva dando una información genérica, más fácilmente comprensible para el usuario medio (Kuner et al, 2017, 2). Esta interpretación parte de la base de que aquella información

Aproximación al estudio de las decisiones automatizadas en el seno del Reglamento General Europeo de Protección de Datos a la luz de las tecnologías big data y de aprendizaje computacional

presentada de forma compleja, con excesivos tecnicismos y en textos largos no cumple con el principio de transparencia.

Sin embargo, un nivel de información genérico podría no ser suficiente para un usuario con mayor conocimiento técnico que el usuario medio, y con una percepción mayor de su privacidad. Por ello, podríamos considerar que dicha información debería poder ser ampliada, a petición de los interesados, a través de un medio gratuito (por ejemplo, por email), en términos similares a los medios que el RGPD establece para ejercer los demás derechos.

Antes de continuar, corresponde detenernos a matizar las diferencias del deber de información en función del espacio temporal en el que este deber puede ser atendido, que será la base de nuestras conclusiones en lo que respecta a este apartado. En primer lugar, podríamos hablar de información proporcionada "*ex ante*", de forma previa a cualquier tipo de acción, es decir, el lapso de tiempo anterior a la creación de un modelo algorítmico y, por tanto, anterior también a la toma de cualquier decisión automatizada sobre una persona concreta. En segundo lugar, podríamos hablar de información "*ex post*", que se refiere a aquella proporcionada tras la modelación del algoritmo, la ingesta de los datos de una persona específica y la toma de una decisión automatizada sobre dicha persona o, en otros términos, la explicación de una decisión particular.

Pues bien, parece que los artículos 13, 14 y 15, indicados anteriormente, se refieren al hecho de proporcionar información *ex ante* sobre el funcionamiento del algoritmo, y no a la información *ex post* sobre una decisión automatizada concreta, interpretación que ha apoyado el GT29 en su borrador de dictamen sobre decisiones automatizadas individuales y elaboración de perfiles⁴.

Con todo, parece relevante que el documento del GT29 únicamente realice tal apreciación en la sección reservada a los comentarios al art. 15 RGPD (que regula el derecho de acceso), y no en la que se refiere a los arts. 13 y 14 (información que debe proporcionarse a los interesados), a pesar de que, como ya se ha mencionado, la redacción de estos artículos es la misma en lo que respecta a la información sobre decisiones automatizadas.

Tras estas reflexiones, cabe preguntarse, qué debe entenderse por información significativa sobre la lógica aplicada. Algunos autores (Veale y Edwards, 2017, 4), señalan que esto comprende: (i) información de partida proporcionada por el interesado, (ii) información relevante aportada por terceras partes, tales como el historial crediticio, y, por último, (iii) información pública relevante utilizada en la decisión, tales como registros públicos de fraudulencia.

⁴ Grupo de Trabajo del Artículo 29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, de 3 de octubre de 2017, p.24.

Esta definición, no obstante, sigue aduciendo ciertas limitaciones, en tanto se refiere a información "relevante", cuya categorización requiere de criterios subjetivos que serán analizados por el responsable que debe proporcionar la información, quien, además, puede tener incentivos para perpetuar una situación de no transparencia. En mi opinión, el deber de información debería entenderse en un sentido amplio de la palabra, incluyendo información concreta sobre los datos utilizados cuando éstos hayan sido aportados por el interesado o provengan de registros públicos, y principalmente cuando se hayan obtenido de terceras partes. Asimismo, la definición de la "lógica" del algoritmo debe incluir aspectos genéricos sobre el modelo o las variables a las que más peso se les otorga.

Por otro lado, hay que recordar que la información de los arts. 13 y 14 debe aportarse en el momento de la recogida de los datos o, en su caso, antes del tratamiento de los datos para un fin diferente al que motivó la recogida. Ello excluye la posibilidad de informar, siquiera en términos genéricos, sobre aquellos datos nuevos obtenidos por el responsable mediante inferencia estadística, esto es, fruto de insertar el conjunto de información de una persona determinada en los parámetros de un algoritmo prediseñado para observar posibles correlaciones y extraer nuevos conocimientos sobre el individuo.

Esta actividad crea un momento intermedio entre lo que hemos considerado *ex ante* (intervalo anterior a la utilización de sistemas algorítmicos y previo a la toma de decisiones automatizadas), y lo que hemos considerado *ex post* (tiempo posterior a la toma de decisiones automatizadas sobre una persona determinada). Éste es el momento en el que el responsable tiene el máximo de información sobre el sujeto, pero aún no se han producido acciones que conduzcan a consecuencias para dicho sujeto. Sería este el instante perfecto para informar, con el mayor grado de transparencia y conocimiento, al individuo sobre la información disponible, el funcionamiento del sistema algorítmico y las consecuencias previsibles.

El Reglamento reconoce, aunque sea implícitamente, la existencia de este momento con la mera existencia del art. 15 (derecho de acceso). En efecto, el derecho de acceso se configura como la oportunidad de ser informado, a petición del interesado, sobre lo relativo al tratamiento de datos personales en cualquier instante posterior a la recogida de los datos, que puede ser previo o posterior a la toma de decisiones, automatizadas o no, sobre el sujeto.

Esencialmente, la toma de decisiones automatizadas, tal y como se ha configurado en el art. 22 RGPD, se fundamenta en el consentimiento explícito, en un contrato del que el interesado es parte o en una norma legal, así como en el principio de transparencia de la información a los sujetos. Esto podría hacer pensar que es innecesario un derecho de acceso, puesto que no es más que una nueva oportunidad del interesado

Aproximación al estudio de las decisiones automatizadas en el seno del Reglamento General Europeo de Protección de Datos a la luz de las tecnologías big data y de aprendizaje computacional

de solicitar información que podría recibir en virtud de otros artículos del Reglamento. Sin embargo, el derecho de acceso se configura, en palabras de Aparicio (2013, 295) como una cautela para la "prevención de la acumulación de datos y las desviaciones de finalidad, puesto que (...) el principal riesgo que existe en el tratamiento de datos de carácter personal es la acumulación de información que puede arrojar, como precipitado, un retrato de la personalidad del individuo, el perfil personal". Estas palabras adquieren aún más relevancia en la sociedad de la información y, concretamente, en entornos big data, donde la toma de decisiones automatizadas y las prácticas de creación de perfiles se multiplican. Por ello, el derecho de acceso tiene como finalidad que el sujeto conozca la información referente a él que está siendo objeto de tratamiento, así como las circunstancias que lo rodean.

En conclusión, parece que el ejercicio de un derecho de acceso es la oportunidad perfecta para imponer al responsable del tratamiento la obligación de aportar información con el máximo nivel de transparencia, incluyendo de este modo conocimientos no disponibles en momentos anteriores, tales como aquellos datos obtenidos por medio de inferencia estadística que serán parte de los modelos algorítmicos y podrán influenciar el sentido de una decisión automatizada que cause efectos significativos al sujeto. Esto supondría, en la práctica, interpretar en un sentido más amplio el texto del art. 15.1 h) (derecho de acceso) que aquél de los arts. 13.2 f), 14.2 g) (información), a pesar de tener todos ellos una redacción idéntica, todo ello en atención al momento en el que se aplica cada disposición.

En este sentido, cabe señalar que el mencionado borrador de Dictamen del GT29 sobre decisiones automatizadas individuales y elaboración de perfiles parte de una premisa contraria a la aquí expuesta, siendo la conclusión por tanto también diferente. En efecto, el Grupo de Trabajo señala⁵ expresamente que el art. 15 otorga un derecho a los interesados a recibir la misma información sobre decisiones individuales automatizadas idéntico a aquél de los artículos 13.2 f), 14.2 g), y señala que, de hecho, cuando un individuo ejerce su derecho de acceso, ya debería haber recibido del responsable esta información en aplicación de los arts. 13 y 14. Únicamente bajo esta interpretación se entiende la conclusión de que el alcance de esta obligación de informar sobre la "lógica aplicada" se refiere únicamente a una información simple y general sobre el fundamento del sistema sin necesidad de intentar proporcionar una explicación compleja sobre los algoritmos utilizados.

B. El derecho a no ser objeto de decisiones automatizadas (artículo 22 y considerando 71 RGPD)

Artículo 22. Decisiones individuales automatizadas, incluida la elaboración de perfiles

⁵ Grupo de Trabajo del Artículo 29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, de 3 de octubre de 2017, p.15.

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.
2. El apartado 1 no se aplicará si la decisión:
 - a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
 - b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
 - c) se basa en el consentimiento explícito del interesado.
3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.
4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Considerando 71

(71) El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar. (...) En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión. Tal medida no debe afectar a un menor.

El artículo 22 del Reglamento dispone que los sujetos tienen derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, si ésta produce efectos jurídicos sobre los individuos o les afecta significativamente. Este precepto se exceptúa en caso de que la toma de este tipo de decisiones automatizadas sea necesaria para la ejecución de un contrato en el que el interesado sea parte, que así lo dispongan las leyes o que exista consentimiento explícito del interesado. En el primer y tercer caso deberán tenerse en cuenta ciertas garantías en la toma de decisiones automatizadas, que incluirán, como mínimo, las siguientes: el derecho a obtener intervención humana, derecho del interesado a expresar su punto de vista y derecho a impugnar la decisión. Por último, dichas deci-

Aproximación al estudio de las decisiones automatizadas en el seno del Reglamento General Europeo de Protección de Datos a la luz de las tecnologías big data y de aprendizaje computacional

siones únicamente podrán basarse en datos especialmente sensibles (definidos en el art. 9) cuando exista consentimiento explícito o interés vital del interesado y, del mismo modo, deberán estar sujetas a garantías adecuadas.

Esta definición ha dado lugar a diversos esfuerzos interpretativos pues, por un lado, adolece de términos necesarios de concreción y, por otro lado, las garantías descritas han dado lugar a una discusión en torno a la posible existencia o no de un derecho a recibir una explicación ex post sobre una determinada decisión automatizada; explicación que, tal y como ha sido argumentado, no cabe bajo el amparo de los artículos 13, 14 y 15.

i. Decisiones tomadas únicamente a través de medios automatizados

En primer lugar, la cuestión en torno a cuándo se considera que una decisión ha sido tomada *únicamente* a través de medios automatizados resulta de enorme importancia. El estado de la técnica hace que las decisiones que en la actualidad se toman sin ningún tipo de intervención humana aún no constituyan una mayoría, pero sin duda cada vez se trata de casos más frecuentes y en los próximos años irán aumentando.

Para la correcta efectividad de esta disposición, algunos autores (Veale y Edwards, 2017, 5) o el propio GT29 defienden que no se tomen por correctas aquellas actuaciones humanas que carecen de fundamento real, es decir, que de facto se destinen meramente a aprobar las decisiones automatizadas previamente tomadas por un modelo algorítmico sin realizar una revisión y valoración real del caso. Para ello, el GT29 propone algunos parámetros para poder comprobar este escenario, concretamente, analizar las veces que la persona se desvía de la recomendación que realiza el sistema o la concesión de autoridad real para modificar dichas decisiones.

Sin embargo, estos requisitos tampoco son sencillos de cumplir. Por un lado, debido a la creciente complejidad de los sistemas, acrecentada por las técnicas de aprendizaje computacional⁶ que provocan que los motivos que han llevado al modelo algorítmico a tomar o sugerir una determinada decisión sean cada vez más difíciles de comprender para un ser humano. Por otro lado, debido a la existencia de un mercado creciente de algoritmos en el que determinadas entidades crean modelos de negocio consistentes en la prestación de servicios de creación de algoritmos, que son por tanto diseñados y entrenados por terceros, diferentes de los responsables sobre los que recae el deber de informar acerca del funcionamiento de los mismos. Así, la persona que debe revisar las conclusiones del sistema automatizado no conoce el funcionamiento del algoritmo ni los motivos que le llevaron a una decisión concreta.

⁶ Debemos diferenciar aquellos sistemas que únicamente siguen pautas concretas para ejecutar de forma automatizada tareas claramente definidas, de aquellos otros sistemas que son capaces de reconfigurar sus propios comportamientos para mejorar automáticamente su rendimiento de forma dinámica y adaptativa, entre los que se encuentran las tecnologías de aprendizaje computacional o machine learning (Hildebrandt, 2016, 2, 4). Estos últimos provocan, por su propio funcionamiento autónomo, mayores problemas de comprensión para un ser humano, que redundan en la dificultad de intervenir y modificar la decisión.

ii. Decisiones que producen efectos jurídicos o afectan significativamente de forma similar

En segundo lugar, el artículo 22 es de aplicación cuando la decisión produce efectos jurídicos sobre los individuos o les afecta *significativamente* de modo similar. Ciertos escenarios parecen fácilmente interpretables en cuando a la importancia o significatividad de los efectos sobre los sujetos, tales como la concesión o denegación de un crédito tras un análisis y decisión automatizados. Otros supuestos, serán claramente no significativos, como la utilización de un perfil para el envío de publicidad personalizada (Veale y Edwards, 2017, 6).

Sin embargo, existen áreas grises de más difícil concreción. Así, por ejemplo, si en lugar de determinar la denegación de un crédito, la consecuencia del uso de un modelo totalmente automatizado es la concesión de dicho crédito con un determinado tipo de interés, que pudiera ser tan solo ligeramente superior al interés que se hubiera obtenido de otro modo, ¿es dicho efecto significativo como para provocar la aplicación del artículo 22? En tal caso, ¿de qué información dispone el interesado para argumentar que dicha decisión le ha causado un efecto significativo que le habilita a ejercer sus derechos o poner en marcha las garantías previstas en este artículo? Esta capacidad de poder conocer y argumentar detalles de mayor sutileza por parte de los interesados puede ser relevante, máxime cuando el responsable goza de información más completa, que podrá utilizar de forma partidaria para argumentar la baja significatividad de las consecuencias de dicha decisión.

Así, la asimetría de información (que, recordemos, puede verse acrecentada en función de cómo se interpreten los artículos 13, 14 y 15 que habilitan al sujeto a recibir información) puede resultar un claro perjuicio para el sujeto cuando esta circunstancia provoca la no aplicación siquiera de las garantías que prevé el art. 22, que podrían llevar, en última instancia, a la impugnación de la decisión.

iii. Las garantías para salvaguardar los derechos y libertades de los interesados en relación con la toma de decisiones automatizadas

En tercer lugar, también conviene realizar ciertas precisiones sobre las garantías que establece el art. 22 para el caso de que la decisión automatizada se haya tomado sobre la base de la necesidad para la ejecución de un contrato o el consentimiento explícito. La primera garantía que menciona el artículo es el derecho a obtener intervención humana. Para que sea efectiva, no obstante, es imprescindible la capacidad de la persona de comprender la decisión tomada por el sistema, así como para modificarla (Hildebrandt, 2016, 3). Sistemas sofisticados de modelado de datos como los *random forest* o aquellos desarrollados mediante técnicas de *deep learning* suponen una dificultad aún mayor por la complejidad de las interacciones que realiza el algoritmo, así

Aproximación al estudio de las decisiones automatizadas en el seno del Reglamento General Europeo de Protección de Datos a la luz de las tecnologías big data y de aprendizaje computacional

como el hecho de que el resultado final deviene de un procedimiento de agregación e interacción de diversos modelos (Goodman y Flaxman, 2016, 6-7).

Además, es posible que una persona no sea capaz de realizar una revisión profunda del procedimiento de decisión automatizada si dicho proceso incluye datos o algoritmos de terceras partes o procesos opacos. Es lo que en la doctrina se ha llegado a definir como cajas negras (Moerel y Prins (2016), Kuner et al (2017, 1-2), Pasquale (2015, 6), Diakopoulos (2014, 14), Hildebrandt (2016, 4)) o espejos de un solo sentido (Pasquale, 2015, 9). Ello implica que los modelos sean difíciles de comprender, incluso para sus creadores, de modo que resulta enormemente complicado dar una explicación sobre los motivos que han llevado a un algoritmo a tomar una determinada decisión e intervenir sobre ella.

La efectividad, por tanto, de dicha garantía afecta de manera directa al resto de las expresadas en el art. 22. Es fácilmente deducible la incertidumbre que genera pues la posibilidad de la aplicar las garantías relativas al derecho del interesado a expresar su punto de vista o su capacidad para impugnar la decisión.

En palabras de un científico de datos de la Universidad Politécnica de Madrid⁷, "es necesario elegir entre interpretabilidad y potencia predictiva. Los sistemas con más capacidad de predicción serán normalmente más difíciles de comprender y viceversa. En todo caso, no se puede tratar el aprendizaje computacional como un oráculo capaz de predecir con certeza una realidad futura".

Por último, un factor de enorme trascendencia en la determinación del alcance de las garantías de los individuos es la existencia o no de un derecho a recibir una explicación ex post acerca de una decisión automatizada concreta. En efecto, el considerando 71 del Reglamento también realiza una mención de las garantías que deben existir en relación con las decisiones automatizadas, indicando que deben incluir "la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a *recibir una explicación de la decisión tomada* después de tal evaluación y a impugnar la decisión" (cursiva añadida).

Es decir, el considerando añade a la lista de garantías el derecho a recibir una explicación de una decisión específica una vez esta se ha producido, lo que otorgaría una opción de recibir una información más amplia y específica que aquella prevista en los arts. 13-15, que recordemos, permite obtener "información significativa sobre la lógica aplicada". Sin embargo, esta disposición del considerando 71 no se ha trasladado a la redacción final del artículo 22 en lo que parece una omisión consciente por parte del legislador a tenor de las siguientes observaciones.

⁷ Conversaciones previas mantenidas en relación con este trabajo en noviembre de 2017

En primer lugar, recordemos el carácter no vinculante de los considerandos, cuya función se restringe a servir de guía a la interpretación del articulado de la norma. En segundo lugar, existen diferencias entre el texto final del Reglamento y versiones previas que sí incluían expresamente el derecho a obtener una explicación sobre la decisión alcanzada. De este modo, la exclusión de esta garantía del artículo 22 en la versión aprobada del Reglamento parece un acto consciente y reflexivo de no atribuir un carácter de derecho imponible a dicha garantía (Wachter et al, 2016). De este modo, una interpretación sistemática de la norma parece llevar a la conclusión de que el derecho de los interesados a recibir una explicación pormenorizada sobre una decisión específica tomada de forma automatizada no existe en la redacción del Reglamento.

No obstante, el Reglamento no excluye la posibilidad de poder configurar dicho derecho en un momento posterior, bien por parte de los Estados miembros, bien por parte de la jurisprudencia. Ello se desprende de la propia redacción del art. 22, que señala que las garantías en él contenidas son de mero carácter mínimo, dejando por lo tanto espacio para su progresivo crecimiento a tenor de las nuevas realidades socio-tecnológicas.

iv. La naturaleza del artículo 22 RGPD

La redacción del artículo 22 parece configurar sus disposiciones como un derecho que el individuo puede decidir ejercitar y hacer efectivo, pero no parece establecerse como una prohibición dirigida al responsable o encargado del tratamiento de abstenerse de llevar a cabo estas prácticas de forma previa.

La primera consecuencia que se extrae de ello es el hecho de que esta provisión solo podrá ejercitarse previa petición por parte del interesado. En la práctica, ello permitiría a los responsables del tratamiento llevar a cabo procesos de decisiones automatizadas sin cumplir con los requisitos del art. 22, y únicamente tras un esfuerzo por parte de los interesados por ejercitar su derecho, el responsable debería demostrar que se cumplen las condiciones de la norma. De este modo, esta interpretación favorece en gran medida la posición de los responsables del tratamiento. Por el contrario, la interpretación del art. 22 como una prohibición expresa aportaría una protección más reforzada para los intereses de los sujetos.

En este sentido, el art. 22 adquiriría una configuración similar al derecho de oposición. Es decir, el responsable puede iniciar tratamientos que culminen con decisiones automatizadas, y deberá abstenerse de ello una vez que el individuo comunique su negativa. Esto provoca que sea el responsable quien valore si se cumplen las condiciones que permiten ejercitar el derecho del art. 22, y decida si debe ser atendido o no. En consecuencia, ello propicia que el responsable tenga incentivos para dificultar el ejercicio de este derecho, así como para no ser transparente en lo que se refiere a

Aproximación al estudio de las decisiones automatizadas en el seno del Reglamento General Europeo de Protección de Datos a la luz de las tecnologías big data y de aprendizaje computacional

la información sobre la existencia misma de las decisiones automatizadas o la lógica aplicada (arts. 13, 14 y 15).

IV. CONCLUSIONES

La literalidad de la norma parece dar mucha importancia a la transparencia y a la protección de los sujetos en relación con la toma de decisiones automatizadas. Sin embargo, la gran cantidad de conceptos indeterminados permite encajar interpretaciones con diversos grados de flexibilidad o restricción que en última instancia determinarán la amplitud de los derechos de los interesados y su capacidad para conocer la existencia de decisiones automatizadas, el funcionamiento de los sistemas que las toman y las garantías que pueden ejercitar para solicitar una revisión o la oposición a este tipo de decisiones.

Una posible vía de acción ante esta situación es la creación de unidades especializadas de auditores de algoritmos que verifiquen su funcionamiento y la calidad. En este esquema, resultaría de utilidad la realización tanto de auditorías obligatorias en aquellos sectores de actividad potencialmente más lesivos, como voluntarias y de oficio. Según este sistema, el objetivo final del proceso de auditoría consistiría en la obtención de una certificación de calidad de los algoritmos utilizados para cada proceso de tratamiento de datos personales, que dotase a dicho proceso de un valor competitivo en el mercado, así como de valor reputacional. Para ello, sería necesaria la creación de un sistema de estándares internacional que sirviera de base a los mecanismos de certificación. En este sentido, una posible futura vía de estudio comprendería la determinación de la idoneidad de orientar este sistema en función de los diferentes sectores de actividad o incluso de las técnicas de análisis de datos que utilicen. Por último, cabría cuestionarse la posibilidad de requerir autorización previa a la comercialización y utilización de aquellos algoritmos cuyo impacto sobre los derechos e intereses de los individuos pudieran ser más lesivos.

BIBLIOGRAFÍA

- Aparicio Salom, J. 2013. *Estudio sobre la protección de datos*. Navarra: Aranzadi Thomson Reuters.
- Butarelli, G. 2016. "The EU GDPR as a clarion call for a new global digital gold standard", *International Data Privacy Law*, Vol 6, 2: 77-78.
- Diakopoulos, N. 2014. "Algorithmic-Accountability: the investigation of Black Boxes". *Tow Center for Digital Journalism*.

- Goodman, B. y Flaxman, S. 2016. "European Union regulations on algorithmic decision-making and a "right to explanation"." arXiv preprint arXiv:1606.08813.
- Hildebrandt, M. 2016. "The new Imbroglia: living with machine learning algorithms", en Janssens, L. (ed), *The Art of Ethics in the Information Society. Mind you*, Amsterdam: Amsterdam University Press, 55-60.
- Hoffman, D.A. y Rimo, P.A. 2017. "It takes data to protect data". *SSRN Electronic Journal*, 2973280: 1-16.
- Kuner, C., Svantesson, D., Kate, F.H., Lynskey, O., Millard, C. 2017. "Machine learning with personal data: is data protection law smart enough to meet the challenge?", *International Data Privacy Law*, Vol 7, 1: 1-2.
- Moerel, L., y Prins, C. 2016. "Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of Big Data and the internet of things". *SSRN Electronic Journal*, 2784123: 1-98.
- Pasquale, F. 2015. *The black box society: The secret algorithms that control money and information*. Cambridge, Londres: Harvard University Press.
- Puyol Montero, J. 2016. "Los principios del derecho a la protección de datos", en Piñar Mañas, J.L, et al, *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*. Madrid: Reus, 135:150.
- Veale, M. y Edwards, L. 2017. "Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling", (borrador) *SSRN Electronic Journal*, 3071679: 1-12.
- Wachter, S., Mittelstadt, B. y Floridi, L. 2016. "Why a right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation". *International Data Privacy*, Vol 7, 2: 76-99.