SCORE AUTOMATIZADO EN LA CONCESIÓN DE CRÉDITO¹

Marta Guerrero Ovejas
Graduada en Derecho
Universitat de Barcelona

Resumen

El presente estudio parte del impacto que ha tenido la reciente sentencia del TJUE recaída en el asunto SCHUFA y relativa al uso de la IA para la evaluación de la solvencia crediticia. En el análisis se ha tenido presente el Reglamento de IA aprobado recientemente, así como la última reforma de la Directiva de crédito al consumo, operada en 2023 para determinar la dirección que está tomando la Unión Europea respecto del uso de la IA en materia de consumo. Teniendo todos estos elementos en cuenta, se han evaluado las cuestiones más problemáticas que se plantean en esta esfera y se apuntan los aciertos y los desafíos pendientes.

Palabras clave: RGPD, *score*, decisiones automatizadas, evaluación de la solvencia crediticia, *credit scoring*, protección de datos, consumidores, IA, Directiva de crédito al consumo, Reglamento de IA, asunto SCHUFA.

SCORE AUTOMATITZAT EN LA CONCESSIÓ DE CRÈDIT

Resum

El present estudi parteix de l'impacte que ha tingut la recent sentència del TJUE recaiguda en l'assumpte SCHUFA i relativa a l'ús de la IA per a l'avaluació de la solvència creditícia. En l'anàlisi s'ha tingut present el Reglament de IA aprovat recentment, així com l'última reforma de la Directiva de crèdit al consum, operada el 2023 per a determinar la direcció que està prenent la Unió Europea respecte de l'ús d'IA en matèria de consum. Tenint tots

1. Quería agradecer y dedicar este trabajo a mi tutora, la Dra. Esther Arroyo Amayuelas, que me ha acompañado en la elaboración de este trabajo y en esta última etapa en la universidad. Sus sabios consejos y su invitación a que intentara reflexionar de manera más crítica me han facilitado enormemente la realización de este proyecto y han hecho que el proceso de investigación haya sido fascinante. Especialmente, quería expresar mi gratitud por su apoyo, tiempo y disponibilidad y, sobre todo, por su confianza no solo en este trabajo, sino también en mi persona.

aquests elements en compte, s'han avaluat les qüestions més problemàtiques que es plantegen en aquesta esfera i s'assenyalen els encerts i els desafiaments pendents.

Paraules clau: RGPD, *score*, decisions automatitzades, avaluació de la solvència creditícia, *credit scoring*, protecció de dades, consumidors, IA, Directiva de crèdit al consum, Reglament d'IA, assumpte SCHUFA.

AUTOMATED CREDIT SCORING

Abstract

This paper builds on the impact of the recent CJEU ruling in the SCHUFA case regarding the use of AI in the creditworthiness assessment. In the analysis, the recently approved AI Regulation, as well as the latest reform of the Consumer Credit Directive in 2023 have been considered in order to determine the path that the European Union is following with regards to the use of AI in the consumer's realm. With all these elements in mind, it has been assessed the most problematic issues arising in this field, in addition to drawing attention to the successes and challenges ahead.

Keywords: GDPR, score, automated decisions, creditworthiness assessment, credit scoring, data protection, consumers, AI, Consumer Credit Directive, AI Act, SCHUFA case.

«AI is a tool. The choice about how it gets deployed is ours.»

OREN ETZIONI

1. INTRODUCCIÓN

El pasado 7 de diciembre de 2023 el Tribunal Superior de Justicia de la Unión Europea (en adelante, TJUE) se pronunció en una sentencia pionera relativa al uso de la inteligencia artificial en la concesión de créditos. El asunto SCHUFA ha sido el resultado de un uso cada vez más intensivo de las nuevas tecnologías en sectores como el bancario y ha puesto de manifiesto los problemas que se derivan de ello, por ejemplo en la protección de datos y del consumidor. Es por dicha razón que este tema ha resultado de interés como objeto de estudio para este trabajo.

En este sentido, los aspectos que se abordarán en esta investigación abarcarán las cuestiones que han preocupado a la doctrina y que han sido aclaradas, en mayor o menor medida, por el TJUE en el asunto SCHUFA. De esta manera, el marco espacio-temporal en el que quedará delimitado este trabajo será el europeo y abarcará una línea temporal que se inicia aproximadamente con la aplicación en 2018 del Reglamento general de protección de datos (en adelante, RGPD), cuyo artículo 22 es objeto de la cuestión prejudicial planteada.

Por consiguiente, el tema que se propone y sobre el que se ahondará en este estudio es determinar qué cuestiones ha solventado la Sentencia relativas al uso de la IA en la evaluación de la solvencia crediticia y de qué manera lo ha hecho. Asimismo, se analizará el impacto que la nueva reforma de la Directiva de crédito al consumo (DCC) y el recién aprobado Reglamento de IA van a tener en este sector.

La metodología y las fuentes empleadas para la realización de este trabajo consistirán en lo siguiente. Por un lado, se investigará acerca de los temas relevantes y de los problemas que se plantean en esta materia a partir de la doctrina académica existente. Asimismo, se consultará jurisprudencia de los diversos tribunales de los estados miembros que han tenido ocasión de resolver cuestiones similares relacionadas con la normativa europea mencionada. Por otro lado, se analizarán en profundidad los instrumentos normativos pertinentes, como son el RGPD, la DCC y el Reglamento de IA, entre otros, para determinar cuáles son sus aciertos y sus deficiencias para resolver conflictos como el que plantean el asunto SCHUFA y otros análogos. Además, también se han llevado a cabo entrevistas con dos bancos (uno de gran tamaño y otro menor) para determinar cuál es la situación actual en España respecto a la utilización de la IA para comprobar la solvencia de los clientes a la hora de concederles créditos.

El trabajo se divide principalmente en tres partes. La primera parte consiste en un marco teórico que introduce los conceptos más relevantes del tema, la normativa aplicable, así como la evaluación de la solvencia crediticia, sus fases y los riesgos que

comporta, como son la protección de datos, la discriminación y el determinismo tecnológico. Este apartado se cierra con las decisiones automatizadas que se adoptan en el seno de dicha evaluación crediticia y que engloban todos los riesgos mencionados previamente. En la segunda parte, a partir del asunto SCHUFA se tratan las cuestiones más problemáticas que plantean las decisiones automatizadas en la concesión de créditos, así como los problemas que han quedado sin resolver por parte del TJUE pero que son de especial importancia. Finalmente, se estudian con más profundidad las novedades legislativas que la Unión Europea (en adelante, UE) ha introducido recientemente y que abordan de frente la cuestión que nos atañe en este trabajo.

2. EL CRÉDITO RESPONSABLE Y LA EVALUACIÓN DE SOLVENCIA: LA PUNTA DEL ICEBERG

2.1. DE DÓNDE VENIMOS Y A DÓNDE VAMOS: CUESTIONES CONCEPTUALES Y MARCO NORMATIVO

A raíz de la crisis económica de 2007 se hizo patente un sobreendeudamiento de los consumidores y la necesidad de poner freno al crédito irresponsable.² Como resultado, la UE impuso a los prestamistas no solo la obligación de llevar a cabo una evaluación de la solvencia del consumidor antes de concluir el contrato, que ya existía como tal en la antigua Directiva 2008/48/CE relativa a los contratos de crédito al consumo, sino también la de conceder el crédito solo en caso de que aquella diera un resultado positivo. Es decir, cuando indicara que era probable que el consumidor iba a ser capaz de devolver el crédito. Dicha obligación fue impuesta primero por la Directiva 2014/17/UE en relación con los contratos de crédito para bienes inmuebles de uso residencial. No ha sido hasta fechas recientes que también se ha impuesto en los contratos de crédito al consumo en general, con la Directiva (UE) 2023/2225. De este modo, se intenta asegurar que se conceden créditos de forma responsable, teniendo en cuenta las circunstancias del consumidor y su capacidad de devolución del crédito.³

Sin embargo, mucho antes de que se exigiera llevar a cabo una evaluación de la solvencia, esta ya se realizaba por parte del prestamista. Estas evaluaciones habitualmente se centraban en el historial de crédito del prestatario y se limitaban a utilizar datos estrechamente relacionados con el préstamo que se solicitaba y con la situación

2. Noah VARDI, *Creditworthiness and «responsible credit»: A comparative study of EU and US law*, Leiden, Brill, 2022, p. 8.

3. Directiva (UE) 2023/2225 del Parlamento Europeo y del Consejo, de 18 de octubre de 2023, relativa a los contratos de crédito al consumo, [2023] DO L, considerando 54.

económica en su mínima expresión.⁴ Eran, por tanto, datos relativos a su salario y estabilidad laboral,⁵ por ejemplo.

No obstante, con el auge de la tecnología, las evaluaciones de solvencia han sufrido una profunda transformación. El uso cada vez más intensivo de los algoritmos y de la inteligencia artificial (en adelante, IA) y su creciente presencia en la actualidad han protagonizado este cambio que, con todo, trae consigo grandes desafíos⁶ que el legislador europeo ha intentado orillar estos últimos años y que solo el futuro dirá si será suficiente para contrarrestarlos.

La predominancia que tienen las nuevas tecnologías, Internet, las redes sociales etc. en nuestro día a día, favorecen que las personas, sin ser plenamente conscientes de ello, dejen una extensa estela de diversas categorías de datos personales que pueden ser fácilmente recogidos posteriormente. El RGPD define los datos personales en su artículo 4:

[...] toda información sobre una persona física [...] cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo [...] uno o varios elementos propios de la identidad física, [...] económica, cultural o social de dicha persona.⁷

Por tanto, al navegar por Internet y usar tecnología se generan datos que se relacionan directamente con la propia persona.

Pues bien, los avances tecnológicos han hecho posible la creación de sistemas informáticos que a través de algoritmos son capaces de procesar una ingente cantidad de datos que han sido recogidos con anterioridad. A través de ese procesamiento es posible de forma «muy precisa» predecir comportamientos de las personas, ya que a través de correlaciones entre sus datos se las encasilla en grupos determinados.⁸ Es decir, se las clasifica según el contenido de los datos que se tienen de ellas. Así, por

4. Klaus WIEDEMANN, *Automated processing of personal data for the evaluation of personality traits: legal and ethical issues*, Múnich, Max Planck Institute for Innovation and Competition, 2018, p. 9 (Max Planck Institute for Innovation and Competition Research Paper No. 18-04), disponible en línea en: <<https://dx.doi.org/10.2139/ssrn.3102933>> (consulta: marzo 2024).

5. Alba SORIANO ARNANZ, *Data protection for the prevention of algorithmic discrimination*, 1ª ed., Cizur Menor, Aranzadi, 2021, p. 48.

6. Manuel MEDINA GUERRERO, «El derecho a conocer los algoritmos utilizados en la toma de decisiones. Aproximación desde la perspectiva del derecho fundamental a la protección de datos personales», *Teoría y Realidad Constitucional*, núm. 49 (2022), p. 151 y 141.

7. 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, DOUE, núm. 119 (4 mayo 2014).

8. Alba SORIANO ARNANZ, «Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos», *Revista de Derecho Público: Teoría y Método*, núm. 3 (2021), p. 85.

ejemplo, según el barrio en el que se resida, no se concede el crédito o se concede en condiciones más gravosas porque se predice que no se devolverá, ya que otras personas con el mismo lugar de residencia no suelen devolverlos o tienen menos capacidad económica⁹ (aunque ello no implique necesariamente que no devuelvan el crédito o no lo vayan a hacer). Esto es, esencialmente, lo que el RGPD ha definido en su artículo 4.4 como «elaboración de perfiles».¹⁰ Resulta cuestionable, a nuestro entender, el nivel de precisión que realmente puedan tener estas correlaciones, por resultar extremadamente más complejas la realidad, las personas y las decisiones que pueden tomar, por ejemplo, respecto a donde deciden vivir. Ello también plantea graves problemas relacionados con la discriminación, que se abordarán más adelante en este trabajo.

La preocupación que subyace en estas cuestiones es el determinismo tecnológico, es decir, que la persona quede sometida a una decisión automatizada basada en datos¹¹ (que, además, pueden ser parciales, imprecisos e incluso incorrectos) que predeterminen aspectos significativos de su vida. En lo que nos atañe en este trabajo, supondría que la huella digital condicionara la posibilidad de obtener o no los recursos financieros necesarios para acceder a servicios que pueden resultar esenciales para la vida, como es la vivienda.¹²

Otra vertiente de este determinismo tecnológico es, precisamente, la perfilarción a la que se ha aludido anteriormente. Es sin duda problemático el hecho de que para la concesión de créditos se utilicen algoritmos, los cuales tienen una tendencia inherente a equiparar conductas pasadas con comportamientos futuros y a extraer conclusiones basadas también en personas con las que se comparten datos similares.¹³

En razón de lo expuesto, se puede concluir que un uso extensivo de los algoritmos que abarque sectores como el crediticio, puede tener un precio demasiado alto a pagar para nuestras democracias. En consecuencia, la UE ha desplegado una intensa actividad legislativa y ha promulgado diversos instrumentos normativos. Por un lado, encontramos unos con un alcance más general, como el RGPD, antes mencionado, y el Reglamento de IA, aprobado definitivamente por el Consejo el pasado 21 de mayo de 2024 y publicado recientemente en el *Diario Oficial de la Unión Europea* (DOUE). Por otro lado, tenemos la ya citada DCC, con un alcance más específico

9. Susana NAVAS NAVARRO, *Inteligencia artificial: Tecnología y derecho*, 1ª ed., Valencia, Tirant lo Blanch, 2017, p. 49-50.

10. «[...] toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos [...] [a la] situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.»

11. Manuel MEDINA GUERRERO, «El derecho a conocer los algoritmos utilizados», p. 141.

12. DCC, considerando 56.

13. Klaus WIEDEMANN, *Automated processing of personal data*, p. 9.

y que en su modificación más reciente ya ha tenido en cuenta, como bien indica su artículo 18.8, «el uso de procesamiento automatizado de datos personales».

Cabe mencionar la importancia que adquiere el hecho de que estos instrumentos normativos estén elaborados, en la medida de lo posible, de tal forma que permitan adaptarse al constante cambio y al rápido avance de la tecnología, para que no queden obsoletos al poco tiempo de ser aprobados. Como veremos, la dificultad de llegar a acuerdos entre los diferentes sectores afectados a la hora de aprobarlos y la presión que algunos de estos ejercen, pueden suponer cierta oscuridad en el significado y el alcance de algunos de sus preceptos de mayor relevancia y, a su vez, pueden mermar la efectividad y los objetivos de estas normas.

En definitiva, resulta interesante ver que en Europa no solo se ha venido exigiendo evaluar la solvencia crediticia, sino que también, y acertadamente, se están imponiendo límites a la utilización de los mecanismos que facilitan tal evaluación, de manera que se garantice su transparencia. El Reglamento de IA está encaminado en esa dirección. La clave es, sin duda, que el hecho de estar cumpliendo con una obligación no excluye hacerlo con unos límites y que el uso de la IA no necesariamente será la opción más satisfactoria si en el camino se generan más problemas que soluciones. El poder de los datos y la tecnología debe llevar inherentemente una correlativa responsabilidad por parte de quien los trata y se lucra con ellos.

2.2. FASES DE LA EVALUACIÓN CREDITICIA

Resulta pertinente dedicar unas líneas a exponer cómo se lleva a cabo la evaluación crediticia, para más adelante poder comprender los problemas que trae consigo el uso de la IA en este campo.

Como se ha mencionado antes, con la aparición de nuevas tecnologías el análisis de la solvencia por parte del prestamista fue sustituido por el *credit scoring*. Este sistema evalúa la solvencia a través de la atribución de una especie de puntuación (*score*) al prestatario que indica las probabilidades de cumplimiento. El *score* se genera a partir de la recolección de datos sobre el prestatario para luego introducirlos en un algoritmo que contiene una secuencia de instrucciones formada por diversas variables a las que se ha atribuido un peso concreto.¹⁴ Es decir, habrá datos que tendrán más relevancia que otros en el resultado final, en función del peso que se les haya atribuido.

14. Noelia COLLADO-RODRÍGUEZ, «La evaluación de la solvencia mediante el uso de sistemas de IA», *Revista CESCO de Derecho de Consumo*, núm. 46 (2023), p. 41 y 43.

2.2.1. Primera fase: la recogida de datos

La primera fase es la recopilación de información,¹⁵ es decir, los datos que alimentarán el algoritmo que luego generará el *score*. Estos datos suelen recopilarse a partir de las siguientes fuentes.

2.2.1.1. Datos pertinentes

En primer lugar, se tendrán en cuenta los ingresos y los gastos. Así lo prevé el artículo 18.3 DCC. Además, el considerando 55 precisa que son gastos aquellos «corrientes del consumidor y de su hogar». Esto, ya de inicio, resulta problemático. El hecho de que se tengan en cuenta los gastos no resulta muy acertado, ya que de ellos se pueden inferir datos e información sobre circunstancias que pueden colisionar con categorías de datos especialmente sensibles que el artículo 9 RGPD salvaguarda prohibiendo su tratamiento.

Así, en los gastos corrientes del consumidor se puede incluir, por ejemplo, medicamentos que revelen datos sobre la salud, que es una de estas categorías de datos protegida. Cabe precisar que, aunque se revelen, estos datos no se pueden utilizar. Sin embargo, esto no es una garantía total, pues ya se conocen e indirectamente pueden afectar de forma eventual la evaluación de solvencia. En resumen, permitir los gastos facilita las discriminaciones, por lo que habría sido mejor no considerarlos en un primer momento.

Por eso es fundamental determinar a partir del artículo 6 RGPD cuál es la base de legitimación para el tratamiento de datos. En el caso que ahora nos atañe, sería o bien que el interesado ha prestado su consentimiento, o bien que es necesario para satisfacer un interés legítimo del banco.

En segundo lugar, también puede incluirse información extraída de registros públicos y privados permitidos por el artículo 19 DCC. Un ejemplo de registro público en nuestro país sería la Central de Información de Riesgos del Banco de España (CIRBE), que indica los préstamos que una persona tiene con entidades bancarias y de crédito. Su cometido es «la supervisión bancaria y el seguimiento de riesgos sistémicos»,¹⁶ es decir, evitar el crédito irresponsable, el sobreendeudamiento y, consecuentemente, el posible riesgo de colapso del sistema bancario. Las bases de datos privadas,

15. Noelia COLLADO-RODRÍGUEZ, «La evaluación de la solvencia», p. 43.

16. M. Dolores MAS BADIA, *Sistemas privados de información crediticia: Nueva regulación entre la protección y el crédito responsable*, 1ª ed., Valencia, Tirant lo Blanch, 2021, p. 50.

gestionadas por entidades privadas, serían las denominadas *agencias de información crediticia*, como, por ejemplo, Equifax o SCHUFA.¹⁷

La función principal de todas estas bases de datos es proporcionar información a los prestamistas sobre la solvencia de las personas que pretenden contratar con ellos, de manera que se evite el sobreendeudamiento y el incumplimiento de las obligaciones crediticias.¹⁸ En el seno de estas bases de datos lo que realmente sucede es un intercambio de información, de manera que los concedentes de crédito no solo reciben información de estas bases de datos, sino que también la proporcionan, entablándose una «relación de reciprocidad».¹⁹ En el caso de la CIRBE, para las entidades de crédito es preceptiva tanto su consulta como proporcionar información sobre sus operaciones y los incumplimientos de sus clientes.²⁰ Asimismo, estos registros pueden contener información negativa, positiva o ambas. La CIRBE contiene una y otra; los registros privados pueden tener también ambas, pero lo más habitual es que sea exclusivamente negativa (ficheros de morosos). Estos últimos no contienen información positiva relativa al prestatario y se limitan a hacer referencia a las deudas no satisfechas, sin mencionar la causa que provocó el incumplimiento o si fue ajena a la voluntad del prestatario.²¹

Esto puede suponer información parcial o poco precisa sobre este, de manera que, a nuestro entender, la entidad concedente debería aproximarse a este tipo de registros con más cautela.

2.2.1.2. Datos no estructurados

Sin embargo, además de datos estrictamente relativos a la situación económica y financiera necesarios para evaluar la solvencia del prestatario y su adecuación al crédito solicitado, existen fuentes adicionales que son más problemáticas. La posibilidad de acceder a ellas ha sido facilitada por la digitalización y por el rastro de datos que dejamos a nuestro paso al navegar por Internet. Algunas agencias de información crediticia tienen en cuenta para generar sus *scores* este tipo de datos²² que comúnmente se denominan *non traditional data*.²³ Aquí se pueden incluir entre otros muchos, por

17. Respecto a la agencia de información crediticia SCHUFA, con fuerte presencia en Alemania, es la que intervino en el asunto SCHUFA, en el que más adelante nos detendremos.

18. M. Dolores MAS BADIA, *Sistemas privados de información crediticia*, p. 62.

19. M. Dolores MAS BADIA, *Sistemas privados de información crediticia*, p. 49.

20. Ley 5/2019, de 15 de marzo, reguladora de los contratos de crédito inmobiliario, artículo 12.1, ap. 2.

21. M. Dolores MAS BADIA, *Sistemas privados de información crediticia*, p. 53-54.

22. Klaus WIEDEMANN, *Automated processing of personal data*, p. 9-10.

23. Noelia COLLADO-RODRÍGUEZ, «La evaluación de la solvencia», p. 49.

ejemplo, el dispositivo desde donde se solicita el crédito,²⁴ lo rápido que se navega y se tarda en leer las condiciones del contrato de crédito (de tal manera que alguien que lo hace rápido se entiende que es poco fiable) e, incluso, la actividad en línea y los contactos en redes sociales, de los que se hace depender el *score*. Es decir, se juzga al prestatario en función de sus contactos en dichas plataformas; este es el caso del *Facebook patent on credit scoring*.²⁵

Es de este tipo de datos de donde surge la preocupación, ya que no reflejan la capacidad de devolución que tiene una persona pues no revelan su capacidad económica. Incluso pueden conducir a conceder el crédito a personas que no pueden devolverlo, por basarse en datos ajenos a su solvencia que incluso podrían haber manipulado los propios usuarios (*game the system*) y que supondría un incumplimiento por parte de las entidades de crédito de su obligación de conceder créditos responsablemente. Es por ello que es necesario hacer una distinción entre datos de contenido financiero y datos que plasman circunstancias de carácter más social y demográfico.²⁶

2.2.1.3. Datos prohibidos expresamente

En Europa se ha intentado frenar el procesamiento de este tipo de datos, aunque con menos fuerza de la que se debería. Como se ha mencionado en líneas anteriores, el artículo 9 RGPD sí que prohíbe algunos de estos datos: los especialmente sensibles y que favorecen especialmente la discriminación (salud, orientación sexual, raza, religión...). Sin embargo, los datos que no acaban de encajar en la enumeración que hace dicho precepto, ni siquiera de forma indirecta, como pueden ser los datos extraídos de la navegación por Internet o en las plataformas sociales, no quedan bajo el paraguas del artículo 9 RGPD y, consiguientemente, tampoco bajo sus exigencias más estrictas.

El considerando 18 del mismo Reglamento sí que los menciona brevemente en una redacción compleja y enrevesada que impide el tratamiento de datos «relacionados con tales actividades [actividad en las redes sociales y la actividad en línea]». El considerando 57 DCC también menciona que las redes sociales no se deben tener en cuenta para evaluar la solvencia, pero guarda silencio respecto de otros datos que pueden extraerse de la actividad en línea y que no son pertenecientes a las redes sociales. Todo ello, además del carácter no preceptivo de los considerandos, que, sin embargo, debe tenerse en cuenta a efectos interpretativos. Asimismo, el artículo 18.3 DCC es-

24. Noelia COLLADO-RODRÍGUEZ, «La evaluación de la solvencia», p. 49.

25. Klaus WIEDEMANN, *Automated processing of personal data*, p. 9, 10 y 25-27.

26. Diogo MORGADO REBELO y Filipa CAMPOS FERREIRA, «AI-based consumer's creditworthiness assessment: era of automation, future of scoring and the EU policymaking on automated decision-making», en Sónia MOREIRA (ed.), *E. tec yearbook: Industry 4.0: legal challenges*, Minho, Universidade do Minho Centro de Investigação em Justiça e Governação (JusGov), 2022, p. 90-91.

tablece que «las redes sociales no se considerarán una fuente externa» en el sentido de que no se considerarán una fuente pertinente y, por lo tanto, no se podrán utilizar para evaluar la solvencia. El artículo 19.5 DCC tampoco permite el procesamiento de datos obtenidos de redes sociales que puedan constar en bases de datos de las cuales los prestamistas obtienen información.

2.2.1.4. Datos cuya prohibición de uso es implícita

A pesar de todo, el RGPD cierra el círculo con dos principios previstos en su artículo 5, el principio de limitación de la finalidad y el de minimización, que permiten reconducir este tipo de datos a su ámbito de aplicación.²⁷ El primero impone la necesidad de que los datos se recojan con una finalidad concreta que, además, ha de ser legítima. Por tanto, por mucho que se recojan datos de la navegación en línea, estos no se podrán utilizar si no se ha previsto expresamente que se destinarán a la finalidad para la que realmente se están utilizando, de tal manera que no podrán ser utilizados para realizar un *credit scoring* si fueron recogidos con otro objetivo. En cuanto al segundo, responde más bien a un requisito cuantitativo, en el sentido de que solo podrán recogerse los que sean estrictamente necesarios para cumplir la finalidad establecida previamente. Este principio también es recogido expresamente por la DCC en su modificación reciente en los considerandos 30 y 55 y en el artículo 18.3, cuando hace referencia a «información pertinente y exacta» y relativa a circunstancias económicas «necesarias y proporcionadas» respecto del crédito. Por consiguiente, si no se puede establecer una conexión entre los datos personales recogidos y la capacidad de devolución del crédito, esos datos no se podrán procesar.

Por ende, algunos de estos datos alternativos tampoco podrán ser utilizados porque, a pesar de no estar contenidos en la prohibición de tratamiento del artículo 9 RGPD, el artículo 5 DCC impide su utilización. Consiguientemente, en principio los datos relativos a las redes sociales y la navegación en línea no se podrán utilizar para evaluar la solvencia crediticia.

2.2.1.5. La gobernanza de datos

El auge de la IA nos sitúa en un panorama totalmente distinto, con nuevos matices que hay que contemplar. Así, los sistemas que se utilizan para evaluar la solvencia crediticia son sistemas de IA que para funcionar se nutren de una inmensa cantidad de

27. Noelia COLLADO-RODRÍGUEZ, «La evaluación de la solvencia», p. 50.

datos²⁸ que se basan en el principio «all data is credit data».²⁹ Por tanto, en un futuro próximo (si no ha sucedido ya) en el que el uso de la IA sea ineludible, el RGPD y los principios de finalidad y minimización corren el riesgo de quedarse cortos por estar en contradicción con el propio funcionamiento de la IA.

Aun así, para garantizar que no se perpetúan discriminaciones a grupos concretos a partir de *non traditional data*, es fundamental que la información que se tenga en cuenta sea exclusivamente relativa a su capacidad de devolución. Por consiguiente, la clave no será cuantos más datos mejor, sino cuantos mejores datos mejor. Por *mejores datos* se entiende solo los necesarios y que, a su vez, sean precisos, veraces y se ajusten a la finalidad para la que han sido recogidos. Por ende, no solo es importante desbancar la creencia de que cuantas más categorías de datos se introduzcan mejor será la perfilación,³⁰ sino también optar por los modelos que, aunque utilicen menos datos, se ciñan a procesar circunstancias económico-financieras.³¹

El Reglamento de IA sigue esta misma lógica en su artículo 10, relativo a la gobernanza de datos, que persigue que los datos utilizados para entrenar el algoritmo sean de calidad; es decir, sean adecuados a los resultados que se quieren obtener, no tengan sesgos, sean completos y permitan localizar sus errores o deficiencias. Por tanto, si se alimenta el sistema con datos correctos y de calidad, sus resultados también lo serán.

2.2.2. Segunda y tercera fases: el procesamiento de datos y la generación del «score»

En la segunda fase tiene lugar el procesamiento de la información y de los datos recogidos previamente. A partir de este procesamiento se generará un *score* que puede basarse en la elaboración previa de un perfil. Es decir, en función del grupo en el que se inserte a la persona a partir de sus datos, el modelo predecirá cuál es la probabilidad de que devuelva el crédito y, por tanto, cuál es su *score*.

28. Boris P. PAAL, «Artificial intelligence as a challenge for data protection law», en Silja VOENEKY *et al.* (ed.), *The Cambridge handbook of responsible artificial intelligence*, Cambridge, Cambridge University Press, 2022, p. 295 y 296.

29. Zofia BEDNARZ y Linda PRZHEDETSKY, «AI opacity in the financial industry and how to break it», en Zofia BEDNARZ y Monika ZALNIERIUTE (ed.), *Money, power, and AI*, 1ª ed., Cambridge, Cambridge University Press, 2023, p. 79.

30. Diogo MORGADO REBELO y Filipa CAMPOS FERREIRA, «AI-based consumer's creditworthiness assessment», p. 80.

31. Sergio GENOVESI *et al.*, «Standardizing fairness-evaluation procedures: interdisciplinary insights on machine learning algorithms in creditworthiness assessments for small personal loans», *AI and Ethics*, núm. 10 (2023), <<https://doi.org/10.1007/s43681-023-00291-8>> (consulta: febrero 2024).

Con el perfilado, lo que lleva a cabo la máquina es «la identificación de patrones de comportamiento»³² que llevarán a clasificar a la persona en un grupo estadístico en el que concurren personas con los mismos atributos. De esta manera, se entiende que las personas que comparten características similares actuarán también de manera similar,³³ por lo que si se comparte atributos con personas que han incumplido con sus obligaciones crediticias, se entiende que hay un riesgo alto de que esa persona también deje impagos, ya que pertenecen al mismo grupo. El problema de la elaboración de perfiles es que se basa en probabilidades y en comportamientos ajenos.³⁴ Lo más significativo es que la relación de causalidad entre compartir atributos similares con un grupo y no cumplir con las obligaciones crediticias, no necesariamente encaja con la realidad individual y que se corre el riesgo de que estas analogías lleguen a ser arbitrarias, algo que en ningún caso debería suceder a la hora de conceder un crédito.

En la tercera fase, como ya se ha adelantado, se obtendrá la probabilidad de devolución del crédito que tiene el consumidor (*score*), que será más o menos determinante para conceder o no el crédito.³⁵ Ello, como se verá, será un factor significativo que ha sido objeto de una cuestión prejudicial en el TJUE.

2.3. DIME DÓNDE VIVES Y TE DIRÉ QUÉ SCORING TIENES Y OTROS PROBLEMAS DE LA DISCRIMINACIÓN ALGORÍTMICA

Mientras que la introducción de la IA y de los algoritmos en la evaluación crediticia pudo verse en un primer momento como la solución para acabar con la opacidad de las decisiones humanas³⁶ y la exclusión de ciertos grupos en la obtención de un crédito, lo cierto es que la aparente objetividad de los algoritmos no es más que supuesta. Es más, en ocasiones no ha hecho más que perpetuar la discriminación de determinados sectores sociales.³⁷

A pesar de que se entendiera que las personas eran capaces de acumular más prejuicios y estereotipos y convertirlos en decisiones sesgadas,³⁸ lo cierto es que los algoritmos y modelos de IA que se usan para evaluar la solvencia son creados también

32. Noelia COLLADO-RODRÍGUEZ, «La evaluación de la solvencia», p. 51.

33. Klaus WIEDEMANN, *Automated processing of personal data*, p. 8.

34. Klaus WIEDEMANN, *Automated processing of personal data*, p. 11.

35. Noelia COLLADO-RODRÍGUEZ, «La evaluación de la solvencia», p. 43.

36. Zofia BEDNARZ y Linda PRZHEDETSKY, «AI opacity in the financial industry», p. 91.

37. Antje von UNGERN-STERNBERG, «Discriminatory AI and the law», en Silja VOENEKY *et al.* (ed.), *The Cambridge handbook of responsible artificial intelligence*, Cambridge, Cambridge University Press, 2022, p. 252.

38. Alba SORIANO ARNAZ, *Data protection for the prevention of algorithmic discrimination*, p. 48.

por personas que repercuten en ellos dichos sesgos, prejuicios y estereotipos. Además, los datos con los que se entrena al modelo también pueden contener información parcial,³⁹ por lo que al final la discriminación subsiste y lo único que cambia es quién o qué la perpetúa.

La discriminación algorítmica no siempre implicará la denegación del crédito, sino que también puede suponer que dicho crédito se conceda pero con condiciones más perjudiciales para el consumidor,⁴⁰ como el aumento del tipo de interés, por ejemplo. Ello sigue suponiendo un perjuicio económico para el consumidor.

Lo más problemático de la utilización de modelos automatizados es, por un lado, la confianza ciega en la imparcialidad de los algoritmos y sus resultados, cuya consecuencia es que las discriminaciones que puedan derivarse pasen desapercibidas. A ello se suma que, a pesar de que se exige informar al consumidor de que sus datos van a ser tratados para la evaluación, puede que no alcance a entender las implicaciones que ello representa.⁴¹ Las consecuencias de la discriminación en el ámbito del crédito pueden ser muy graves para los intereses económicos del consumidor y, además, pueden anclarlo más en la exclusión social. Así también lo entiende el considerando 71 RGPD.

La discriminación puede tener lugar por diversas razones. Por ejemplo, porque a partir de los datos de esa persona que se han introducido el algoritmo la ha clasificado en un grupo ya predeterminado (*profiling*) que, además, es discriminado indirectamente al tener en cuenta factores aparentemente objetivos pero que son propios de ese grupo.⁴² Esto sucede porque comparte ciertos atributos (como el lugar de residencia) que en ocasiones están estrechamente vinculados, por ejemplo, con la raza (*redlining*), o porque se relaciona con personas pertenecientes a dicho grupo, por ejemplo, por sus redes sociales (*weblining*).⁴³ Como ya se ha mencionado, el uso de este tipo de datos está prohibido, lo que no excluye que los sistemas computacionales los procesen y generen un *score* a partir de ellos, especialmente si son modelos cuyos algoritmo y funcionamiento son de difícil o imposible acceso y comprensión, fenómeno conocido como *black box*. De todos modos, con el Reglamento de IA esto ya no será un problema porque no permite el uso de sistemas así.

Otra razón por la que los algoritmos pueden conducir fácilmente a la discriminación es cómo se configuran los modelos, es decir, qué valor se asigna a cada factor o variable.⁴⁴ Por ejemplo, las mujeres suelen tener *scores* más bajos a pesar de que normalmente su porcentaje de impago es menor que el de los hombres. Esto se debe

39. Alba SORIANO ARNAZ, «Decisiones automatizadas: problemas y soluciones jurídicas», p. 90.

40. Noelia COLLADO-RODRÍGUEZ, «La evaluación de la solvencia», p. 57.

41. Susana NAVAS NAVARRO, *Inteligencia artificial: Tecnología y derecho*, p. 50.

42. Noelia COLLADO-RODRÍGUEZ, «La evaluación de la solvencia», p. 57.

43. Susana NAVAS NAVARRO, *Inteligencia artificial: Tecnología y derecho*, p. 49-51.

44. Noelia COLLADO-RODRÍGUEZ, «La evaluación de la solvencia», p. 56.

a la brecha salarial, ya que al tener sueldos inferiores consumen más crédito y eso provoca un descenso significativo del *score*.⁴⁵ Otra posible razón es que se asocie al sueldo un peso mayor y se otorgue un valor insignificante a otras circunstancias económico-financieras —como, por ejemplo, que se tiene un endeudamiento menor (que también respecto a los hombres es inferior)—, lo que provocará que su *score* se vea perjudicado.⁴⁶ Precisamente por motivos como estos es necesaria la revisión humana, para poder detectar estas incongruencias.

También se da una especie de paradoja respecto de aquellas personas de las que apenas se tienen datos. Por un lado, que no se disponga de muchos datos, más allá de los estrictamente económicos, será beneficioso para la persona, pues se evitará que a través de datos alternativos pueda ser objeto de discriminación. Sin embargo, por otro lado, muchos sistemas de *credit scoring* funcionan a partir de *big data*, es decir, del procesamiento de grandes cantidades de datos. Ello puede significar que sean excluidas del crédito o que tengan condiciones más gravosas, precisamente, por carecer de información suficiente.⁴⁷ Además, estas situaciones suelen darse con personas en situación vulnerable y en riesgo de discriminación.⁴⁸

Sin embargo, hay autores que tienen una visión más optimista al respecto y muestran la otra cara de la moneda. Así, puede suceder también que personas sin historial crediticio resulten favorecidas en la concesión de un crédito al tenerse en cuenta otros tipos de datos, como los obtenidos de la navegación en línea.⁴⁹ Estos datos son los únicos de los que puede que se disponga y no necesariamente revelarán información negativa sobre ellas, por lo que les facilitarán el acceso a un crédito. Los ejemplos más recurrentes son los estudiantes y los refugiados.

No obstante, debido al riesgo que existe de que a través de la elaboración de perfiles y la automatización de las decisiones respecto a la concesión de créditos haya colectivos que queden excluidos del acceso al crédito, es importante que los datos que se introduzcan sean fieles a la realidad, veraces y completos. Por tanto, han de ser de calidad⁵⁰ para que el modelo pueda realizar un *score* justo y realista con la solvencia del individuo. Por ello, la Autoridad Bancaria Europea (en adelante, ABE; en inglés, European Banking Authority, EBA) establece, para el prestador que utiliza innovaciones tecnológicas, una serie de directrices que garantizan la prevención de sesgos y la no discriminación. Entre ellas encontramos la de asegurarse de la calidad de los datos que se introducen en el modelo, así como el seguimiento de la calidad de

45. Alba SORIANO ARNAZ, *Data protection for the prevention of algorithmic discrimination*, p. 49.

46. Noelia COLLADO-RODRÍGUEZ, «La evaluación de la solvencia», p. 57.

47. Zofia BEDNARZ y Linda PRZHEDETSKY, «AI opacity in the financial industry», p. 71.

48. Zofia BEDNARZ y Linda PRZHEDETSKY, «AI opacity in the financial industry», p. 71.

49. Federico FERRETTI, «Consumer access to capital in the age of fintech and big data: the limits of EU law», *Maastricht Journal of European and Comparative Law*, núm. 25 (2018), p. 486-487.

50. Sergio GENOVESI *et al.*, «Standardizing fairness-evaluation procedures», p. 4.

los resultados (*output*). La ABE también establece las medidas y los procedimientos para ello.⁵¹

Asimismo, otra manera de evitar la discriminación es mediante la transparencia. Tanto la Directiva de crédito inmobiliario como la DCC (art. 18.2 y 18.4, respectivamente) contienen obligaciones prácticamente idénticas con respecto a la transparencia del proceso de evaluación de la solvencia crediticia. Se exige al prestamista que establezca y documente cómo se llevará a cabo dicho proceso. Ambas obligaciones denotan el interés del legislador en que quede constancia de dichos procesos y se garantice que es un proceso justo y libre de discriminaciones, debido a la transcendencia que tiene para los intereses económicos de los consumidores.

2.4. DECISIONES AUTOMATIZADAS

Las cuestiones que se han expuesto en los epígrafes anteriores, vinculadas con la facilidad de obtener información muy diversa de las personas, la recogida de datos especialmente sensibles y el consecuente riesgo de discriminación que ello puede suponer en la concesión de un crédito, no son más que la parte visible de algo mucho más complejo y problemático: las decisiones automatizadas.

La introducción de medios automatizados en el proceso de evaluación de la solvencia crediticia no ha hecho más que agravar los problemas ya existentes de protección de datos. Ello es debido precisamente a que con los datos personales se elaboran perfiles a partir de los cuales se toman las decisiones automatizadas relativas a la concesión de un crédito. Por tanto, hoy en día parece que la preocupación ya no solo estriba en que de forma cada vez más recurrente se deleguen funciones a las máquinas, sino en que de forma acrítica y automática hagamos nuestras sus decisiones automatizadas.

A continuación se analizará qué se entiende por *decisiones automatizadas*, así como los derechos que amparan a las personas sometidas a ellas. Estas cuestiones han sido las que se han trasladado al TJUE en el asunto SCHUFA, que trata de dilucidar cuáles de las decisiones presentes en la evaluación de la solvencia para la concesión de un crédito son automatizadas a efectos del artículo 22 RGPD.

51. EUROPEAN BANKING AUTHORITY (EBA), *Directrices sobre concesión y seguimiento de préstamos*, París, European Banking Authority, 2020, párr. 53, 54 y 55.

2.4.1. *Intervención humana y los diversos grados de automatización*

2.4.1.1. La importancia de la intervención humana

La intervención humana está prevista en el artículo 22.3 RGPD y, como se verá más adelante, es a la vez un derecho y un elemento esencial de las decisiones automatizadas.⁵² Su importancia es trascendental por dos motivos conexos.

En primer lugar, la intervención humana evita o al menos pretende paliar la tendencia que las personas tienen a sobrestimar la precisión y la bondad de la tecnología. Es decir, existe una inclinación natural a dar mucho peso a los resultados que las máquinas nos proporcionan, sin intención de actuar de manera diferente⁵³ o de cuestionar su acierto. En parte, esto es un resultado natural del afán del ser humano de delegar cada vez más tareas a las máquinas, que, sin embargo, no debería implicar la claudicación de sus responsabilidades y una supervisión adecuada y significativa.⁵⁴ Con esto en mente, el legislador europeo, que desconfía de la supuesta imparcialidad y los posibles fallos de las máquinas, ha intentado que por medio de la intervención humana se soslayen los inconvenientes de la automatización.

En segundo lugar, con la intervención humana se intenta mitigar las consecuencias de la abdicación de responsabilidades de los seres humanos hacia las máquinas. Esto es, preservar la dignidad humana y evitar que una máquina cosifique a las personas,⁵⁵ definiéndolas a partir de sus datos⁵⁶ y determinando a lo que pueden o no acceder; en lo que ahora nos atañe, el acceso a una fuente de financiación como es la obtención de un crédito. La intervención humana es el equivalente a la capacidad de poder influir⁵⁷ y de que, por lo tanto, los algoritmos no predeterminen a las personas, sino al revés: que estas puedan intervenir en el proceso e impugnar sus resultados. Así también lo ha expresado el abogado general del TJUE en sus conclusiones para el asunto SCHUFA.⁵⁸

52. Guillermo LAZCOZ y Paul de HERT, «Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities», *Computer Law and Security Review*, núm. 50 (2023), p. 1 y 9.

53. Arno R. LODDER y Zachary COOPER, «Do algorithms need to be regulated?», en Andrej SAVIN y Jan TRZASKOWSKI (ed.), *Research handbook on EU Internet Law*, 2ª ed., Cheltenham, Edward Elgar Publishing Ltd., 2023, p. 89.

54. Guillermo LAZCOZ y Paul de HERT, «Humans in the GDPR», p. 2.

55. Alba SORIANO ARNAZ, *Data protection for the prevention of algorithmic discrimination*, p. 141.

56. Guillermo LAZCOZ y Paul de HERT, «Humans in the GDPR», p. 13.

57. Guillermo LAZCOZ y Paul de HERT, «Humans in the GDPR», p. 13.

58. Asunto C-634/2021, O. Q. contra Land Hessen con intervención de SCHUFA Holding AG [2023], conclusiones del abogado general Sr. Priit Pikamäe, ECLI:EU:C:2023:220, párr. 19.

2.4.1.2. Distinción conceptual: «human in and out of the loop»

Conviene hacer una distinción conceptual respecto a la intervención humana. Debemos entenderla, en primer lugar, como el derecho a obtener una intervención humana posterior, previsto expresamente en el artículo 22.3 RGPD como una de las garantías de protección que, como mínimo, se han de otorgar frente a una decisión automatizada. Y, en segundo lugar, como presupuesto para que no resulte aplicable el artículo 22 RGPD, ya que si concurre, la decisión no podrá considerarse exclusivamente automatizada. Estos conceptos son también denominados *human out of the loop* y *human in the loop*, respectivamente, y el primero tiene lugar después de la decisión automatizada y el segundo, durante la toma de la decisión.⁵⁹

La Sentencia no hace mención especial del derecho del artículo 22.3 RGPD, más allá de citarlo brevemente en los párrafos 54 y 66. En cambio, el abogado general del TJUE, en los párrafos 36 y 42 de sus conclusiones, sí que presta atención a la ausencia de intervención humana como requisito esencial para que el artículo 22 RGPD resulte aplicable, ya que ello será determinante para que una decisión pueda calificarse como «basada únicamente en el tratamiento automatizado».

En este sentido, el Reglamento de IA prevé en su artículo 14.1 precisamente la intervención humana, pues impone la obligación de que los sistemas de IA estén «dotados de una herramienta de interfaz humano-máquina», es decir, de una persona que pueda supervisar su funcionamiento. Un precepto así supone un avance, ya que la intervención humana tendrá lugar siempre que el sistema de IA sea de alto riesgo y cause perjuicios al interesado. Este es el caso de los sistemas de evaluación y calificación crediticia según el anexo III del citado RGPD, al que se remite su artículo 6. De esta manera, se ha superado la concepción de que solo los sistemas exclusivamente automatizados conllevan un riesgo grave. Precisamente, el artículo 86.1 del Reglamento de IA elimina la expresión «exclusivamente automatizado» y usa la de «decisiones tomadas individualmente», ignorando el grado de automatización.

Asimismo, se utiliza el concepto de *human over the loop* para referirse a aquellas situaciones en las que el algoritmo hace una sugerencia que la persona luego puede o no desdeñar.⁶⁰ En el caso de la concesión de créditos y a partir de las entrevistas que se han llevado a cabo en este trabajo con bancos y entidades de crédito,⁶¹ parece una práctica habitual utilizar una herramienta de IA que, con base en el *score* de los clientes, en su área personal en la *web* o *app* les ofrezca un crédito rápido con una cantidad y unas condiciones preestablecidas y que para obtenerlo solo baste con aceptar la acción señalada.

59. Guillermo LAZCOZ y Paul de HERT, «Humans in the GDPR», p. 2 y 9.

60. Arno R. LODDER y Zachary COOPER, «Do algorithms need to be regulated?», p. 90.

61. Véanse anexos I y II.

Estas prácticas pueden resultar problemáticas porque la cuantía y las condiciones se basan en el *score*, es decir, en una elaboración de perfil que puede haberse creado a partir de datos parciales o incorrectos. Por consiguiente, pueden estar concediendo un crédito a una persona que solo sea solvente aparentemente. De todos modos, a través de las entrevistas hemos conocido que en algunas entidades es una práctica habitual que el gestor encargado de la cuenta avise al cliente de que puede obtener el mismo crédito en unas condiciones más beneficiosas. Por tanto, hay una intervención humana posterior.

2.4.1.3. ¿Qué se entiende por *decisión basada únicamente en un tratamiento automatizado*?

Los términos en los que está redactado el artículo 22 RGPD parecen ser contundentes y taxativos respecto al grado de automatización necesario para que su prohibición resulte aplicable: basado «únicamente en el tratamiento automatizado». Por consiguiente, a pesar de que existen diversos grados de automatización, es decir, diversos momentos y formas en los que puede haber participación humana, parece que una interpretación restrictiva vendría a referirse a una ausencia total de esta.⁶² Ello, como se verá, resulta problemático, ya que no están protegidas de igual manera aquellas situaciones en las que, a pesar de existir intervención humana, las decisiones se han basado en parte en un tratamiento automatizado.

Parece entonces que cualquier intervención humana que se incluya debería precluir la aplicación del artículo 22 RGPD. Sin embargo, esta concepción ha sido rechazada por la doctrina, los tribunales y otros operadores jurídicos por lo sencillo que resultaría esquivar la prohibición que dicho precepto contiene⁶³ (así como sus garantías, en caso de permitirse excepcionalmente) introduciendo «un elemento humano [que] se comporte como una mera correa de transmisión».⁶⁴ Es decir, se podría evadir «inventándose una participación humana», como bien expresa el Grupo de Trabajo sobre Protección de Datos del Artículo 29 (en adelante, GTPD-29) en sus *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, de 2018.

62. Philipp HACKER y Jan-Hendrik PASSOTH, «Varieties of AI explanations under the law. From the GDPR to the AIA, and beyond», en Andreas HOLZINGER *et al.* (ed.), *xxAI - Beyond explainable AI*, Nueva York, Springer, 2022, p. 348, <<https://doi.org/10.1007/978-3-031-04083-2>> (consulta: febrero 2024).

63. Manuel MEDINA GUERRERO, «El derecho a conocer los algoritmos utilizados», p. 151.

64. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), *Adecuación al RGPD de tratamientos que incorporan inteligencia artificial. Una introducción*, Madrid, Agencia Española de Protección de Datos, 2020, p. 34 y 35.

Por tanto, para que una decisión no sea considerada exclusivamente automatizada, la intervención humana tiene que ser significativa, y no un mero formalismo. Por *significativa* se entiende que la persona involucrada en la supervisión debe ser competente para revertir o modificar esa decisión.⁶⁵ Por ende, la persona ha de tener capacidad de influir,⁶⁶ de tal manera que si sucede lo contrario, es decir, si el procesamiento automático es lo que directamente predetermina la decisión final, esta se considerará exclusivamente automatizada.⁶⁷

En el mismo sentido apunta el abogado general del TJUE en sus conclusiones sobre el asunto SCHUFA. En el párrafo 44 sostiene que habrá tratamiento automatizado cuando no se pueda influir en el paso intermedio entre el tratamiento automatizado (*score*) y la decisión final de conceder o denegar el crédito, en el sentido que el *score* determinará el resultado final. Todo ello, con independencia de que haya habido o no intervención humana.

No obstante, para poder influir efectivamente es necesario tener no solo la autoridad para ello, sino también los conocimientos adecuados sobre el funcionamiento y los riesgos del modelo computacional. Así lo prevé la ABE cuando establece que las entidades garantizarán la formación adecuada de sus empleados.⁶⁸ Asimismo, el Reglamento de IA también incide en ello en el considerando 73 y en su artículo 15 cuando dice que los modelos han de ser vigilados de manera efectiva por personas físicas y que estas han de poder interpretar correctamente la información de salida, algo que sin formación adecuada no se podrá hacer. Con ello se intenta disminuir esa tendencia humana a seguir acríticamente los dictados de una máquina y a colocar a las personas que trabajan con ella en igualdad de condiciones.

En este sentido, parece relevante mencionar el asunto Uber que se dirimió en primera instancia y más tarde en apelación en Ámsterdam.⁶⁹ Los tribunales respectivos tuvieron que evaluar si, a raíz de los hechos, había habido una intervención humana significativa a la hora de desactivar las cuentas de Uber de varios conductores

65. GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 (GTPD-29), *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, Bruselas, Dirección General de Justicia de la Comisión Europea, 2018, p. 23.

66. Sebastião BARROS VALE y Gabriela ZANFIR-FORTUNA, *Automated-making under the GDPR: Practical cases from courts and data protection authorities*, Washington, Future of Privacy Forum, 2022, p. 29.

67. Diogo MORGADO REBELO y Filipa CAMPOS FERREIRA, «AI-based consumer's creditworthiness assessment», p. 89.

68. EUROPEAN BANKING AUTHORITY (EBA), *Directrices sobre concesión y seguimiento de préstamos*, p. 66.

69. S. E. BIBER, *Between humans and machines: Judicial interpretation of the automated decision-making practices in the EU*, Luxemburgo, University of Luxembourg, 2023, p. 32 (Law Research Paper No. 2023-19), <<http://dx.doi.org/10.2139/ssrn.4662152>> (consulta: abril 2024); véase también Sebastião BARROS VALE y Gabriela ZANFIR-FORTUNA, *Automated-Making Under the GDPR*, p. 29.

por detección de fraude, y que ello precluyese la posibilidad de que fuera una decisión automatizada.

El tribunal de primera instancia entendió que, efectivamente, se había dado una intervención humana significativa. La razón fue que los protocolos de la empresa, tras la señal de fraude automática, obligaban a los empleados encargados de desactivar las cuentas a analizar otros factores relacionados con los hechos. A partir de una investigación exhaustiva y de sus conocimientos, dos empleados de forma unánime tenían que decidir desactivarlas o no. En caso de conflicto, sería necesaria la intervención un tercer empleado.⁷⁰ Esto demuestra la importancia fundamental que tienen dos factores, mencionados anteriormente, para poder considerar que existe participación humana: poder revertir la decisión de la máquina (es decir, tomar una decisión distinta a la de la máquina) y formar adecuadamente a los empleados.

Sin embargo, en apelación el tribunal no compartió este razonamiento, ya que existía cierta oscuridad en el proceso que se llevaba a cabo para demostrar la existencia de participación humana y el nivel de conocimiento de los empleados.⁷¹ En cualquier caso, ello sigue demostrando la importancia que tiene que los trabajadores que intervienen en el proceso decisorio estén formados adecuadamente y tengan en consideración factores adicionales para entender que hay una participación humana significativa.

También se han dirimido varios casos en el ámbito del *credit scoring*, que tocan más de cerca a este trabajo.⁷² Tanto el Tribunal Federal de Justicia de Alemania (Bundesgerichtshof, BGH) en 2014 como la Agencia Española de Protección de Datos (en adelante, AEPD) en 2021 llegaron a una conclusión similar en sus respectivas resoluciones: se entenderá que hay participación humana suficiente cuando los mecanismos automatizados se utilicen solo como apoyo para la toma de la decisión crediticia.⁷³

Así, el BGH en el párrafo 34 de su Sentencia de 28 de enero de 2014, basándose en el instrumento normativo de protección de datos vigente en ese momento (Directiva 95/46/EC), declaró que no era una decisión automatizada «si los resultados

70. Rechtbank Amsterdam (Juzgado de Primera Instancia de Ámsterdam), Sentencia de 11 de marzo de 2021, C/13/692003 / HA RK 20-302, ECLI:NL:RBAMS:2021:1018, 4.19-4.24; véase en A. J. WULF y O. SEIZOV, «Please understand we cannot provide further information»: evaluating content and transparency of GDPR-mandated AI disclosures», *AI and Society*, núm. 39 (2024), p. 235 y 237.

71. Gerechtshof Amsterdam (Tribunal de Apelación de Ámsterdam), Sentencia de 4 de abril de 2023, 200.295.742/01, ECLI:NL:GHAMS:2023:793, 3.24.

72. Casos mencionados en Diogo MORGADO REBELO y Filipa CAMPOS FERREIRA, «AI-based consumer's creditworthiness assessment».

73. BGH (Tribunal Federal de Justicia de Alemania), Sentencia de 28 de enero de 2014, VI ZR 156/13, y AEPD, Resolución del procedimiento sancionador núm. PS/00477/2019, de 13 de enero de 2021.

obtenidos mediante el tratamiento automatizado de datos eran simplemente la base de una decisión final que aún debía ser adoptada por un ser humano».⁷⁴

La AEPD utilizó las directrices del GTPD-29 para determinar que a CaixaBank no le era aplicable el artículo 22 RGPD, ya que incluía intervención humana al conceder créditos.⁷⁵ Esto es porque las directrices hacen una distinción entre las decisiones basadas en la elaboración de perfiles y las decisiones basadas únicamente en el tratamiento automatizado del artículo 22.1 RGPD. La diferencia radica en que en las primeras la persona encargada concede un crédito sobre la base de una decisión basada únicamente en un tratamiento automatizado (que sería el perfil o *score*). Es decir, la decisión únicamente automatizada solo lo utiliza como apoyo y valora, en principio, otros factores. Por lo tanto, existe una participación humana en el proceso decisorio. Esto era lo que consideró la AEPD que sucedía en el caso de CaixaBank. En cambio, en las segundas es la propia decisión exclusivamente automatizada de conceder o no el crédito la definitiva, sin mediar una persona entre la decisión elaborada por el algoritmo y la decisión final.⁷⁶

Aquí es donde reside el problema que se mencionaba al inicio de este subepígrafe respecto a la desigualdad entre los individuos que están sujetos a decisiones basadas en un tratamiento automatizado (decisiones semiautomatizadas) y los individuos que lo están a decisiones basadas *únicamente* en el tratamiento automatizado. Ello estriba en que se hace una distinción entre los diferentes grados de automatización,⁷⁷ de modo que, en función del grado de participación humana que exista, se tomará una decisión u otra, con todo lo que eso conlleva en cuanto a las diferencias en derechos y garantías.

A este respecto cabe decir que, tal y como señala la sentencia del caso SCHUFA, el objetivo real del RGPD —y, en especial, el del artículo 22— es proteger a las personas de los riesgos inherentes a un procesamiento de datos automatizado.⁷⁸ Por tal

74. BGH, Sentencia de 28 de enero de 2014, VI ZR 156/13, [34]. Original: «[...] wenn die mittels automatisierter Datenverarbeitung gewonnenen Erkenntnisse lediglich Grundlage für eine von einem Menschen noch zu treffende abschließende Entscheidung sind».

75. AEPD, Resolución del procedimiento sancionador núm. PS/00477/2019, p. 21.

76. GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 (GTPD-29), *Directrices sobre decisiones individuales automatizadas*, p. 9.

77. P. DAVIS y S. SCHWEMER, «Rethinking decisions under article 22 of the GDPR: implications for semi-automated legal decision-making», *Proceedings of the Third International Workshop on Artificial Intelligence and Intelligent Assistance for Legal Professionals in the Digital Workplace (LegalAIIA 2023), held in conjunction with ICAIL 2023* (2023), p. 2, <<https://dx.doi.org/10.2139/ssrn.4478107>> (consulta: marzo 2024). Respecto a la necesidad de equiparar derechos entre afectados por el tratamiento automatizado de datos, véase Esther ARROYO AMAYUELAS, «El scoring de Schufa», *InDret*, año 2024, núm. 3 (en prensa), p. 15 del original, que consulto por amabilidad de la autora.

78. Asunto C-634/2021, O. Q. contra Land Hessen con intervención de SCHUFA Holding AG, ECLI:EU:C:2023:957, 2023, párr. 22.

razón, tanto una situación como la otra deberían quedar protegidas de igual manera, pues ambas se encuentran a merced de un algoritmo y, debido a que la letra del artículo 22 RGPD establece unos requisitos especiales para que se aplique su prohibición, muchas situaciones en las que hay tratamiento automatizado quedarán fuera. Es decir, lo único que debería importar es que en algún momento del proceso decisorio de la concesión de un crédito haya un tratamiento automatizado.

En este sentido, ha habido una mejora con la reciente reforma de la DCC. En su artículo 18.8 DCC, relativo a la evaluación de la solvencia, no se realiza ninguna distinción respecto al grado de automatización de los tratamientos de datos que se puedan utilizar para determinar la solvencia. De modo que tanto a las situaciones completamente automatizadas como a las que son semiautomatizadas, se les otorgan los mismos derechos (intervención humana posterior, expresar punto de vista, obtener una revisión y una explicación sobre la lógica de la evaluación de la solvencia). Lo mismo recoge el artículo 86.1 del Reglamento de IA,⁷⁹ aunque exige que la decisión automatizada tenga un efecto perjudicial para los derechos fundamentales (como la no discriminación o la privacidad). Por tanto, la denegación de un crédito como tal no supone una lesión de los derechos fundamentales, pues no hay un derecho a obtener el crédito.

Ello no solo representa un avance respecto a la antigua DCC, que ni siquiera preveía la posibilidad de evaluar la solvencia a través de modelos automatizados, sino también respecto al propio RGPD, que solo concedía dichos derechos a las decisiones exclusivamente automatizadas que cumplieran los requisitos del artículo 22 RGPD.

2.4.2. *Derecho a obtener una explicación: artículos 13.2f, 14.2g y 15.1h RGPD*

El RGPD prevé unos derechos adicionales de información para la persona sujeta a una decisión basada únicamente en un tratamiento automatizado de datos del artículo 22 RGPD. Estos derechos se encuentran en tres preceptos distintos (artículos 13.2f, 14.2g y 15.1h RGPD) y tienen idéntica redacción. Sin embargo, se inscriben en circunstancias y momentos diferentes. En todos, el derecho consiste en dar información relativa a la existencia de dichas decisiones, así como de su relevancia y repercusiones, y en proveer información significativa sobre la lógica aplicada.

El derecho a obtener información significativa sobre la lógica aplicada se predica de las decisiones de los apartados 1 y 4 del artículo 22 RGPD. No obstante, la redacción de estos tres preceptos del RGPD con la apostilla «y, al menos en tales casos, [refiriéndose al artículo 22.1 y 4] información significativa sobre la lógica aplicada» quizá podría entenderse en el sentido de que el RGPD está previendo que este dere-

79. Esther ARROYO AMAYUELAS, «El scoring de Schufa», p. 14 y 15 de la paginación original.

cho pueda facultativamente predicarse de otras situaciones con tratamiento de datos automatizado que no sean las del artículo 22 RGPD; es decir, de decisiones que no necesariamente sean exclusivamente automatizadas. En parte, una interpretación así resultaría positiva porque no cerraría la puerta a otras situaciones que, sin ser tan gravosas para el interesado, siguen presentando los riesgos de la automatización. Con independencia de que esto sea o no lo que se pretendía disponer en estos preceptos, cabe recordar que la reforma de la DCC deja definitivamente de lado esta distinción en su artículo 18.8, con lo que supera el error en el que el RGPD cae al hacer distinciones, en relación con los derechos y las garantías, entre situaciones con diferente grado de automatización.

También es necesario precisar que la repetición de este derecho en varios preceptos no es en vano, porque realmente no supone una reiteración como tal. Esto se debe a que este derecho de información se contempla en circunstancias diversas. En el artículo 13 RGPD se refiere a las situaciones en las que los datos que se van a procesar se recaban del propio interesado. En cambio, se aplicará el artículo 14 RGPD cuando dichos datos no sean obtenidos por el propio interesado. Finalmente, el artículo 15 RGPD es el que más problemas plantea a la hora de determinar en qué circunstancias será aplicable. Sin embargo, como se verá más adelante, el asunto SCHUFA consigue resolver este interrogante y cerrar el debate doctrinal que suscitaba.

3. ASUNTO SCHUFA (C-634/21)

3.1. LITIGIO PRINCIPAL Y CUESTIONES PREJUDICIALES

El creciente uso de medios automatizados y de la IA para la generación de *scores* y, a su vez, la utilización de estos como fundamento para determinar si una persona es solvente y va a poder devolver el crédito, han planteado numerosas cuestiones relacionadas con la protección de datos y el determinismo tecnológico. Por ello, no es de extrañar que esto haya desembocado en que uno de los preceptos europeos de mayor trascendencia en esta materia, el artículo 22 RGPD, haya sido objeto de una cuestión prejudicial en el TJUE.

El planteamiento de un caso como el asunto SCHUFA⁸⁰ revela que existen problemas de fondo en esta materia a los que no se ha dado solución ni desde el RGPD ni desde la normativa europea de protección al consumidor.

De los hechos que se extraen de la sentencia de este caso,⁸¹ a la demandante persona física, O. Q., le fue denegado un crédito por una entidad crediticia debido

80. Asunto C-634/2021, O. Q. contra Land Hessen con intervención de SCHUFA.

81. Se expondrán brevemente los hechos descritos en la Sentencia, en concreto los párr. 14 y 27.

a que SCHUFA emitió un *score* negativo al predecir que existían probabilidades de que no lo pudiera devolver. SCHUFA es una empresa cuya actividad económica es proporcionar a sus clientes (que normalmente son entidades de crédito o bancos) un pronóstico en forma de *score* sobre si una persona devolverá o no un crédito. El *score* lo elabora a partir de modelos computacionales que funcionan con IA y procesan datos personales a partir de los cuales se encuentran correlaciones con grupos de personas respecto de los que se prevén comportamientos similares. Es decir, informa a sus clientes o socios sobre la solvencia de los consumidores con los que estos quieren contratar.

Como consecuencia de la denegación del crédito, O. Q. requirió a SCHUFA para que le proporcionara acceso a sus datos y suprimiera su registro, ejerciendo así los derechos que le amparaban bajo el RGPD. Sin embargo, SCHUFA se limitó a presentarle su *score* y le explicó en términos muy generales cómo se había alcanzado esa calificación. Se escudó en el secreto comercial para denegarle información relativa a los datos personales que se habían tenido en cuenta, así como el peso que se había adjudicado a cada uno.

Esto es lo que, tanto a partir de las conclusiones del abogado general como de la Sentencia, permite explorar qué se entiende y cuál es el alcance del derecho a obtener «información significativa sobre la lógica aplicada» previsto en los artículos 13.2f, 14.2g y 15.1b RGPD.

No habiendo satisfecho SCHUFA la petición, O. Q. se dirigió al delegado de protección de datos y de libertad de información competente para que reclamara a SCHUFA el cumplimiento de su petición. Sin embargo, el delegado no consideró pertinente la solicitud de O. Q., ya que consideraba que no se apreciaban razones para entender que SCHUFA había incumplido con sus obligaciones. En consecuencia, O. Q. recurrió la decisión del delegado al Tribunal Contencioso-Administrativo de Wiesbaden (Alemania), que se planteó si el artículo 22 RGPD podía resultar aplicable en este supuesto.

El artículo 22 RGPD, a grandes rasgos, prohíbe las decisiones exclusivamente automatizadas, en las que también se incluye el análisis de perfiles (*profiling*), cuando tengan efectos jurídicos o afecten significativamente a la persona de un modo similar. Se prevén excepciones y se otorgan una serie de derechos a la persona objeto del tratamiento, como son la intervención humana, expresar el punto de vista e impugnar la decisión.

Una de las razones que condujo al tribunal recurrente a plantearse si el *score* que realizaba SCHUFA podía considerarse directamente una decisión automatizada era que la decisión posterior del banco de conceder o denegar el crédito se basaba exclusivamente en dicho *score*; es decir, en una decisión exclusivamente automatizada, pues consiste en la elaboración de un perfil. Sin embargo, un aspecto que quedaba por dirimir era si el propio *score* producía esos efectos significativos en la persona sujeta al tratamiento de datos que exigía el artículo 22 RGPD, ya que *a priori* la decisión final

siempre quedaba en manos de la entidad crediticia. No obstante, el *score* no parecía servir como mero apoyo a la decisión de concesión del crédito, sino que más bien era determinante. Por tanto, el *score* parecía poder encajar en la definición de decisión basada únicamente en el tratamiento automatizado del citado precepto.

En consecuencia, el tribunal remitente elevó como cuestión prejudicial al TJUE la siguiente pregunta:⁸²

¿Debe interpretarse el artículo 22 [...] en el sentido de que la generación automatizada de un [...] [*score*] constituye ya una decisión basada únicamente en el tratamiento automatizado, [...] cuando dicho valor, hallado a partir de datos personales del interesado, es transmitido por el responsable del tratamiento a un tercero [que] [...], de un modo determinante, basa en dicho valor su decisión sobre el establecimiento, la ejecución o la extinción de una relación contractual con el interesado?

Asimismo, también se remitió una segunda cuestión prejudicial referente a la normativa alemana de protección de datos, a la que no se hará referencia por encontrarse fuera del objeto de este trabajo.⁸³

3.2. EL ASUNTO SCHUFA: RESPUESTAS E INTERROGANTES PENDIENTES

En los siguientes epígrafes se abordarán diversas cuestiones que han preocupado a la doctrina y que, en mayor o menor medida, han sido tratadas en el asunto SCHUFA o están estrechamente relacionadas con la materia.

3.2.1. ¿Cuál es la «decisión» a efectos del artículo 22 RGPD?

Como ya se ha avanzado en epígrafes anteriores, existen dos actos susceptibles de calificarse como «decisiones» a los efectos del artículo 22 RGPD: por un lado, la elaboración del perfil o *score* relativo a la solvencia; por el otro, la decisión del banco de conceder o denegar un crédito.⁸⁴

82. Asunto C-634/2021, O. Q. contra Land Hessen con intervención de SCHUFA Holding AG, párr. 27.

83. Sobre esta cuestión profundiza Esther ARROYO AMAYUELAS, «El scoring de Schufa», p. 8 y 9 de la paginación original.

84. Asunto C-634/2021, conclusiones del abogado general Sr. Priit Pikamäe, párr. 40.

El artículo 4 RGPD entiende que la elaboración de un perfil es un tratamiento automatizado de datos personales. El artículo 22 RGPD la integra como subcategoría de decisiones basadas únicamente en el tratamiento automatizado, siempre que produzca efectos jurídicos o similares en la persona cuyos datos hayan sido tratados y no medie participación humana. En este sentido, el considerando 71 RGPD, a modo de ejemplo, entiende que es una decisión «la denegación automática de una solicitud de crédito» cuando no exista intervención humana alguna.

A este respecto, el asunto SCHUFA planteó la situación a la que da lugar el hecho de que en las entidades de crédito sea una práctica habitual y reiterada dar una importancia fundamental al *score* para tomar la decisión de concesión del crédito⁸⁵ (algo que, como se verá, no es un fenómeno extendido en todos los países europeos ni en todas las entidades crediticias);⁸⁶ es decir, el caso en el que no hay participación humana entre el perfilado a partir del cual se genera el *score* (y que es un tratamiento automatizado) y la decisión de concesión del crédito. Por tanto, la cuestión a resolver era si, a pesar de que la entidad crediticia tuviera la última palabra, el *score* podía considerarse la propia «decisión» del artículo 22 RGPD, cuando la entidad se limita a aplicar el *score* en la decisión final.⁸⁷

La respuesta del abogado general del TJUE fue que se había de valorar a la luz de las «reglas y prácticas internas de la entidad financiera»⁸⁸ y que el juez nacional debería considerarlo a raíz de los hechos que se planteasen en cada caso concreto.⁸⁹ En el supuesto de que efectivamente la práctica habitual fuera que la elaboración del perfil es concluyente para conceder o denegar el crédito, tanto el abogado general del TJUE en sus conclusiones⁹⁰ como el TJUE en su sentencia posterior⁹¹ llegan al mismo resultado: se deberá entender que la propia elaboración del perfil (o *score*) es la «decisión» del artículo 22 RGPD.

Asimismo, en estos supuestos no concurren tampoco los requisitos que la jurisprudencia y las resoluciones previas a este caso, mencionadas en apartados anteriores, entienden necesarios para que exista una intervención humana significativa.⁹² El tra-

85. Asunto C-634/2021, conclusiones del abogado general Sr. Priit Pikamäe, párr. 43.

86. En España, sin ir más lejos, no parece ser una práctica habitual de las entidades de crédito. Véanse los anexos I y II.

87. Asunto C-634/2021, conclusiones del abogado general Sr. Priit Pikamäe, párr. 44.

88. Asunto C-634/2021, conclusiones del abogado general Sr. Priit Pikamäe, párr. 40 y 44.

89. Asunto C-634/2021, conclusiones del abogado general Sr. Priit Pikamäe, párr. 45. Así, Esther ARROYO AMAYUELAS, «El scoring de Schufa», p. 12 de la paginación original, apunta al problema de inseguridad jurídica que puede generar el hecho de tener que analizar caso por caso si el *scoring* es o no determinante.

90. Asunto C-634/2021, conclusiones del abogado general Sr. Priit Pikamäe, párr. 47 y 59.

91. Asunto C-634/2021, O. Q. contra Land Hessen con intervención de SCHUFA, párr. 50 y 73.

92. Véase el epígrafe 2.4.1.3, «¿Qué se entiende por basado únicamente en un tratamiento automatizado?», donde se hace mención del asunto Uber y de resoluciones del BGH y de la AEPD.

tamiento automatizado no se utiliza como mero apoyo, sino que es la decisión en sí. Además, no existe la posibilidad de que las personas competentes que han de tomar la decisión final tengan la posibilidad de revertirla, pues las reglas internas de la entidad trasladan el resultado del perfilado (*score*) a la decisión final.

3.2.2. *El momento de dar la explicación: ¿ex ante, ex post o ambas?*

El derecho a obtener una explicación significativa sobre la lógica se puede ejercer en momentos diferentes del procesamiento de datos y, por lo tanto, del proceso decisorio de concesión del crédito. No parece haber discusión respecto al momento de ejercicio de los artículos 13 y 14 RGPD, que se entiende que implican una explicación *ex ante* a la adopción de la decisión automatizada,⁹³ cuando se obtienen los datos o bien del propio interesado o bien por terceras vías. Sin embargo, la doctrina se encuentra más dividida respecto al alcance del artículo 15 RGPD.

Se planteó si existía una explicación *ex post*, es decir, si se podrían pedir explicaciones sobre la lógica aplicada a la decisión concreta, en lugar de explicaciones genéricas sobre el funcionamiento del sistema. Un sector protagonizado por Wachter, Mittelstadt y Floridi⁹⁴ se posicionó en contra de la existencia de tal derecho, mientras que otros autores sí estimaban posible su existencia.⁹⁵ A este respecto, entre los argumentos que se esgrimieron en contra de la existencia de un derecho de explicación *ex post*, el principal se centraba en que el único lugar donde aparecía dicho derecho en el RGPD era el considerando 71,⁹⁶ que carece de valor normativo.⁹⁷

Sin embargo, este razonamiento ha sido refutado aludiendo a varios motivos. Para empezar, a pesar de que los considerandos no tienen valor normativo, sí que se utilizan por el TJUE para esclarecer conceptos o preceptos oscuros del instrumento normativo europeo en el que se encuentran.⁹⁸ Así, a pesar de que la jurisprudencia europea es clara respecto a que no se pueden invocar «ni para establecer excepciones [...] ni para interpretarlas en un sentido manifiestamente contrario a su tenor lite-

93. Gerald SPINDLER, «Algorithms, credit scoring, and the new proposals of the EU for an AI Act and on a Consumer Credit Directive», *Law and Financial Markets Review*, núm. 15 (2021), p. 239 y 250, <<https://doi.org/10.1080/17521440.2023.2168940>> (consulta: abril 2024).

94. Sandra Wächter, Brent Mittelstadt y Luciano Floridi, «Why a right to explanation of automated decision-making does not exist in the general data protection regulation?», *International Data Privacy Law*, núm. 76 (2017), p. 79-80, <<https://doi.org/10.1093/idpl/ix005>> (consulta: mayo 2024).

95. Maja Brkan, «Do algorithms rule the world? Algorithmic decision-making in the framework of GDPR and beyond», 15 (2017), <<https://dx.doi.org/10.2139/ssrn.3124901>> (consulta: abril 2024).

96. Considerando 71 del RGPD: «[...] incluir la información específica al interesado y el derecho a [...] recibir una explicación de la decisión tomada después de tal evaluación».

97. Gerald Spindler, «Algorithms, credit scoring», p. 249.

98. Manuel Medina Guerrero, «El derecho a conocer los algoritmos utilizados», p. 166.

ral»,⁹⁹ en este caso hacer una interpretación sistemática del artículo 15.1*b* RGPD junto con el considerando 71 no supondría ninguno de estos supuestos. Es más, la propia letra del artículo 22.3 RGPD enumera los derechos que «como mínimo» protegen al interesado, es decir, no descarta otras garantías posibles, entre las que se podría encontrar el derecho a obtener una explicación después de la decisión.¹⁰⁰

Asimismo, a raíz de los trabajos preparatorios del RGPD se conoce que este derecho efectivamente estaba en mente, pues el propio Parlamento Europeo sugirió su incorporación, que, más tarde, el Consejo rechazaría. Finalmente, se incorporó en los considerandos y se añadió la coletilla «como mínimo» en el artículo 22.3 RGPD a modo de obtener consenso.¹⁰¹ De ello se desprende que una interpretación amplia haría que su existencia fuera innegable. A mayor abundamiento, rechazar su existencia desvirtuaría el objetivo del propio RGPD y haría muy difícil el ejercicio de los demás derechos, como es el de impugnar la decisión, ya que sin conocer el razonamiento que hay detrás de su adopción será muy difícil sostener que la decisión es incorrecta.¹⁰² Finalmente, cabe decir que tanto el GTPD-29¹⁰³ como la AEPD, entre otros organismos expertos en la materia, han secundado esta visión y han reconocido la existencia de este derecho.¹⁰⁴

El asunto SCHUFA finalmente cierra este debate doctrinal a favor de la existencia del derecho a una explicación *ex post*, sobre todo a partir de las conclusiones del abogado general del TJUE. La interpretación que proporciona del artículo 15 RGPD ha de referirse necesariamente a una explicación posterior a la decisión, ya que entiende que la información significativa sobre la lógica incluye «las razones que han conducido a un resultado determinado»,¹⁰⁵ que solo se podrán dar una vez ha tenido lugar la decisión.

99. Asunto C-136/04, Deutsches Milch-Kontor GmbH contra Hauptzollamt Hamburg-Jonas ECR 2005 I-10095, ECLI:EU:C:2005:716, párr. 32, y otra jurisprudencia; véase Manuel MEDINA GUERRERO, «El derecho a conocer los algoritmos utilizados», p. 166.

100. Maja BRKAN, «Do algorithms rule the world?», p. 18.

101. Manuel MEDINA GUERRERO, «El derecho a conocer los algoritmos utilizados», p. 165.

102. Adrián PALMA ORTIGOSA, *Decisiones automatizadas y protección de datos: Especial atención a los sistemas de inteligencia artificial*, 1ª ed., Madrid, Dykinson, 2022, p. 291.

103. GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 (GTPD-29), *Directrices sobre decisiones individuales automatizadas*, p. 19.

104. Adrián PALMA ORTIGOSA, *Decisiones automatizadas y protección de datos*, p. 291, cita a la AEPD, Resolución del procedimiento sancionador núm. PS/00070/2019, p. 109.

105. Asunto C-634/2021, conclusiones del abogado general Sr. Priti Pikamäe, párr. 58.

3.2.3. ¿Qué implica información significativa sobre la lógica?

Una vez confirmada por el TJUE la existencia de un derecho de explicación posterior a la decisión, a efectos de garantizar su plena efectividad y la transparencia que precisamente persigue resulta conveniente determinar qué conlleva exactamente información significativa sobre la lógica, es decir, qué información incluye este derecho.

La doctrina ha intentado dar respuesta a esta pregunta proponiendo diversas interpretaciones. Por un lado, existía un sector que creía necesario que para satisfacer este derecho se desvelara información relativa al modelo que se había empleado para tomar la decisión, como el tipo, los datos de entrenamiento y los parámetros que se utilizaron para construirlo, así como los aspectos concretos de la situación individual, como el perfil que se le atribuyó y las características personales específicas que llevaron a ello.¹⁰⁶ Otro sector entiende que los algoritmos del modelo deberían ser revelados de manera que sean comprensibles para la persona.¹⁰⁷ Algunos se posicionaron en contra de que se hubiera de desvelar el código fuente, porque lo creían excesivo al resultar demasiado complejo de entender, y adujeron que con una información más superficial sería suficiente.¹⁰⁸

Además, las agencias de protección de datos que operan en los diversos estados miembros también han propuesto diversas interpretaciones a este respecto. Por ejemplo, la AEPD publicó un documento en el que abordaba esta cuestión y proponía categorías de información que podían facilitar la comprensión de los resultados y, por tanto, de la lógica subyacente de la decisión. Así, algunos ejemplos que mencionaba eran: la importancia relativa de los datos personales utilizados, la calidad de los datos de entrenamiento, el tipo de patrones utilizados, el perfilado realizado, la precisión de los resultados, etc.¹⁰⁹

También la Agencia de Protección de Datos Sueca (IMY) en 2022 sancionó a Klarna, una empresa de tecnologías financieras (*fintech*) sueca que ofrece servicios en línea, entre otros motivos por no facilitar información sobre la lógica en su aviso de privacidad.¹¹⁰ Así, la IMY llegó a esa conclusión porque «no se facilita[ba] in-

106. Antoni ROIG, *Las garantías frente a las decisiones automatizadas: Del Reglamento general de protección de datos a la gobernanza algorítmica*, 1ª ed., Barcelona, J. M. Bosch, 2020, p. 97.

107. Gerald SPINDLER, «Algorithms, credit scoring», p. 250.

108. Alba SORIANO ARNAZ, *Data Protection for the Prevention of Algorithmic Discrimination*, p. 169.

109. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), *Adecuación al RGPD de tratamientos que incorporan inteligencia artificial*, p. 24.

110. Sebastião BARROS VALE y Gabriela ZANFIR-FORTUNA, *Automated-Making Under the GDPR*, p. 21.

formación sobre las circunstancias que podrían ser determinantes para una decisión de crédito negativa».¹¹¹

Asimismo, una decisión de la Agencia de Protección de Datos de Islandia (Persónuvernd), que, a pesar de no ser un estado miembro, ha transpuesto el RGPD, entendió que Creditinfo, una empresa de información crediticia análoga a SCHUFA, no vulneró el derecho a obtener información sobre la lógica.¹¹² La razón fue que Creditinfo facilitó al interesado a través de un correo electrónico la información relativa a los factores que tuvieron mayor impacto en la reducción de su *score*; es decir, los que le perjudicaron, como, por ejemplo, estar en una base de datos de morosos.¹¹³

Por otro lado, el GTPD-29 también trató de averiguar qué implicaba esta información significativa sobre la lógica subyacente. Entendió que la información debía «ser suficientemente exhaustiva» y proporcionarse de forma sencilla para su comprensión (probablemente para no contravenir otros preceptos del RGPD, como el artículo 12, que dispone que la información se ha de proporcionar de forma clara y sencilla). A pesar de todo ello, rechazó la necesidad de revelar el algoritmo.¹¹⁴ Además, en cuanto al *credit scoring*, indicó que deben explicarse los motivos que han conducido a la calificación crediticia individual, así como los parámetros que tienen más peso en el *score*.

Recientemente, como ya se ha visto, el TJUE tuvo ocasión de abordar este aspecto también a través de la cuestión prejudicial que dio lugar al asunto SCHUFA. En este caso, fue especialmente el abogado general en sus conclusiones el que intentó precisar el alcance de la obligación de proporcionar información sobre la lógica subyacente. Y es en su párrafo 58 donde determina que las explicaciones deben incluir información sobre el «método de cálculo» que se ha utilizado para obtener el *score*, así como los motivos por los que se ha obtenido el resultado concreto. Para ello, será preciso facilitar información relativa a los elementos que se han tenido en cuenta y el valor que se les ha otorgado.¹¹⁵ Ello confirma lo que había venido diciendo el GTPD-29 en sus directrices, a las que directamente se remite. Asimismo, tampoco se aparta de lo que ha conformado la reciente práctica de las agencias de protección de

111. Integritetsskyddsmyndigheten (IMY) (Agencia de Protección de Datos Sueca), Decisión núm. DI-2019-4062, Klarna Bank AB, 28 de marzo de 2022, p. 21. Traducción: «Det ges ingen information om vilka omständigheter som kan vara av avgörande betydelse för ett negativt kreditbeslut».

112. Sebastião BARROS VALE y Gabriela ZANFIR-FORTUNA, *Automated-Making Under the GDPR*, p. 46.

113. Persónuvernd (Agencia de Protección de Datos Islandesa), caso núm. 2020010592, Creditinfo Lánstraust hf., 22 de septiembre de 2022, párr. 4.2.

114. GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 (GTPD-29), *Directrices sobre decisiones individuales automatizadas*, p. 28.

115. Asunto C-634/2021, conclusiones del abogado general Sr. Priit Pikamäe, párr. 58.

datos que han tenido ocasión de valorar esta cuestión y a las que se ha aludido anteriormente con los asuntos referentes a Klarna y Creditinfo.

En resumen, la información que se ha de incluir en las explicaciones correspondientes a la lógica subyacente de la decisión vendría a ser la que ha conducido a una determinada calificación y a la consiguiente decisión (por ejemplo, las circunstancias que han tenido un impacto negativo en el resultado), y también los datos a los que se ha atribuido mayor peso (como constar en un registro de impagados).

Por consiguiente, una vez se ha corroborado la existencia de una explicación *ex post* y se ha delimitado la información que debe facilitarse, se plantean algunas dificultades que pueden convertirse en trabas para la efectividad de este derecho. Pueden consistir tanto en límites internos como externos del propio algoritmo o modelo. En el caso de los primeros, son los relativos a la propia complejidad que pueden albergar y, por ende, también a una explicación sobre su funcionamiento. Respecto a los segundos, son la forma en la que se han de ponderar estas explicaciones con el secreto comercial que las empresas que elaboran los algoritmos alegan a la hora de denegar unas explicaciones más precisas. En los apartados siguientes se incidirá en estos aspectos y se intentará determinar si son realmente obstáculos insalvables o sencillamente un pretexto para perpetuar el fenómeno de la *black box* y la opacidad, cuyos beneficios se encuentran muy lejos de favorecer al consumidor.¹¹⁶

3.2.4. *La complejidad de la explicación*

Como ya se ha avanzado, la transparencia es fundamental para poder ejercer adecuadamente los derechos que garantizan al consumidor poder conocer cómo se ha llegado a la decisión de denegarle el crédito y poder impugnarla, si así lo cree conveniente, o simplemente asegurarse de que hay un motivo justificado detrás.

Sin embargo, la introducción de la IA y la automatización en los procesos de evaluación crediticia puede dificultar, e incluso frustrar, los objetivos del legislador europeo en cuanto a la transparencia.¹¹⁷ Y es que los algoritmos introducen una opacidad sin precedentes debido, en parte, a su propia configuración.¹¹⁸ Es decir, algoritmos y opacidad van inescindiblemente de la mano, uno forma parte del otro, como consecuencia de las dificultades técnicas que supone explicarlos —al menos, algunos de ellos—. En efecto, se podría distinguir, en función de la técnica utilizada, entre los algoritmos que sí que se pueden explicar y los que no.

116. «As Pasquale points out, “finance industries profit by keeping us in the dark”»; véase en Zofia BEDNARZ y Linda PRZHEDETSKY, «AI opacity in the financial industry», p. 70.

117. Noelia COLLADO-RODRÍGUEZ, «La evaluación de la solvencia», p. 55.

118. Zofia BEDNARZ y Linda PRZHEDETSKY, «AI opacity in the financial industry», p. 70.

En cuanto a los primeros, incluiríamos los llamados *árboles de decisión*, a cuyo resultado se llega a partir de una secuencia de pruebas. En cada una se prevén posibles respuestas que a su vez plantean nuevas preguntas, y así sucesivamente hasta que se alcanza una solución.¹¹⁹ Se fundamentan en un proceso inductivo, por lo que resultará relativamente sencillo saber cómo se ha llegado a una conclusión determinada, retrocediendo los pasos que se han seguido. Por ende, en estos casos se entiende que no existe la *black box*.¹²⁰

Respecto a los segundos, en los que encontramos, por ejemplo, la red neuronal, plantean más problemas de transparencia porque resultan casi imposibles de explicar. Utilizan aprendizaje automático (*machine learning*), que se asemeja al proceso que puede hacer el cerebro humano y es un método que permite al algoritmo encontrar patrones con los que luego hacer predicciones.¹²¹ Y no solo eso, sino que, además, es capaz de aprender de sus análisis previos y afinar su procesamiento para conseguir una mayor precisión en sus siguientes correlaciones y predicciones.¹²² Es esta capacidad de autoaprendizaje la que implicará una gran falta de transparencia, porque al final resulta inexplicable cómo aprende y hace correlaciones, pues lo hace de forma autónoma.¹²³

Por lo tanto, existirán muchas dificultades a la hora de determinar y explicar cómo el algoritmo ha llegado al resultado individual; por ejemplo, qué patrones ha encontrado y sobre qué datos lo ha hecho.¹²⁴ Es en estos últimos casos donde esencialmente reside el problema para dar una explicación, pero el GTPD-29 advierte que la complejidad de las explicaciones no puede utilizarse como disculpa para eludir las obligaciones de información.¹²⁵

Asimismo, la ABE exige que cuando se utilicen innovaciones tecnológicas en la concesión de créditos, como es el uso de modelos con IA, se conozca cómo operan. Ello permite dar explicaciones adecuadas, pues implica conocer su funcionamiento y cómo se ha llegado a un resultado determinado. Por ello, exige a las entidades de crédito que garanticen la trazabilidad de los resultados, conozcan los modelos que utilizan y, si van a ser necesarias explicaciones durante la utilización del modelo (como

119. Maja BRKAN, «Do algorithms rule the world?», p. 20.

120. Antoni ROIG, *Las garantías frente a las decisiones automatizadas*, p. 140.

121. Alba SORIANO ARNAZ, *Data Protection for the Prevention of Algorithmic Discrimination*, p. 38 y 39.

122. Michal S. GAL y Niva ELKIN-KOREN, «Algorithmic consumers», *Harvard Journal of Law & Technology*, núm. 30 (2017), p. 309 y 313, <<https://ssrn.com/abstract=2876201>> (consulta: marzo 2024).

123. P. PAAL, «Artificial intelligence as a challenge for data protection law», p. 295 y 296.

124. Ralf POSCHER, «Artificial intelligence and the right to data protection», en Silja VOENEKY *et al.* (ed.), *The Cambridge handbook of responsible artificial intelligence*, Cambridge, Cambridge University Press, 2022, p. 283.

125. GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 (GTPD-29), *Directrices sobre decisiones individuales automatizadas*, p. 28 (nota al pie de página 40).

es el caso del artículo 15.1*b* RGPD cuando se usa un *score* para valorar la concesión de un crédito), utilicen uno que sea interpretable.¹²⁶ A pesar de que las directrices que proporciona la ABE no tienen carácter vinculante, ello no significa que puedan ser inobservadas, ya que aun así tienen gran relevancia en el sector bancario europeo e incluso se citan en la propia DCC a efectos interpretativos en el considerando 55.

El razonamiento de la ABE está bien encaminado, pues si las entidades crediticias no son capaces de explicar cómo funcionan los medios que utilizan para tomar decisiones, ello no estaría muy lejos de suponer que deliberadamente no quieren dar las razones por las que toman una decisión determinada, lo que convertiría en arbitrario todo su proceso decisorio. Por consiguiente, si los medios utilizados son técnicamente inexplicables, o bien se usan como apoyo para la toma de decisiones o bien, directamente, no se utilizan.¹²⁷ A veces parece que esta última opción no se pueda contemplar y que si algo existe, necesariamente se ha de utilizar,¹²⁸ sin pensar si realmente aporta algo útil o si, por el contrario, da más problemas que soluciones.

El Reglamento de IA dirime en este sentido de forma más contundente, ya que prohíbe los modelos cuyo funcionamiento y resultados no puedan entenderse. Así se deriva del artículo 13 RGPD, que obliga a que se desarrollen los sistemas de IA de alto riesgo, de modo que quien los utilice pueda interpretar fácilmente sus resultados y, por tanto, su funcionamiento sea transparente. El artículo 15 RGPD continúa exigiendo que dichos sistemas funcionen de manera consistente durante todo su ciclo de vida en términos de precisión. Ello implica que si los creadores o usuarios del modelo no conocen constantemente su funcionamiento, es decir, no saben cómo aprende, a qué variables atribuye más peso, cómo correlaciona, parametriza y perfila, no se podrá utilizar. Estos artículos tienen una importancia significativa porque suponen pasar de una recomendación, como son las directrices de la ABE, a una obligación, la de que los bancos entiendan los algoritmos que utilizan. Algo que, como adelantamos, la sentencia del asunto SCHUFA fracasó en hacer.

Por ende, la preocupación o excusa que venía resonando en la doctrina respecto a aquellos sistemas que ni los propios creadores o expertos podían comprender,¹²⁹ ha dejado de tener sentido con la adopción del Reglamento de IA.

A mayor abundamiento, cabe señalar que las dificultades de explicación referentes a los sistemas de aprendizaje autónomo, señaladas anteriormente, podrían empe-

126. EUROPEAN BANKING AUTHORITY (EBA), *Directrices sobre concesión y seguimiento de préstamos*, párr. 53 y 54.

127. Manuel MEDINA GUERRERO, «El derecho a conocer los algoritmos utilizados», p. 171.

128. Michal S. GAL y Niva ELKIN-KOREN, «Algorithmic consumers», p. 88.

129. Paul VOGEL, «A “Right to Explanation” for Algorithmic Decisions?», en Amedeo SANTOSSO y Giulia PINOTTI (ed.), *Data-driven decision making. Law, ethics, robotics, health*. Pavia, Pavia University Press, 2020, p. 50, <<http://archivio.paviauniversitypress.it/oa/9788869521348.pdf>> (consulta: abril 2024).

zar a ser superadas gracias a nuevas innovaciones como la que propusieron Datta, Sen y Zick.¹³⁰ En su trabajo de investigación publicado en 2016 desarrollaron un método que permite explicar los resultados que se obtienen mediante aprendizaje automático, introduciendo unas medidas de influencia cuantitativa de entrada (en inglés, *quantitative input influence*, QII) que posibilitan conocer la influencia que los datos o variables introducidos (*inputs*) han tenido en el resultado (*output*).¹³¹ Ello permite explicar cómo ha llegado el sistema a una decisión concreta que, además, los propios autores ejemplifican con una decisión crediticia. Aún está por ver la eficacia de este sistema, pero es evidente que abre una puerta a sistemas algorítmicos más transparentes, que se ajusten a las exigencias legales y que eviten un uso arbitrario y abusivo de la IA que perjudique a los consumidores.

En esta misma línea se dirigen también las técnicas de inteligencia artificial explicable (en inglés, *explainable artificial intelligence*, XAI), cuyo objetivo es diseñar los algoritmos de manera que ellos mismos puedan explicar su propio funcionamiento y los factores que tienen en cuenta para dar un cierto resultado, convirtiendo la *black box* en una *glass box*.¹³² Asimismo, facilitan el proceso de proporcionar explicaciones, ya que estas técnicas se dan de manera que resulten comprensibles al receptor, que en este caso es el consumidor.¹³³ Así, se intenta evitar que cuando se tengan que prestar dichas explicaciones, se conviertan en un mero formalismo y el interesado realmente no tenga información que le permita entender los resultados e impugnar la decisión, desvirtuándose por completo el contenido de su derecho.

En este mismo sentido se encamina el artículo 18.8a DCC, que obliga al prestador a dar una explicación clara y comprensible cuando la evaluación crediticia se haga a través de medios automatizados. Que las explicaciones se adecuen al nivel de comprensión de un usuario medio, y no al de un experto (a pesar de que pueden verse como una renuncia a una explicación precisa y detallada), puede ser favorable para que no se desvelen secretos comerciales, que es la baza que las empresas utilizan para no proporcionar explicaciones suficientes. Esto se debe a que la información que se proporcione debe ser acotada y sencilla, simplificada para que el consumidor pueda comprenderla.

130. Maja BRKAN, «Do algorithms rule the world?», p. 21.

131. Anupam DATTA, Shayak SEN y Yair ZICK, «Algorithmic transparency via quantitative input influence: theory and experiments with learning systems», en *2016 IEEE Symposium on Security and Privacy*, Los Alamitos (CA), IEEE Computer Society, 2016, p. 598, <<https://doi.org/10.1109/sp.2016.42>> (consulta: abril 2024).

132. Paul VOGEL, «A “Right to Explanation” for Algorithmic Decisions?», p. 56.

133. Philipp HACKER y Jan-Hendrik PASSOTH, «Varieties of AI explanations under the law», p. 362 y 365.

3.2.5. Secretos comerciales: ¿excusa o necesidad?

El otro problema al que se enfrenta el derecho de explicación es el secreto comercial al que las empresas se aferran para no dar a conocer cómo se obtiene el cálculo del *score* y, por tanto, su funcionamiento, los datos que se procesan y su peso respectivo. Ello puede tener consecuencias muy graves en la transparencia, que es un elemento clave de la protección de datos, y en la evitación de la discriminación. Pero la mayor contrariedad en este aspecto proviene de la negligencia con la que el legislador europeo y otros operadores jurídicos han abordado esta cuestión, ya que no han dedicado muchos esfuerzos a prestar atención a este evidente conflicto de intereses.

El RGPD se limita a exponer la existencia de un conflicto de intereses y la necesidad de encontrar un equilibrio entre ambos derechos, pero no propone soluciones o indicaciones sobre cómo se han de ponderar. El abogado general del TJUE, en sus conclusiones para el asunto SCHUFUFA, en cambio, sí que parece más consciente de la necesidad de proponer una solución. En concreto, entiende que es necesario conocer qué datos y qué peso ponderado tienen para satisfacer el derecho a conocer la lógica subyacente.¹³⁴ La sentencia del asunto SCHUFUFA directamente guarda silencio en este aspecto que resulta clave en el caso que se planteó. Precisamente el conflicto se derivó, en parte, de la negativa de SCHUFUFA a proporcionar información sobre el *score* a la demandante utilizando como pretexto los secretos comerciales.

En el RGPD el considerando 63 afirma que conocer la lógica implícita del tratamiento automatizado no puede afectar negativamente los derechos de terceros, y menciona especialmente los secretos comerciales. Seguidamente, da un paso atrás y vuelve a recordar que ello no puede significar que se niegue toda la información al interesado. Su redacción es confusa, en el sentido de que no se puede descifrar por cuál de los intereses en conflicto se inclina. El GTPD-29 se aproxima a esta cuestión en términos similares, pues únicamente alude al ya citado considerando 63. Por tanto, de los recursos de donde se podría conseguir una respuesta más concluyente, no se obtiene indicio alguno que ayude a disipar las dudas al respecto.

Además, a nivel internacional se encuentra en proceso de negociación un acuerdo comercial sobre comercio electrónico promovido por la Organización Mundial del Comercio (World Trade Organization, WTO), en el que participa la UE, que puede implicar una dificultad añadida en este sentido porque es probable que contenga una prohibición de acceso al código fuente de los algoritmos por parte de los gobiernos, de manera que será más difícil llevar a cabo controles de los sistemas automatizados,¹³⁵ como los que elaboran perfiles para el *credit scoring*.

134. Asunto C-634/2021, conclusiones del abogado general Sr. Priit Pikamäe, párr. 58.

135. Zofia BEDNARZ y Linda PRZHEDETSKY, «AI opacity in the financial industry», p. 78.

Sin embargo, parece necesario hacer una ponderación justa y proporcionada de ambos derechos, atendiendo a los intereses en conflicto. De esta forma, sería problemático que la empresa de información crediticia o el banco que desarrolla el modelo con el que realizará el *credit scoring*, pueda blindarse de cualquier obligación de explicar la lógica subyacente a través de los secretos comerciales. Resulta desproporcionado que se obtenga un gran lucro y un gran poder a costa de procesar y utilizar esos datos y que ello no lleve aparejada una responsabilidad acorde.

3.2.5.1. Preceptos normativos contrarios a la protección absoluta del secreto comercial

Cabe señalar que, a pesar de que la UE directamente no ha abordado este conflicto de intereses, o al menos no lo ha hecho con la contundencia y determinación suficientes, existen varias disposiciones en normativa diversa que podrían contribuir a pensar que el secreto comercial no siempre prevalece.

En primer lugar, si acudimos a la Directiva de secretos comerciales,¹³⁶ en su artículo 5d se prevé poder excepcionar los secretos comerciales en el supuesto de que se hayan de proteger intereses legítimos reconocidos por la UE. En este caso, la protección de datos parece que podría cumplir con este requisito, ya que está también salvaguardado como derecho en el artículo 8 de la Carta Europea de Derechos Fundamentales, que constata el gran valor que tiene a nivel europeo.

En segundo lugar, el Reglamento de IA contiene varios preceptos que se decantan por el derecho a la información y la transparencia de los sistemas de IA. En este instrumento normativo encontramos por primera vez un verdadero posicionamiento por parte de la UE en favor de la transparencia por encima del secreto comercial. Así, por ejemplo, el considerando 71 cree necesario poseer información, entre otras cosas, sobre los algoritmos, sobre los datos utilizados por el sistema de IA y sobre su funcionamiento durante todo su ciclo de vida, para verificar que se cumple con las exigencias impuestas por el Reglamento. Por otro lado, el artículo 74.13 permite a las autoridades competentes de vigilancia del mercado acceder al código fuente cumpliendo ciertos requisitos. Esto probablemente lo avalaría el artículo 5 de la Directiva de secretos comerciales, confirmando lo que se había propuesto anteriormente: que la protección de datos es un interés legítimo salvaguardado por la UE. Finalmente, el artículo 78 permite y da por hecho que puede ser necesario desvelar información

136. Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas, DOUE núm. 157 (15 julio 2016).

sujeta a secreto comercial, aunque imponiendo un deber de confidencialidad a las autoridades involucradas.

Una postura similar se ha adoptado también tanto en el Reglamento de servicios digitales¹³⁷ como en el Reglamento de mercados digitales.¹³⁸ A pesar de alejarse un poco del ámbito que nos concierne en este trabajo, resulta pertinente porque la ponderación de intereses que se hace es la misma. Ambas normativas permiten acceso y explicaciones detalladas sobre el algoritmo a la Comisión Europea y, en el caso del Reglamento de servicios digitales, también a la autoridad competente encargada de supervisar su cumplimiento,¹³⁹ que es el coordinador de servicios digitales. Así, cualquiera de ellos podrá exigir explicaciones relativas al diseño, la lógica, el funcionamiento y la realización de pruebas de sus sistemas algorítmicos.¹⁴⁰

Sin embargo, cabe hacer una precisión a todo esto: no es lo mismo proporcionar esta información a autoridades competentes, como tribunales o autoridades de vigilancia, que a todo consumidor que solicite información sobre la lógica subyacente del modelo de *credit scoring*. Y ello por la falta de confidencialidad y por el consecuente riesgo que puede suponer que cualquiera que lo solicite pueda tener acceso a información confidencial. Sin embargo, esto no debe servir como pretexto para directamente no conceder la información de los artículos 13, 14 y 15 RGPD.

A nivel estatal, se ha permitido a personas que no ejercen competencias con tanta autoridad como las mencionadas anteriormente, el acceso a información susceptible de constituir secretos comerciales. Así lo ha dispuesto el Estatuto de los trabajadores en una modificación reciente.¹⁴¹ Su artículo 64.4d establece:

El comité de empresa, con la periodicidad que proceda en cada caso, tendrá derecho a:

[...]

d) ser informado por la empresa de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial que afectan a

137. Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de servicios digitales), DOUE núm. 277 (27 octubre 2022).

138. Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de mercados digitales), DOUE, núm. 265 (12 octubre 2022).

139. Emily M. WEITZENBOECK, «User Empowerment in the Age of Algorithms», en Andrej SAVIN y Jan TRZASKOWSKY (ed.), *Research handbook on EU Internet Law*, 2ª ed., Cheltenham, Edward Elgar Publishing, 2023, p. 407.

140. Reglamento de servicios digitales, art. 40.3.

141. Adrián PALMA ORTIGOSA, *Decisiones automatizadas y protección de datos*, p. 197 y 198.

la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles.

El comité de empresa es un órgano representativo de los trabajadores de una empresa determinada, formado por ellos mismos. Por tanto, si se ha permitido y priorizado que personas que no tienen en absoluto competencias análogas a las de las personas autorizadas por el Reglamento de IA y los Reglamentos de servicios y mercados digitales, parece difícil comprender por qué un consumidor afectado por el *score* crediticio no podría hacer lo mismo, ya que no se encuentra en una situación muy dispar respecto a la de los trabajadores, a los que sí se ha concedido acceso a información susceptible de constituir secretos comerciales.

Esto, además, supone un avance significativo en el derecho privado que podría extrapolarse a otros ámbitos, como la concesión de créditos, además de poder constituir el inicio de una nueva tendencia en la consecución de equilibrios reales y sustantivos en este choque de derechos que hasta ahora se encontraba estancado en obligaciones y derechos difusos. Además, cabe destacar que el hecho de que la empresa tenga que informar a los trabajadores implica primero que esta conozca el funcionamiento del algoritmo. Esta asunción resulta especialmente pertinente al asunto SCHUFa, en el cual el TJUE hizo todo lo contrario, pues descargó al banco/entidad crediticia de toda obligación de conocimiento y explicación respecto del tratamiento que se hacía de los datos y de su resultado posterior.

3.2.5.2. Existencia de medios para proteger el secreto comercial

En otro orden de cosas, es significativa la insistencia en denegar cualquier petición de información sobre la lógica subyacente, cuando existen medios suficientes para cumplir con la obligación de explicación y preservar adecuadamente el secreto comercial.

En primer lugar, el propio abogado general del TJUE en el asunto SCHUFa, en su única mención de este conflicto, expuso que el hecho de que la información que se haya de facilitar sea comprensible para el interesado, precluye «ya la posibilidad de una obligación de divulgar el algoritmo, habida cuenta de su complejidad».¹⁴²

En segundo lugar, cabe mencionar que tanto en la Directiva sobre reclamación de daños derivados de las infracciones del derecho de la competencia¹⁴³ como en la

142. Asunto C-634/2021, conclusiones del abogado general Sr. Priit Pikamäe, párr. 57.

143. Directiva 2014/104/UE del Parlamento Europeo y del Consejo, de 26 de noviembre de 2014, relativa a determinadas normas por las que se rigen las acciones por daños en virtud del derecho nacional, por infracciones del derecho de la competencia de los estados miembros y de la Unión Europea, DOUE

Ley de enjuiciamiento civil (en adelante, LEC), se establecen medidas protectoras para acceder a fuentes de prueba susceptibles de contener información confidencial. El artículo 283 bis^b LEC, que parte del considerando 18 de la citada Directiva, establece las medidas que se deberán adoptar. Entre ellas encontramos las de llevar a cabo las audiencias a puerta cerrada o restringir su acceso, eliminar la información especialmente sensible de los documentos que la contengan, etc. Por tanto, existen medios para acceder a información sensible garantizando la confidencialidad, de manera que si esto se prevé en el seno de los procesos judiciales en acciones por daños en la competencia, no parece que haya inconveniente en que ello se pueda extrapolar a otros ámbitos, como el bancario y el *credit scoring*.

Es preciso decir que en materia de competencia el Tribunal Federal de Justicia de Alemania el pasado febrero de 2024 se pronunció a favor de revelar secretos comerciales a los competidores en un procedimiento de investigación sobre falseamiento de la competencia, atendiendo al principio de proporcionalidad.¹⁴⁴ Esta sentencia resulta especialmente relevante porque, por primera vez, se resuelve a favor de otros intereses que colisionan con los secretos comerciales y, particularmente, a favor de competidores. A nuestro entender, ello resulta más comprometedor que revelar secretos comerciales a un particular, cuyo único interés es conocer cómo se ha tomado una decisión determinada para poder impugnarla, sin con ello poder obtener ningún lucro. Por tanto, sería del todo incongruente e inverosímil que se siguiera negando al interesado de manera rotunda el acceso a la lógica subyacente.

En tercer lugar, existen formas alternativas para explicar cómo se calcula el *score* sin comprometer los secretos comerciales. Por ejemplo, podría facilitarse la información explicando las categorías de datos que se tienen en cuenta y el valor correspondiente que se les otorga de forma «ruidosa» (*in a noisy fashion*). Es decir, dar unos intervalos en vez de porcentajes exactos.¹⁴⁵ Otra manera podría ser a través de las demostraciones contrafactuales consistentes en explicar qué parámetros personales hubieran hecho que la decisión fuera otra¹⁴⁶ y han sido decisivos para no conceder el crédito. Esta es una medida muy útil para el consumidor porque le permite entender la decisión, detectar si ha habido errores o incongruencias y adaptarse a los requisitos de la máquina para poder obtener el crédito en el futuro. Por ejemplo, en el supuesto de que el factor decisivo sea que si se hubiera tenido más ingresos el *score* hubiera sido satisfactorio, el consumidor tendría la posibilidad de facilitar información adicional

núm. 349 (5 diciembre 2014).

144. «Google (Schutz von Betriebs— Und Geschäftsgeheimnissen Bei Beteiligung von Wettbewerbern Durch DasBundeskartellamt)», <<https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2024/2024033.html>> (consulta: 17 mayo 2024); nota de prensa relativa al BGH (Tribunal Federal de Justicia de Alemania), Sentencia de 20 de febrero de 2024, KVB 69/23 13.

145. Philipp HACKER y Jan-Hendrik PASSOTH, «Varieties of AI explanations under the law», p. 350.

146. Zofia BEDNARZ y Linda PRZHEDETSKY, «AI opacity in the financial industry», p. 90.

que a lo mejor no se había tenido en cuenta (ingresos que se desconocían) o bien la de solicitar un crédito inferior que se ajustara más a su situación económica.¹⁴⁷ Otras opciones que facilitarían la transparencia sin comprometer la confidencialidad, y que han sido mencionadas en apartados anteriores, son las técnicas XAI y el método de *quantitative input reference*. Ambas son alternativas explicativas para la IA que permiten informar sobre cómo ha llegado el modelo a un resultado concreto sin abrir la caja negra.

Finalmente, cabe hacer referencia a FICO, una de las mayores empresas de información crediticia de Estados Unidos, que utiliza medios automatizados para elaborar los *credit scorings*.¹⁴⁸ Es interesante el contraste con otras empresas de información crediticia por el nivel de transparencia que provee en su página web. Publica los porcentajes que otorga a cada factor que se tiene en consideración para calcular el *score*:¹⁴⁹ 35 % al historial de pagos, 30 % a las deudas, 15 % a la duración del historial crediticio, 10 % a los nuevos créditos y 10 % a la combinación de créditos. Además, explica de cada factor qué se tiene en cuenta exactamente y por qué. Por ejemplo, explica qué componentes se tienen en cuenta para valorar el 35 % correspondiente al historial de pagos, los datos que en caso de tenerse afectarían negativamente al *score* y consejos para mejorarlo.¹⁵⁰

Toda esta información es la que tribunales y operadores jurídicos entendieron que era significativa sobre la lógica implícita del artículo 15 RGPD, por lo que remitimos a apartados anteriores.

Por ello resulta difícil comprender por qué se plantean tantos problemas en Europa acerca de dar esta información y se alude rápidamente a secretos comerciales, cuando existen ejemplos en otros países donde esto no sucede y se proporciona voluntariamente. Además, existen medios muy diversos para facilitar dicha información, por lo que persistir en negar un acceso total a la lógica subyacente no hace sino despertar ciertas dudas sobre por qué no se quiere dar una información que empresas análogas no tienen reparos en facilitar.

147. Sergio GENOVESI *et al.*, «Standardizing fairness-evaluation procedures», p. 10 y 11.

148. Hicham SADOK, Fadi SAKKA y Mohammed El Hadi El MAKNOUZI, «Artificial intelligence and bank credit analysis: a review», *Cogent Economics and Finance*, núm. 10 (2022), p. 6, <<https://doi.org/10.1080/23322039.2021.2023262>> (consulta: febrero 2024).

149. Zofia BEDNARZ y Linda PRZHEDETSKY, «AI opacity in the financial industry», p. 73.

150. FICO, «What's in my FICO® Scores?», <<https://www.myfico.com/credit-education/whats-in-your-credit-score>> (consulta: mayo 2024).

3.2.5.3. Nueva cuestión prejudicial en el TJUE de un tribunal austriaco

Para finalizar, resulta pertinente destacar un caso reciente que ha supuesto la interposición por parte de un tribunal austriaco de una cuestión prejudicial en el TJUE¹⁵¹ para que dirima cómo se han de conjugar los derechos de los artículos 15.1*b* y 22.3 RGPD con el secreto comercial de las empresas de información crediticia. De los hechos del caso se extrae que a una persona le fue denegada la posibilidad de contratar con una compañía telefónica debido a su *score* crediticio. El consumidor requirió a la Agencia de Protección de Datos austriaca para que solicitara a la empresa de información crediticia que le facilitara información significativa sobre la lógica subyacente del algoritmo que había elaborado el *score*. Sin embargo, la empresa se negó aludiendo a que la información solicitada era constitutiva de secreto comercial y se acudió a los tribunales. El Tribunal Administrativo de Viena (Verwaltungsgericht Wien) plantea entonces una cuestión prejudicial al TJUE para que aclare cómo se ha de dirimir este conflicto.¹⁵²

Este caso resulta interesante por dos motivos. En primer lugar, porque muestra que a día de hoy, tras varios años de aplicación del RGPD, esta cuestión no ha quedado resuelta por ninguna autoridad europea ni por otros operadores jurídicos. Y ello a pesar de la trascendencia que tiene y la infinidad de casos que se han podido dar a raíz de que el interesado ejerza un derecho tan relevante como el del artículo 15.1*b* RGPD. El propio tribunal austriaco lo reitera en la formulación de las preguntas que remite al TJUE:

[...] para ejercer estos dos derechos, es necesario que el interesado obtenga primero información suficiente sobre los datos tratados y la lógica implícita en el proceso de toma de decisiones automatizadas [...], de modo que pueda comprender [...] y comprobar su exactitud.¹⁵³

En segundo lugar, el tribunal austriaco también pregunta, para el caso de que efectivamente la información que se ha de conceder fuera constitutiva de secretos comerciales, «si esta tensión puede resolverse, por ejemplo, revelando la información

151. Sebastião BARROS VALE y Gabriela ZANFIR-FORTUNA, *Automated-Making Under the GDPR*, p. 19.

152. Asunto C-203/22, CK contra Dun & Bradstreet Austria [2022], petición de decisión prejudicial planteada por el Verwaltungsgericht Wien (Austria) el 16 de marzo de 2022.

153. Verwaltungsgericht Wien (Tribunal Administrativo de Viena), VGW-101/042/791/2020-44, 11 de febrero de 2022, ap. III, p. 29. Traducción: «Um diese beiden Rechte wahrzunehmen ist es aber erforderlich, dass der Betroffene zuvor eine ausreichende Auskunft über die verarbeiteten Daten und die involvierte Logik der automatisierten [...] erlangt, sodass er diese Weise in der Lage ist, die automatisierte Entscheidungsfindung nachzuvollziehen und auf deren Richtigkeit».

que debe clasificarse como secreto comercial [...] exclusivamente a la autoridad o al tribunal».¹⁵⁴ Por tanto, no parece desencaminada la opción propuesta anteriormente de que se puedan revelar los secretos comerciales adoptando medidas de confidencialidad como las que prevén la LEC y la Directiva sobre reclamación de daños derivados de las infracciones del derecho de la competencia. De esta forma, se podría encontrar un punto intermedio entre desvelar por completo la fórmula algorítmica y todo lo que queda cubierto por el secreto comercial, y no facilitar ningún tipo de información que impida al consumidor ejercer los derechos que el RGPD le concede para poder impugnar adecuadamente la decisión automatizada de su artículo 22.

De todo lo mencionado anteriormente, cabe extraer la conclusión de que los secretos comerciales pueden suponer una dificultad añadida a la hora de dar explicaciones adecuadas en el sentido del artículo 15.1*b* RGPD, pero no deben utilizarse como pretexto para no proporcionarlas en absoluto. Existen medios diversos que mitigan el impacto negativo de revelar información sensible y garantizan la confidencialidad, por lo que una negación sistemática a ello puede llevar a pensar que lo que realmente sucede es que no se quiere dar la información y, por tanto, la pregunta que irremediablemente sigue es por qué.

3.2.6. *Todos se lavan las manos: ¿laguna normativa de protección jurídica?*

Tanto el órgano jurisdiccional remitente como el abogado general del TJUE en sus conclusiones y el TJUE en la sentencia del asunto SCHUFA, entienden que si no se interpretase el propio *score* como una decisión exclusivamente automatizada del artículo 22 RGPD, existiría una laguna normativa que impediría al interesado obtener la información que le corresponde por derecho.¹⁵⁵ Esto se debe a que tanto la empresa que elabora el *score* como el banco intentan desentenderse del deber de información del artículo 15.1*b* RGPD. Por tanto, la forma de evitar que lo hagan implica atribuir a la empresa de información crediticia el deber de información, considerando el *score* la decisión automatizada del artículo 22 RGPD.

El razonamiento que se sigue es que, de lo contrario, la empresa de información crediticia se ampararía en que es un intermediario y que el resultado que transmite (*score*) es más bien orientativo, ya que el banco aún tiene la última palabra respecto de si concede o no el crédito. Si no fuera, pues, una decisión a efectos del artículo 22

154. Verwaltungsgericht Wien, VGW-101/042/791/2020-44, ap. VIII, p. 38. Traducción: «[...] ob dieses Spannungsverhältnis etwa dahingehend aufzulösen ist bzw. aufgelöst werden kann, indem die als Geschäftsgeheimnis [...] einzustufenden Informationen ausschließlich der Behörde oder dem Gericht offen gelegt werden [...]».

155. Asunto C-634/2021, O. Q. contra Land Hessen con intervención de SCHUFA, párr. 61.

RGPD, no tendría que cumplir con las obligaciones que ello conlleva;¹⁵⁶ es decir, con la obligación de facilitar información significativa sobre la lógica subyacente del artículo 15.1*b* RGPD, para que el interesado pueda ejercer adecuadamente los derechos del artículo 22.3 RGPD (intervención humana, impugnar la decisión y expresar el punto de vista).

Por otro lado, se entiende que el banco no puede cumplir con el deber de información del artículo 15.1*b* RGPD porque no dispone de la información,¹⁵⁷ ya que ni gestiona ni controla el algoritmo o los datos que este procesa, sino que subcontrata a un tercero (SCHUFA) para que lo haga. Por ese motivo, para el abogado general del TJUE resulta necesario interpretar el artículo 22 RGPD de manera que incluya el *score*. Así se evitaría que el interesado se viera perjudicado por la delegación de funciones¹⁵⁸ del banco en un tercero al que ha subcontratado para llevar a cabo los *scores* que, además, predeterminan la evaluación crediticia.

Resulta sorprendente que esta haya sido la conclusión a la que han llegado el abogado general y posteriormente el TJUE, que suscribió su razonamiento. Esto es debido a que, a pesar de que estaba claro que no era la intención del legislador otorgar un derecho de información vacío de contenido, parece que tampoco se tendría que descargar de toda obligación al banco, que es, en definitiva, el que ha de evaluar la solvencia y el que decide subcontratar el servicio de generación de *scores*.¹⁵⁹

Ello, sobre todo, cuando la ABE indica que, cuando los bancos empleen innovaciones tecnológicas para la concesión de créditos (como es el caso, aunque lo hagan a través de un tercero), han de comprender los modelos utilizados y su metodología, y han de conocer los datos que se introducen y su calidad.¹⁶⁰ Por lo tanto, si los bancos cumplieran debidamente con las directrices de la ABE, que sin ser vinculantes constituyen buenas prácticas y que la propia DCC tiene en consideración a efectos interpretativos, esta supuesta laguna normativa no existiría y se podría atribuir el deber de información a los bancos.

Por eso, no tiene sentido que la sentencia desplace toda la responsabilidad a SCHUFA e ignore las responsabilidades que los bancos tienen de conocer cómo trabaja un tercero con el que contratan, por un lado,¹⁶¹ y las que deberían tener al poder sus operaciones afectar significativamente a la situación económica de sus clientes, por el otro.

156. Asunto C-634/2021, conclusiones del abogado general Sr. Priit Pikamäe, párr. 48.

157. Asunto C-634/2021, O. Q. contra Land Hessen con intervención de SCHUFA, párr. 63.

158. Asunto C-634/2021, conclusiones del abogado general Sr. Priit Pikamäe, párr. 50.

159. Véase también Esther ARROYO AMAYUELAS, «El scoring de Schufa», p. 10 de la paginación original.

160. EUROPEAN BANKING AUTHORITY (EBA), *Directrices sobre concesión y seguimiento de préstamos*, párr. 54.

161. Esther ARROYO AMAYUELAS, «El scoring de Schufa», p. 11 y 15 de la paginación original.

Igualmente, tener que acudir a SCHUFA para reclamar la información en lugar de dirigirse al banco o a la entidad crediticia donde ha solicitado el crédito, puede ser un obstáculo añadido para el consumidor porque le será más difícil identificar y reclamar a un tercero desconocido que no acudir al banco, que es, probablemente, con el que ha mantenido más contacto.

3.3. FALLO DE LA SENTENCIA

Como se ha podido avanzar en los apartados anteriores, el TJUE hizo suya la respuesta que el abogado general proporcionó en sus conclusiones del asunto SCHUFA. De esta manera, ambos entendieron que la generación de un *score* por una empresa de información crediticia que transmitía a un tercero, el cual le daba un valor determinante para establecer, ejecutar o poner fin a una relación contractual con la persona objeto del *score*, es una decisión a efectos del artículo 22 RGPD.¹⁶²

Con esta respuesta se han valorado varios de los aspectos mencionados en este trabajo relativos a la intervención humana, al concepto de *decisión* y al derecho de información del artículo 15.1*b* RGPD. Con esta decisión el Tribunal ha conseguido dar respuesta a algunos de los interrogantes que preocupaban a la doctrina en esta materia: ha señalado qué se entiende por *intervención humana* y cuándo será suficiente para precluir la aplicación del artículo 22 RGPD, ha confirmado la existencia de un derecho de información posterior a la decisión y ha precisado el alcance del artículo 15.1*b* RGPD, es decir, qué se entiende por información significativa sobre la lógica subyacente.

Sin embargo, ha desperdiciado la ocasión de precisar cómo se debería resolver el conflicto entre el derecho de información y los secretos comerciales. No obstante, el Tribunal Administrativo de Viena (Verwaltungsgericht Wien) ha planteado una cuestión prejudicial que está pendiente de ser resuelta por el TJUE¹⁶³ y que le permitirá abordar este conflicto directamente.

Finalmente, resulta conveniente mencionar algunos de los reparos que se pueden tener respecto a la decisión del TJUE en el asunto SCHUFA. Como ya se ha introducido en el apartado anterior, resulta problemático que se haya eximido del deber de informar de la lógica subyacente a los bancos o entidades crediticias que utilizan los *scores* y se haya descargado toda la responsabilidad en la empresa de información crediticia. La contrariedad que se aprecia es que, para impedir la existencia de una supuesta laguna normativa, esta responsabilidad haya acabado atribuyéndose a la empresa que genera el *score*, acudiendo al pretexto de que, como los bancos no generan

162. Asunto C-634/2021, O. Q. contra Land Hessen con intervención de SCHUFA, párr. 73.

163. Asunto C-203/22, CK contra Dun & Bradstreet Austria GmbH.

el *score*, no conocen cómo se elabora ni su lógica subyacente. Es por este motivo que, en gran parte, se acaba calificando al *score* de decisión exclusivamente automatizada según el artículo 22 RGPD.

Sin embargo, resulta poco convincente la excusa a la que alude la entidad crediticia para lavarse las manos respecto a sus deberes de información. En primer lugar, porque es suyo el deber de evaluar la solvencia de sus clientes a la hora de conceder el crédito y también es suya la decisión de delegar a un tercero la generación de un valor que determine la capacidad futura de devolución y que acriticamente considera para decidir sobre la concesión del crédito. Y, en segundo lugar, porque lo habitual es conocer con quién y qué se está contratando. De manera que los bancos o entidades de crédito, como cualquier otra empresa que subcontrate servicios a terceros, en los acuerdos que alcancen deberían conocer los pormenores de cómo se va a llevar a cabo la subcontratación. Por tanto, resulta improbable que el banco desconozca los detalles de cómo se realiza el *score* realmente. Pero sería incluso peor si se desconocieran efectivamente, pues supondría una negligencia por su parte no conocer el proceso de un elemento esencial y determinante de la evaluación crediticia que, además, se ha de ajustar a unos estándares impuestos por la DCC.

Por consiguiente, en este trabajo no se cuestiona la conclusión del TJUE acerca de considerar el *score* una decisión automatizada del artículo 22 RGPD para poder vincularle las garantías que dicho precepto concede por ser un acto de especial relevancia en la decisión final,¹⁶⁴ sino que se cuestiona cómo se ha llegado a ella. Es decir, las razones que han conducido a dar esta respuesta a la cuestión prejudicial planteada por el tribunal alemán.

4. UN CAMBIO DE MENTALIDAD: LA NUEVA REFORMA DE LA DIRECTIVA DE CRÉDITO AL CONSUMO Y EL REGLAMENTO DE INTELIGENCIA ARTIFICIAL

Recientemente el legislador europeo ha puesto el foco en adaptar la normativa existente al creciente uso de la IA y en aprobar un instrumento normativo que regule exclusivamente el desarrollo y el uso de la IA. La reforma operada en la DCC en octubre de 2023 y el ya aprobado Reglamento de IA son los instrumentos que nos han interesado en este trabajo y que muestran los intentos por parte de la UE de soslayar los efectos negativos que la IA puede tener en distintas esferas de la realidad. Por ello

164. Lorenzo COTINO HUESO, «La primera sentencia del TJUE sobre decisiones automatizadas y sus implicaciones para la protección de datos del Reglamento de IA», *Diario La Ley*, núm. 80 (2024), sección II.

resulta pertinente hacer un esbozo de todas las novedades que han traído consigo y que se han ido mencionando de forma diseminada en este trabajo.

En cuanto a la reforma de la DCC, se ha considerado necesario incorporar aspectos relacionados con la IA debido a su uso intensivo en sectores como el de la concesión de créditos en los que los consumidores son la parte más débil. Como ya sabemos, los algoritmos que emplea la IA se basan en conductas pasadas propias y de otros para determinar la probabilidad de que una persona devuelva el crédito. Como ello tiene consecuencias directas para los consumidores a la hora de solicitar un crédito, sobre su concesión, sobre el tipo de interés que se le aplicará, etc., resulta fundamental que se aborden estas cuestiones no solo desde el RGPD, sino también desde la propia DCC, pues la protección de datos es también protección al consumidor.¹⁶⁵

Como ya se ha dicho, una de las grandes novedades que la DCC trae consigo respecto al RGPD es la extensión de las garantías y derechos que el artículo 22 RGPD predicaba de las decisiones exclusivamente automatizadas, a cualquier decisión automatizada. Es decir, la intervención humana, el derecho a una explicación sobre la lógica subyacente, expresar el propio punto de vista y solicitar una revisión, ahora son derechos que se ostentan con independencia del grado de automatización de la decisión. El artículo 18.6 DCC solo menciona el «procesamiento automatizado», sin distinguir si el procesamiento de datos es únicamente automatizado o no.

El abogado general del TJUE en las conclusiones para el asunto SCHUFA utiliza un razonamiento similar al que sigue el artículo 18 DCC: no hacer distinción entre diversos grados de automatización. De esta forma, para él, el factor decisivo para que el *score* se considere por sí solo una decisión a efectos del artículo 22 RGPD es el efecto que tiene la «decisión» en el interesado.¹⁶⁶ Es precisamente esta lógica la que probablemente también llevó a la DCC a conceder las mismas garantías a decisiones exclusivamente automatizadas y semiautomatizadas. Esto responde a que los efectos que las decisiones automatizadas, en sentido amplio, tienen en la persona es lo que realmente se quiere proteger. El abogado general acierta cuando incide en que lo esencial son los efectos de la decisión y, del mismo modo, la DCC entiende que esos efectos negativos también pueden tener lugar en tratamientos semiautomatizados en los que hay intervención humana. Es consciente de que, aunque exista dicha participación humana, la decisión sigue basándose en un *score* que es un tratamiento automatizado de datos, por lo que también traslada los efectos negativos de la automatización a la decisión final, aunque sea de forma más diluida.

Asimismo, la DCC es también novedosa en el sentido de que tiene en cuenta el uso del procesamiento de datos automatizado, y no solo la propia elaboración, como

165. Alexander ROBNAGEL y Christian L. GEMINN, «The GDPR Five Years On - A Retrospective from the Viewpoint of Consumers», *European Journal of Consumer Law*, año 2024, núm. 1, p. 109.

166. Asunto C-634/2021, conclusiones del abogado general Sr. Priti Pikamäe, párr. 43.

hace el RGPD. La legislación alemana en materia de protección de datos ya se había anticipado en este sentido.¹⁶⁷

Respecto al Reglamento de IA, es interesante el enfoque basado en el riesgo que ha utilizado para regular la creación, el desarrollo y el uso de sistemas que incorporan IA. El anexo III 5b considera que son sistemas de IA de alto riesgo los que se utilicen para evaluar la solvencia y establecer una calificación crediticia (*score*) en servicios privados esenciales. Esto puede ser uno de los grandes avances en el ámbito de la IA en la evaluación de solvencia. Ello implica que en este sector ahora debe cumplirse con las exigencias previstas para este tipo de sistemas, a pesar de que para obtener explicaciones adecuadas sobre el papel del sistema de IA y su funcionamiento aún sea necesario acreditar que los derechos fundamentales del interesado han sido perjudicados, por ejemplo. A pesar de ello, con la inclusión del Reglamento de IA en el marco normativo europeo ya no solo se derivan derechos y obligaciones del RGPD —desde la perspectiva de la protección de datos— y de la DCC —desde la de la defensa del consumidor—, sino también de este instrumento normativo en el que la IA es su razón de ser y se aborda en todas sus fases y formas.

Sin embargo, un detalle que se debe considerar es qué se entiende por *servicios privados esenciales*, pues solo cuando se lleve a cabo la evaluación de la solvencia para acceder a estos, se considerará un sistema de alto riesgo. El considerando 58 del Reglamento de IA pone como ejemplo los servicios relativos a la vivienda, la electricidad y los servicios de telecomunicación, pero queda por determinar si es una lista tasada. Una interpretación restrictiva tanto del anexo III como del citado considerando en lo que respecta a «servicios privados esenciales» podría constituir una limitación preocupante, pues podría suponer que otras calificaciones crediticias realizadas con IA para obtener financiación por otros motivos no fueran recogidas por el Reglamento de IA y carecieran de las garantías que se imponen a otras evaluaciones de solvencia.¹⁶⁸

Otra novedad que incorpora el Reglamento de IA es, como ya se ha mencionado, la cuestión de cómo se podrían explicar los sistemas de IA de aprendizaje autónomo, ya que tras su puesta en marcha sus propios creadores desconocen cómo han llegado a los resultados. Esta circunstancia no será ya un problema, pues quedan prohibidos. Los artículos 13 y 15 del Reglamento exigen que sus resultados se puedan interpretar de manera transparente y que funcionen de forma consistente durante todo su ciclo de vida.

Finalmente, el Reglamento de IA introduce la obligación de que los sistemas de alto riesgo incorporen durante su uso necesariamente intervención humana. Algo que, hasta ahora, tanto en el RGPD como en la DCC solo se preveía como un derecho

167. Bundesdatenschutzgesetz v. 30 de junio de 2017 (BGBl. S. 2097), § 31.

168. Gerald SPINDLER, «Algorithms, credit scoring», p. 243 y 244.

(*human out of the loop*) o, solo en el caso del RGPD, para descartar que fuera una decisión exclusivamente automatizada (*human in the loop*).

5. CONCLUSIONES

Tras un análisis intensivo de la doctrina académica, de las directrices y resoluciones de diversos operadores jurídicos expertos en la materia, así como de la jurisprudencia de los tribunales de diversos países europeos y poniendo el foco especialmente en el asunto SCHUFA, cabe destacar las siguientes conclusiones a las que se ha llegado en este trabajo.

La sentencia y también las conclusiones del abogado general del asunto SCHUFA han permitido abordar la cuestión de las decisiones automatizadas y la protección de datos en la concesión de créditos, que ya estaba pendiente en la doctrina desde tiempo atrás, y han arrojado luz en algunos aspectos inciertos.

En primer lugar, se ha precisado qué grado de intervención humana durante el proceso de evaluación crediticia es suficiente para precluir la aplicación del artículo 22 RGPD y, consiguientemente, no considerar una decisión exclusivamente automatizada a sus efectos. El razonamiento final ha secundado doctrina académica y jurisprudencial previa relativa a la necesidad de que dicha intervención sea significativa, de que se pueda influir y revertir la decisión dada por el sistema, si se considera necesario, y de que, por lo tanto, sirva de mero apoyo a una decisión final.

En segundo lugar, se ha confirmado la existencia de un derecho a una explicación *ex post* a la decisión crediticia individual, ya que se ha interpretado que dicha explicación ha de contener una información que necesariamente implica que esta explicación sea posterior. Asimismo, lo contrario supondría no poder ejercer los demás derechos del artículo 22.3 RGPD para impugnar la decisión.

En tercer lugar, se ha precisado exactamente qué información se ha de prestar al ejercer el artículo 15 RGPD, es decir, qué se entiende por «información significativa sobre la lógica» subyacente de una decisión automatizada. Las conclusiones del abogado general y de forma más sintética la sentencia, han secundado lo que ya iban apuntando la doctrina predominante y otros en este aspecto. Dicha información ha de comprender las razones que han conducido a una determinada calificación y los datos a los que se ha atribuido mayor importancia.

No obstante, el TJUE parece no haber sido consciente de la oportunidad que con este caso se le presentaba de abordar el preocupante obstáculo que suponen los secretos comerciales para impedir un cumplimiento real y efectivo del derecho de información expresado antes. Afortunadamente, esta cuestión no tardará en quedar dirimida, si eso es lo que realmente se quiere, ya que se ha planteado una cuestión prejudicial en el TJUE que está pendiente de resolverse y que directamente incide sobre cómo se han de conjugar los secretos comerciales con el derecho de información del RGPD.

Ciertamente, una de las mayores críticas a la Sentencia que este trabajo ha intentado reflejar es la creación de una «laguna normativa» para resolver este asunto del modo que se ha hecho. Se ha aludido al desconocimiento de las entidades crediticias sobre cómo se obtiene el *score* que ellas utilizan para determinar si se concede o no el crédito, y se ha desplazado toda la responsabilidad al tercero que subcontratan para elaborar los *scores*.

A nuestro entender, ello no parece razonable porque es suyo el deber de evaluar la solvencia de sus clientes. Además, lo razonable es conocer con quién se contrata y cómo se desempeñará la tarea encomendada. Lo que resulta desmesurado y alarmante es que se les exonere de responsabilidades inherentemente propias sencillamente porque existe otro sujeto que lo puede hacer mejor, cuando, en teoría, ambas deberían poder hacerlo igual de bien. Como ya se ha mencionado, aquí no se cuestiona el resultado al que ha llegado el Tribunal al considerar el *score* una decisión automatizada del artículo 22 RGPD, sino el camino que ha decidido recorrer para llegar a él.

Por lo que se refiere al impacto de la nueva reforma de la DCC y del Reglamento de IA en este ámbito, cabe mencionar que ha sido y va a ser muy significativo y positivo, aparte de que va a superar al RGPD en algunos aspectos cuestionables o a los que sencillamente no proporcionaba una solución clara.

Por un lado, la DCC ha eliminado la distinción que el RGPD hacía entre decisiones automatizadas y decisiones exclusivamente automatizadas, de manera que ambas llevarán aparejados los mismos derechos y garantías para el consumidor sometido a ellas. Esto es relevante, como se ha dicho, porque el efecto que pueden tener en el individuo puede ser el mismo independientemente de su grado de automatización. Además, incorpora a su regulación tanto el propio procesamiento de datos como el uso que se hace de él, superando también en este respecto al RGPD.

Por otro lado, el Reglamento de IA va a dar solución al problema que presentaban algunos sistemas por la imposibilidad de explicar su funcionamiento interno y, por ende, sus resultados debido a su capacidad de autoaprendizaje, ya que ha quedado prohibido su uso. Asimismo, los sistemas para evaluar la solvencia crediticia se consideran de alto riesgo si además afectan a derechos fundamentales del interesado, circunstancia que implicará la adopción de mayores garantías para este y obligaciones para quien los utilice.

En otro orden de cosas, cabe mencionar la cuestión del secreto comercial, que, a pesar de que se ha abordado en este trabajo, aún queda pendiente de ser resuelta por el TJUE, pero, como ya se ha dicho, lo hará próximamente. En este trabajo se ha intentado, a partir de la diversa normativa europea, de la jurisprudencia y de los avances tecnológicos existentes, determinar si se podría resolver el conflicto en favor del derecho de información y aventurar con base en qué instrumentos normativos se haría, así como el modo de ponderarlo con el secreto comercial. El posicionamiento que se adopta aquí es contrario a proteger de forma absoluta el secreto comercial, pues existen medios para asegurar un cierto nivel de confidencialidad sobre cómo

se han elaborado los algoritmos y, al mismo tiempo, proporcionar la suficiente información para poder contestar las decisiones que estos toman. De tal manera que, a nuestro entender, excusarse en el secreto comercial siembra ciertas dudas acerca de lo que realmente se quiere proteger.

Finalmente, resulta importante hacer una reflexión general. La IA es nuestro presente y ha venido para quedarse. Ello no impide aceptar que no todo lo que tenemos a nuestro alcance debe ser utilizado. Se ha de reflexionar sobre su utilidad, la mejora que conlleva y si los problemas asociados son soslayables y mínimos en comparación con las ventajas que aporta. A veces parece que esta reflexión no pueda ser considerada, que una propuesta tan «drástica» como prohibir el uso de ciertas tecnologías no pueda ser admisible. Afortunadamente, la normativa europea y especialmente el necesario Reglamento de IA parecen ser conscientes de esto y caminar hacia una ponderación real de poder y responsabilidad.

BIBLIOGRAFÍA

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS [AEPD]. *Adecuación al RGPD de tratamientos que incorporan inteligencia artificial. Una introducción*. Madrid: Agencia Española de Protección de Datos, 2020.
- ARROYO AMAYUELAS, E. «El scoring de Schufa». *InDret*, año 2024, núm. 3 [en prensa].
- BARROS VALE, S.; ZANFIR-FORTUNA, G. *Automated-making under the GDPR: Practical cases from courts and data protection authorities*. Washington: Future of Privacy Forum, 2022.
- BEDNARZ, Z.; PRZHEDETSKY, L. «AI opacity in the financial industry and how to break it». En: BEDNARZ, Zofia; ZALNIERIUTE, Monika [ed.]. *Money, power, and AI*. 1ª ed. Cambridge: Cambridge University Press, 2023.
- BIBER, S. E. *Between humans and machines: Judicial interpretation of the automated decision-making practices in the EU*. Luxemburg: University of Luxembourg, 2023 (Law Research Paper No. 2023-19). Disponible en línea en: <<http://dx.doi.org/10.2139/ssrn.4662152>> [consulta: abril 2024].
- BRKAN, M. «Do algorithms rule the world? Algorithmic decision-making in the framework of GDPR and beyond». *International Journal of Law and Information Technology*, vol. 27, núm. 2 (2019), p. 91-121.
- COLLADO-RODRÍGUEZ, N. «La evaluación de la solvencia mediante el uso de sistemas de IA». *Revista CESCO de Derecho de Consumo*, núm. 46 (2023), p. 41-67.
- COTINO HUESO, L. «La primera sentencia del TJUE sobre decisiones automatizadas y sus implicaciones para la protección de datos del Reglamento de IA». *Diario La Ley*, núm. 80 (2024).
- DATTA, A.; SEN, S.; ZICK, Y. «Algorithmic transparency via quantitative input in-

- fluence: theory and experiments with learning systems». En: *2016 IEEE Symposium on Security and Privacy*. Los Alamitos (CA): IEEE Computer Society, 2016, p. 598-617. <<https://doi.org/10.1109/sp.2016.42>> [consulta: abril 2024].
- DAVIS, P.; SCHWEMER, S. «Rethinking decisions under article 22 of the GDPR: implications for semi-automated legal decision-making». En: *Proceedings of the Third International Workshop on Artificial Intelligence and Intelligent Assistance for Legal Professionals in the Digital Workplace (LegalAIIA 2023), held in conjunction with ICAIL 2023* [en línea] (CEUR Workshop Proceedings; 3423). Disponible en línea en: <<https://dx.doi.org/10.2139/ssrn.4478107>> [consulta: marzo 2024].
- EUROPEAN BANKING AUTHORITY [EBA]. *Directrices sobre concesión y seguimiento de préstamos*. París: European Banking Authority, 2020.
- FERRETTI, F. «Consumer access to capital in the age of fintech and big data: the limits of EU law». *Maastricht Journal of European and Comparative Law*, núm. 25 (2018), p. 476-499.
- FICO. «What's in my FICO® scores?». *myFICO* [en línea], <<https://www.myfico.com/credit-education/whats-in-your-credit-score>> [consulta: mayo 2024].
- GAL, M. S.; ELKIN-KOREN, N. «Algorithmic consumers». *Harvard Journal of Law & Technology*, núm. 30 (2017), p. 309-353. Disponible en línea en: <<https://ssrn.com/abstract=2876201>> [consulta: marzo 2024].
- GENOVESI, S.; MÖNIG, J. M.; SCHMITZ, A. *et al.* «Standardizing fairness-evaluation procedures: interdisciplinary insights on machine learning algorithms in creditworthiness assessments for small personal loans». *AI Ethics*, vol. 4 (2024), p. 537-553, <<https://doi.org/10.1007/s43681-023-00291-8>> [consulta: febrero 2024].
- GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 (GTPD-29). *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679* [en línea]. Bruselas: Dirección General de Justicia de la Comisión Europea, 2018.
- HACKER, P.; PASSOTH, J. «Varieties of AI explanations under the law. From the GDPR to the AIA, and beyond». En: HOLZINGER, Andreas *et al.* [ed.]. *xxAI - Beyond Explainable AI*. Nueva York: Springer: 2022. Disponible en línea en: <<https://doi.org/10.1007/978-3-031-04083-2>> [consulta: febrero 2024].
- LAZCOZ, G.; HERT, P. de. «Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities». *Computer Law and Security Review*, núm. 50 (2023), p. 1-20.
- LODDER, A. R.; COOPER, Z. «Do algorithms need to be regulated?». En: SAVIN, Andrej; TRZASKOWSKI, Jan [ed.]. *Research handbook on EU Internet Law*. 2ª ed. Cheltenham: Edward Elgar Publishing Ltd., 2023.
- MAS BADIA, M. D. *Sistemas privados de información crediticia: Nueva regulación entre la protección y el crédito responsable*. 1ª ed. Valencia: Tirant lo Blanch, 2021.

- MEDINA GUERRERO, M. «El derecho a conocer los algoritmos utilizados en la toma de decisiones. Aproximación desde la perspectiva del derecho fundamental a la protección de datos personales». *Teoría y Realidad Constitucional*, núm. 49 (2022), p. 151-171.
- MORGADO REBELO, D.; CAMPOS FERREIRA, F. «AI-based consumer's creditworthiness assessment: era of automation, future of scoring and the EU policy-making on automated decision-making». En: MOREIRA, Sónia [ed.]. *E. Tec yearbook: Industry 4.0: legal challenges*. Minho: Universidade do Minho Centro de Investigação em Justiça e Governação (JusGov), 2022.
- NAVAS NAVARRO, S. *Inteligencia artificial: Tecnología y derecho*. 1ª ed. Valencia: Tirant lo Blanch, 2017.
- PAAL, B. «Artificial Intelligence as a Challenge for Data Protection Law». En: VOENEKY, Silja et al. [ed.]. *The Cambridge handbook of responsible artificial intelligence*. Cambridge: Cambridge University Press, 2022.
- PALMA ORTIGOSA, A. *Decisiones automatizadas y protección de datos: Especial atención a los sistemas de inteligencia artificial*. 1ª ed. Madrid: Dykinson, 2022.
- POSCHER, R. «Artificial intelligence and the right to data protection». En: VOENEKY, Silja et al. [ed.]. *The Cambridge handbook of responsible artificial intelligence*. Cambridge: Cambridge University Press, 2022.
- ROBNAGEL, A.; GEMINN, C. L. «The GDPR five years on - A retrospective from the viewpoint of consumers». *European Journal of Consumer Law*, año 2024, núm. 1, p. 109-129.
- ROIG, A. *Las garantías frente a las decisiones automatizadas: Del Reglamento general de protección de datos a la gobernanza algorítmica*. 1ª ed. Barcelona: J. M. Bosch, 2020.
- SADOK, H.; SAKKA, F.; EL HADI EL MAKNOUZI, M. «Artificial intelligence and bank credit analysis: a review». *Cogent Economics and Finance*, núm. 10 (2022). Disponible en línea en: <<https://doi.org/10.1080/23322039.2021.2023262>> [consulta: febrero 2024].
- SORIANO ARNAZ, A. *Data protection for the prevention of algorithmic discrimination*. 1ª ed. Cizur Menor: Aranzadi, 2021.
- SORIANO ARNAZ, A. «Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos». *Revista de Derecho Público: Teoría y Método*, núm. 3 (2021), p. 85-127.
- SPINDLER, G. «Algorithms, credit scoring, and the new proposals of the EU for an AI Act and on a Consumer Credit Directive». *Law and Financial Markets Review*, núm. 15 (2021), p. 239-261. Disponible en línea en: <<https://doi.org/10.1080/17521440.2023.2168940>> [consulta: abril 2024].
- VARDI, N. *Creditworthiness and «responsible credit»: A comparative study of EU and US law*. Leiden: Brill, 2022.
- VOGEL, P. «A “right to explanation” for algorithmic decisions?». En: SANTOSUOSSO,

- Amedeo; PINOTTI, Giulia [ed.]. *Data-driven decision making. Law, ethics, robotics, health*. Pavia: Pavia University Press, 2020. Disponible en línea en: <<http://archivio.paviauniversitypress.it/oa/9788869521348.pdf>> [consulta: abril 2024].
- UNGERN-STERNBERG, A. von. «Discriminatory AI and the law». En: VOENEKY, Silja *et al.* [ed.]. *The Cambridge handbook of responsible artificial intelligence*. Cambridge: Cambridge University Press, 2022.
- WACHTER, S.; MITTELSTADT, B.; FLORIDI, L. «Why a right to explanation of automated decision-making does not exist in the general data protection regulation?». *International Data Privacy Law*, núm. 7 (2017), p. 76-99. Disponible en línea en: <<https://doi.org/10.1093/idpl/ix005>> [consulta: mayo 2024].
- WEITZENBOECK, E. M. «User empowerment in the age of algorithms». En: SAVIN, Andrej; TRZASKOWSKY, Jan [ed.]. *Research handbook on EU Internet Law*. 2ª ed. Cheltenham: Edward Elgar Publishing Ltd., 2023.
- WIEDEMANN, K. *Automated processing of personal data for the evaluation of personality traits: legal and ethical issues*. Múnich: Max Planck Institute for Innovation and Competition, 2018 (Max Planck Institute for Innovation and Competition Research Paper No. 18-04). Disponible en línea en: <<https://dx.doi.org/10.2139/ssrn.3102933>> [consulta: marzo 2024].
- WULF, A. J.; SEIZOV, O. «“Please understand we cannot provide further information”: evaluating content and transparency of GDPR-mandated AI disclosures». *AI and Society*, núm. 39 (2024), p. 235-256.