ISSN 1981-3694
(DOI): 10.5902/1981369483679

LA INTELIGENCIA ARTIFICIAL Y LA PROTECCIÓN DE DATOS: LA "ELABORACIÓN DE PERFILES" PARA LA PREVENCIÓN DE DELITOS GRAVES Y DEL TERRORISMO EM LAS FUENTES DE LA UNIÓN EUROPEA[i]

A INTELIGÊNCIA ARTIFICIAL E A PROTEÇÃO DE DADOS: A "DEFINIÇÃO DE PERFIS" PARA A PREVENÇÃO DE CRIMES GRAVES E DO TERRORISMO NAS FONTES DA UNIÃO EUROPEIA

ARTIFICIAL INTELLIGENCE AND DATA PROTECTION: "PROFILING" FOR THE PREVENTION OF CRIMINAL OFFENCES AND TERRORISM AT THE EUROPEAN UNION SOURCES

MANUEL DAVID MASSENO
https://orcid.org/0000-0001-8861-0337 / mdmasseno@gmail.com
Instituto Politécnico de Beja, Portugal

RESUMEN
Este texto busca poner de manifiesto los riegos para los derechos fundamentales resultantes de la utilización de sistemas de inteligencia artificial para prevenir delitos graves y el terrorismo en el marco de los actuales actos legislativos de la Unión Europea en lo que se refiere a la protección de datos personales, sobre todo los relacionados con la «elaboración de perfiles» por medio de algoritmos de aprendizaje profundo. Asimismo, intenta prospectar las respuestas legislativas que puedan resultar de la Propuesta Ley de Inteligencia Artificial de la Comisión Europea, teniendo en cuenta la Jurisprudencia más reciente del Tribunal de Justicia de la Unión Europea y las posiciones institucionales asumidas sobre esas cuestiones en la Propuesta.
Palabras clave: Crímenes; Inteligencia Artificial; Protección de Datos; Seguridad; Unión Europea.

RESUMO
O texto procura evidenciar os riscos para os direitos fundamentais resultantes da utilização de sistemas de inteligência artificial para a prevenção de crimes graves e do terrorismo no quadro dos atuais atos legislativos da União Europeia em matéria de proteção de dados pessoais, sobretudo os relacionados com a «definição de perfis» por algoritmos de aprendizado profundo. Adicionalmente, intenta perspectivar as respostas legislativas que possam resultar da Proposta de Regulamento Inteligência Artificial da Comissão Europeia, tendo em atenção a Jurisprudência mais recente do Tribunal de Justiça da União Europeia e as posições institucionais assumidas sobre tais questões na Proposta.
Palavras-chave: Crimes; Inteligência Artificial; Proteção de Dados; Segurança; União Europeia.

ABSTRACT
This paper intents to put into evidence the risk for fundamental rights resulting from the use of Artificial Intelligence systems for the prevention of serious criminal offences and terrorism in the framework of the current legislative acts of the European Union for personal data protection, those related to «profiling» by deep learning algorithms. Besides, it aims to examine the legal answers than may result from the Proposal of Artificial Intelligence Act of the European Commission, having in mind the most recent Case Law of the Court of Justice of European Union and institutional statements regarding those issues in the Proposal.
Keywords: Artificial Intelligence; Crimes; Data Protection; European Union; Security.

ISSN 1981-3694
(DOI): 10.5902/1981369483679

SUMÁRIO

INTRODUCCIÓN; 1 LAS FUENTES SECUNDARIAS; 1.1 La Directiva LED; 1.2 La Directiva PNR; 2 MIRANDO EL FUTURO... INMEDIATO; REFERÊNCIAS.

INTRODUCCIÓN

Desde hace casi 5 años, toda mención a la protección de datos en la UE – Unión Europea aboca al Reglamento general de protección de datos[1], el *RGPD*. A veces, con menciones a la Directiva sobre la privacidad y las comunicaciones electrónicas – la *Directiva ePrivacy*[2] o al Reglamento sobre la protección de datos en las instituciones, órganos e instituciones de la UE[3].

Como mucho, en diálogo y complemento con los instrumentos legislativos de defensa de los consumidores y usuarios[4] o con la regulación de los mercados[5] que han enfrentado las cuestiones relacionadas con la utilización creciente de sistemas de IA – Inteligencia Artificial en la Economía.

Sin embargo, el *RGPD* "no se aplica al tratamiento de datos personales: […] por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención." (Art. 2 2. d), o sea, de nuestro objeto.

[1] El Reglamento (UE) 2016/679 del Parlamento Europeo y de 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 https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679.

[2] La Directiva 2002/58/CE del Parlamento Europeo y de Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32002L0058.

[3] El Reglamento (UE) 2018/1725 del Parlamento Europeo y de Consejo, 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32018R1725.

[4] La Directiva (UE) 2019/2161 del Parlamento Europeo y de Consejo, de 27 de noviembre, por la que se modifica las Directivas 93/13/CEE, Directivas 98/6/CE, 2005/29/CE y 2011/83/UE, en lo que atañe a la mejora de la aplicación y la modernización de las normas de protección de los consumidores de la Unión https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32019L2161 y el Reglamento (UE) 2022/2065 del Parlamento Europeo y de Consejo, de 19 de octubre, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (*Reglamento de Servicios Digitales*), el *DSA* https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

[5] El Reglamento (UE) 2022/1925 del Parlamento Europeo y de Consejo, de 14 de septiembre, 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*), el *DMA* https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022R1925.

Por consiguiente, se hizo necesario adoptar en simultaneo actos legislativos específicos, como los que complementaron el *RGPD*, también publicados en la misma fecha. Las llamadas *Directiva de Ámbito Penal* – la *Directiva LED*[6]-[7] *y Directiva sobre los Registros de Nombres de los Pasajeros* – la *Directiva PNR*[8]-[9].

Además de los aplicables a los tratamientos de datos personales en el marco del control de las fronteras exteriores de la UE[10] y, específicamente, al asilo y la inmigración[11].

[6] La Directiva (UE) 2016/680 del Parlamento Europeo y de Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016L0680. En lo que se refiere a la articulación entre el *RGPD* y la *Directiva LED*, sobre todo en lo concerniente a la elaboración de perfiles y a la actuación policial predictiva, es de atender a SAJFERT y QUINTEL (2017) y a LYNSKEY (2019).

[7] No obstante, "Los Estados miembros pueden encomendar a las autoridades competentes, tal como se definen en la Directiva (UE) 2016/680, funciones que no se lleven a cabo necesariamente con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluida la protección frente a las amenazas a la seguridad pública y su prevención, de tal forma que el tratamiento de datos personales para estos otros fines, en la medida en que esté incluido en el ámbito del Derecho de la Unión, entra en el ámbito de aplicación del presente Reglamento." (*Considerando* (19) del *RGPD*).

[8] La Directiva (UE) 2016/681 del Parlamento Europeo y de Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L0681.

[9] Recordo que, no Brasil, a Lei º 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), dispõe que a mesma "não se aplica ao tratamento de dados pessoais: III - realizado para fins exclusivos de: a) segurança pública; [ou] d) atividades de investigação e repressão de infrações penais; § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei." (Art. 4º). Porém, mais de quatro anos depois, a referida lei está por aprovar, embora já existam Projetos com esse propósito. Para um recente ponto da situação, a título apenas informativo, FERNANDES, Maíra; MEGGIOLARO, Daniela; PRATES, Fernanda. Lei de Proteção de Dados para segurança pública e persecução penal. São Paulo: Consultor Jurídico, 28 out. 2022 Disponível em: https://www.conjur.com.br/2022-out-28/escritos-mulher-lei-protecao-dados-seguranca-publica-persecucao-penal

[10] El Reglamento (UE) 2018/1240 del Parlamento Europeo y de Consejo, de 12 de septiembre, por el que se establece un Sistema Europeo de Información y Autorización de Viajes (SEIAV / ETIAS) y por el que se modifican los Reglamentos (UE) n.º 1077/2011, (UE) n.º 515/2014, (UE) 2016/399, (UE) 2016/1624 y (UE) 2017/2226, que estará operativo en finales del año que viene https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32018R1240, y el Reglamento (UE) 2019/817 del Parlamento Europeo y de Consejo, de 20 de mayo, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 y (UE) 2018/1861 del Parlamento Europeo y del Consejo, y las Decisiones 2004/512/CE y 2008/633/JAI del Consejo https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32019R0817. Sobre la utilización de sistemas de IA prevista en estos Actos legislativos y sus efectos en lo concerniente a la vigilancia de las personas, tienen un gran interés los informes de GONZÁLEZ FUSTER (2020) y de DUMBRAVA (20221) para el Parlamento Europeo y el estudio monográfico de MATOS (2019); además, son de tener en cuenta las

ISSN 1981-3694
(DOI): 10.5902/1981369483679

Por supuesto, sin olvidar, la interconexión de todas estas clases de datos por Europol – la Agencia Europea para la Cooperación Policial[12], incluso a través de herramientas de IA[13].

Por otra parte, si la base constitucional material estes actos legislativos es el "respeto de la dignidad humana" (Art. 2 del *Tratado de la Unión Europea – TUE* y Art. 1 de la *Carta de los Derechos Fundamentales de la Unión Europea – CDFUE*), principalmente en lo que concierne al "respeto de la vida privada y familiar" y a la "protección de datos de carácter personal" (Arts. 7 y 8 de la *CDFUE*). En el tratamiento de datos para la prevención de delitos y del terrorismo, utilizando sistemas de IA, la necesaria proporcionalidad de las restricciones hace aún más apremiante la consideración adicional de los derechos "a la integridad de la persona", a la "igualdad ante la ley", a la "no discriminación" y también el "derecho de asilo", manteniendo firme la "presunción de inocencia" (Arts. 52 1., 3, 20, 21, 18 y 48 de la *CDFUE*)[14].

reflexiones de ZANDTRA y BROWER (2022), quienes ponen de manifiesto las previsibles consecuencias de la muy reciente Sentencia *Ligues des droits humains*, del TJUE, en lo que se refiere a la aplicación de los sistemas de IA previstos en tales Actos.

[11] El Reglamento (UE) 2019/818 del Parlamento Europeo y de Consejo, de 20 de mayo, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816 https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32019R0818, sobre los cuales, están disponibles os mencionados informes de GONZÁLEZ FUSTER (2020) y de DUMBRAVA (2021), además de las aportaciones de BLASI CASAGRAN (2021) y BLASI CASAGRAN et al. (2021).

[12] El Reglamento (UE) 2016/794 del Parlamento Europeo y de Consejo, de 11 de mayo, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32016R0794; para un análisis de este Acto, incluso señalando los riegos potenciales que podrían resultar de la interconexión de los datos aportados, como de hecho ocurrió, BLASI CASAGRAN (2016).

[13] Principalmente, después de la adopción del Reglamento (UE) 2022/991 del Parlamento Europeo y de Consejo, de 8 de junio, por el que se modifica el Reglamento (UE) 2016/794 en lo que se refiere a la cooperación de Europol con entidades privadas, el tratamiento de datos personales por Europol en apoyo de investigaciones penales y el papel de Europol en materia de investigación e innovación https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022R0991, el cual fue objeto de una demanda de anulación por parte del Supervisor Europeo de Protección de Datos, presentada en 16 de setiembre en el Tribunal de Justicia de la Unión Europea https://edps.europa.eu/press-publications/press-news/press-releases/2022/edps-takes-legal-action-new-europol-regulation-puts-rule-law-and-edps-independence-under-threat_en> y, además, en Prensa <https://www.euractiv.com/section/data-protection/news/eus-data-protection-authority-brings-europol-mandate-to-court/.

[14] En su informe, GONZÁLEZ FUSTER (2020) puso de manifiesto y desarrolla esta conexión, incluso antes de la Propuesta de la Comisión Europea; asimismo, en una perspectiva más bien genérica, MASSENO (2022) y MANEA y DRAGOS (2022); desde una perspectiva más amplia, incluso transcendiendo la UE, resultan de gran interés los planteamientos de BORGESIUS (2018), de ZAVRSNIK (2020), de DE GREGORIO (2022) y, incluso, la alternativa heurística propuesta por POSCHER (2022).

ISSN 1981-3694
(DOI): 10.5902/1981369483679

Como también resulta de la *Propuesta de Ley de Inteligencia Artificial*, presentada por la Comisión Europea hace un año y medio[15], en coherencia con los planteamientos del Parlamento Europeo[16] y del Consejo[17], ambos del otoño inmediatamente anterior.

Resumiendo, se trata de platear como la UE afronta la regulación de los sistemas de IA con aptitudes predictivas, para fines de seguridad y de prevención de delitos[18], incluyendo el futuro más cercano.

1 LAS FUENTES SECUNDARIAS

1.1 La Directiva LED

Explícitamente, esta Directiva "establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública" (Art. 1 1.), en regla a través de "tratamientos automatizados" (Art. 2 2.).

Lo que incluye "[…] la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción" (Art. 3 2).

[15] La Propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (*Ley de Inteligencia Artifici*al) y se modifican determinados actos legislativos de la Unión Europea (COM(2021)206 final), de 21 de abril https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52021PC0206 y la Comunicación "Planteamiento europeo en materia de inteligencia artificial" (COM(2021) 205 final), que la acompañó https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=COM%3A2021%3A205%3AFIN. Sobre la *Propuesta* y el correspondiente *iter* prelegislativo, me perito indicar tan solo la síntesis que destiné a Diputados mexicanos, MASSENO (2022), además de los artículos de VEALE y BORGESIUS (2021) y de BURRI (2022), en presencia de una multiplicidad de publicaciones al respecto.

[16] La *Resolución sobre el Marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas* (2020/2012(INL), de 20 de octubre https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020IP0275.

[17] Así, las Conclusiones de la Presidencia [alemana] *La Carta de los Derechos Fundamentales en el contexto de la inteligencia artificial y el cambio digital* (11481/20, de 21 de octubre) https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/es/pdf.

[18] Para una identificación de los puntos clave al respecto, se atiendan al informe de GONZÁLEZ FUSTER (2020) y los artículos de BONFANTI (2018), de ZAVRSNIK (2020) y de MANEA y DRAGOS (2022), además de la perspectiva centrada en criterios de naturaleza supra legislativa de MIRÓ-LLINARES (2020).

ISSN 1981-3694
(DOI): 10.5902/1981369483679

En particular, está prevista la "«elaboración de perfiles» [es decir] 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 al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física" (Art. 3 4). Lo que supone la utilización de sistemas de IA con funciones predictivas y en contexto de megadatos (*Big Data*), conllevando graves "riesgos para los derechos y libertades de los interesados" (Considerandos 51 y 38)[19].

De manera que, la Directiva busca restringir los límites de licitud de tales tratamientos, al regular el "mecanismo de decisión individual automatizado", con (Art. 11):

> 1 […] la prohibición de las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o le afecten significativamente, salvo que estén autorizadas por el Derecho de la Unión o del Estado miembro a la que esté sujeto el responsable del tratamiento y que establezca medidas adecuadas para salvaguardar los derechos y libertades del interesado, al menos el derecho a obtener la intervención humana por parte del responsable del tratamiento [además] 2. Las decisiones a que se refiere el apartado 1 del presente artículo no se basarán en las categorías especiales de datos personales […] salvo que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado [y, aún más] 3. La elaboración de perfiles que dé lugar a una discriminación de las personas físicas basándose en las categorías especiales de datos personales establecidas en el artículo 10 quedará prohibida, de conformidad con el Derecho de la Unión.

Por lo que, el margen dejado a los Legisladores nacionales es más bien limitado, en especial en lo que atañe a los "datos sensibles"[20].

Además, este tratamiento debe estar en conformidad con los Principios de [«limitación de la finalidad»], al ser "recogidos con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con esos fines" y de [«minimización de datos»], *id est*, ser

[19] Mas aún que en el *RGPD*, Art. 20 y, *maxime*, *Considerandos* (71) a (75). Para un análisis comparado de ambos regímenes, son de atender las aportaciones de SAJFERT y QUINTEL (2017), de BORGESIUS (2018), de BONFANTI (2018), de GARSTKA (2018), de LYNSKEY (2019) y, especialmente, de BRKAN (2019) y de GONZÁLEZ FUSTER (2020), esta sobre todo en el "Anexo" que complementa el informe, además de la perspectiva sociológica de NEIVA y MACHADO (2021).

[20] Según el Art. 10 1, se trata de los "datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona física".

"adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados" (Art. 3 1 b) y c), recurriendo a los calificativos del *RGPD*. Sin embargo, el "derecho de acceso del interesado", incluyendo la información cuanto a ser un "tratamiento automatizado", está muy restringido (Art. 11, 13 y 14), sobre todo si lo contrastamos con lo previsto en el *RGPD* (Art. 15)[21],

Por otra parte, es necesario proceder a una "distinción clara entre los datos personales de las distintas categorías de interesados", o sea (Art. 6):

> a) personas respecto de las cuales existan motivos fundados para presumir que han cometido o van a cometer una infracción penal; b) personas condenadas por una infracción penal; c) víctimas de una infracción penal o personas respecto de las cuales determinados hechos den lugar a pensar que puedan ser víctimas de una infracción penal, y. d) terceras partes involucradas en una infracción penal como, por ejemplo, personas que puedan ser citadas a testificar en investigaciones relacionadas con infracciones penales o procesos penales ulteriores, o personas que puedan facilitar información sobre infracciones penales, o personas de contacto o asociados de una de las personas mencionadas en las letras a) y b).

Asimismo, cumple también mantener neta la distinción entre "datos personales basados en hechos" y "datos personales basados en apreciaciones personales" (Art. 12 1.).

Lo que conlleva que la "elaboración de perfiles", aún más con fines predictivos, queda restringida a las "personas respecto de las cuales existan motivos fundados [en evidencias materiales] para presumir que han cometido o van a cometer una infracción penal" (Art. 6 a), excluyendo tratamientos indiscriminados.

Pero, siempre, con la elaboración previa de una "evaluación del impacto de las operaciones de tratamiento suponiendo", al ser utilizadas "nuevas tecnologías" [las de IA], que "por su naturaleza, alcance, contexto o fines, suponga[n] un alto riesgo para los derechos y libertades de las personas físicas" (Art. 27 1.).

Al mismo tiempo, "el derecho a obtener la intervención humana por parte del responsable del tratamiento" (Art. 11 1. *in fine*), suponiendo la determinación previa de los procedimientos y de los criterios de evaluación, no es compatible con la utilización de tecnologías de aprendizaje automático, o de "cajas negras", exigiendo siempre una verificación

[21] En este apartado y para la *Directiva LED*, se considere a SAJFERT y QUINTEL (2017), a GARSTKA (2018), a LISERS y CUSTERS (2019), a CALDAS (2019) y a VOGIATZOGLOU et al. (2019), además de la perspectiva extrajurídica de NEIVA y MACHADO (2021); mientras que SELBST y POWLES (2017), y, aún más, LA DIEGA (2018), ANALIDE y REBELO (2019) y BRKAN (2019), después desarrollado en BRKAN y BONNET (2020), DE GREGORIO (2022), KUMBAR y ROTH-ISIGKEIT (2021) y PAAL (2022), profundizan el tema en el marco del *RGPD*, con aportaciones también pertinentes en este particular.

por procedimientos no automatizados, como aclaró el TJUE – Tribunal de Justicia de la Unión Europea, como veremos a continuación[22].

Cumple añadir el relieve, en este particular, de los Dictámenes del Grupo de trabajo del artículo 29 [*WP 29*, actual CEPD – Comité Europeo de Protección de Datos][23].

1.2 La Directiva PNR

Empiezo por recordar que, a su vez, esta Directiva "regula: a) la transferencia por las compañías aéreas de datos del registro de nombres de los pasajeros (PNR) de vuelos exteriores de la UE; [y] b) el tratamiento de los datos a que se refiere la letra a), incluida su recogida, utilización y conservación por los Estados miembros, así como el intercambio de los mismos entre dichos Estados miembros" (Art. 1 1.), los cuales "podrán tratarse únicamente con fines de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves"[24] (Art. 1 2.).

[22] Sobes estas cuestiones, son de tomar en especial consideración las aportaciones de SAJFERT y QUINTEL (2017), de GARSTKA (2018), de CALDAS (2019), de LYNSKEY (2019), de ZAVRSNIK (2020) y, sobre todo, de LA DIEGA (2018), de ANALIDE y REBELO (2019) y de BRKAN (2019), profundizado en BRKAN y BONNET (2020), y asimismo de GREE (2022) y de POSCHER (2022), los cuales ponen de manifiesto los limites técnicos del control humano y, incluso, señalan algunas alternativas posibles.

[23] En especial, el Dictamen 01/2013, de 2 abril, sobre la "limitación de la finalidad" https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp201_es.pdf, 03/2015, de 1 de diciembre, sobre la "propuesta de Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos" https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp201_en.pdf [este no disponible en español] y, sobre todo, el Dictamen de 27 de noviembre de 2017, sobre "algunas cuestiones fundamentales de la Directiva sobre protección de datos en el ámbito penal (UE 2016/680)" https://ec.europa.eu/newsroom/article29/items/610178/en.

[24] Específicamente, según el Art. 3 9), los «delitos graves» son definidos como "los delitos incluidos en el anexo II que son punibles con una pena privativa de libertad o un auto de internamiento de una duración máxima no inferior a tres años con arreglo al derecho nacional de un Estado miembro", o sea, un rol muy largo, incluyendo "1. pertenencia a una organización delictiva; 2. trata de seres humanos; 3. explotación sexual de niños y pornografía infantil; 4. tráfico ilícito de estupefacientes y sustancias psicotrópicas; 5. tráfico ilícito de armas, municiones y explosivos; 6. corrupción; 7. fraude, incluido el que afecte a los intereses financieros de la Unión; 8. blanqueo del producto del delito y falsificación de moneda, con inclusión del euro; 9. delitos informáticos/ciberdelincuencia; 10. delitos contra el medio ambiente, incluido el tráfico ilícito de especies animales protegidas y de especies y variedades vegetales protegidas; 11. ayuda a la entrada y residencia ilegales; 12. homicidio voluntario, agresión con lesiones graves; 13. tráfico ilícito de órganos y tejidos humanos; 14. secuestro, detención ilegal y toma de rehenes; 15. robo organizado y a mano armada; 16. tráfico ilícito de bienes culturales, incluidas las antigüedades y las obras de arte; 17. falsificación y violación de derechos de propiedad intelectual o industrial de mercancías; 18. falsificación de documentos administrativos y tráfico de documentos administrativos falsos; 19. tráfico ilícito de sustancias hormonales y otros factores de crecimiento; 20. tráfico ilícito de materiales

En la perspectiva que nos importa, se prevé que la Unidad de Información sobre los Pasajeros – UIP de cada Estado miembro "tratará los datos PNR solo para realizar:

> a) una evaluación de los pasajeros antes de su llegada o salida programada del Estado miembro, a fin de identificar a toda persona que deba ser examinada de nuevo por las autoridades competentes […] y, en su caso, por Europol […] ante la posibilidad de que pudiera estar implicada en un delito de terrorismo o delito grave; [o] c) analizar los datos PNR con el fin de actualizar o establecer nuevos criterios que deben utilizarse en las evaluaciones realizadas […] a fin de identificar a toda persona que pueda estar implicada en un delito de terrorismo o delito grave. (Art. 6 2.)

Para la mencionada evaluación, cada UIP podrá: (Art. 6 3.)

> a) comparar los datos PNR con las bases de datos pertinentes a los efectos de la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, incluidas las bases de datos sobre personas u objetos buscados o bajo alerta, de acuerdo con las normas de la Unión, internacionales y nacionales aplicables a dichas bases de datos" [o] b) tratar los datos PNR con arreglo a criterios predeterminados.

Lo que,

> […] se realizará de forma no discriminatoria con arreglo a criterios de evaluación establecidos por su UIP. Estos criterios predeterminados de evaluación deben ser orientados, proporcionados y específicos. Los Estados miembros se asegurarán de que las UIP establezcan esos criterios y los revisen periódicamente, en cooperación con las autoridades competentes […]. Los criterios no se basarán en ningún caso en el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud o la vida u orientación sexual de la persona. (4.)

Además,

> […] los Estados miembros velarán por que se revise individualmente, por medios no automatizados, todo resultado positivo que arroje el tratamiento automatizado de los datos PNR efectuado […], con el fin de comprobar si es necesario que las autoridades competentes […] emprendan una acción en virtud del derecho nacional. (5.)[25]

radiactivos o sustancias nucleares; 21. Violación; 22. delitos incluidos en la jurisdicción de la Corte Penal Internacional; 23. secuestro de aeronaves y buques; 24. Sabotaje; 25. tráfico de vehículos robados; 26. espionaje industrial.".

[25] Para un análisis de las cuestiones planteadas son interesantes las reflexiones de BIRZU y BONFANTI (2018) y de ORRÙ (2022).

Pero, sin atribuir un derecho a la revisión a los pasajeros, como resulta de la remisión hecha hacia los derechos de "acceso, rectificación, supresión y restricción" (Arts. 17 e 18 de la Decisión Marco 2008/977/JAI, actuales Arts. 12 a 16 de la *Directiva LED*, *ex vi* Art. 13 1.)[26]. Cumple aún señalar que, para la construcción de este régimen, contribuyeron los Dictámenes del Supervisor Europeo de Protección de Datos[27]. A los que debemos añadir el Dictamen del GT 29 sobre la "Propuesta de Directiva"[28].

Por su parte, el TJUE, ya en su Dictamen 1/15, de 26 de julio de 2017, sobre el Proyecto de Acuerdo entre Canadá y la Unión Europea – Transferencia de los datos del registro de nombres de los pasajeros aéreos desde la Unión a Canadá[29], puso en evidencia los riesgos inherentes a los tratamientos automatizados, al ser susceptibles de "proporcionar información adicional sobre la vida privada de los pasajeros aéreo", produciendo "efectos perjudiciales" para los pasajeros, "sin que existan razones fundadas en circunstancias individuales que permitan considerar que las personas afectadas podrían presentar un riesgo para la seguridad pública"[30].

Ahora, en la muy reciente Sentencia *Ligue des droits humains*,[31], en el marco de un criterio estricto de interpretación de la Directiva en conformidad con la *CDFUE*, el TJUE añadió,

[26] Específicamente, sobre este apartado, se tenga en consideración el estudio de VOGIATZOGLOU et al. (2021), además de los antes señadas a propósito del *RGPD*.

[27] El Dictamen de 1 de mayo de 2008, aún "acerca de la propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (*Passenger Name Record* – PNR) con fines represivos (COM(2007) 654 final, de 6 de noviembre)" https://edps.europa.eu/data-protection/our-work/publications/opinions/european-pnr_en y el Dictamen de 25 de marzo de 2011, sobre la "propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves (COM(2011) 32 final, de 2 de febrero)" https://edps.europa.eu/data-protection/our-work/publications/opinions/passenger-name-record-0_en.

[28] El Dictamen 10/2011, de 5 de abril, "relativo a la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para prevención, detección, investigación y enjuiciamiento de los delitos terroristas y delitos graves" https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp181_es.pdf.

[29] El Dictamen emitido con arreglo al artículo 218 TFUE, apartado 11 — Proyecto de Acuerdo entre Canadá y la Unión Europea — Transferencia de los datos del registro de nombres de los pasajeros aéreos desde la Unión a Canadá — Bases jurídicas adecuadas — Artículo 16 TFUE, apartado 2, artículo 82 TFUE, apartado 1, párrafo segundo, letra d), y artículo 87 TFUE, apartado 2, letra a) — Compatibilidad con los artículos 7 y 8 y con el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea https://curia.europa.eu/juris/document/document.jsf?text=&docid=193216&doclang=ES.

[30] Sobre los fundamentos y consecuencias del Dictamen, incluso para la interpretación y aplicación de la Directiva PNR, además de las otras Fuentes de la UE en sede de tratamiento de dados personales para fines de seguridad y prevención de delitos, específicamente, se detienen MENDEZ (2017) y VILLANI (2018), sin olvidar la conexión, señalada por CALDAS (2019), con las tecnologías de tratamiento automatizado.

[31] El 21 de junio de 2022, en el Asunto C-817/19 *Ligue des droits humains* c. *Conseil des ministres* https://curia.europa.eu/juris/liste.jsf?num=C-817/19. En lo que atañe al contexto y las consecuencias

en el marco de una reinterpretación muy estricta, o incluso restrictiva, de la Directiva y con una aproximación novedosa, específicamente:

> 193. El artículo 6, apartado 3, letra b), de la Directiva PNR establece que la UIP también puede tratar los datos PNR con arreglo a criterios predeterminados. A tenor del artículo 6, apartado 2, letra a), de esta Directiva, la finalidad de la evaluación previa y, por ende, la del tratamiento de los datos PNR con arreglo a criterios predeterminados es, en esencia, identificar a toda persona que pudiera estar implicada en un delito de terrorismo o delito grave.
> 194. En cuanto a los criterios a los que la UIP puede recurrir a estos efectos, es preciso señalar, en primer lugar, que, según los propios términos del artículo 6, apartado 3, letra b), de la Directiva PNR, debe tratarse de criterios «predeterminados». Como observa el Abogado General en el punto 228 de sus conclusiones, este requisito se opone a la utilización de las tecnologías de inteligencia artificial en el marco de sistemas de autoaprendizaje (*machine learning*), que puedan alterar, sin intervención y sin control humanos, el proceso de evaluación y, en particular, los criterios de evaluación en los que se basa el resultado de la aplicación del proceso, así como la ponderación de dichos criterios.
> 195. Es preciso añadir que el recurso a estas tecnologías entrañaría el riesgo de privar de efecto útil a la revisión individualizada de los resultados positivos y al control de licitud exigido por las disposiciones de la Directiva PNR. En efecto, como hace constar, en esencia, el Abogado General en el punto 228 de sus conclusiones, habida cuenta de la opacidad que caracteriza el funcionamiento de las tecnologías de inteligencia artificial, puede resultar imposible comprender la razón por la cual un determinado programa ha alcanzado una concordancia positiva. En estas circunstancias, el uso de esas tecnologías también podría privar a las personas afectadas de su derecho a la tutela judicial efectiva, que consagra el artículo 47 de la Carta y que la Directiva PNR pretende, a tenor de su considerando 28, garantizar en un nivel elevado, en particular para cuestionar el carácter no discriminatorio de los resultados obtenidos.
> 196. Por otra parte, en lo tocante a los requisitos establecidos en el artículo 6, apartado 4, de la Directiva PNR, esta disposición prescribe, en su primera frase, que la evaluación previa con arreglo a criterios predeterminados se realice de forma no discriminatoria y precisa, y en su cuarta frase, que estos criterios no se basen en ningún caso en el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud o la vida u orientación sexual de la persona.

De esta manera, el TJUE siguió los criterios firmados en sus Sentencias sobre conservación de datos relativos a las comunicaciones electrónicas[32], ahora en un ámbito de los tratamientos automatizados.

previsibles de esta Sentencia, además do lo planteado por ORRÙ (2022) en el momento anterior a la publicación del fallo, tiene mucho interés lo planteado por THONNES (2022) y, sobre todo, por los efectos en las demás Fuentes relacionadas con el control de accesos al territorio de la Unión Europea a través de la definición automatizada de perfiles de los viajeros, ZANDTRA y BROWER (2022).

[32] Desde los Asuntos *Digital Rights Ireland* y *Seitlinger* y otros (C-293/12 y C-594/12, de 8 de abril de 2014) https://curia.europa.eu/juris/liste.jsf?num=C-293/12 hasta los *SpaceNet* y *Telekom Deutschland* (C-793/19 y C-794/19, de 20 de setiembre de 2022) https://curia.europa.eu/juris/liste.jsf?num=C-793/19.

ISSN 1981-3694
(DOI): 10.5902/1981369483679

No obstante, sin presentar justificación alguna, dejó por enfrentar el problema de la reversibilidad de la "despersonalización […] mediante enmascaramiento" de los datos (Art. 12 2.) por medio de sistemas de IA, al evaluar la conformidad de las reglas relativas al "periodo de conservación de los datos"[33].

Por ende, la Corte de Luxemburgo trazó una línea roja con efectos muy significativos sea para la aplicación de todos los regímenes vigentes, incluyendo los méritos de la demanda presentada por el SEPD para la anulación del nuevo *Reglamento Europol*. Lo mismo vale para la conformación de la futura *Ley de Inteligencia Artificial*, en especial en lo que atañe a las "Estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado y el realizado por refuerzo, que emplean una amplia variedad de métodos, entre ellos el aprendizaje profundo" (Anexo I a).

2 MIRANDO EL FUTURO... INMEDIATO

Más allá de la, ahora mismo mencionada, Sentencia *Ligue des droits humains*, cumple poner en evidencia la Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales, la cual:

> 15. Señala que si los seres humanos se basan únicamente en datos, perfiles y recomendaciones generados por máquinas, no podrán realizar una evaluación independiente; resalta las consecuencias negativas potencialmente graves, particularmente en el ámbito de las actividades policiales y judiciales, que pueden derivarse de una confianza excesiva en la naturaleza aparentemente objetiva y científica de las herramientas de IA, sin tener en cuenta la posibilidad de que sus resultados sean incorrectos, incompletos, irrelevantes o discriminatorios; hace hincapié en que debe evitarse el exceso de confianza en los resultados ofrecidos por sistemas de IA y destaca la necesidad de que las

Sobre la Sentencia y anticipando la conexión, no asumida por el Tribunal de Luxemburgo, como pode de manifiesto THONNES (2022), ya mi ponencia MASSENO (2017) y BONFANTI (2018); además, cumple señalar como GALÁN MUÑOZ (2016), también se dio cuenta de los efectos de la Sentencia *Digital Rights Ireland* en materia de seguridad y lucha contra el crimen en la UE, mucho más allá de la retención y acceso a los metadatos de las comunicaciones electrónicas; y, incluso antes, cuando salieron las Propuestas de la Comisión Europeo para la Reforma de la Protección de Datos, lo puso de manifiesto ROBINSON (2012). Mientras que, para un análisis retrospectivo, poniendo de manifiesto las tenciones entre el Tribunal de Luxemburgo y los Gobiernos de una buena parte de los Estados miembros, podemos apuntar el texto reciente de ROJSZCZAK (2021), sin olvidar las reflexiones de naturaleza constitucional de DE GREGORIO (2022).

[33] En lo que concierne los problemas de reidentificación de los datos PNR, además de las prevenciones, KORFF y GEORGES (2015), me permito indicar las referencias contextuales que ya hice, MASSENO (2017), además del análisis jurídico y técnico de CHIAPPETTA y BATTAGLIA (2018).

> autoridades adquieran confianza y conocimientos para poner en cuestión recomendaciones algorítmicas o hacer caso omiso de ellas; considera importante tener expectativas realistas sobre estas soluciones tecnológicas y no prometer soluciones policiales perfectas y la detección de todas las infracciones que se cometan.
> 16. Subraya que, en el contexto de las actividades judiciales y policiales, todas las decisiones con efectos legales deben ser tomadas siempre por un ser humano al que puedan pedirse cuentas de las decisiones adoptadas; resalta las consecuencias negativas potencialmente graves, particularmente en el ámbito de las actividades policiales y judiciales, que pueden derivarse de una confianza excesiva en la naturaleza aparentemente objetiva y científica de las herramientas de IA, sin tener en cuenta la posibilidad de que sus resultados sean incorrectos, incompletos, irrelevantes o discriminatorios [y, por ello]
> 22. […] se opone, por tanto, al uso de la IA por parte de las autoridades policiales para hacer predicciones conductuales relativas a individuos o grupos sobre la base de datos históricos y comportamientos pasados, pertenencia a un grupo, ubicación o cualquier otra característica de este tipo, para tratar así de identificar a personas que probablemente vayan a cometer un delito.

Además, ya en la *Propuesta de Ley de Inteligencia Artificial*, de la enumeración de los "sistemas de IA de Alto Riesgo" (Anexo III), constan los:

> […] destinados a utilizarse por parte de las autoridades encargadas de la aplicación de la ley para llevar a cabo evaluaciones de riesgos individuales de personas físicas con el objetivo de determinar el riesgo de que cometan infracciones penales o reincidan en su comisión, así como el riesgo para las potenciales víctimas de delitos" (6. a) o "[…] destinados a utilizarse por parte de las autoridades públicas competentes para evaluar un riesgo, como un riesgo para la seguridad, la salud o relativo a la inmigración ilegal, que plantee una persona física que pretenda entrar o haya entrado en el territorio de un Estado miembro" (7. b).

Lo que presupone la posibilidad real de una intervención humana, incluso en el aprendizaje automático, con criterios insertados o controlados estrictamente, por lo menos en línea con lo dispuesto en la redacción actual del *Reglamento Europol* (Art. 33 bis), pero bajo supervisión efectiva de una Autoridad independiente, y obedeciendo a reglas más rigurosas que las previstas en la *Propuesta* de la Comisión (*maxime* en los Arts. 9, 10 y 14).

De otro modo, habrá que considerar esos tratamientos como análogos a la "utilización de sistemas de IA por parte de las autoridades o en su representación con el fin de evaluar o clasificar la fiabilidad de personas físicas durante un período determinado de tiempo atendiendo a su conducta social o a características personales o de su personalidad conocidas o predichas", *id est*, entre las "prácticas inteligencia artificial prohibidas" (Art. 5 1. c).

Sin embargo, la *Propuesta* contiene una "cláusula del abuelo", ya que:

> 1. El presente Reglamento no se aplicará a los sistemas de IA que sean componentes de sistemas informáticos de gran magnitud establecidos en virtud de los actos legislativos enumerados en el anexo IX[34] que hayan sido introducidos en el mercado o puestos en servicio antes de [12 meses después de la fecha de aplicación del presente Reglamento a que se refiere el artículo 85, apartado 2], salvo que la sustitución o modificación de dichos actos legislativos redunde en un cambio significativo en el diseño o la finalidad prevista del sistema o sistemas de IA de que se trate. (Art. 83 1.).

En conclusión y como resulta del Dictamen conjunto de CEPD y SEPD sobre la Propuesta[35], por lo menos:

> […] es necesario un enfoque regulador más coherente, ya que las disposiciones actuales no parecen lo suficientemente claras como para crear una base jurídica para el tratamiento de las categorías especiales de datos, y deben complementarse con medidas de protección adicionales que aún deben evaluarse. Además, cuando los datos personales se hayan recogido mediante tratamiento dentro del ámbito de aplicación de la LED, deberán tenerse en cuenta las posibles salvaguardias y limitaciones adicionales derivadas de las transposiciones nacionales de la LED.

REFERÊNCIAS

ANALIDE, César; REBELO, Diogo Morgado. Inteligência artificial na era *data-driven*, a lógica *fuzzy* das aproximações *soft computing* e a proibição de sujeição a decisões tomadas exclusivamente com base na exploração e prospeção de dados pessoais. **Fórum de Proteção de Dados**, Comissão Nacional de Proteção de Dados, Lisboa, n. 6, p. 60-91, 2019. Disponible en: https://www.cnpd.pt/media/y1nosvyp/forum6_af_web_low.pdf.

BIRZU, Bogdan. Prevention, detection, investigation and prosecution of terrorist offenses and other serious crimes by using Passenger Name Record (PNR) data. Critical opinions. *De lege ferenda* proposals. **Perspectives of Business Law Journal**, v. 5, n. 1, p. 195-206, 2016. Disponible en: https://www.businesslawconference.ro/revista/articole/an5nr1/Art.%2027%20Bogdan%20Birzu.pdf.

BLASI CASAGRAN, Cristina. El reglamento europeo de Europol: Un nuevo marco jurídico para el intercambio de datos policiales en la UE. **Revista General de Derecho Europeo**, Madrid, n. 40, p. 202-221, 2016. Disponible en: https://www.researchgate.net/profile/Cristina-Blasi-

[34] Incluyendo, explícitamente, el Sistema de Información de Schengen, el Sistema de Entradas y Salidas o el Sistema Europeo de Información y Autorización de Viajes…

[35] El Dictamen conjunto 5/2021 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_es.

Casagran/publication/316286371_El_Reglamento_Europeo_de_Europol_Un_nuevo_marco_juridico_para_el_intercambio_de_datos_policiales_en_la_UE/links/58f9fdc94585152edece7b6b/El-Reglamento-Europeo-de-Europol-Un-nuevo-marco-juridico-para-el-intercambio-de-datos-policiales-en-la-UE.pdf.

BLASI CASAGRAN, Cristina. Fundamental rights implications of interconnecting migration and policing databases in the EU. **Human Rights Law Review**, Oxford, Oxford University Press, v. 21, n. 2, p. 433-457, 2021. Disponible en: https://academic.oup.com/hrlr/article-pdf/21/2/433/36582235/ngaa057.pdf.

BLASI CASAGRAN, Cristina *et al*. The role of emerging predictive IT tools in effective migration governance. **Politics and Governance**, Lisboa, v. 9, n. 4, p. 133-145, 2021. Disponible en: https://www.cogitatiopress.com/politicsandgovernance/article/view/4436.

BONFANTI, Angelica. *Big data* e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali. **MediaLaws – Rivista di diritto dei media**, Milano, n. 3, p. 206-218, 2018. Disponible en: https://www.medialaws.eu/rivista/big-data-e-polizia-predittiva-riflessioni-in-tema-di-protezione-del-diritto-alla-privacy-e-dei-dati-personali/.

BORGESIUS, Frederik Zuiderveen. **Discrimination, Artificial Intelligence, and Algorithmic Decision Making**. Strasbourg: Consejo de Europe, 2018. Disponible en: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73.

BRKAN, Maja. Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. **International journal of law and information technology**, Oxford, v. 27, n. 2, p. 91-121, 2019. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901.

BRKAN, Maja; BONNET, Grégory. Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas European. **Journal of Risk Regulation**, Cambridge, v. 11, n. 1, p. 18-50, 2020. Disponible en: https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/legal-and-technical-feasibility-of-the-gdprs-quest-for-explanation-of-algorithmic-decisions-of-black-boxes-white-boxes-and-fata-morganas/7324CDE80A300179C170C5BA8CA7E851.

BURRI, Thomas. The New Regulation of the European Union on Artificial Intelligence. *In*: VOENEKY, Silja *et al*. (Orgs.). **The Cambridge Handbook of Responsible Artificial Intelligence**: Interdisciplinary Perspectives. Cambridge: Cambridge University Press, 2022. p. 104-122. Disponible en: https://www.cambridge.org/core/books/cambridge-handbook-of-responsible-artificial-intelligence/new-regulation-of-the-european-union-on-artificial-intelligence/C7FBB429998C4AC5ABBCAA594D2F8970.

CALDAS, Gabriela. O direito à explicação no Regulamento Geral sobre a Proteção de Dados. *In*: COUTINHO, Francisco Pereira; MONIZ, Graça Canto (Coords.). **Anuário da Proteção de Dados - 2019**. Lisboa: CEDIS; Universidade Nova de Lisboa, 2019. p. 37-53. Disponible en: https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/2.-Gabriela-Caldas.pdf.

CHIAPPETTA, Andrea; BATTAGLIA, Andrea. The impact of privacy andcybersecurity on e-record: The PNR Directive Adoption and the impact of GDPR. **Journal of Sustainable Development of Transport and Logistics**, Ternopil, v. 3, n. 3, p. 77-87, 2018. Disponible en: https://jsdtl.sciview.net/index.php/jsdtl/article/view/58/43.

DE GREGORIO, Giovanni. **Digital Constitutionalism in Europe**: Reframing Rights and Powers in the Algorithmic Society. Cambridge: Cambridge University Press, 2022. Disponible en: https://www.cambridge.org/core/books/digital-constitutionalism-in-europe/A3F61C6368D17D953457234B8A59C502.

DUMBRAVA, Costica. **Artificial intelligence at EU borders** - Overview of applications and key issues. Brussels: Parlamento Europeo, 2021. Disponible en: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf.

GALÁN MUÑOZ, Alfonso. La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos hacia una nueva orientación de la política criminal de la Unión Europea. **Cyberlaw by CIJIC**, Lisboa, n. 1, p. 22-57, 2016. Disponible en: https://www.iuris.edu.pt/xms/files/Cyberlaw-by-CIJIC_1.pdf.

GARSTKA, Krzysztof. **Between Security and Data Protection**: Searching for a Model of a Legal Big Data Surveillance Scheme within the European Union Data Protection Framework. University of Essex: HRBDT Occasional Paper Series, 2018. Disponible en: https://www.researchgate.net/publication/329339463_Between_Security_and_Data_Protection_Searching_for_a_Model_of_a_Legal_Big_Data_Surveillance_Scheme_within_the_European_Union_Data_Protection_Framework_2018_HRBDT_Occasional_Paper_Series.

GONZÁLEZ FUSTER, Gloria. **Artificial Intelligence and Law Enforcement** - Impact on Fundamental Rights. Brussels: Parlamento Europeo, 2020. Disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf.

GREE, Ben. The flaws of policies requiring human oversight of government algorithms. **Computer Law & Security Review**, Amsterdam, n. 45, 2022. Disponible en: https://www.sciencedirect.com/science/article/pii/S0267364922000292.

KORFF, Douwe; GEORGES, Marie. **Passenger Name Records, data mining & data protection**: the need for strong safeguards. Strasbourg: Directorate General of Human Rights and Rule of Law; Council of Europe, 2015. Disponible en: https://rm.coe.int/16806a601b.

KUMBAR, Lea Katharina; ROTH-ISIGKEIT, David. A criterion-based approach to GDPR's explanation requirements for automated individual decision-making. **Journal of intellectual property, information technology and electronic commerce law**, v. 12, n. 4, 2021. Disponible en: https://www.jipitec.eu/issues/jipitec-12-4-2021/5403.

LA DIEGA, Guido Noto. Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information. **Journal of intellectual property, information technology and electronic commerce law**, v. 9, n. 4, 2018. Disponible en: https://www.jipitec.eu/issues/jipitec-9-1-2018/4677.

LISERS, Mark; CUSTERS, Bart. Conceptual Challenges of EU Directive 2016/680. **European Data Protection Law Review**, Berlin, v. 5, n. 3, p. 367-378, 2019. Disponible en: https://scholarlypublications.universiteitleiden.nl/handle/1887/79246.

LYNSKEY, Orla. Criminal justice profiling and EU data protection law: Precarious protection from predictive policing. **International Journal of Law in Context**, Cambridge, v. 15, n. 2, p. 162-176, 2019. Disponible en: https://www.cambridge.org/core/journals/international-journal-of-law-in-context/article/criminal-justice-profiling-and-eu-data-protection-law-precarious-protection-from-predictive-policing/10FD4B64364191B619FBCB864CD40A7F.

MANEA, Teodor; DRAGOS, Ivan Lucian. AI Use in Criminal Matters as Permitted under EU Law and as Needed to Safeguard the Essence of Fundamental Rights. **International Journal of Law in Changing World**, Chelyabinsk, v. 1, n. 1, 2022. Disponible en: https://ijlcw.emnuvens.com.br/revista/article/view/15.

MASSENO, Manuel David. El tratamiento de datos PNR en tiempos de datos masivos ('Big Data') - un análisis desde la perspectiva de las Sentencias 'Digital Rights Ireland' y 'Tele2 Sverige' del TJUE. *In*: **Jornada sobre Derecho, Turismo y Nuevas Tecnologías**. Palma de Mallorca: Universitat de les Illes Balears, 2017. Disponible en: https://www.academia.edu/31301045/El_tratamiento_de_datos_PNR_en_tiempos_de_datos_masivos_Big_Data_un_an%C3%A1lisis_desde_la_perspectiva_de_las_Sentencias_Digital_Rights_Ireland_y_Tele2_Sverige_del_TJUE.

MASSENO, Manuel David. Consideraciones breves sobre los Fundamentos de la Propuesta de Ley de Inteligencia Artificial de la Comisión Europea. **Revista de Ciencia de la Legislación**, Buenos Aires, n. 12, 2022. Disponible en: https://ar.ijeditores.com/pop.php?option=articulo&Hash=fc2693b96bdc49a24d23863bd43ef39c.

MATOS, Sara. Privacy and data protection in the surveillance society: The case of the Prüm system. **Journal of Forensic and Legal Medicine**, Amsterdam, n. 66, p. 155-161, 2019. Disponible en: https://www.sciencedirect.com/science/article/pii/S1752928X1930068X.

MENDEZ, Mario. Opinion 1/15: The Court of Justice Meets PNR Data (Again!). **European Papers** - A Journal on Law and Integration, Roma, v. 2, n. 3, p. 803-818, 2017. Disponible en: https://www.europeanpapers.eu/en/e-journal/opinion-1-15-court-of-justice-meets-pnr-data-again.

MIRÓ-LLINARES, Fernando. Predictive policing: Utopia or dystopia? On attitudes towards the use of big data algorithms for law. **Revista de Internet, derecho y política**, Universitat Oberta de Catalunya, n. 30, 2020. Disponible en: https://raco.cat/index.php/IDP/article/view/373608.

NEIVA, Laura; MACHADO, Helena. *Big data* na investigação criminal: "Imaginário Europeu" e orientações para o futuro. *In*: ARAÚJO, Emília Rodrigues; MACHADO, Helena y COSTA; Anyónio J. B. F. Jardim (Coord.). **Ciência & política**: fronteiras e interseções. II Jornadas Doutorais em Sociologia. Braga: Universidade do Minho, 2021. p. 28-41. Disponible en: https://repositorium.sdum.uminho.pt/bitstream/1822/74887/1/Big%20Data%20e%20imagina%cc%81rio%20europeu.pdf.

ORRÙ, Elisa. The European PNR Directive as an instance of pre-emptive, risk-based algorithmic security and its implications for the regulatory framework. **Information Polity**, Amsterdam, v. 27, n. 2, p. 131-146, 2022. Disponible en: https://content.iospress.com/download/information-polity/ip211531?id=information-polity%2Fip211531.

PAAL, Boris. Artificial Intelligence as a Challenge for Data Protection Law. *In*: VOENEKY, Silja et al. (Orgs.). **The Cambridge Handbook of Responsible Artificial Intelligence**: Interdisciplinary Perspectives. Cambridge: Cambridge University Press, 2022. p. 290-308. Disponible en: https://www.cambridge.org/core/books/cambridge-handbook-of-responsible-artificial-intelligence/artificial-intelligence-as-a-challenge-for-data-protection-law/84B9874F94043E8AFC81616A60BA69CC.

POSCHER, Ralf. Artificial Intelligence and the Right to Data Protection. *In*: VOENEKY, Silja et al. (Orgs.). **The Cambridge Handbook of Responsible Artificial Intelligence**: Interdisciplinary Perspectives. Cambridge: Cambridge University Press, 2022. p. 281-289. Disponible en: https://www.cambridge.org/core/books/cambridge-handbook-of-responsible-artificial-intelligence/artificial-intelligence-and-the-right-to-data-protection/26AB000E713FBF3BDB89067C23B118F1.

ROBINSON, Gavin. Data protection reform, passenger name record and telecommunications data retention. **Critical Quarterly for Legislation and Law**, Baden-Baden, v. 95, n. 4, p. 394-416, 2012. Disponible en: https://orbilu.uni.lu/bitstream/10993/44953/1/2193-7869-2012-4-394.pdf.

ROJSZCZAK, Marcin. The uncertain future of data retention laws in the EU: Is a legislative reset possible? **Computer Law & Security Review**, Amsterdam, n. 41, 2021. Disponible en: https://www.sciencedirect.com/science/article/pii/S0267364921000455.

SAJFERT, Juraj; QUINTEL, Teresa. Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities. **SSRN**, Amsterdam, Elsevier, 2017. Disponible en: https://ssrn.com/abstract=3285873.

SELBST, Andrew D.; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, Oxford, v. 7, n. 4, p. 233–242, 2017. Disponible en: https://academic.oup.com/idpl/article/7/4/233/4762325.

THONNES, Christian. A Directive altered beyond recognition - On the Court of Justice of the European Union's PNR decision (C-817/19). **Verfassungsblog** – on matters constitutional. Berlin: Max Steinbeis Verfassungsblog gGmbH, 2022. Disponible en: https://verfassungsblog.de/pnr-recognition/.

VEALE, Michael; BORGESIUS, Frederik J. Zuiderveen. Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach. **Computer Law Review International**, Berlin, v. 22, n. 4, p. 97-112, 2021. Disponible en: https://arxiv.org/ftp/arxiv/papers/2107/2107.03721.pdf.

VILLANI, Susanna. Some further reflections on the Directive (EU) 2016/681 on PNR data in the light of the CJEU Opinion 1/15 of 26 July 2017. **Revista de derecho político**, Madrid, n. 101, p. 899-928, 2018. Disponible en: https://revistas.uned.es/index.php/derechopolitico/article/view/21982/17970.

VOGIATZOGLOU, Plixavra *et al*. From Theory to Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives. **Journal of intellectual property, information technology and electronic commerce law**, v. 11, n. 3, 2021. Disponible en: https://www.jipitec.eu/issues/jipitec-11-3-2020/5191.

ZANDTRA, Timo; BROWER, Evelien. Fundamental Rights at the Digital Border - ETIAS, the Right to Data Protection, and the CJEU's PNR judgment. **Verfassungsblog** – on matters constitutional. Berlin: Max Steinbeis Verfassungsblog gGmbH, 2022. Disponible en: https://verfassungsblog.de/digital-border/.

ZAVRSNIK, Aleš. Criminal justice, artificial intelligence systems, and human rights. **ERA Forum**, Academy of European Law, n. 20, p. 567–583, 2020. Disponible en: https://link.springer.com/article/10.1007/s12027-020-00602-0.

Artigo convidado estrangeiro

COMO FAZER REFERÊNCIA AO ARTIGO (ABNT):

MASSENO, Manuel David. La inteligencia artificial y la protección de datos: la "elaboración de perfiles" para la prevención de delitos graves y del terrorismo en las fuentes de la Unión Europea. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria, RS, v. 17, n. 2, e83679, 2022. ISSN 1981-3694. DOI: http://dx.doi.org/10.5902/1981369483679. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/83679 Acesso em: dia mês. ano.

Editores responsáveis: Rafael Santos de Oliveira, Bruna Bastos e Angela Araujo da Silveira Espindola

SOBRE O AUTOR

MANUEL DAVID MASSENO
Professor Adjunto de Graduação e Mestrado e Pesquisador Sênior no Laboratório UbiNET - Segurança Informática e Cibercrime do Instituto Politécnico de Beja, Portugal.

[i] Este texto corresponde à "Conferencia Inaugural" proferida pelo Autor na "III Jornada sobre el marco jurídico de la Ciencia de Datos: perspectivas de la inteligencia artificial", organizada pela "Universitat Politècnica de Valencia", em Espanha, no dia 17 de novembro de 2022; estando para publicação nas respetivas "Actas", a serem editadas pela Tirant Lo Blanch.