



UNIVERSIDADE DA CORUÑA

TRABALLO FIN DE MÁSTER

MÁSTER UNIVERSITARIO EN DEREITO DIXITAL E DA INTELIXENCIA ARTIFICIAL (MUDDIA)

**OS SISTEMAS DE PREDICIÓN DE RISCO DOTADOS DE INTELIXENCIA
ARTIFICIAL: REFLEXIÓNS SOBRE O SEU PRESENTE E FUTURO**

*RISK PREDICTION SYSTEMS ENDOWED WITH ARTIFICIAL INTELLIGENCE: REFLECTIONS ON THEIR
PRESENT AND FUTURE*

*LOS SISTEMAS DE PREDICCIÓN DE RIESGO DOTADOS DE INTELIGENCIA ARTIFICIAL. REFLEXIONES
SOBRE SU PRESENTE Y FUTURO*

AUTORA: ANDREA VÁZQUEZ RICO

TUTORA: PATRICIA FARALDO CABANA

Índice

1. Introducción.....	3
2. O emprego de sistemas de predición do risco no eido penal e policial. Situación actual.....	6
3. Regulación actual	12
4. Riscos e afectación a dereitos fundamentais	19
A) Nesgos	20
B) Afectación a dereitos fundamentais.....	25
I. O dereito a un xuíz imparcial	26
II. O dereito á presunción de inocencia.....	28
III. O dereito de defensa	29
IV. O dereito á protección de datos	31
5. ¿Cara un dereito penal do inimigo?.....	32
6. Algunhas conclusión para debate	39
Bibliografía	43
Xurisprudencia.....	51

1. Introducción

Dicir que vivimos na era do *Big Data* semella a estas alturas unha frase redundante. Ou cuestionarse se a tecnoloxía veu para quedarse ao proceso xudicial incluso parece un absurdo. Non temos máis que mirar ao noso redor ou observar o noso día a día. A tecnoloxía constitúe unha ferramenta esencial á hora de relacionarnos, de traballar, de coidarnos ou, incluso de desfrutar. Concibir un sistema xudicial ou policial sen o uso da tecnoloxía nun mundo dixital como no que vivimos podería supoñer que estas institucións deixasen de ser funcionais ou que incluso perdesen o seu sentido.

Tamén podemos observar isto no mundo profesional. Non só nas empresas privadas onde o traballo sen algún tipo de ferramenta tecnolóxica fai anos que non se concibe, senón tamén na propia Administración Pública. Vimos como nos últimos anos as máis importantes organizacións internacionais e os Estados comezan a poñer o mundo dixital no centro da súa axenda xunto con cuestións tan importantes como o cambio climático ou o futuro da economía¹.

Afortunadamente a tecnoloxía xa fixo presenza tamén no procedemento xudicial vai anos. Algún dos feitos máis relevantes neste sentido foron a aprobación da Lei 18/2011, do 5 de xullo, reguladora do uso das tecnoloxías da información e a comunicación na Administración de Xustiza ou a implementación definitiva de Lexnet para as comunicacións entre órganos xudiciais e os operadores xurídicos como avogados e procuradores.

¹ “*Una Europa adaptada a la era digital*” é a segunda das seis prioridades da Comisión Europea para o período 2019-2024. Tamén podemos mencionar aquí todas os textos ou propostas lexislativas que, dende vai varios anos mostran como a cuestión tecnolóxica comeza a ser un dos epicentros da política europea e española: Directiva (UE) 2018/1972 do Parlamento Europeo e do Consello, do 11 de decembro do 2018, pola que se establece o Código Europeo das Comunicacións Electrónicas; Regulamento (UE) 2021/694 do Parlamento Europeo e do Consello do 29 de abril do 2021 polo que se establece o Programa Europa Dixital e polo que se derroga a Decisión (UE) 2015/2240; Proposta de Regulamento do 21 de abril do 2021 pola que se establecen normas armonizadas sobre a intelixencia artificial na Unión ou o plan de Xustiza Dixital 2030 en España. Para unha maior profundidade nestas cuestións *vid.* BUENO DE MATA, Federico (2022). La necesidad de regular la inteligencia artificial y su impacto como tecnología disruptiva en el proceso: de desafío utópico a cuestión de urgente necesidad. En: BUENO DE MATA, Federico (dir.). *El impacto de las tecnologías disruptivas en el derecho procesal*. España: Thomson Reuters Aranzadi, pp. 15 – 41. ISBN: 9788413455885.

Tamén, en concreto, no proceso penal. Por exemplo nas investigacións policiais e xudiciais. Cada avance científico como a luz ultravioleta, os reactivos químicos ou o microscopio foron introducíndose dun xeito case paralelo aos seus descubrimentos e ao seu uso no mundo empresarial ou civil para a mellora da eficacia e rapidez da procura dos vestixios do delito².

Unha das manifestacións que máis chamou a atención nos últimos anos desta chegada das tecnoloxías da información³ ao dereito e, en concreto á orde xurisdiccional penal e ás súas fases previas de investigación, son os coñecidos como sistemas de predición do risco dotados de intelixencia artificial⁴. Realmente as funcionalidades que presentan e que veremos neste traballo, de determinar que individuo pode ter máis posibilidades de cometer un delito ou onde é máis probable que se cometa un ilícito penal nas próximas horas podería cambiar dun xeito notable tal e como entendemos a labor xudicial e policial. Se cumprisen a súa función, os delitos poderían ser radicalmente diminuídos. Dentro deste estudo analizaremos estas ferramentas. Abarcaremos tanto os que veñen sendo chamados sistemas de Intelixencia Artificial Xudicial para a Valoración do Risco⁵ como os sistemas de predición de risco no ámbito policial, coñecidos polo seu termo en inglés *predictive policing*, dotados de IA.

² ORTIZ PRADILLO, Juan Carlos (2022). Inteligencia artificial, Big Data, tecnovigilancia y derechos fundamentales en el proceso penal. En: VILLEGAS DELGADO, César y MARTÍN RÍOS, Pilar (ed.). *El derecho en la encrucijada tecnológica. Estudios sobre derechos fundamentales, nuevas tecnologías e inteligencia artificial*. Valencia: Tirant lo Blanch, p. 107. ISBN: 9788411132947.

³ En adiante, poderemos referirnos a elas deste de xeito ou pola súas siglas en inglés, IT (*information technology*).

⁴ Esta será a denominación que empregaremos ao longo deste traballo para referirnos ao termo amplo, o que engloba os sistemas de IA no eido xudicial e no policial, por considerar que é a máis axeitada. Pero o certo é que ao longo de toda a literatura escrita sobre o tema non hai unanimidade na doutrina xurídica respecto a designación deste tipo de sistemas. Para referirnos á intelixencia artificial, tamén poderemos facelo empregando IA.

⁵ SIMÓN CASTELLANO, Pere (2021). *Justicia cautelar e inteligencia artificial. La alternativa a los atávicos heurísticos judiciales*. España: Bosch Editor, pp. 130 e ss. ISSN: 9788412315417. Nesta obra reciben esta denominación, que nos parece a máis axustada para referirnos aos sistemas de IA que se empregan no eido xudicial. Isto, por consideralo un termo que abrangue tanto aqueles sistemas que teñen unha función asistencial como os que puidesen ter unha capacidade de decisión autónoma. En adiante denominarémolos polas súas siglas IAXVR, denominación tamén empregada polo autor mencionado.

Neste punto semella oportuno fixar a definición de IA que imos a empregar neste traballo porque o certo é que é un termo no que non existe un acordo absoluto na doutrina. Para esta tarefa, consideramos que o máis óptimo vai ser referirnos á delimitación deste fenómeno contida na Proposta de Regulamento do Parlamento Europeo e do Consello polo que se establecen normas armonizadas en materia de intelixencia artificial (Lei de Intelixencia Artificial) e se modifican determinados actos lexislativos da Unión⁶. Segundo este texto, un sistema de IA é aquel software que pode, para un conxunto determinado de obxectivos definidos polos seres humanos, xerar información de saída como contidos, predicións, recomendacións ou decisións que inflúan nos medios cos que se relaciona. Ademais, este debe desenvolverse empregando unha ou varias das seguintes técnicas e estratexias: de aprendizaxe automático, incluídos o aprendizaxe automático supervisado, o non supervisado e o levado a cabo por reforzo, que empregan unha ampla variedade de metodoloxía, entre eles o aprendizaxe profundo; estratexias baseadas na lóxica e no coñecemento, especialmente a representación do coñecemento, a programación (lóxica) indutiva, as bases do coñecemento, os motores de inferencia e dedución, os sistemas expertos e de razoamento (simbólico); e estratexias estatísticas, estimación bayesiana, métodos de procura e optimización⁷.

Un exemplo claro deste sistemas de predición de risco dotados de IA segundo a definición que acabamos de fixar poderían ser COMPAS ou HART, que non deixaron indiferente a ninguén. Fronte os argumentos que os fomentan por supoñer unha mellora e un aumento da eficiencia destes operadores xurídicos, xurdiron as queixas, as advertencias e as reticencias pola súa afectación a varios dereitos fundamentais ou ás garantías procesuais tradicionais. Un dos debates máis distópicos arredor destes sistemas dotados de IA probablemente sexa aquel que se refire á posibilidade de que cheguen a substituír a algún operador xurídico⁸. Tamén houbo voces que quedaron a medio camiño e que afirmaban que o fenómeno da IA era unha innovación tecnolóxica con

⁶ En adiante, Proposta Regulamento IA ou PRIA.

⁷ Artigo 3.1 da Proposta de Regulamento de IA en relación co seu Anexo I.

⁸ BUENO DE MATA, Federico (2022). La necesidad de regular la inteligencia artificial y su impacto como tecnología disruptiva en el proceso: de desafío utópico a cuestión de urgente necesidad. En: BUENO DE MATA, Federico (dir.). *El impacto de las tecnologías disruptivas en el derecho procesal*. España: Thomson Reuters Aranzadi, p. 16. ISBN: 9788413455885.

características que se axustaban á normativa nese momento en vigor, pero advertindo que determinadas funcionalidades precisaban dunha adaptación ou replantexamento⁹.

A intención deste traballo é recoller e reflexionar sobre todas estas cuestións. Sobre os riscos deste tipo de ferramentas, como poderían afectar no noso actual procedemento xudicial, cales serían os dereitos fundamentais afectados e as consecuencias que poderían chegar a ter na nosa política criminal. O noso obxectivo é organizar todas esas ideas e reticencias.

Tamén queremos aportar novas dúbidas ou cuestións, moitas delas, sen considerar que poidamos ofrecerlle pola contra unha resposta totalmente axeitada. Pero será un primeiro paso. Cuestionarnos todas as variables posibles e reflexionar sobre elas é o xeito que consideramos óptimo para avanzar no estado do asunto. Pois só cas preguntas axeitadas, pode evolucionar o eido científico¹⁰.

Tamén queremos reflexionar sobre os elementos positivos. Sobre como poder regulalos nesta fase inicial da súa introdución no noso procedemento xudicial. O medo e as reticencias neste momento son necesarios. Este temor fronte unha tecnoloxía emerxente fainos estar nas mellores condicións para decidir se definir e limitar o seu progreso ou ampliar o seu alcance¹¹.

2. O emprego de sistemas de predición do risco no eido penal e policial.

Situación actual

Cómpre dicir que a avaliación do risco de comisión ou reiteración delituosa non é algo novo no noso sistema criminal, non vén necesariamente da man desta denominada

⁹ VIDA FERNÁNDEZ, José (2018) Los retos de la regulación de la inteligencia artificial: algunas aportaciones desde la perspectiva europea. En: DE LA QUADRA-SALCEDO, Tomás (dir.) et al. *Sociedad digital y derecho*. Madrid: Ministerio de Industria, Comercio y Turismo, Red.es, Boletín Oficial del Estado, pp. 205 – 206. ISBN: 9788434024830.

¹⁰ GRECO, Luís (2019). La criminalización en el estado previo: un balance del debate alemán. En: ALONSO RIMO, Alonso (dir.) y COLOMER BEA, David (coord.). *Derecho penal preventivo, orden público y seguridad ciudadana*. España: Aranzadi Thomson Reuters, p. 108. ISBN: 9788413099316.

¹¹ MIRÓ LLINARES, Fernando (2020) Predictive Policing: Utopia or Dystopia? On attitudes towards the use of Big Data algorithms for law enforcement. En: *Revista de internet, derecho y política*, núm. 30, p. 10. ISSN: 16998154.

cuarta revolución industrial, aínda que agora chame tanto a atención da doutrina ou da sociedade en xeral.

A “seguridade” e todo o relacionado con ela vén adquirindo nos últimos anos un protagonismo indiscutible en todos os eidos entre eles, o institucional. Os Estados e as entidades supranacionais veñen adoptando medidas de todo tipo neste sentido, das que aínda non se coñece cal son o seu verdadeiro alcance ou consecuencias. Tamén asumiron que o poder e a forza non son suficientes, que é preciso outro tipo de medidas como poden ser as accións conxuntas entre varios Estados ou o emprego doutro tipo de ferramentas como a diplomacia, a intelixencia ou a axuda humanitaria. É dicir, a seguridade non só se limita á súa perspectiva tradicional senón que vai máis alá, tendo en conta perspectivas políticas, económicas, socioculturais e ambientais¹². O problema atopámolo principalmente cando estas novas medidas chegan a limitar dereitos dos cidadáns. É dicir, cando se levan a cabo políticas ou leis que recortan eses dereitos dos cidadáns para protexelos doutras ameazas a eses mesmos dereitos¹³. Cuestión que, en todo caso, non forma parte do obxecto deste estudo, pero que xa están sendo criticadas duramente por gran parte da doutrina e que incluso comeza a ser comparada co fenómeno do *Gran Hermano* representado pola coñecida novela de George Orwell, 1984^{14/15}. Se ben é certo, esta fixación pola seguridade e, seguindo a liña de González Cussac, consideramos que

¹² GONZÁLEZ CUSSAC, José Luís (2019). Seguridad e incertidumbre: un derecho penal híbrido. En BARONA VILAR, Silvia (ed.), *Claves de la justicia penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad*, Valencia: Tirant lo Blanch, p. 504. ISBN: 9788413360744.

¹³ GONZÁLEZ CUSSAC, José Luís y FLORES GIMÉNEZ, Fernando (2018). Seguridad global y derechos fundamentales. Una propuesta metodológica. En GONZÁLEZ CUSSAC José Luis y FLORES GIMÉNEZ, Fernando (coord.) *Seguridad y derechos. Análisis de las amenazas, evaluación de las respuestas y valoración del impacto en los derechos fundamentales*. Valencia: Tirant lo Blanch, pp. 32 e 33. ISSN: 9788413130873.

¹⁴ Vid. COLMENERO GUERRA, José Antonio (2022). La protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales vinculados al «discurso terrorista». En GALÁN MUÑOZ, Alfonso y GÓMEZ RIVERO, María del Carmen (dir.) *La represión y persecución penal del discurso terrorista*. Valencia: Tirant lo Blanch, pp. 627-720. ISBN: 9788413979700; SILVA SÁNCHEZ, Jesús María (2011). *La expansión del derecho penal: aspectos de la política criminal en las sociedades postindustriales*, Madrid: Edisofer. ISBN: 9788496261914.

¹⁵ De feito, o recente artigo 15 da Lei Orgánica 7/2021, do 26 de maio, de protección de datos persoais tratados para fins de prevención, detección, investigación e axuízamento de infraccións penais e de execución de sancións penais que, dun xeito bastante amplo, permite os sistemas de gravación de imaxes e son polas Forzas e Corpos de Seguridade en prol de “prever, detectar ou investigar a comisión de infraccións penais e a protección e prevención fronte as ameazas contra a seguridade pública”

non é que non estea xustificada. Só temos que botar unha ollada ao noso arredor: pensemos na nova realidade do terrorismo, nos conflitos armados que cada vez están máis preto da antiga Europa, da espionaxe, do crime organizado transnacional, dos ciberataques ou nas novas técnicas de ciberdelincuencia que cada vez afectan máis ao cidadán de a pé^{16/17}.

Da man desta fixación que acabamos de destacar, vén unha evidente sensación social de inseguridade ou de risco que non deixou indiferente ao noso dereito penal e, especialmente, á política criminal española e europea. Esta evocación xeneralizada non se debe de xeito exclusivo ao aumento dos perigos obxectivos, senón á súa percepción subxectiva, colectiva, como riscos¹⁸. Deste xeito, o dereito penal, cun corte anglosaxón, está comezando a deixar de lado o criterio de perigosidade criminal, entendida como característica psicolóxica, é dicir, individual e subxectiva do delincuente, para impoñer por exemplo unha medida de seguridade e, pola contra, está abrazando un criterio establecido no risco¹⁹.

Segundo Beck, o risco é un intento institucionalizado de colonizar o futuro, un mapa cognitivo²⁰. É dicir, o risco é a estimación da probabilidade da exposición a un perigo. Este risco non existe máis alá do coñecemento que temos del, ten unha categoría diferenciada do perigo e ten a capacidade de determinar a interpretación e os

¹⁶ Segundo o *Estudio sobre la cibercriminalidad en España* do Ministerio de Interior, a falsificación informática duplicou as súas cifras dende o ano 2016 ata o ano 2020. Pero, no mesmo período de tempo, a fraude informática pasou de 70.178 feitos coñecidos a 257.907 no 2020. LÓPEZ GUTIÉRREZ, Javier, et al. (2020) *Estudios sobre la cibercriminalidad en España*. España: Ministerio de Interior, Gobierno de España.

¹⁷ GONZÁLEZ CUSSAC, José Luís (2019). *Seguridad e incertidumbre, cit.*, p. 504.

¹⁸ BRANDARIZ GARCÍA, José Ángel (2014) *El gobierno de la penalidad: la complejidad de la política criminal contemporánea*, Madrid: Dykinson, p. 76. ISBN: 9788490851005.

¹⁹ ROMEO CASABONA, Carlos María (2018) Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad. *Revista de Derecho, Empresa y Sociedad (R.E.D.S)*, núm. 13, p. 40. ISSN-e: 23404647.

²⁰ BECK, Ulrich (2002). *La sociedad del riesgo global*, Madrid: Siglo XXI de España Editores, p. 5. ISBN: 8432310832. A partir de cuxa obra comezou a denominarse a este modelo social postindustrial na que vivimos como “sociedade do risco”.

comportamentos colectivos²¹. Levado ao ámbito que nos incumbe neste traballo, o risco é a posibilidade de que se produza un evento delituoso ou a probabilidade de delinquir que presenta unha persoa de forma obxectiva²².

Como xa remarcamos en liñas anteriores, esta procura da predición do risco de delinquir non comeza cos sistemas de intelixencia artificial que nas seguintes liñas serán enumerados, senón que tal e como expón Romeo Casabona ten a súa orixe nos coñecidos como métodos estatísticos e actuariais^{23/24}. Este tipo de métodos procuran realizar un prognóstico de inserción dun suxeito concreto sobre o que se está levando a cabo o estudo, nun grupo prototípico de delincuentes. Esta clasificación realízase mediante a apreciación dunha serie de características cuxa frecuencia no grupo apunta cara unha maior reiteración delituosa, e non tanto pola propia individualidade do suxeito²⁵. É dicir, estamos ante o emprego de métodos estatísticos, en vez de clínicos, que consisten en grandes bases de datos para determinar os diferentes niveis de actuación criminal relacionados cun ou máis trazos grupais co obxectivo de predicir a conducta criminal pasada, presente ou futura e de administrar unha solución político-criminal²⁶.

Na nosa opinión esta é a idea fundamental que debemos ter en conta durante calquera análise dos sistemas de IA que van a ser examinados nestas liñas, e que

²¹ BRANDARIZ GARCÍA, José Ángel (2014). *El gobierno de la penalidad*, cit., pp. 76-77.

²² ROMEO CASABONA, Carlos María (2018). *Riesgo*, cit., p. 40.

²³ *Ibid*, pp. 39-55.

²⁴ O termo de xustiza actuarial ou *actuarial justice* foi acuñado por Malcolm Feeley e Jonathan Simon a comezos dos anos 90 e encadrárono no que eles definiron como a Nova “Penoloxía” ou *the New Penology*, definíndoo como unha metodoloxía específica que engloba unha serie de prácticas concretas, e descartan a súa definición como unha corrente política. *Vid.* FEELEY, Malcon y SIMON, Jonathan (1994). *Actuarial Justice: The Emerging New Criminal Law*. En NELKEN, David (ed.) *The futures of Criminology*, London: SAGE Publications, pp. 173-201. ISBN: 0803987145.

²⁵ ROMEO CASABONA, Carlos María (2018). *Riesgo*, cit., p. 42. A crítica deste tipo de metodoloxías encadradas dentro do adxectivo actuariais non é escasa e serve para comprender en que consisten exactamente *vid.* RIVERA BEIRAS, Iñaki. (2015) *Actuarialismo penitenciario: su recepción en España. Crítica penal y poder: una publicación del Observatorio del Sistema Penal y los Derechos Humanos*, núm. 9, pp. 102-144. ISSN-e: 20143753; GUTIÉRREZ, Mariano Hernán (2008). *Punitivismo y actuarialismo en la Argentina. V Jornadas de Sociología de la UNLP*, 10, 11 y 12 de diciembre de 2008, La Plata, Argentina: Memoria Académica.

²⁶ HARCOURT, Bernard E. (2007). *Against prediction: profiling, policing and punishing in an actuarial age*. Chicago: The University of Chicago Press, p. 1. ISBN: 9780226316147.

consideramos que en moitas exposicións sobre o tema se obvia ou se esquece. O método vai basearse sempre no encaixe do suxeito nun grupo determinado, conformado por mostras que aglomeran numerosas experiencias de suxeitos anteriores. É dicir, estamos valorando a probabilidade da futura comisión delituosa dunha persoa polo comportamento pasado doutros suxeitos.

Quizais un dos sistemas de predición de risco baseados en intelixencia artificial máis coñecidos é o famoso COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*) desenvolto por Northpointe, Inc. Este sistema comezou a resoar e a ser coñecido ao longo do mundo tras a famosa sentenza *State vs. Loomis* da *Wisconsin Supreme Court* do 13 de xullo do 2016. COMPAS é un sistema de predición de risco cuxos principais obxectivos son establecer unha escala de risco e unha escala de necesidades dun determinado suxeito. Este sistema naceu co obxectivo de ser empregado nunha fase de execución e establece un nivel de risco de reincidencia dunha determinada persoa e cales son os ámbitos nos que se deben tomar medidas (emprego, educación e coñecemento) para procurar a súa rehabilitación e reinserción²⁷. Centrándonos no que é obxecto de estudo deste traballo, a predición do risco de reincidencia de COMPAS realízase cun cuestionario cun total de 137 preguntas que se separan en varias seccións nas que, ademais de procurar coñecer os antecedentes criminais do individuo, posibles adicións, ou cales poderían ser as reaccións ante determinadas situacións, tamén se analizan os antecedentes criminais da familia, a formación do individuo, a súa residencia, cales son os seus “colegas” ou o ambiente social no que se relaciona. Con estas respostas, o sistema COMPAS realiza unha predición do risco de reincidencia dese suxeito poñéndoo en relación cunha gran base de datos e establecendo un nivel de risco como “baixo”, “medio” ou “alto”²⁸. Se ben as críticas a COMPAS foron numerosas e de distinta índole, a máis coñecida e coa que imos a quedarnos neste punto, sen prexuízo de que máis adiante analicemos cada unha delas en profundidade, é a que sinala que este sistema posúe un criterio de corte racista. Pois aprecia de xeito evidente, un maior risco de reincidencia

²⁷ Este último aspecto da ferramenta COMPAS apenas se menciona cando se fala dela e consideramos que, se ben non é algo novidoso, podería chegar a ser de gran utilidade se se puidesen chegar a realizar estas intervencións.

²⁸ FREEMAN, Katherine (2016). Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in *State v. Loomis*. *North Carolina Journal of Law & Technology*, v. 18, 2016, pp. 79 – 83.

nas persoas de raza negra. Volvendo á sentenza mencionada, esta confirma a decisión do tribunal de primeira instancia de darlle valor a esta estimación do risco do recorrente de volver a delinquir, de empregala en sede de imposición da pena e nega que, efectivamente, houbera unha vulneración do dereito ao debido proceso.

Outro sistema moi coñecido neste eido é PredPol²⁹ que agora, tal e como podemos ver na súa páxina web, intégrase dentro dunha ferramenta de xestión de comisarías chamada Geolitica³⁰. PredPol emprégase en numerosas comisarías de EE.UU. e preséntase como un instrumento de auxilio policial con capacidade de “predicir eventos críticos”. Realmente o que fai PredPol é facer unha sorte de mapa onde fixa puntos de calor ou *hot spot*, fixando onde é máis probable que se cometa un determinado tipo de delito. Segundo a súa páxina web, PredPol ten en conta unha máxima que considera practicamente absoluta: no lugar onde foi cometido un tipo de delito é máis probable que se cometa outro semellante. Deste xeito, empregando datos de entre os últimos 2 e 5 anos, como o número do que aquí coñecemos como atestado, o tipo de crime ou “evento” e a localización do incidente, o sistema crea estes puntos de calor que van actualizándose diariamente. A mesma páxina resalta que non se recollen datos demográficos, étnicos ou socio-económicos, mais as críticas dos posibles riscos que poden provocar este tipo de sistemas non foron escasas. Críticas que, aínda que teremos ocasión de comentalas máis en profundidade, resaltan o perigo efectivo de estigmatizar determinadas zonas dunha cidade, parece que liberando aos métodos policiais “tradicionais” de toda posibilidade de estigmatización.

No eido europeo, en concreto nos Países Baixos, podemos atopar outro exemplo dunha ferramenta semellante á anterior: CAS, probada en varias cidades holandesas e que, como PredPol, ten o obxectivo de proporcionar presenza policial en zonas previsiblemente máis necesitadas da mesma.

Tamén deste lado do Atlántico podemos falar de HART (*Hart Assessment Risk Tool*), ferramenta implementada pola Policía de Durham, no Reino Unido. Este sistema

²⁹ <https://www.predpol.com/> [data de acceso: 6 de setembro do 2022]

³⁰ <https://geolitica.com/> [data de acceso: 6 de setembro do 2022]

fai unha predición de cal é o risco de que un determinado suxeito volva a cometer máis crimes nun período de dous anos. Se ben non é unha ferramenta decisoria de se un detido ten que manterse en dependencias policiais ou non, emprégase para determinar se unha persoa ten que formar parte dun determinado programa de rehabilitación ou non.

Finalmente, e aínda que nun primeiro momento semelle que non estamos ante un sistema de predición do risco no sentido exposto neste traballo, temos que traer a colación a VeriPol. Esta ferramenta que foi creada para a detección de denuncias falsas para todo tipo de delitos, pero hoxe en día só se emprega para o eido dos roubos de teléfonos móbiles. Aínda que o Ministerio de Interior presumiu dende un primeiro momento da súa gran importancia e a súa gran eficacia, o certo é que tampouco VeriPol quedou exento de polémica. Do mesmo xeito que as anteriores, estas cuestións serán tratadas nos seguintes apartados, cando falemos da afectación que este tipo de tecnoloxías poden provocar aos dereitos fundamentais³¹.

Ata o momento procuramos dar unha definición o máis exhaustiva posible do que son os sistemas de intelixencia artificial de predición de risco, así como unha mostra dos exemplos que xa están funcionando, mais aínda non falamos de que di o lexislador sobre este tipo de metodoloxías.

3. Regulación actual

No momento de elaboración do presente traballo, non existe unha regulación específica sobre este tipo de sistemas. Se ben é certo, e como teremos a ocasión de expoñer nas seguintes liñas, os documentos de traballo, de recomendacións, textos de *soft law* ou incluso a Proposta de Regulamento sobre intelixencia artificial que xa mencionamos, viñéronse sucedéndose durante os últimos tempos de xeito moi cuantioso, tanto no relativo ao propio eido xudicial, como de xeito xeral³².

³¹ *Infra* apartado 4.B).

³² Nesta materia, é dicir, a intelixencia artificial podemos mencionar as Directrices éticas para unha IA fiable do Grupo de expertos de alto nivel sobre intelixencia artificial constituído pola Comisión Europea de 8 de abril do 2019, dispoñible en: <https://op.europa.eu/o/opportal-service/download-handler?identifier=d3988569-0434-11ea-8c1f->

Pero antes diso, aínda que como xa expuxemos, non existe unha regulación dirixida específica e exclusivamente a este tipo de ferramentas, si que podemos encaixalas dentro do marco normativo da Unión Europea sobre a protección de datos. Pois, os datos, aos que moitos autores, empresarios e políticos veñen denominando como o petróleo deste século XXI, son a unidade que nutre este tipo de sistemas³³. O paquete de normas sobre esta materia está conformado polo recente Regulamento (UE) 2022/868 do Parlamento Europeo e do Consello do 30 de maio do 2022 relativo á gobernanza europea de datos e polo que se modifica o Regulamento (UE) 2018/1724 (Regulamento de Gobernanza de Datos)³⁴, o Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello do 27 de abril do 2016 relativo á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos e polo que se derroga a Directiva 95/46/CE³⁵ e a Directiva (UE) 2016/680 do Parlamento Europeo e do Consello do 27 de abril do 2016 relativa á protección das persoas físicas no que respecta ao tratamento de datos persoais por parte das autoridades competentes para fins de prevención, investigación, detección ou axuizamento de infraccións penais ou de execución de sancións penais, e á libre circulación destes datos e pola que se derroga a

[01aa75ed71a1&format=pdf&language=es&productionSystem=cellar&part=](https://op.europa.eu/o/opportal-service/download-handler?identifier=ac957f13-53c6-11ea-aece-01aa75ed71a1&format=pdf&language=es&productionSystem=cellar&part=); o Libro Branco sobre intelixencia artificial, un enfoque europeo orientado á excelencia e á confianza do Grupo de expertos de alto nivel sobre intelixencia artificial constituído pola Comisión Europea do 19 de febreiro do 2020, dispoñible en: <https://op.europa.eu/o/opportal-service/download-handler?identifier=ac957f13-53c6-11ea-aece-01aa75ed71a1&format=pdf&language=es&productionSystem=cellar&part=>; a Proposta de Regulamento de Intelixencia Artificial, dispoñible en: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF ou *Regulatory divergences in the draft AI act. Differences in public and private sector obligations* do Parlamento Europeo de maio do 2022, dispoñible en: [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729507/EPRS_STU\(2022\)729507_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729507/EPRS_STU(2022)729507_EN.pdf). Se ben é certo, existen outros textos procedentes da UE que abordan de xeito indirecto cuestións sobre IA, estes son os máis destacados nesta materia específica.

³³ Segundo o Libro Branco sobre Intelixencia Artificial do Grupo de expertos de alto nivel sobre intelixencia artificial constituído pola Comisión Europea, os sistemas de intelixencia artificial son aqueles sistemas “deseñados por seres humanos que, tendo un obxectivo complexo, actúan na dimensión física ou dixital mediante a percepción do seu entorno a través da obtención de datos, a interpretación dos datos estruturados ou non estruturados que recompilan, o razoamento sobre o coñecemento ou o procesamento da información derivados deses datos, e decidindo a acción ou accións óptimas que deben levar a cabo para acadar o obxectivo establecido.”

³⁴ O cal, será de aplicación a partir do vindeiro 24 de setembro do 2023.

³⁵ En adiante, Regulamento Xeral de Protección de Datos ou RXPD.

Decisión Marco 2008/977/JAI del Consello³⁶. Esta última foi incorporada recentemente ao ordenamento xurídico español a través da tan esperada Lei Orgánica 7/2021, do 26 de maio, de protección de datos persoais tratados para fins de prevención, detección, investigación e axuizamento de infraccións penais e de execución de sancións penais^{37/38}.

No suposto de que nos atopemos dentro do seu eido de aplicación, é dicir, no tratamento automatizado ou non automatizado de datos persoais contidos ou destinados a ser incluídos nun ficheiro, realizado polas autoridades competentes con fins de prevención, detección, investigación e axuizamento de infraccións penais e de execución de sancións penais, ademais da protección e prevención fronte ás ameazas contra a seguridade pública (art. 2 LOPDIP), poderemos aplicar a LO 7/2021. É dicir, semella que será de aplicación ao tratamento de datos realizados nos sistemas de predición de risco dotados de IA empregados en España, aos que vimos facendo referencia neste traballo. Aínda que este texto legislativo merece moitas máis liñas de análise, non é materia deste estudo esa labor, polo que imos a centrarnos na cuestión que nos ocupa.

O artigo 14 da LO 7/2021 prohíbe as decisións baseadas unicamente nun tratamento automatizado, incluída a elaboración de perfís que produzan efectos xurídicos negativos para o interesado ou que lle afecten de xeito significativo. É dicir, prohíbense a toma de decisións mediante ferramentas nas que a intervención humana é nula ou, incluso, meramente simbólica^{39/40}. Polo tanto, as ferramentas das que vimos falando, os

³⁶ En adiante, Directiva 2016/680.

³⁷ En adiante, LO 7/2021 ou LOPDIP.

³⁸ E, dicimos esperada, porque a demora na transposición da Directiva 2016/680 supuxo a imposición a España por parte do Tribunal de Xustiza da Unión Europea o pago dunha suma ao tanto alzado de 15.000.000 de euros e unha multa coercitiva diaria de 89.000 euros ata a súa efectiva transposición o comunicación de medidas de transposición desta [Sentencia do Tribunal de Xustiza (Sala Octava) do 25 de febreiro do 2021 do asunto C-658/19].

³⁹ GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*. Adoptadas el 3 de octubre de 2017 y revisadas el 6 de febrero de 2018, p. 23.

⁴⁰ Palma Ortigosa dun xeito moi claro establece catro grados de intervención do humano en función da súa presencialidade. En primeiro lugar, a plena automatización, onde é o sistema impón un resultado e este se convirte automaticamente nunha decisión que afecta a un particular. En segundo lugar teríamos os supostos nos que aínda existindo unha plena automatización, ofrécenselle ao humano varias opcións para

sistemas de predición de risco dotados de IA, poderían encaixar de xeito evidente dentro desta definición. É dicir, as decisións que sexan única e exclusivamente tomadas con este tipo de sistemas estarían, nun principio, prohibidas coas salvagardas que nas seguintes liñas analizaremos⁴¹. Aínda que non sería obxecto deste traballo, consideramos que é relevante reparar e definir cuestións como que se consideran “efectos xurídicos negativos” ou que “afecten significativamente” ao interesado. Moi acertadamente, Guzmán Fluja pon enriba da mesa estas dúas incógnitas. Por un lado, pregúntase que sucedería coas decisións individuais baseadas en tratamentos automatizados que poidan producir un “efecto xurídico positivo”, que incluso poderían encaixar na “afectación significativa” para o interesado. Pero, ademais, o autor tamén cuestiónase que debe entenderse por “afectación significativa”⁴². Ademais, na nosa opinión debe engadirse outra incógnita. O tratamento automatizado prohibese respecto a todo tipo de datos persoais e interesados⁴³. Non debemos esquecer que nun procedemento penal non só estamos tratando datos do investigado, acusado ou condenado, senón que tamén da propia

que el decida entre os distintos resultados. Nesta última, a relevancia principal posúea a máquina que é quen toma realmente a decisión, pois o humano non pode ter en conta outras variables e, en moitos supostos, incluso non poderá saber cales foron as variables que se tiveron en conta. En terceiro lugar, fala das “decisións semiautomatizadas” onde o resultado ofrecido polo sistema de intelixencia artificial é valorado pola persoa, xunto outros elementos para a toma de decisións. Finalmente, atopamos os supostos nos que a decisión do sistema é un elemento menor dentro de todo o proceso moito máis amplo. *Vid.* PALMA ORTIGOSA, Adrián (2022). El ciclo de vida de los sistemas de inteligencia artificial. Aproximación técnica de las fases presentes durante el diseño y despliegue de los sistemas algorítmicos. En COTINO HUESO, Lorenzo (dir.) y BAUZÁ REILLY, Marcelo (coord.). *Derechos y garantías ante la inteligencia artificial y las decisiones automatizada*, Madrid: Thomsom Reuters Aranzadi, pp. 45 – 48. ISBN: 9788411244992.

⁴¹ Temos que mencionar neste punto que existen autores que aínda que asumen que a neutralidade tecnolóxica non existe pero, advirten que tampouco deberíamos caer no extremo oposto de considerar que toda intervención humana é sempre mellor. Chegan a dicir que incluso podería introducir discriminacións ausentes polo sistema. *Vid.* ROIG I BATALLA, Antoni (2020). *Las garantías frente a las decisiones automatizadas. Del Reglamento General de Protección de Datos a la gobernanza algorítmica*, Barcelona: Bosch Constitucional, pp. 67 – 68. ISBN: 9788412201574.

⁴² GUZMÁN FLUJA, Vicente C. (2021). Proceso penal y justicia automatizada, *Revista General de Derecho Procesal*, núm. 53, pp. 26 – 27. ISSN: 16969642.

⁴³ Segundo o artigo 3.1 da Directiva 2016/680 e o 5.a) da LO 7/2021 o interesado é toda persoa física identificada ou identificable titular dos datos persoais que están sendo tratados. Engaden estes dous textos legais que “se considerará persoa física identificable a toda persoa cuxa identidade poida determinarse, directa ou indirectamente, en particular mediante un identificador, como por exemplo un nome, un número de identificación, uns datos de localización, un identificador en liña ou un ou varios elementos propios da identidade física, fisiolóxica, xenética, psíquica, económica, cultural ou social da mencionada persoa.”

vítima. Unha cuestión que debemos formularnos é que sucedería cando se produza un efecto positivo para, por exemplo, o autor, pero un efecto negativo para a vítima do delito.

Como xa adiantamos, este precepto do mesmo xeito que se reflexa no artigo 11 da Directiva, dun modo semellante a como o fai o 22 do RXPD⁴⁴, non establece unha prohibición absoluta sobre esta toma de decisións totalmente automatizada, senón que deixa en mans do lexislador, estatal ou europeo, a posibilidade de habilitalas. Esta concesión estaría condicionada a uns mínimos de respecto aos dereitos e liberdades do interesado, fixando, como un dos requisitos de salvagarda destes a obrigaón de intervención humana no proceso de revisión da decisión adoptada.

Esta decisión, moi acertada, do lexislador europeo⁴⁵ prevía o futuro ao que nos estábamos dirixindo, a inminente e, en moitos casos, necesaria, automatización de parte da Xustiza. Visto o anterior, podemos comprobar que a liña seguida pola UE neste punto é non atender única e exclusivamente ao grao de autonomía do sistema de toma de decisións automatizados, senón fixarse máis nos efectos que estes sistemas poden xerar nese concreto sector na esfera dos particulares afectados por esta⁴⁶.

Non podemos obviar tampouco neste punto que, de acordo co artigo 27 da Directiva 2016/680 e o artigo 35 da LO 7/2021 deberá realizarse unha avaliación de impacto relativa á protección de datos polo responsable do tratamento⁴⁷ pois co emprego destes sistemas de predición de risco atopariámonos antes esas “novas tecnoloxías” que pola súa natureza, alcance, contexto e fins suporían un alto risco para os dereito e

⁴⁴ Palma Ortigosa di que no artigo 22, máis que ante unha prohibición xeral, o que existe en realidade é a definición dun tratamento particular que só poderá levarse a cabo a través dunhas determinadas bases de lexitimación que o responsable deberá ter en conta á hora de levar a cabo este tratamento. *Vid.* PALMA ORTIGOSA, Adrián (2019) Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos. *Revista General de Derecho Administrativo*, núm. 17, 2019, p. 4. ISSN: 16969650.

⁴⁵ Que posteriormente foi confirmada e seguida polo lexislador español.

⁴⁶ PALMA ORTIGOSA, Adrián (2019) El ciclo de vida de los sistemas, *cit.*, p. 47.

⁴⁷ Segundo o artigo 5.g) da LO 7/2021 será responsable do tratamento a autoridade que soa ou conxuntamente con outra, determine os fins e os medios de tratamento de datos persoais; no suposto de que os fins e medios do tratamento esteen determinados polo Dereito da Unión Europea ou pola lexislación española, estas normas poderán designar ao responsable do tratamento, ou ben os criterios para o seu nomeamento.

liberdades das persoas físicas. Con anterioridade á modificación introducida pola LO 7/2021, o artigo 236 sexies da Lei Orgánica 6/1985, do 1 de xullo, do Poder Xudicial⁴⁸ establecía que serían responsables dos ficheiros xurisdicionais o órgano xudicial ou a oficina xudicial ante os que se tramiten os procesos cuxos datos se incorporen ao ficheiro. En cambio, tras a modificación introducida pola Disposición Adicional Terceira da LO 7/2021, retirouse a atribución expresa deste papel ao órgano xudicial. Polo tanto, na nosa opinión, non deixa claro o ordenamento xurídico español quen son os responsables do tratamento no proceso xudicial penal. Se acudimos ao portal web institucional do Consello Xeral do Poder Xudicial podemos observar como este atribúe este papel de responsable ao órgano xudicial onde se tramite o procedemento que conteña os datos obxecto do tratamento⁴⁹. Se ben parece lóxico que o Consello siga mantendo esta atribución, chama a atención o despoxo lexislativo desta competencia.

Aínda que serán precisas normas nacionais de desenvolvemento^{50/51}, semella que a norma que permita o emprego de ferramentas de predición de risco dotadas de IA vai ser o futuro e posible Regulamento sobre IA do que, dende vai pouco máis dun ano xa coñecemos o seu proxecto. Esta Proposta de Regulamento sobre IA pretende establecer, dun xeito armonizado⁵², un marco de regulación nesta materia, fixando unha definición deste fenómeno, a prohibición dunha serie de prácticas e a clasificación de determinados sistemas de IA. Esta restrición e ordenación que, como podemos ver neste texto, realizárase segundo a afectación sobre os dereitos e liberdades ademais de polo tipo de

⁴⁸ En adelante, LOPX.

⁴⁹ Enlace directo a esta información institucional: <https://www.poderjudicial.es/cgpj/es/Temas/Direccion-de-supervision-y-control-de-proteccion-de-datos/Proteccion-datos-en-Justicia/Responsables-y-encargados-de-tratamiento/> [data de acceso: 6 de setembro do 2022].

⁵⁰ DE HOYOS SANCHO, Montserrat (2022). El proyecto de Reglamento de la Unión Europea sobre inteligencia artificial, los sistemas de alto riesgo y la creación de un ecosistema de confianza. En BARONA VILAR, Silvia (ed.) *Justicia poliédrica en periodo de mudanza (Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad)*, Valencia: Tirant lo Blanch, 2022, p. 416. ISBN: 9788411135702.

⁵¹ Para comezar, parece evidente que, como mínimo, o emprego dos sistemas de predición de risco dotados de IA deberían vir acompañados dunha reforma, polo menos, parcial, da nosa decimónica Lei de Axuízamento Criminal.

⁵² De feito, de aí a elección do regulamento como instrumento para levar a cabo esta regulación tal e como se expón no propio Proxecto no apartado 2.4 da Exposición de Motivos.

tecnoloxía empregada, permitiría establecer unha serie de garantías ou cautelas mínimas que deberían tomarse para a posibilidade de comercialización e uso no sector privado e público. A estrutura da Proposta está condicionada pola clasificación do risco atribuído ao sistema de IA concreto: inadmisible, alto, limitado e mínimo. Son os sistemas da segunda categoría os que ocupan a maior parte do texto e están integrados por dous grupos: os compoñentes de seguridade dos produtos que de acordo coa lexislación sectorial da UE enumerada no Anexo II están sometido a unha avaliación de conformidade por terceiros e, os sistemas enumerados no Anexo II, que poderá ser modificado pola Comisión mediante actos delegados⁵³.

Como podemos observar neste último Anexo, serán considerados sistemas de IA de alto risco aqueles destinados a “empregarse por parte das autoridades encargadas da aplicación da lei para levar a cabo avaliación de riscos individuais de persoas físicas co obxectivo de determinar o risco de que cometan infraccións penais ou reincidan na súa comisión, así como o risco para as potenciais vítimas dos delitos”, as destinadas “a empregarse por parte das autoridades encargadas da aplicación da lei para predicir a frecuencia ou reiteración dunha infracción penal real ou potencial coa base de elaboración de perfís de persoas físicas”, as “destinadas a empregarse para levar a cabo análises sobre infracción penais en relación con persoas físicas que permitan ás autoridades encargadas da aplicación da lei examinar grandes conxuntos de datos complexos vinculados ou non vinculados, dispoñibles en diferentes fontes e formatos, para detectar modelos descoñecidos ou descubrir relación ocultas nos datos” ou as orientadas a “axudar a unha autoridade xudicial na investigación e interpretación de feitos e da lei, así como a aplicación da lei a un conxunto concreto de feitos”. Semella, polo tanto, que as ferramentas das que vimos falando encaixarían perfectamente nesta clasificación. En consecuencia, para poder empregalas, previsiblemente terían que cumprir toda unha serie de requisitos enumerados nos artigos 9 a 51 deste texto, sobre sistemas de xestión de risco, gobernanza de datos, documentación técnica, transparencia e comunicación e información aos usuarios, etc. Salvo que nos atopemos ante sistemas de identificación biométrica remota, nos que será preciso unha auditoría externa de cumprimento

⁵³ DE MIGUEL ASENSIO, Pedro Alberto (2021). Propuesta de Reglamento sobre inteligencia artificial. *Diario la Ley Unión Europea*, núm. 92, pp. 23 – 24. ISSN-e: 2255551X.

normativo, semella previsible que a consumación dos requisitos destes sistemas se confirme cunha sorte de declaración responsable de cumprimento normativo.

Visto o anterior, polo momento e durante os vindeiros meses, imos ter que conformarnos ca exclusión deste tipo de sistemas de IA na nosa xustiza penal. Por un lado, pola prohibición non absoluta da LO 7/2021 de toma de decisións totalmente automatizada e pola ausencia de regulación expresa que autorice este tipo de sistemas. Pero, non sería unha sorpresa que, a partir do vindeiro 2023, comecemos a ver na propia UE, ou incluso en países do noso entorno, a proliferación de normativa que controle o emprego da IA e incluso regule o uso deste tipo de ferramentas no eido da investigación e axuízamento de delitos, que en moitos supostos tan necesarias se fan nesta era dixital⁵⁴.

4. Riscos e afectación a dereitos fundamentais

As bondades que poden ter este tipo de ferramentas son evidentes: a celeridade dos procedementos, a eficiencia dos mesmos e, como non podía ser doutra forma, o aumento da seguridade⁵⁵. Realmente parece que este último é o obxectivo principal que procuran estes sistemas, a certeza en todas as súas manifestacións⁵⁶. Concepto que no eido penal, tradúcese nun sentido amplo nunha redución da comisión de delitos. Os seus beneficios semellan evidentes. Poden xerar paz e benestar social, pero os seus perigos tamén son numerosos⁵⁷: o aumento da discriminación, a desigualdade, a perversión do

⁵⁴ VALLS PRIETO, Javier (2017). *Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial*. Madrid: Dykinson, p. 49. ISBN: 9788491484752.

⁵⁵ Seguridade que, segundo Barona Vilar, deixa atrás a súa categoría de garantía constitucional para erixirse nun ben e incluso, nun dereito esixible. *Vid.* BARONA VILAR, Silvia (2021) *Algoritmización del derecho y de la justicia. De la Inteligencia Artificial a la Smart Justice*. Valencia: Tirant lo Blanch, p. 434. ISBN 9788413786650.

⁵⁶ A seguridade de que un candidato vai a ser o mellor cualificado para un determinado posto de traballo, a certeza de que unha determinada persoa vaia a ser capaz de asumir a devolución do préstamo que lle vai ser concedido ou a evidencia de que unha empresa vaia a abonarlle a un traballador todas as horas extras realizadas. Respecto a esta última cuestión, nos días nos que está sendo redactado este traballo está transcendendo na prensa nacional a intención da actual ministra de Traballo, Yolanda Díaz, de crear para o Organismo de Inspección de Traballo e Seguridade Social unha ferramenta dotada de IA para detectar o non abono de horas extras por parte dos empresarios aos traballadores.

⁵⁷ Neste sentido pronunciouse por exemplo, o Parlamento Europeo na súa Resolución do 16 de febreiro do 2017 con recomendacións destinadas á Comisión sobre normas de Dereito Civil sobre robótica

sistema e a aniquilación das liberdades e das garantías⁵⁸. Destas últimas cuestións será das que nos encarguemos neste apartado. Dos perigos que supoñen este tipo de sistemas ao noso Estado de Dereito. Porque aínda que os beneficios están claros, unha avaliación das posibles consecuencias negativas é básica para a ponderación da introdución deste tipo de sistemas no noso procedemento penal⁵⁹.

A) Nesgos

Unha das cuestións que máis polémica, debate e estudo suscitou nos sistemas de predición de risco dotados de IA e, en xeral, na intelixencia artificial é a cuestión dos posibles nesgos nos que poden chegar a incorrer. Pero non só iso, senón da situacións discriminatorias que poden supoñer. Non é unha cuestión baladí. É un perigo do que xa puidemos observar varios supostos en distintos ámbitos e que xa chamou a atención das propias empresas, varias autoras do ámbito tecnolóxico e social, de organizacións supranacionais e da doutrina xurídica⁶⁰. Tal é a relevancia desta cuestión que todos os textos xurídicos e de *soft law* que viñemos vendo ao longo deste traballo realizan unha advertencia sobre esta cuestión, defínena e incluso introducen cautelas ao respecto. Neste punto, tamén debemos destacar que, aínda que non sexa exclusivamente referido á IA, a

(2015/2103(INL)): “(...) aprendizaxe automática ofrece enormes vantaxes económicas e innovadoras á sociedade, ao mellorar enormemente a capacidade de analizar datos, aínda que tamén presenta retos á hora de velar pola non discriminación, as garantías procesuais, a transparencia e a intelixibilidade dos procesos decisorios.”

⁵⁸ BARONA VILAR, Silvia (2021) Una justicia “digital” y “algorítmica” para una sociedad en estado de mudanza. En Silvia BARONA VILAR, editora. *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar*. Valencia: Tirant lo Blanch, p. 59, ISBN: 9788413972022.

⁵⁹ O certo é que as críticas e cautelas con este tipo de sistemas son moi numerosas. *Vid.* HESTER, Rhys. Risk Assessment at Sentencing (2019). The Pennsylvania Experiencie. En: DE KEIJSER, Jan W; ROBERTS, Julian V y RYBERG, Jesper, (ed.) *Predictive Sentencing. Normative and empirical perspectives*. Oxford, UK; Chicago, Illinois: Hart Publishing, pp. 213 – 238. ISBN 9781509921416; BARONA VILAR, Silvia (2021) *Algoritmización del derecho* cit., pp. 424 – 503; MIRÓ LLINARES, Fernando (2020) Predictive Policing, cit.

⁶⁰ Fóra do ámbito xurídico ou institucional gustaríanos facer referencia ao seguintes libros que poñen o problema sobre a mesa e que dun xeito moi claro e accesible poñen en mans do cidadán de a pé os riscos que poden supoñer este tipo de sistemas. Nestes libros as súas autoras poñen o foco nos perigos que supoñen os sistemas automatizados en xeral e a intelixencia artificial en concreto para todos os cidadáns e, no segundo deles, para as clases sociais con menos recursos. *Vid.* O’NEIL, Cathy (2017). *Armas de destrución matemática. Cómo el big data aumenta la desigualdad y amenaza la democracia*. Madrid: Capitán Swing. ISBN: 9788494740848; EUBANKS, Virginia (2021) *La automatización de la desigualdad: herramientas de tecnología avanzada para supervisar y castigar a los pobres*. Madrid: Capitán Swing. ISBN: 9788412281866.

propia Rede Europea de Expertos xurídicos en igualdade de xénero e non discriminación elaborou un estudo específico sobre estes posibles nesgos e as súas consecuencias. En concreto, sobre a discriminación á que podemos chegar no suposto de non corríxilos no eido da igualdade de xénero. Este texto aclara qué son os nesgos e cómo poden producirse, os retos que supoñen para o marco legal europeo e para os propios Estados membros. Ademais, propón unha serie de posibles ou potenciais solucións ao respecto⁶¹.

Un nesgo algorítmico é un erro sistemático de calquera tipo no resultado das operacións algorítmicas. É dicir, non leva necesariamente a unha situación de discriminación ou inxusta, pois pode deberse a un erro estrutural ou de tipo estatístico. Só falaremos de discriminación algorítmica cando o erro concreto coloque a uns grupos privilexiados nunha vantaxe sistemática e aos grupos non privilexiados nunha desvantaxe sistemática⁶². Cabe dicir que non existen solucións absolutas e únicas para estes nesgos pois a súa orixe pode ser variada.

Por un lado, poder ser endóxena ou esóxena. Serán factores esóxenos aqueles que veñan determinados polo propio deseño do sistema de IA. É dicir, cada programador ou empresa, ca súa determinada orixe racial, cultural e económica desenvolverá e condicionará o deseño en maior ou menor medida. Pola contra, o problema dos nesgos pode ter a súa orixe en cuestións esóxenas. É dicir, que procedan do tipo de dato empregado, da propia calidade do dato ou incluso do volume de datos empregados para adestrar o sistema⁶³. Ademais, dentro destes nesgos de orixe esóxena podemos clasificalos en outros tres tipos: de interacción, latente e de selección. O primeiro deles prodúcese polo xeito no que o usuario ou o programador se relaciona co sistema, por exemplo ao definir a función de éxito. O nesgo latente prodúcese cando o modelo realiza

⁶¹ GERARDS, Janneke y XENEDIS, Raphaële (2020). *Algorithmic discrimination in Europe. Challenges and opportunities for gender equality and non-discrimination law*. Luxemburgo: Publications Office of the European Union. ISBN: 9789276207467.

⁶² GERARDS, Janneke y XENEDIS, Raphaële (2020). *Algorithmic discrimination in Europe*, cit. p. 47.

⁶³ VIDA FERNÁNDEZ, José (2018). Los retos de la regulación, *cit.*, pp. 219 – 220.

correlacións inapropiadas⁶⁴, é dicir, establece falsos nexos entre puntos de datos. Finalmente, o nesgo de selección ten lugar cando a base de datos non é suficientemente representativa da diversidade presente nun determinado entorno social⁶⁵

Nas seguintes liñas imos a referirnos aos nesgos do tipo que sexan, que provocan discriminación algorítmica e perpetúan estruturas que prexudican ás persoas pertencentes a grupos que, historicamente, atopáronse nunha posición de subordinación ou desvantaxe. Isto, como consecuencia de determinados elementos da persoa como o xénero, a idade, a raza, as crenzas relixiosas ou opinións políticas⁶⁶.

O exemplo máis paradigmático sobre a cuestión dos nesgos e a discriminación que provocan puidemos vela no caso *State vs. Loomis* da *Wisconsin Supreme Court* do 13 de xullo do 2016. Nesta sentenza aválase o emprego do sistema COMPAS para fixar a pena dun condenado, un sistema que, con anterioridade, fora examinado en profundidade por Propublica⁶⁷, unha organización xornalística sen ánimo de lucro que centra a súa investigación en cuestións de interese público. Esta entidade confirmou que esta ferramenta tiña unha tendencia evidente a etiquetar a persoas negras cun maior risco de reincidencia que ás persoas brancas. As cifras que recolle o mencionado informe e expostas por Freeman son realmente demoledoras⁶⁸: as persoas negras cuxa predición de risco foi positiva e finalmente errada duplicaba a porcentaxe das persoas brancas nesta mesma situación, as persoas brancas tiñan un 63% máis de probabilidades de ter sido clasificados erroneamente como de baixo risco que as persoas negras e estas, tiñan un

⁶⁴ Neste punto é moi importante lembralo: os algoritmos non elaboran conceptos, senón que detectan correlacións. *Vid.* AMUNÁTEGUI PERELLÓ, Carlos (2020), *Arcana technicae. El derecho y la inteligencia artificial*. Valencia: Tirant lo Blanch, pp. 45 – 46. ISBN: 9788413550213.

⁶⁵ AMUNÁTEGUI PERELLÓ, Carlos (2020), *Arcana, cit.*, p. 58.

⁶⁶ SORIANO ARNANZ, Alba (2021). Decisiones automatizadas y discriminación: aproximación y propuestas generales. *Revista General de Derecho Administrativo*, núm. 56, p. 5, ISSN: 16969650.

⁶⁷ O estudo en concreto ao que fai referencia Freeman no se artigo é do 23 de maio do 2016 e que está disponible en: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> [derradeira data de acceso: 6 de setembro do 2022]

⁶⁸ FREEMAN, Katherine (2016). *Algorithmic Injustice, cit.*, pp. 84-85.

77% máis de probabilidades de ser clasificados como de moi alto risco que as persoas brancas.

Do mesmo xeito foron criticados os sistemas de mapas de calor aos que fixemos referencia no apartado 2. De acordo co funcionamento destes, a realización de prognósticos de acontecementos criminais aínda non coñecidos poderían chegar a estigmatizar unha determinada zona dunha cidade. Estas seleccións tenderán a perpetuarse pois a actividade de vixilancia dirixirase a esa área da urbe que, polas condicións que sexan, teña unha actividade delituosa maior anterior e producírase un círculo vicioso, mantendo sobre ela unha maior vixilancia e como consecuencia, un maior número de delitos⁶⁹. Aumentaríase a seguridade sobre unha área determinada dunha cidade, chamando a atención sobre a inseguridade, creando medo sobre a mesma e botando aos cidadáns que fuxirán, se teñen a posibilidade. Unha das cuestións que debemos plantexarnos neste punto é se a estigmatización é exclusiva destes sistemas. O certo que é que cando se fala dos perigos destas ferramentas semella que esquecemos que as propias persoas que forman parte das Forzas e Corpos de Seguridade ou que son operadores do sistema xudicial tamén teñen prexuízos e nesgos.

Non debemos esquecer que a toma de decisións levada a cabo por seres humanos non é obxectiva. Cando as persoas decidimos adoitamos facelo mediante atallos mentais, chamados heurísticas. Que, se ben poden ser eficaces, poden propiciar decisións baseadas en información parcial e, polo tanto, pode xerar nesgos cognitivos⁷⁰. Pretender asumir que estes operadores xurídicos tanto xudiciais como policiais son totalmente imparciais e que se atopan illados do seu entorno social é unha falacia⁷¹.

⁶⁹ Vid. HARCOURT, Bernard E. (2003) From the Ne'er-do-well to the criminal history category: the refinement of the actuarial model in criminal law. *Law and contemporary problems*, vol. 66, p. 135; BRANDARIZ GARCÍA, José Ángel (2014). *El gobierno de la penalidad*, cit., pp. 132 – 133; BARONA VILAR, Silvia (2021). *Algoritmización del Derecho*, cit., p. 460.

⁷⁰ SORIANO ARNANZ, Alba (2021). Decisiones automatizadas: problemas y soluciones jurídicas más allá de la protección de datos. *Revista de Derecho Público: Teoría y Método*, v. 3, p. 89. ISSN: 26957191.

⁷¹ SIMÓN CASTELLANO, Pere (2021). *Justicia cautelar*, cit., p. 115.

Moi relacionado co anterior é o coñecido como a ancoraxe xudicial⁷². É un nesgo cognitivo no que quen dicide baséase demasiado, cando non en exclusiva, nun trazo ou peza de información que se centra nun marco conceptual limitado e que obvia unha visión sistemática ou xeral⁷³. E é un dos maiores problemas que poden aparecer no emprego de ferramentas de predición de risco dotadas de IA dun xeito asistencial á toma de decisións dos xuíces. Existe polo tanto, o risco latente de que “se oficialicen” determinadas aversións sociais cara determinados colectivos⁷⁴. Se un operador xurídico ou policial ten á súa disposición unha ferramenta destas que lle mostra un resultado de que unha determinada zona ou unha determinada persoa é perigosa, moitas veces a necesidade, as presións externas de rapidez ou de eficiencia ou incluso a propia comodidade podería levarnos á ausencia de crítica por parte do suxeito do resultado ofrecido pola ferramenta⁷⁵. De feito, é unha das cuestións que pretendía evitar a Corte Suprema de Wisconsin establecendo como necesarias unha serie de advertencias sobre esta ferramenta nos informes que conteñan unha valoración de risco elaborada polo sistema COMPAS⁷⁶. Nunha sociedade como a nosa na que os prexuízos e os nesgos están tan arraigados en

⁷² Aínda que tamén podería ser policial. Unha a crítica ao ancoraxe policial provocada por ferramentas de predición de risco, aínda que non dotadas de intelixencia artificial, é a Sentencia da Audiencia Nacional da Sala do Contencioso-administrativo do 30 de setembro do 2020. Aínda que non se atopa directamente relacionada con temas de discriminación, considéramola moi interesante neste eido. A resolución en cuestión condena ao Ministerio de Interior pola deficiente protección que recibiu unha vítima de violencia machista, que posteriormente foi asasinada nas mans do seu marido, por parte da Garda Civil. Esta fora a solicitar unha orde de protección ás dependencias deste corpo que finalmente lle foi denegada despois de que a ferramenta de valoración de risco lle outorgase un “risco baixo” e sen que os membros deste corpo realizasen máis pescudas cualificaron o risco como “non apreciado”. É moi interesante o comentario que realiza a profesora Marta del Pozo Pérez sobre esta sentenza. Neste sentido *vid.* DEL POZO PÉREZ, Marta (2022). ¿Los algoritmos sirven para proteger a las víctimas de violencia de género? En: BUENO DE MATA, Federico (dir). *El impacto de las tecnologías disruptivas en el derecho procesal*. España: Thomson Reuters Aranzadi, pp. 168 – 179. ISBN: 9788413455885.

⁷³ SIMÓN CASTELLANO, Pere (2021). *Justicia cautelar, cit.*, p. 117.

⁷⁴ NIEVA FENNOL, Jordi (2021). Tecnología y derechos fundamentales en el proceso judicial. En MORENO CATENA, Víctor; ROMERO PRADAS, M^a Isabel (dirs.) y LARO GONZÁLEZ, Elena (ed.). *Nuevos postulados de la cooperación judicial en la Unión Europea. Libro homenaje a la Prof. M^a Isabel González Cano*. Valencia: Tirant lo Blanch, p. 1015. ISBN: 9788413781211.

⁷⁵ HARVARD LAW REVIEW (2016) *State vs. Loomis*. Criminal law. Sentencing guidelines. Wisconsin Supreme Court requires warning before use of algorithmic risk assessments in sentencing, p. 1536.

⁷⁶ As advertencias en cuestión son as seguintes: 1) un acta escrita que enumera as súas limitacións; 2) unha lista que inclúa información sobre a natureza de propiedade privada de COMPAS; 3) o feito de que se basea en datos grupais; 4) as cuestións relativas a delincuentes pertencentes a minorías (que existen máis probabilidades de establecer un risco alto); 5) a composición nacional das mostras empregadas.

problemas sociais e estruturais é difícil pensar que unha simple advertencia ou incluso solucións técnicas puntuais poidan resolver a cuestión dos nesgos discriminatorios dun xeito pleno⁷⁷. Neste punto tamén deberíamos plantexarnos se a solución que está sendo tan aclamada de *human on command* é capaz de mellorar o proceso decisorio automatizado e non incluír máis nesgos discriminatorios⁷⁸. Non esquezamos que os datos que nutren este tipo de sistemas son derivados de decisións xudiciais e policiais previas, que os programadores e arquitectos de sistemas tamén poden ter prexuízos e que o propio sistema no que vivimos clasifica e discrimina⁷⁹. Dende o noso punto de vista, este tipo de sistemas non “crean” decisións discriminatorias, senón que as reforzan e as manteñen.

B) Afectación a dereitos fundamentais

Outro dos riscos dos que veu advertindo a doutrina sobre o emprego de ferramentas de predición de risco dotadas de intelixencia artificial é a posible afectación de varios dereitos fundamentais. Fronte o gran poder do Estado son estes dereitos fundamentais os que protexen á cidadanía que cada vez semella menos consciente deles⁸⁰. A observancia absoluta a estes dereitos fundamentais no emprego de sistemas de IA é a “clave de bóveda” para o seu futuro emprego no eido xudicial⁸¹. En concreto nas seguintes liñas imos a referirnos ás posibles vulneracións dalgúns dereitos e garantías do artigo 24 da Constitución Española.

⁷⁷ KIM, Pauline T. (2017). Auditing algorithms for discrimination. *University of Pennsylvania Law Review Online*, vol. 166, p. 191.

⁷⁸ ROIG, A., *Las garantías frente a las decisiones automatizadas. Del Reglamento General de Protección de Datos a la gobernanza algorítmica*, Bosch Constitucional, Barcelona, 2020, pp. 67 – 68.

⁷⁹ Xa sexa por razón, de raza, xénero, identidade sexual, etc.

⁸⁰ NIEVA FENOLL, Jordi (2018), *Inteligencia artificial y proceso judicial*. Madrid: Marcial Pons, p. 127. ISBN: 9788491238218.

⁸¹ MARTÍN DIZ, Fernando (2021) *Inteligencia artificial y derecho procesal: luces, sombras y cábalas en clave de derechos fundamentales*. En MORENO CATENA, Víctor; ROMERO PRADAS, M^a Isabel (dirs.) y LARO GONZÁLEZ, Elena (ed.). *Nuevos postulados de la cooperación judicial en la Unión Europea. Libro homenaje a la Prof. M^a Isabel González Cano*. Valencia: Tirant lo Blanch, p. 994. ISBN: 9788413781211.

I. *O dereito a un xuíz imparcial*

En primeiro lugar debemos cuestionarnos se este tipo de sistemas poderían vulnerar o dereito a un xuíz imparcial. A imparcialidade xudicial, ademais de atoparse explicitamente recoñecida no artigo 6.1 do Convenio Europeo para a protección dos Dereitos Humanos e as liberdades fundamentais, podemos vela implícita no dereito a un proceso con todas as garantías (art. 24.2 CE)⁸², cunha especial relevancia no eido penal⁸³. A imparcialidade vai implicar a ausencia de prexuízos ou de toma de posición polo xulgador⁸⁴. É dicir, o xuíz ou maxistrado debe atoparse por riba do conflito existente entre as partes e as súas correspondentes pretensións. Isto non supón a obrigação de neutralidade absoluta das persoas que forman parte da función xurisdiccional. Para salvagardar esta imparcialidade no noso sistema xudicial, podemos acudir ás causas de recusación recollidas no artigo 219 da LOPX⁸⁵. Se observamos a lista destes motivos de recusación o certo é que poderíamos resumilos en que debe evitarse que o xuíz ou a xuíza teñan unha proximidade ou aversión coas partes ou co obxecto do proceso⁸⁶. Para examinar esta posible vulneración debemos de facelo dende dous puntos de vista: de que sexa o propio sistema o que de xeito autónomo tome decisións que forman parte das potestades xurisdiccionais e que este sistema de predición de risco teña unha labor meramente asistencial do xuíz ou maxistrado.

En primeiro lugar imos examinar o suposto no que o sistema de predición de risco, de xeito totalmente autónomo ou cunha intervención humana practicamente nula, tome unha decisión en determinados momentos procesuais. É dicir, que o sistema asuma algunha sorte de potestade xudicial. Nese suposto, segundo Nieva Fenoll non poderíamos valorar a existencia de imparcialidade xudicial pois, as emocións, que son as que

⁸² A STC núm. 145/1988, do 12 de xullo, no seu fundamento xurídico 5 recoñece por primeira vez este dereito dentro do artigo 24.2 CE: “...debe incluírse, aunque no se cite en forma expresa, el derecho a un Juez imparcial, que constituye sin duda una garantía fundamental de la Justicia en un Estado de Derecho, como lo es el nuestro, de acuerdo con el art. 1.1 de la Constitución.”

⁸³ STC núm. 133/2014, do 22 de xullo.

⁸⁴ STS núm. 507/2020, do 14 de outubro (Sala 2ª).

⁸⁵ SIMÓN CASTELLANO, Pere (2021). *Justicia cautelar*, cit., pp. 179 – 180.

⁸⁶ NIEVA FENOLL, Jordi (2018), *Inteligencia*, cit., p. 127.

realmente condicionan esta inclinación do xuíz por unha das partes ou por unha das pretensións é exclusiva dos seres humanos. Na opinión deste autor, tampouco poderíamos cuestionar esta imparcialidade respecto ao propios deseñadores ou arquitectos do sistema pois, a imparcialidade é algo só pode observarse no caso concreto e non, nun principio, nunha multitude de casos xerais⁸⁷. En publicacións posteriores o mesmo autor advertiu que isto non obsta dun necesario control dos profesionais que elaboran estas ferramentas e incluso das empresas onde estas se elaboran pois, pese as directrices e normas que lle poida dar o Goberno ou o mesmo Poder Xudicial, estes poden manipular a configuración destes sistemas⁸⁸.

No suposto de que este tipo de ferramentas teña un uso meramente asistencial do xuíz ou da xuíza é certo que existe algunha autora que defende que este tipo de ferramentas empregadas dun xeito asistencial poderían condicionar a imparcialidade xudicial. Isto, con independencia de se o sistema en concreto reproducise nesgos discriminatorios ou non⁸⁹. Neste traballo quedámonos co exposto por Simón Castellano⁹⁰ que defende todo o contrario. Que, no suposto de que este tipo de ferramentas estivesen correctamente deseñadas para evitar imitar e afianzar nesgos, serían moito máis fiables incluso que o xulgador. Evitaríanse así as posibles motivacións persoais do xulgador en favor dunha ou doutra parte que, nunha máquina, sería imposible reproducir. Ademais, debemos destacar, que no caso de que fosen ferramentas que si que adoeceran de imitar decisións con nesgos discriminatorios, non estaríamos xa no campo da imparcialidade xudicial, senón que volveríamos ao campo do dereito á igualdade e non discriminación que xa expuxemos.

⁸⁷ NIEVA FENOLL, Jordi (2018), *Inteligencia*, *cit.*, p. 130. ISBN: 9788491238218.

⁸⁸ NIEVA FENNOL, Jordi (2021). *Tecnología y derechos fundamentales*, *cit.*, p. 1017.

⁸⁹ *Vid.* PÉREZ ESTRADA, Miren Josune (2022). *Fundamentos jurídicos para el uso de la inteligencia artificial en los órganos judiciales*. Valencia: Tirant lo Blanch, p. 130. ISBN: 9788411137621.

⁹⁰ SIMÓN CASTELLANO, Pere (2021). *Justicia cautelar*, *cit.*, pp. 179 – 184.

II. O dereito á presunción de inocencia

Outro dos dereitos consagrados no artigo 24 CE que se cuestiona se se vería vulnerado polos sistemas de predición de risco dotados de IA é o dereito á presunción de inocencia⁹¹. A presunción de inocencia é unha regra de xuízo e dende unha perspectiva constitucional é o dereito a non ser condenado sen probas de cargo válidas⁹². Segundo o Tribunal Constitucional só estaremos ante unha vulneración do dereito á presunción de inocencia cando non existan probas de cargo válidas, é dicir cando os órganos xudiciais valorasen unha actividade probatoria lesiva de outros dereitos fundamentais, carente de garantías, cando non se motive o resultado ou cando por ilóxico ou insuficiente non sexa razoable o iter discursivo que conduce da proba ao feito probado⁹³.

Simón Castellano defende que, no suposto de que este tipo de ferramentas se empreguen en sede de medidas cautelares, si que podería existir unha vulneración deste principio pois esa ferramenta estaría prexulgando o fondo do asunto. Sen embargo remata por consideralos óptimos e defende o seu emprego neste eido para evitar que o xulgador, sen apenas indicios ou elementos a valorar, poida tomar esta decisión baseándose en automatismos ou atallos intuitivos que son, pouco fiables cando está en xogo a liberdade e a presunción de inocencia dunha persoa. Na nosa opinión, se este tipo de ferramentas se empregasen como un elemento probatorio máis nun xuízo penal si que podería haber unha quebra do dereito á presunción de inocencia pois non estamos ante un feito ou elemento do mundo real. É un cálculo de probabilidade, baseado en feitos anteriores de persoas totalmente alleas ao procedemento, de que un determinado suxeito poida cometer un delito ou sexa máis ou menos perigoso. Non podemos esquecer que estes sistemas baséanse en correlacións e non en causalidade. Aínda que, como este tipo de ferramentas hoxe en día teñen un gran volume de datos, considéranse fiables aínda que non exista esa proba de causalidade⁹⁴. De todos xeitos, tampouco pode ser admisible en relación co dereito fundamental á presunción de inocencia que o feito de ter sido condenado no

⁹¹ *Ibid.*, pp. 184 – 188.

⁹² SSTS núm. 171/2018, do 11 de abril (Sala 2ª) e núm. 143/2013, do 28 de febreiro (Sala 2ª).

⁹³ STC núm. 189/1998, do 28 de setembro.

⁹⁴ SORIANO ARNANZ, Adriana (2021) Decisiones automatizadas: problemas, *cit.*, p. 91.

pasado pola comisión dun delito, como dato obxectivo real, poida condicionar a un sistema de IA á hora de interpretar os datos que afecten a esa persoa en relación cun novo, diferente e posterior delito⁹⁵.

Segundo Barona Vilar tamén podería verse cuestionado este dereito á presunción de inocencia cando estas ferramentas son empregadas en sede policial se chegásemos a un punto de valorar máis a súa eficiencia para a persecución da delincuencia e da criminalidade sobre a base dos “riscos” sobre a proba dos feitos que se perseguen⁹⁶. O axente da autoridade que acuda a un determinado punto da cidade guiado pola ferramenta de mapa de calor irá con outra disposición ou actitude. En caso de dúbida, é probable que opte por considerar que os feitos que acaba de presenciar sexan constitutivos de delito. Incluso a idea pode ser máis simple: imos a atopar unha maior cantidade de delitos nas zonas nas que máis busquemos⁹⁷. Non esquezamos o poder de suxestión que posúen estes “oráculos dixitais”⁹⁸. Semella polo tanto que este dereito penal predictivo ao que imos dirixíndonos dun xeito progresivo, fronte a protección da liberdade e a presunción de inocencia, parece que quere basearse no principio de culpabilidade cas consecuencias que isto supón para, por exemplo, a valoración da proba⁹⁹.

III. O dereito de defensa

Moi relacionado co anterior, tamén podemos cuestionarnos se existe unha vulneración do dereito de defensa. Entendido dende un dobre punto de vista. Por un lado, que as partes poidan coñecer todos os materiais de feito e de dereito que poidan influír na convicción do xulgador no momento de ditar sentenza. Pero, ademais, é a facultade de poder alegar, probar e argumentar coa mesma idea de incidir na convicción xudicial. E,

⁹⁵ MARTÍN DIZ, Fernando (2021) Inteligencia artificial y derecho procesal, *cit.*, p. 971.

⁹⁶ BARONA VILAR, Silvia (2021). *Algoritmización del*, *cit.*, pp. 459 – 460.

⁹⁷ HARCOURT, Bernard E. (2003) From the Ne'er-do-well, *cit.*, p. 147.

⁹⁸ GALGANI, Benedetta (2021). Consideraciones sobre los “antecedentes” del acusado y del juez frente a la inteligencia artificial (IA) en el proceso penal. En MORENO CATENA, Víctor; ROMERO PRADAS, M^a Isabel (dirs.) y LARO GONZÁLEZ, Elena (ed.). *Nuevos postulados de la cooperación judicial en la Unión Europea. Libro homenaje a la Prof. M^a Isabel González Cano*. Valencia: Tirant lo Blanch, p. 1154. ISBN: 9788413781211.

⁹⁹ BARONA VILAR, Silvia (2021). *Algoritmización del*, *cit.*, p. 444.

neste punto atopámonos cunha das notas máis comentadas deste tipo de ferramentas que é a opacidade das mesmas¹⁰⁰. O dereito de defensa supón polo tanto que un litigante debe ter a posibilidade de poder desenvolver todos os seus argumentos e as probas que precise para a súa corroboración¹⁰¹.

Non cabe dúbida que unha solución como a que se deu no asunto *State vs. Loomis* da *Wisconsin Supreme Court* é totalmente inviable no noso dereito: ampararse nun segredo empresarial para xustificar a non difusión ás partes do código fonte e o funcionamento efectivo considerando suficiente que coñecera o contido das preguntas que se lle realizaran para a avaliación do risco. Se isto chegase a permitirse, atopariámonos en situacións nas que as partes só poderían presentar argumentos superficiais contra os elementos que puido valorar ou non o sistema¹⁰². As partes atoparíanse nunha situación na que terían que defenderse nun proceso sen coñecer a lei aplicable¹⁰³. Incluso, tampouco sería admisible que por exemplo, só os xuíces coñecesen esta información, o código fonte e o funcionamento do sistema en cuestión pois estariámonos nunha circunstancia semellante de indefensión das partes, onde seguirían sen saber cal é o contido dos materiais que van a ser usados para valorar os feitos que son obxecto do procedemento¹⁰⁴.

Non podería ser admisible polo tanto nun procedemento xudicial, en calquera da súas fases, o fenómeno coñecido como caixa negra ou *black box* onde quedarían espazos reservados nos que nin os cidadáns nin os propios xuristas que interveñan non procedemento poidan entrar e informarse. Deste xeito estaríanse vulnerando as garantías esenciais do dereito de defensa pois podería supoñer un control e unha manipulación arbitraria por parte do Estado sobre as vidas da cidadanía¹⁰⁵. O respecto do dereito de

¹⁰⁰ PÉREZ ESTRADA, Miren Josune (2022). *Fundamentos jurídicos para el uso de la inteligencia artificial en los órganos judiciales*. Valencia: Tirant lo Blanch, p. 139. ISBN: 9788411137621.

¹⁰¹ NIEVA FENOLL, Jordi (2018), *Inteligencia, cit.*, p. 138.

¹⁰² FREEMAN, Katherine (2016) *Algorithmic Injustice, cit.*, p. 94.

¹⁰³ NIEVA FENOLL, Jordi (2018), *Inteligencia, cit.*, p. 140.

¹⁰⁴ ROMEO CASABONA, Carlos María (2018) *Riesgo, procedimientos actuariales, cit.*, p. 53.

¹⁰⁵ NIEVA FENOLL, Jordi (2018), *Inteligencia, cit.*, pp. 143 – 144.

defensa neste eido e no relativo a este tipo de ferramentas só poderá garantirse cunha regulación previa ao respecto que estableza as condicións e os límites para o seu emprego¹⁰⁶.

Neste punto non podemos deixar de mencionar un dos principios éticos que expoñen as Directrices Éticas para unha IA fiable do Grupo independente de Experto de Alto Nivel sobre Intelixencia Artificial creado pola Comisión Europea: a explicabilidade. Segundo este dogma, os procesos deben ser transparentes. É dicir, que deben ser comunicadas e explicadas, na medida do posible, ás partes que se vexan afectadas dun xeito directo ou indirecto as capacidades e a finalidade do sistema concreto de IA. No suposto de que nos atopemos ante estes algoritmos de caixa negra deberán tomarse outras medidas relacionadas con este valor como a trazabilidade¹⁰⁷, a auditabilidade¹⁰⁸ e a comunicación transparente sobre as prestacións do sistema. O mesmo texto recalca que xusto no eido penal, tendo en conta o contexto e a gravidade das consecuencias derivadas dun posible resultado erróneo ou inaxeitado fai de maior importancia este principio¹⁰⁹.

IV. O dereito á protección de datos

Finalmente, aínda que non se atopa expresamente consagrado no artigo 24 CE, non podemos deixar de falar do dereito fundamental á protección de datos. Segundo o Tribunal Constitucional este dereito garante ao individuo un poder de control ou disposición sobre os seus datos persoais, sobre o seu emprego e destino, co propósito de

¹⁰⁶ MARTÍN DIZ, Fernando (2021) Inteligencia artificial y derecho procesal, cit., p. 1000.

¹⁰⁷ A trazabilidade dun sistema de IA refírese á súa capacidade para levar a cabo un seguimento dos datos, o desenvolvemento e o proceso de despregue do sistema, xeralmente a través dun proceso de identificación e rexistro documentados. Neste sentido *vid.* GRUPO INDEPENDIENTE DE EXPERTOS DE ALTO NIVEL SOBRE INTELIGENCIA ARTIFICIAL (2019). *Directrices éticas para una IA fiable*. Bruselas: Comisión Europea, p. 50. ISBN: 9789276119944.

¹⁰⁸ A auditabilidade é a capacidade de avaliar os algoritmos, os datos e os procesos de deseño. Isto non quere dicir que deba dispoñerse dun xeito inmediato desta información. A avaliación por parte dos auditores internos e externos e a dispoñibilidade dos correspondentes informes de avaliación poden contribuír á fiabilidade desta tecnoloxía. Neste tipo de aplicacións nas que pode afectar a dereitos fundamentais, incluídas as aplicacións esenciais dende o punto de vista da seguridade, os sistemas de IA deberían poder someterse a auditorías independentes. GRUPO INDEPENDIENTE DE EXPERTOS DE ALTO NIVEL SOBRE INTELIGENCIA ARTIFICIAL (2019). *Directrices éticas*, cit., p. 24.

¹⁰⁹ GRUPO INDEPENDIENTE DE EXPERTOS DE ALTO NIVEL SOBRE INTELIGENCIA ARTIFICIAL (2019). *Directrices éticas*, cit., p. 16.

impedir o seu tráfico ilícito e lesivo para a dignidade e dereitos do afectado¹¹⁰. A protección de datos cada vez está adquirindo maior importancia no eido procesual. Especialmente, dende a introdución no noso ordenamento xurídico da LO 7/2021. Non debemos esquecer que a fase de instrución constitúe unha continuada intromisión no eido que tutela esta normativa¹¹¹. O certo é que este dereito tamén podería verse seriamente comprometido no emprego destas ferramentas. Debemos de partir do axioma de que non hai desenvolvemento deste tipo de ferramentas dotadas da IA sen datos, de feito unha enorme cantidade deles. Pero tampouco é posible unha xestión de datos semellante eficiente, segura e correcta dos mesmos, sen IA¹¹². Por iso, no previsible momento de empregalas¹¹³, o lexislador español, xunto ao Poder Xudicial, deberán poñer especial empeño na xestión do risco do datos que van a ser tratados con estas ferramentas ca utilización de distintas medidas de seguridade contempladas no paquete normativo de protección de datos como poden ser a anonimización ou a seudonimización.

5. ¿Cara un dereito penal do inimigo?

As reservas e reticencias sobre o emprego deste tipo de ferramentas non foron poucas na doutrina¹¹⁴. É máis, incluso houbo quen foi máis alá e mostrou o seu total

¹¹⁰ STC núm. 292/2000, do 30 de novembro.

¹¹¹ ORTIZ PRADILLO, Juan Carlos (2022). Inteligencia artificial, Big Data, cit., p. 113. Este mesmo autor tamén propón que este dereito fundamental debería quedar incluído entre as garantías do proceso.

¹¹² ESPARZA LEIBAR, Iñaki (2021). La Inteligencia Artificial y el derecho fundamental a la protección de datos de carácter personal. La aplicación integral de la inteligencia artificial: una oportunidad para dar un salto cualitativo en la correcta actuación de los poderes públicos, en general, y en el campo de la justicia, en particular. En: BARONA VILAR, Silvia (ed.). *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar*. Valencia: Tirant lo Blanch, p. 270. ISBN: 9788413972022.

¹¹³ Empregamos o termo previsible pois tal e como xa explicamos neste traballo é moi probable que máis cedo que tarde vaian a empregarse este tipo de ferramentas pois, aínda que actualmente exista unha prohibición que abarcaría a este tipo de sistemas o certo é que o propio Proxecto de Regulamento de IA contempla como un dos sistemas que aínda que posúan un alto risco, son admisibles para o uso, ferramentas como as que versa este estudo.

¹¹⁴ Neste sentido *vid.* ALONSO SALGADO, Cristina (2021) Acerca de la inteligencia artificial en el ámbito penal: especial referencia a la actividad de las fuerzas y cuerpos de seguridad. *Ius et Scientia*. Sevilla: Editorial Universidad de Sevilla, vol. 7, núm. 1, p. 36. ISSN: 24448478; ANÓN ROIG, María José (2022). Desigualdades algorítmicas: conductas de alto riesgo para los Derechos Humanos. *Derechos y libertades*. Madrid: Dykinson, núm. 47, pp. 48 – 49. ISSN: 11330937; GUZMÁN FLUJA, Vicente C.

rexeitamento cara este tipo de ferramentas¹¹⁵. As razóns para as cautelas sobre empregar sistemas de predición de risco no noso procedemento penal foron fundamentalmente as que viñemos expoñendo ata agora de xeito sintetizado: a afectación a distintos dereitos fundamentais e os nesgos discriminatorios que poden producir estas ferramentas. Xa expuxemos tamén en anteriores liñas como, en xeral, os métodos actuariais¹¹⁶ e a xustiza predictiva ou a baseada no risco¹¹⁷ nas que podemos encaixalas, nunca estiveron exentas de polémica. A principal pregunta que xurdiu arredor desta cuestión é como pode previr a comisión de delitos o Estado, como protector dos cidadáns, sen erosionar a liberdade¹¹⁸. Como podemos chegar a evitar que a demolición do Estado de Dereito proceda da desmedida reacción interna ante as ameazas de seguridade externas?¹¹⁹ Outras autoras, máis que formularse estas incógnitas, critican esta procura dun sistema penal máis “eficaz” fronte un dereito penal máis xusto¹²⁰. Neste debate, o dereito penal do inimigo é unha constante que aparece para facer referencia á deriva á que se está dirixindo o noso sistema penal¹²¹

(2021). Proceso penal y justicia, *cit.*, p. 40; SUÁREZ XAVIER, Paulo Ramón, et al. (2022). Policía predictiva e <<negritude>>: modelos para a reprodución de un estado sem dereitos. En: SUÁREZ XAVIER, Paulo Ramón y FONTESTAD PORTALÉS, Leticia (2022). *Seguridad y los retos de la jurisdicción en el siglo XXI: justicia, sostenibilidad y paz*. A Coruña: Colex, pp. 49 – 50. ISBN: 9788413595160 entre outros.

¹¹⁵ Neste sentido *vid.* ROMEO CASABONA, Carlos María (2018) Riesgo, procedimientos actuariales, *cit.*, pp. 54 – 55.

¹¹⁶ Neste sentido *vid.* GUTIÉRREZ, Mariano Hernán (2008). Punitivismo y actuarialismo, *cit.*

¹¹⁷ Neste sentido *vid.* GONZÁLEZ CUSSAC, José Luís y FLORES GIMÉNEZ, Fernando (2018). Seguridad global y derechos, *cit.*; GONZÁLEZ CUSSAC, José Luís (2019). Seguridad e incertidumbre, *cit.*; JUAN SÁNCHEZ, Ricardo (2019) Proceso penal preventivo en España: elementos y criterios de contención. En BARONA VILAR, Silvia (ed.) *Claves de la justicia penal: feminización, inteligencia artificial, supranacionalidad y seguridad*. Valencia: Tirant lo Blanch, pp. 555 – 584. ISBN: 9788413360744; SILVA SÁNCHEZ, Jesús María (2011). *La expansión del derecho penal*, *cit.*

¹¹⁸ ZEDNER, Lucía (2019). El debate sobre el estado preventivo: aportaciones y retos doctrinales en materia de justicia preventiva. En: ALONSO RIMO, Alonso (dir.) y COLOMER BEA, David (coord.). *Derecho penal preventivo, orden público y seguridad ciudadana*. España: Aranzadi Thomson Reuters, p. 62. ISBN: 9788413099316.

¹¹⁹ GONZÁLEZ CUSSAC, José Luís (2019). Seguridad e incertidumbre, *cit.*, p. 505.

¹²⁰ GALGANI, Benedetta (2021). Consideraciones sobre los “antecedentes”, *cit.*, p. 1149.

¹²¹ GONZÁLEZ CUSSAC, José Luís (2019). Seguridad e incertidumbre, *cit.*, p. 518; BORJA JIMÉNEZ, Emiliano (2019). Seguridad como producto de mercado en la justicia penal globalizada. En

A desconfianza cara os sistemas de predición de risco tamén provocou que algunha autora incluso encadrase a introdución e uso destes sistemas nesta teoría do dereito penal do inimigo¹²². Nas seguintes liñas queremos analizar esta afirmación. Se realmente o emprego deste tipo de ferramentas poderían dirixirnos a este. É dicir, cara un sistema que, dende o medo, procúrese restablecer un discurso do nós fronte aos outros, fronte aos contrarios¹²³.

Nos anos 80 Günther Jakobs introduce a expresión “dereito penal do inimigo” para describir o que semella que se foi consolidando como unha manifestación propia da política criminal moderna: o paulatino avance do *ius puniendi* do Estado contra certas formas de manifestacións delituosas caracterizadas por representar un *perigo permanente* para a sociedade civil¹²⁴. Esta teoría que nun primeiro momento nacería como unha crítica a este fenómeno, co paso dos anos foi perdendo para Jakobs esa connotación “peyorativa”¹²⁵, para finalmente considerala polo penalista e filósofo do dereito como un xeito totalmente válido de estruturar e configurar a política criminal dun Estado fronte determinados comportamentos criminais¹²⁶. Varios autores fixeron referencia a esta teoría para expoñer unha crítica fronte a un determinado fenómeno de política criminal¹²⁷.

BARONA VILAR, Silvia (ed.) *Claves de la justicia penal: feminización, inteligencia artificial, supranacionalidad y seguridad*. Valencia: Tirant lo Blanch, p. 528. ISBN: 9788413360744.

¹²² Neste sentido *vid.* BARONA VILAR, Silvia (2021) *Algoritmización del derecho*, *cit.*, p. 463 – 464 ou BORGES BLÁZQUEZ, Raquel (2021) La inteligencia artificial en el proceso penal y el ¿regreso? de Lombroso. En: BARONA VILAR, Silvia (ed.). *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar*. Valencia: Tirant lo Blanch, p. 173. ISBN: 9788413972022.

¹²³ GONZÁLEZ CUSSAC, José Luís (2019). *Seguridad e incertidumbre*, *cit.*, p. 518.

¹²⁴ ABOSO, Gustavo Eduardo (2006). El llamado “derecho penal del enemigo” y el ocaso de la política criminal racional: el caso argentino. En: CANCIO MELIÁ, Manuel (coord.) y GÓMEZ-JARA DÍEZ, Carlos (coord.). *Derecho penal del enemigo. El discurso penal de la exclusión. Volumen 1*. Madrid: Edisofer, p. 53. ISBN: 849626128X.

¹²⁵ JAKOBS, Günther (2006). Derecho penal del ciudadano y derecho penal del enemigo. En: JAKOBS, Günther y CANCIO MELIÁ, Manuel. *Derecho penal del enemigo*. 2ª edición. Navarra: Aranzadi Editorial, p. 24. ISBN: 8447025365.

¹²⁶ Neste sentido *vid.* JAKOBS, Günther (2008). ¿Derecho penal del enemigo? Un estudio de los presupuestos de la juridicidad. En: CANCIO MELIÁ, Manuel (ed.) y FEIJOO SÁNCHEZ, Bernardo (ed.). *Teoría funcional de la pena y de la culpabilidad. Seminario con Günther Jakobs en la UAM*. 1ª edición. Pamplona: Aranzadi Editorial, pp. 23 – 62. ISBN: 9788447029112.

¹²⁷ Como exemplo, *vid.* notas 122 e 123.

Especialmente en supostos de extralimitación do dereito penal ou expansión do mesmo non só no eido que nos ocupa neste traballo senón en materia de delitos fronte o terrorismo¹²⁸, delitos relacionados cas drogas, inmigración, criminalidade organizada¹²⁹, o ámbito penitenciario¹³⁰ e, incluso, chegou a falarse por algún autor do dereito administrativo do inimigo¹³¹.

Segunda a teoría do dereito penal do inimigo unha sociedade estará composta por dous tipos de suxeitos. Por un lado, están aqueles que cumpren o contrato social e que dun xeito ocasional poden cometer algún erro e delinquir, os cidadáns¹³². Por outro, atópanse os inimigos. É dicir, aqueles suxeitos que mediante o seu comportamento, a súa ocupación profesional ou mediante a vinculación a unha determinada organización abandonou o Dereito dun xeito duradeiro¹³³. Segundo o autor alemá, os individuos sen seguridade cognitiva non deben ser tratados xuridicamente como persoas pois, isto podería chegar a vulnerar a seguridade dos demais¹³⁴. Falaríamos entón de inimigos para referirnos a aqueles delincuentes dos que cabe supoñer que son permanentemente perigosos¹³⁵. Para combater estes riscos creados polos inimigos deberá aplicarse unhas normas concretas ou distintas, dirixidas especialmente a eles. Deste xeito, o dereito penal

¹²⁸ Do cal podemos dicir que supón o exemplo máis evidente e claro deste tipo de política criminal.

¹²⁹ CANCIO MELIÁ, Manuel (2006). De nuevo: ¿“derecho penal” del enemigo? En: JAKOBS, Günther y CANCIO MELIÁ, Manuel. *Derecho penal del enemigo*. 2ª edición. Navarra: Aranzadi Editorial, pp. 117 – 118. ISBN: 8447025365.

¹³⁰ FARALDO CABANA, Patricia (2006). Medidas *premales* durante la ejecución de condenas por terrorismo y delincuencia organizada: consolidación de un subsistema penitenciario de excepción. En: CANCIO MELIÁ, Manuel (coord.) y GÓMEZ-JARA DÍEZ, Carlos (coord.). *Derecho penal del enemigo. El discurso penal de la exclusión. Volumen 1*. Madrid: Edisofer, p. 765. ISBN: 849626128X.

¹³¹ O primeiro eido no que se fai referencia a este termo do dereito administrativo do inimigo é á hora de comentar á Lei Orgánica 4/2015, do 30 de marzo, de protección da seguridade cidadá. A coñecida popularmente como Lei Mordaza. RIVERO ORTEGA, Ricardo (2015). La nueva Ley Orgánica de Seguridad Ciudadana: ¿Estado de prevención o Derecho administrativo del enemigo? *Ars Iuris Salmanticensis*. Salamanca: Ediciones Universidad de Salamanca, v. 3, p. 12. eISSN: 23405155.

¹³² JAKOBS, Günther (2006). Derecho penal del ciudadano, *cit.*, p. 47.

¹³³ SILVA SÁNCHEZ, Jesús María (2011). *La expansión del derecho penal*, *cit.*, p. 184.

¹³⁴ JAKOBS, Günther (2006). Derecho penal del ciudadano, *cit.*, p. 47.

¹³⁵ JAKOBS, Günther (2008). ¿Derecho penal del enemigo?, *cit.*, p. 50.

do inimigo fronte a estes individuos, ten as seguintes notas características: o adiantamento da punibilidade, penas desproporcionadamente altas e a supresión ou relativización de determinadas garantías procesuais¹³⁶.

Para levar a cabo esta análise, do xeito que sexa o máis ilustrativa posible, debemos situarnos no hipotético de que as ferramentas das que vimos falando ao longo deste de traballo se atopan todas instauradas. Tanto aquelas que poderían ser empregadas no eido policial como HART como as que atoparíamos en sede xudicial ou cumprimento da condena como COMPAS. Non facelo así podería facer que nos centrásemos demasiado nas medidas individuais e non tanto nas consecuencias finais, que son ás que realmente debemos darlle importancia á hora de valorar unha determinada política estatal no eido da loita contra a criminalidade¹³⁷.

En primeiro lugar, debemos falar do adiantamento da punibilidade. Isto, o que realmente supón é un cambio de perspectiva. A persecución penal deixa de ser retrospectiva, como ata agora, onde o punto de referencia é o feito cometido e comezamos a fixarnos no feito futuro, é dicir, cambiamos a unha perspectiva prospectiva¹³⁸. Esta característica puidemos observala de xeito evidente nas ferramentas que fomos comentando ata este momento. A súa esencia é poñer o ollo no que vai a suceder para evitar futuros e hipotéticos perigos. Pensemos nun barrio dunha gran cidade, que unha ferramenta empregada polas Forzas e Corpos de Seguridade de realización de mapas de calor fixa como unha zona cun evidente perigo. Se este corpo de Policía aumenta ás súas patrullas nunha determinada zona, está asumindo que nela vanse a cometer máis delitos. Non porque efectivamente fose a ser así pois non hai unha previsión de futuro real, só é

¹³⁶ CANCIO MELIÁ, Manuel (2006). De nuevo, *cit.*, p. 112.

¹³⁷ ZEDNER, Lucía (2019). El debate sobre el estado preventivo, *cit.*, p. 69. Esta autora defende a idea de que para poder observar cales son as implicacións totais que pode ter unha determinada medida na política criminal dun Estado non podemos fixarnos só nunha medida concreta senón que debemos observar como isto interacciona co resto do ordenamento xurídico. Un exemplo moi claro é a seguinte pregunta que se fai a autora: *¿Cómo, por ejemplo, afecta el alcance de la actividad policial la interacción entre la extensión cada vez mayor de las formas imperfectas de realización del delito en el Derecho penal y las facultades cada vez más amplias para parar, detener y registrar a individuos, especialmente como puede suceder en algunos casos en el Reino Unido sin el requisito de existencia de motivos de sospecha razonables?*

¹³⁸ CANCIO MELIÁ, Manuel (2006). De nuevo, *cit.*, p. 112.

un cálculo estatístico. Pero, como vai aumentar a vixilancia nesa zona, evidentemente, atoparanse máis delitos, reforzando ese círculo vicioso castigando e perseguindo sistematicamente unha determinada poboación que se atopa asentada nun determinado lugar. Centrando a nosa atención polo tanto neste determinado barrio, non nos feitos que xa aconteceron, senón naqueles que “estatisticamente” poderían chegar a suceder.

Pensemos agora en sede xudicial ou xa no eido penitenciario. Nesta fase centrarémonos nas ferramentas de predición de risco individual para a imposición dunha determinada pena ou para a valoración da concesión dun concreto beneficio penitenciario. Para ser máis ilustrativo, deberíamonos situar nun país como Brasil onde o 64% da poboación reclusa é negra pero, no que hai estados como Acre, Amapá ou Bahía onde esta porcentaxe ascende a 95%, 91% e 89% respectivamente¹³⁹. Se nun escenario como ese empregásemos ese tipo de ferramentas de predición de risco individual para a imposición da pena ou para o seu cumprimento dun xeito claro, estas ferramentas dependendo de como chegasen a empregarse, poderían chegar a considerar que unha persoa negra tería máis risco de reincidencia ou perigosidade. Polo tanto, impoñeríaselle unha pena maior ou máis requisitos para poder acceder a determinados grados de cumprimento da pena de prisión pois dese xeito evitaremos que esas persoas anden polas rúas e poidan cometer delitos. De novo, estamos empregando unha perspectiva prospectiva, imos protexer á sociedade destes individuos polo que imos a metelos si ou si en prisión¹⁴⁰ ou polo menos, imos procurar mantelos o maior tempo posible nela. A pena non só vai servir para castigar aqueles feitos cometidos senón tamén ao aseguramento fronte aos feitos futuros¹⁴¹.

Moi relacionado co anterior, está a segunda das notas definatorias do dereito penal do inimigo: as penas desproporcionadamente altas. De novo, por consideralo un exemplo máis evidente, pedímoslle ao lector que se sitúe nunha situación semellante á da

¹³⁹ FRIEDE, Reis (2019). As prisões brasileiras e a condição humana do encarcerado. *Revista Interdisciplinar de Direito*. Valença: Faculdade de Direito de Valença, v.17, n.1, p. 224.

¹⁴⁰ Lembremos que, en España segundo os artigos 80 e seguintes a imposición dunha pena de prisión inferior a 2 anos pode supoñer, en función de determinadas circunstancias, a entrada ou non nunha institución penitenciaria. De feito, unha das cuestións a valorar segundo este artigo 80 é a perigosidade criminal do suxeito.

¹⁴¹ JAKOBS, Günther (2006). *Derecho penal del ciudadano*, cit., pp. 40 – 41.

poboación negra no Brasil. Se unha persoa negra, é considerada estatisticamente máis perigosa que unha persoa branca, no suposto de que se empreguen ferramentas de predición de risco dotadas de IA en sede de imposición da pena, o certo é que as persoas negras, maioritariamente, serán consideradas máis perigosas e polo tanto terán unha pena maior. Pensemos no informe de Propublica sobre COMPAS do que xa falamos neste texto, por exemplo. Pero non só neste eido, de novo pensemos na sede de cumprimento da pena, as persoas negras serán máis castigadas, pois limitarase dalgún xeito o seu acceso a determinados beneficios penitenciarios. É dicir, para as persoas que estes sistemas consideren inimigos, aqueles máis perigosos, as penas non aumentarán en canto a dereito substantivo pero si que sufrirán unhas consecuencias xurídicas do delito máis duras: tanto na imposición da pena como no cumprimento da mesma.

Finalmente, chegamos á derradeira das notas características do dereito penal do inimigo: a relativización ou supresión de determinadas garantías procesuais. Sobre este punto, xa falamos en liñas anteriores¹⁴². Dun xeito ou outro este tipo de ferramentas de predición do risco polo menos, no máis leve dos supostos, cuestionarían ou diminuirían determinadas garantías procesuais e constitucionais, entre elas a presunción de inocencia ou o dereito á protección de datos¹⁴³. No exemplo do que vimos falando neste apartado o dereito á igualdade veríase damnificado dun xeito evidente, pero tamén poderían verse cuestionados todos aqueles dereitos que xa mencionamos. A decisión para esta limitación responderá probablemente a criterios de eficacia¹⁴⁴. Cabe a posibilidade de que o Estado, por razóns políticas, queira responder ás demandas dos seus cidadáns¹⁴⁵ e fomentar o emprego deste tipo de ferramentas prexudicando a aqueles individuos que pola razón que

¹⁴² *Supra* apartado 4.B).

¹⁴³ DAMIÁN MORENO, Juan (2006) ¿Un derecho procesal de enemigos? En: CANCIO MELIÁ, Manuel (coord.) y GÓMEZ-JARA DÍEZ, Carlos (coord.). *Derecho penal del enemigo. El discurso penal de la exclusión. Volumen I*. Madrid: Edisofer, p. 458. ISBN: 849626128X.

¹⁴⁴ DAMIÁN MORENO, Juan (2006) ¿Un derecho procesal de enemigos?, cit., p. 468.

¹⁴⁵ DAMIÁN MORENO, Juan (2006) ¿Un derecho procesal de enemigos?, cit., p. 459.

sexa teñan máis probabilidades de cometer un delito. Parece polo tanto, que nos dirixiríamos a un dereito penal de autor¹⁴⁶.

Semella que no suposto de chegar ao hipotético que formulamos nas anteriores liñas, estaríamos nunha evidente aplicación do dereito penal do inimigo. Probablemente sería inxenuo non asumir que a chegada de ferramentas de predición de risco dotadas de IA é inminente¹⁴⁷. Polo que agora é o momento de cuestionarse ata onde imos empregar estes sistemas e ata que punto, preferimos a procura dunha decisión máis eficiente fronte a dunha decisión máis xusta¹⁴⁸.

6. Algunhas conclusión para debate¹⁴⁹

Visto todo o anterior podemos dicir sen ningún tipo de dúbida que os sistemas de predición de risco dotados de intelixencia artificial poden encaixarse dentro desta nova corrente que nos últimos anos están tomando as políticas estatais e internacionais de preservación da seguridade. Da loita contra o risco. Esta procura constante da aparición dun posible risco, colectivo ou individual, non é algo novo e que nacesse da man da intelixencia artificial ou deste tipo de ferramentas. De feito podemos encaixalas dentro dos coñecidos como métodos actuariais que levan empregándose no noso sistema penal dende vai anos.

Polo momento non existe en España nin na UE lexislación que regule de xeito específico e concreto este tipo de ferramentas pero, vimos que poderíamos encaixalo dentro do paquete normativo sobre protección de datos. Dentro deste, existe a prohibición da toma de decisións baseadas unicamente no tratamento automatizado de datos, incluída a elaboración de perfís no eido da prevención, detección, investigación e axuizamento de infraccións penais e de execución de sancións penais segundo a Directiva 2016/680 e a

¹⁴⁶ CANCIO MELIÁ, Manuel (2006). De nuevo, cit., p. 128.

¹⁴⁷ MIRÓ-LLINARES, Fernando (2020) Predictive Policing, cit., p. 10.

¹⁴⁸ GALGANI, Benedetta (2021). Consideraciones sobre los “antecedentes”, cit., p. 1149.

¹⁴⁹ Tomamos este título para as nosas conclusións de Romeo Casabona por consideralo o máis axeitado pois, aínda que deste traballo puidésemos sacar moitas cousas en claro, o certo é que o estado embrionario da cuestión merece aínda, un arduo debate. ROMEO CASABONA, Carlos María (2018). Riesgo, cit., p. 54.

LO 7/2021. O encaixe neste artigo non ten dúbida algunha polo que, ata o de agora, o seu uso está limitado. De todos xeitos esta prohibición é relativa pois estará condicionada á non existencia dunha posterior norma nacional ou transnacional que permita o seu uso. O texto xurídico que previsiblemente permitirá o emprego deste tipo de sistemas será o Regulamento sobre IA da UE do que xa coñecemos a Proposta e onde se contemplan especificamente os sistemas dos que vimos falando ao longo deste traballo. Veremos nos vindeiros meses cales van ser os requisitos específicos que terán que cumprir e en que eidos poderemos velo.

Tampouco podemos negar a afectación de distintos fundamentais que poden provocar este tipo de sistemas. Dende o dereito á igualdade en todas as súas manifestacións ata a protección de datos. Vimos tamén como esta afectación é máis evidente e perigosa en aqueles sistemas nos que os controis sobre este tipo de ferramentas son nulas ou moi limitadas. O caso máis claro é o de COMPAS onde nin o compromiso do principio de transparencia, do dereito ao debido proceso ou o principio de igualdade provocaron o rexeitamento do seu uso polos tribunais estadounidenses.

Unha lectura do Proxecto de Regulamento sobre IA fai inminente a chegada deste tipo de ferramentas aos nosos sistemas policiais e xudiciais. É o momento de que técnicos e xuristas traballen para evitar que a incidencia sobre os nosos dereitos fundamentais sexa o mínima posible. Só mediante a regulación deste tipo de ferramentas poderemos protexelos. Establecendo os límites do emprego deste tipo de ferramentas, delimitando o seu eido de aplicación así como a fixación clara e explícita de cales van a ser as súas funcións. O recoñecemento de todos os defectos e riscos que poden provocar o emprego deste tipo de tecnoloxía ao servizo do control e da vixilancia do Estado non pode ser excusa para a tecnofobia¹⁵⁰.

Deixarnos levar polo medo e prohibir este tipo de ferramentas poderá provocar que os nosos sistemas xudiciais e policiais queden atrasados respecto dos de outros lugares do mundo e que se volvan incluso deficientes. Tamén poderemos estar perdendo a oportunidade de controlar mellor e inspeccionar a labor dos membros da policía e do sistema xudicial. Porque aínda que á hora de falar sobre estas ferramentas moitas veces

¹⁵⁰ MIRÓ-LLINARES, Fernando (2020) Predictive Policing, *cit.*, p. 10.

esquécese esta cuestión, non podemos obviar que calquera ser humano non está exento de erros ou de nesgos. Non podemos afirmar con rotundidade que non haxa ou que non vaia a haber erros nos membros dos sistemas xudiciais e policiais ou que non haxa vulneracións de dereitos fundamentais pola súa parte. Saber ou detectar isto nun ser humano é unha tarefa moi complexa pero non nun sistema de predición de risco dotado de IA que, sempre que cumpra uns mínimos, poderá ser supervisado e controlado evitando todos estes erros ou intencións tan humanas.

Pola contra, se deixásemos que se empregasen este tipo de sistemas dun xeito máis libre. Sen control, sen establecemento duns mínimos ou decantándonos pola autorregulación poderíamos dirixirnos, sen ningún xénero de dúbidas, cara un escenario perverso e perigoso para o sistema xudicial e policial¹⁵¹. Cara un dereito penal do inimigo. Onde, un ou varios determinados grupos de persoas serán estigmatizados e expulsados do sistema. Non deixándoos saír desa dinámica de delincuencia e castigo e menos aínda, permitirilles unha reinserción efectiva na sociedade. Poderíamos chegar ao punto polo tanto, de que un concreto grupo de persoas pola súa idade, xénero, capacidade económica, orixe ou raza se atopen sempre sinalados e expulsados da cidadanía.

É agora o momento no que temos que decidir cal vai ser o camiño que queremos cruzar. Deberemos acordar cales van ser os límites destas ferramentas, cando van ser empregadas, por quen e baixo que situacións. Negarnos a que veñan ou a que vaian a formar parte do noso sistema penal non nos servirá de nada. Teremos que facer todo o posible para que a súa chegada supoña o menor risco posible para as persoas e para os seus dereitos fundamentais.

¹⁵¹ BUENO DE MATA, Federico (2022). La necesidad de regular la inteligencia artificial., cit., p. 18.

Bibliografía

ABOSO, Gustavo Eduardo (2006). El llamado “derecho penal del enemigo” y el ocaso de la política criminal racional: el caso argentino. En: CANCIO MELIÁ, Manuel (coord.) y GÓMEZ-JARA DÍEZ, Carlos (coord.). *Derecho penal del enemigo. El discurso penal de la exclusión. Volumen 1*. Madrid: Edisofer, pp. 53 – 78. ISBN: 849626128X.

ALONSO SALGADO, Cristina (2021) Acerca de la inteligencia artificial en el ámbito penal: especial referencia a la actividad de las fuerzas y cuerpos de seguridad. *Ius et Scientia*. Sevilla: Editorial Universidad de Sevilla, vol. 7, núm. 1, pp. 25 – 36. ISSN: 24448478.

AMUNÁTEGUI PERELLÓ, Carlos (2020), *Arcana technicae. El derecho y la inteligencia artificial*. Valencia: Tirant lo Blanch. ISBN: 9788413550213.

AÑÓN ROIG, María José (2022). Desigualdades algorítmicas: conductas de alto riesgo para los Derechos Humanos. *Derechos y libertades*. Madrid: Dykinson, núm. 47, pp. 17 – 49. ISSN: 11330937.

BARONA VILAR, Silvia (2021) *Algoritmización del derecho y de la justicia. De la Inteligencia Artificial a la Smart Justice*. Valencia: Tirant lo Blanch. ISBN 9788413786667.

- (2021) Una justicia “digital” y “algorítmica” para una sociedad en estado de mudanza. En BARONA VILAR, Silvia (ed.). *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar*. Valencia: Tirant lo Blanch, pp. 21 – 64. ISBN: 9788413972015.

BECK, Ulrich (2002). *La sociedad del riesgo global*, Madrid: Siglo XXI de España Editores. ISBN: 8432310832.

BELLOSO MATÍN, Nuria (2019), Algoritmos predictivos al servicio de la justicia: ¿una nueva forma de minimizar el riesgo y la incertidumbre? *Revista da Faculdade Mineira de Direito*, v. 22, núm. 43, pp. 1-31.

BRANDARIZ GARCÍA, José Ángel (2014) *El gobierno de la penalidad: la complejidad de la política criminal contemporánea*, Madrid: Dykinson. ISBN: 9788490851005.

BORJA JIMÉNEZ, Emiliano (2019). Seguridad como producto de mercado en la justicia penal globalizada. En BARONA VILAR, Silvia (ed.) *Claves de la justicia penal: feminización, inteligencia artificial, supranacionalidad y seguridad*. Valencia: Tirant lo Blanch, pp. 523 – 553. ISBN: 9788413360744.

BUENO DE MATA, Federico (2022). La necesidad de regular la inteligencia artificial y su impacto como tecnología disruptiva en el proceso: de desafío utópico a cuestión de urgente necesidad. En: BUENO DE MATA, Federico (dir.). *El impacto de las tecnologías disruptivas en el derecho procesal*. España: Thomson Reuters Aranzadi, pp. 15 – 41. ISBN: 9788413455885

CANCIO MELIÁ, Manuel (2006). De nuevo: ¿“derecho penal” del enemigo? En: JAKOBS, Günther y CANCIO MELIÁ, Manuel. *Derecho penal del enemigo*. 2ª edición. Navarra: Aranzadi Editorial, pp. 85 – 152. ISBN: 8447025365.

COLMENERO GUERRA, José Antonio (2022). La protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales vinculados al «discurso terrorista». En GALÁN MUÑOZ, Alfonso y GÓMEZ RIVERO, María del Carmen (dir.) *La represión y persecución penal del discurso terrorista*. Valencia: Tirant lo Blanch, 2022, pp. 627-720. ISBN: 9788413979700.

DAMIÁN MORENO, Juan (2006) ¿Un derecho procesal de enemigos? En: CANCIO MELIÁ, Manuel (coord.) y GÓMEZ-JARA DÍEZ, Carlos (coord.). *Derecho penal del enemigo. El discurso penal de la exclusión. Volumen 1*. Madrid: Edisofer, pp. 457 – 472. ISBN: 849626128X.

DE HOYOS SANCHO, Montserrat (2022). El proyecto de Reglamento de la Unión Europea sobre inteligencia artificial, los sistemas de alto riesgo y la creación de un ecosistema de confianza. En BARONA VILAR, Silvia (ed.) *Justicia poliédrica en periodo de mudanza (Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad)*, Valencia: Tirant lo Blanch, pp. 403 – 421. ISBN: 9788411135702.

DE MIGUEL ASENSIO, Pedro Alberto (2021). Propuesta de Reglamento sobre inteligencia artificial. *Diario la Ley Unión Europea*, núm. 92, pp. 19 – 35. ISSN-e: 2255551X.

DEL POZO PÉREZ, Marta (2022). ¿Los algoritmos sirven para proteger a las víctimas de violencia de género? En: BUENO DE MATA, Federico (dir). *El impacto de las tecnologías disruptivas en el derecho procesal*. España: Thomson Reuters Aranzadi, pp. 155 – 181. ISBN: 9788413455885.

ESPARZA LEIBAR, Iñaki (2021). La Inteligencia Artificial y el derecho fundamental a la protección de datos de carácter personal. La aplicación integral de la inteligencia artificial: una oportunidad para dar un salto cualitativo en la correcta actuación de los poderes públicos, en general, y en el campo de la justicia, en particular. En: BARONA VILAR, Silvia (ed.). *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar*. Valencia: Tirant lo Blanch, pp. 265 – 286. ISBN: 9788413972022.

EUBANKS, Virginia (2021) *La automatización de la desigualdad: herramientas de tecnología avanzada para supervisar y castigar a los pobres*. Madrid: Capitán Swing. ISBN: 9788412281866.

FEELEY, Malcon y SIMON, Jonathan (1994). Actuarial Justice: The Emerging New Criminal Law. En NELKEN, David (ed.). *The futures of Criminology*, London: SAGE Publications, pp. 173 – 201. ISBN: 080397145.

FREEMAN, Katherine (2016). Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in *State v. Loomis*. *North Carolina Journal of Law & Technology*, v. 18, 2016, pp. 75 – 106.

FRIEDE, Reis (2019). As prisões brasileiras e a condição humana do encarcerado. *Revista Interdisciplinar de Direito*. Valença: Faculdade de Direito de Valença, v.17, n.1, pp. 215 – 230.

GALGANI, Benedetta (2021). Consideraciones sobre los “antecedentes” del acusado y del juez frente a la inteligencia artificial (IA) en el proceso penal. En MORENO CATENA, Víctor; ROMERO PRADAS, M^a Isabel (dirs.) y LARO GONZÁLEZ, Elena (ed.). *Nuevos postulados de la cooperación judicial en la Unión Europea. Libro*

homenaje a la Prof. M^a Isabel González Cano. Valencia: Tirant lo Blanch, pp. 1147 – 1169. ISBN: 9788413781211.

GERARDS, Janneke y XENEDIS, Raphaële (2020). *Algorithmic discrimination in Europe. Challenges and opportunities for gender equality and non-discrimination law*. Luxemburgo: Publications Office of the European Union. ISBN: 9789276207467.

GRECO, Luís (2019). La criminalización en el estado previo: un balance del debate alemán. En: ALONSO RIMO, Alonso (dir.) y COLOMER BEA, David (coord.). *Derecho penal preventivo, orden público y seguridad ciudadana*. España: Aranzadi Thomson Reuters, pp. 93 – 115. ISBN: 9788413099316.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, Adoptadas el 3 de octubre de 2017 y revisadas el 6 de febrero de 2018.

GRUPO INDEPENDIENTE DE EXPERTOS DE ALTO NIVEL SOBRE INTELIGENCIA ARTIFICIAL (2019). *Directrices éticas para una IA fiable*. Bruselas: Comisión Europea. ISBN: 9789276119944.

GONZÁLEZ CUSSAC, José Luís y FLORES GIMÉNEZ, Fernando (2018). Seguridad global y derechos fundamentales. Una propuesta metodológica. En GONZÁLEZ CUSSAC José Luis y FLORES GIMÉNEZ, Fernando (coord.) *Seguridad y derechos. Análisis de las amenazas, evaluación de las respuestas y valoración del impacto en los derechos fundamentales*. Valencia: Tirant lo Blanch, pp. 25 – 98. ISSN: 9788413130873.

GONZÁLEZ CUSSAC, José Luís (2019). Seguridad e incertidumbre: un derecho penal híbrido. En BARONA VILAR, Silvia (ed.). *Claves de la justicia penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad*, Valencia: Tirant lo Blanch, pp. 503 – 522. ISBN: 9788413360744.

GUTIÉRREZ, Mariano Hernán (2008). Punitivismo y actuarialismo en la Argentina. *V Jornadas de Sociología de la UNLP*, 10, 11 y 12 de diciembre de 2008, La Plata, Argentina: Memoria Académica.

GUZMÁN FLUJA, Vicente C. (2021). Proceso penal y justicia automatizada, *Revista General de Derecho Procesal*, núm. 53, pp. 1 – 40. ISSN: 16969642.

HARCOURT, Bernard E. (2007). *Against prediction: profiling, policing and punishing in an actuarial age*. Chicago: The University of Chicago Press, p. 1. ISBN: 9780226316147.

- (2003) From the Ne'er-do-well to the criminal history category: the refinement of the actuarial model in criminal law. *Law and contemporary problems*, vol. 66, pp. 99 – 152.

HARVARD LAW REVIEW (2016). *State vs. Loomis*. Criminal law. Sentencing guidelines. Wisconsin Supreme Court requires warning before use of algorithmic risk assessments in sentencing.

HESTER, Rhys (2019). Risk Assessment at Sentencing. The Pennsylvania Experience. En DE KEIJSER, J. W.; ROBERTS, J. V.; RYBERG, J., (ed.) *Predictive Sentencing. Normative and empirical perspectives*, Oxford, UK; Chicago, Illinois: Hart Publishing, pp. 213 – 238.

JAKOBS, Günther (2008). ¿Derecho penal del enemigo? Un estudio de los presupuestos de la juridicidad. En: CANCIO MELIÁ, Manuel (ed.) y FEIJOO SÁNCHEZ, Bernardo (ed.). *Teoría funcional de la pena y de la culpabilidad. Seminario con Günther Jakobs en la UAM*. 1ª edición. Pamplona: Aranzadi Editorial, pp. 23 – 62. ISBN: 9788447029112.

- (2006) Derecho penal del ciudadano y derecho penal del enemigo. En: JAKOBS, Günther y CANCIO MELIÁ, Manuel. *Derecho penal del enemigo*. 2ª edición. Navarra: Aranzadi Editorial, pp. 21 – 56. ISBN: 8447025365.

JUAN SÁNCHEZ, Ricardo (2019). Proceso penal preventivo en España: elementos y criterios de contención. En BARONA VILAR, Silvia (2019) *Claves de la justicia penal: feminización, inteligencia artificial, supranacionalidad y seguridad*. Valencia: Tirant lo Blanch, pp. 555 – 584. ISBN: 9788413360744.

KIM, Pauline T. (2017). Auditing algorithms for discrimination. *University of Pennsylvania Law Review Online*, vol. 166, pp. 189 – 203.

LÓPEZ GUTIÉRREZ, Javier, et al. (2020). *Estudios sobre la cibercriminalidad en España*. España: Ministerio de Interior, Gobierno de España.

MARTÍN DIZ, Fernando (2021). Inteligencia artificial y derecho procesal: luces, sombras y cábales en clave de derechos fundamentales. En MORENO CATENA, Víctor; ROMERO PRADAS, M^a Isabel (dirs.) y LARO GONZÁLEZ, Elena (ed.). *Nuevos postulados de la cooperación judicial en la Unión Europea. Libro homenaje a la Prof. M^a Isabel González Cano*. Valencia: Tirant lo Blanch, pp. 969 – 1006. ISBN: 9788413781211.

MARTÍNEZ GARCÍA, Jesús Ignacio (2020). Inteligencia y derechos humanos en la sociedad digital, *Cuadernos Electrónicos de Filosofía del Derecho*, núm. 40, pp. 168 – 189. ISSN: 11389877.

MIRÓ-LLINARES, Fernando (2020). Predictive Policing: Utopia or Dystopia? On attitudes towards the use of Big Data algorithms for law enforcement. *Revista d'internet, dret i política*, n. 30, pp. 1 – 18. ISSN: 16998154.

NIEVA FENNOL, Jordi (2021). Tecnología y derechos fundamentales en el proceso judicial. En MORENO CATENA, Víctor; ROMERO PRADAS, M^a Isabel (dirs.) y LARO GONZÁLEZ, Elena (ed.). *Nuevos postulados de la cooperación judicial en la Unión Europea. Libro homenaje a la Prof. M^a Isabel González Cano*. Valencia: Tirant lo Blanch, pp. 1007 – 1033. ISBN: 9788413781211.

- (2018) *Inteligencia artificial y proceso judicial*. Madrid: Marcial Pons. ISBN: 9788491238218.

O'NEIL, Cathy (2017). *Armas de destrucción matemática. Cómo el big data aumenta la desigualdad y amenaza la democracia*. Madrid: Capitán Swing. ISBN: 9788494740848.

ORTIZ PRADILLO, Juan Carlos (2022). Inteligencia artificial, Big Data, tecnovigilancia y derechos fundamentales en el proceso penal. En: VILLEGAS

DELGADO, César y MARTÍN RÍOS, Pilar (ed.). *El derecho en la encrucijada tecnológica. Estudios sobre derechos fundamentales, nuevas tecnologías e inteligencia artificial*. Valencia: Tirant lo Blanch, pp. 103 – 127. ISBN: 9788411132947.

PALMA ORTIGOSA, Adrián (2022). El ciclo de vida de los sistemas de inteligencia artificial. Aproximación técnica de las fases presentes durante el diseño y despliegue de los sistemas algorítmicos. En COTINO HUESO, Lorenzo (dir.) y BAUZÁ REILLY, Marcelo (coord.). *Derechos y garantías ante la inteligencia artificial y las decisiones automatizada*, Madrid: Thomsom Reuters Aranzadi, pp. 29 – 50. ISBN: 9788411244992.

- (2019) Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos. *Revista General de Derecho Administrativo*, núm. 17, 2019, pp. 1 – 35. ISSN: 16969650.

RIVERA BEIRAS, Iñaki. (2015) Actuarialismo penitenciario: su recepción en España. *Crítica penal y poder: una publicación del Observatorio del Sistema Penal y los Derechos Humanos*, núm. 9, pp. 102 – 144. ISSN-e: 20143753.

RIVERO ORTEGA, Ricardo (2015). La nueva Ley Orgánica de Seguridad Ciudadana: ¿Estado de prevención o Derecho administrativo del enemigo? *Ars Iuris Salmanticensis*. Salamanca: Ediciones Universidad de Salamanca, v. 3, pp. 11 – 16. eISSN: 23405155.

ROIG I BATALLA, Antoni (2020). *Las garantías frente a las decisiones automatizadas. Del Reglamento General de Protección de Datos a la gobernanza algorítmica*. Barcelona: Bosch Constitucional. ISBN: 9788412201574.

ROMEO CASABONA, Carlos María (2018) Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad. *Revista de Derecho, Empresa y Sociedad (R.E.D.S)*, núm. 13, pp. 39 – 45, ISSN-e: 23404647.

SILVA SÁNCHEZ, Jesús María (2011). *La expansión del derecho penal: aspectos de la política criminal en las sociedades postindustriales*, Madrid: Edisofer. ISBN: 9788496261914.

SIMÓN CASTELLANO, Pere (2021). *Justicia cautelar e inteligencia artificial. La alternativa a los atávicos heurísticos judiciales*. España: Bosch Editor, pp. 130 e ss. ISSN: 9788412315417.

SORIANO ARNANZ, Alba (2021). Decisiones automatizadas y discriminación: aproximación y propuestas generales. *Revista General de Derecho Administrativo*, núm. 56, p. 1 – 45. ISSN: 1696-9650.

- (2021). Decisiones automatizadas: problemas y soluciones jurídicas más allá de la protección de datos. *Revista de Derecho Público: Teoría y Método*, v. 3, p. 85 – 128. ISSN: 26957191.

SUÁREZ XAVIER, Paulo Ramón, et al. (2022). *Polícia predictiva e <<negritude>>: modelos para a reprodução de um estado sem direitos*. En: SUÁREZ XAVIER, Paulo Ramón y FONTESTAD PORTALÉS, Leticia (2022). *Seguridad y los retos de la jurisdicción en el siglo XXI: justicia, sostenibilidad y paz*. A Coruña: Colex, pp. 27 – 53. ISBN: 9788413595160.

VALLS PRIETO, Javier (2017). *Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial*. Madrid: Dykinson. ISBN: 9788491484752.

VIDA FERNÁNDEZ, José (2018). Los retos de la regulación de la inteligencia artificial: algunas aportaciones desde la perspectiva europea. En: DE LA QUADRASALCEDO FERNÁNDEZ DEL CASTIGO, Tomás y PIÑAR MAÑAS, José Luís (dir.). *Sociedad digital y derecho*. Madrid: Ministerio de Industria, Comercio y Turismo, Red.es: Boletín oficial del Estado, pp. 203 – 224. ISBN: 9788434024830.

ZEDNER, Lucía (2019). El debate sobre el estado preventivo: aportaciones y retos doctrinales en materia de justicia preventiva. En: ALONSO RIMO, Alonso (dir.) y COLOMER BEA, David (coord.). *Derecho penal preventivo, orden público y seguridad ciudadana*. España: Aranzadi Thomson Reuters, pp. 61 – 92. ISBN: 9788413099316.

Xurisprudencia

- STC núm. 145/1988, do 12 de xullo
- STC núm. 189/1998, do 28 de setembro
- STC núm. 292/2000, do 30 de novembro.
- STC núm. 133/2014, do 22 de xullo
- STS núm. 507/2020, do 14 de outubro (Sala 2ª)
- STS núm. 171/2018, do 11 de abril (Sala 2ª)
- STS núm. 143/2013, do 28 de febreiro (Sala 2ª)