Parlamento Europeu
2019-2024

Documento de sessão

A9-0232/2021

13.7.2021

RELATÓRIO

sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais
(2020/2016(INI))

Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos

Relator: Petar Vitanov

PR_INI

ÍNDICE

Página

PROPOSTA DE RESOLUÇÃO DO PARLAMENTO EUROPEU

sobre a inteligência artificial no Direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais
(2020/2016(INI))

O Parlamento Europeu,

– Tendo em conta o Tratado da União Europeia (TUE), nomeadamente os artigos 2.º e 6.º, e o Tratado sobre o Funcionamento da União Europeia (TFUE), em particular o artigo 16.º,

– Tendo em conta a Carta dos Direitos Fundamentais da União Europeia (a Carta), nomeadamente os artigos 6.º, 7.º, 8.º, 11.º, 12.º, 13.º, 20.º, 21.º, 24.º e 47.º,

– Tendo em conta a Convenção para a Proteção dos Direitos Humanos e das Liberdades Fundamentais,

– Tendo em conta a Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção 108), e o protocolo que a altera («Convenção 108+»),

– Tendo em conta a Código Europeu de Ética para o Uso da Inteligência Artificial nos Sistemas Judiciais e seu Ambiente, publicada pela Comissão Europeia para a Eficiência da Justiça (CEPEJ) do Conselho da Europa,

– Tendo em conta a comunicação da Comissão, de 8 de abril de 2019, intitulada «Aumentar a confiança numa inteligência artificial centrada no ser humano» (COM(2019)0168),

– Tendo em conta o documento intitulado «Ethics Guidelines for Trustworthy Artificial Intelligence» (Orientações éticas para uma IA de confiança) publicado pelo Grupo de Peritos de Alto Nível sobre inteligência artificial publicado em 8 de abril de 2019,

– Tendo em conta o Livro Branco da Comissão Europeia de 19 de fevereiro de 2020, intitulado «A inteligência artificial - Uma abordagem europeia virada para a excelência e a confiança» (COM(2020)0065),

– Tendo em conta a comunicação da Comissão, de 19 de fevereiro de 2020, intitulada «Uma estratégia europeia para os dados» (COM(2020)0066),

– Tendo em conta o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)[1],

[1] JO L 119 de 4.5.2016, p. 1.

– Tendo em conta a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho[2],

– Tendo em conta o Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE[3],

– Tendo em conta a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas)[4],

– Tendo em conta o Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho[5],

– Tendo em conta a sua resolução, de 19 de junho de 2020, sobre as manifestações de protesto contra o racismo na sequência da morte de George Floyd[6],

– Tendo em conta a sua resolução, de 14 de março de 2017, sobre as implicações dos grandes volumes de dados nos direitos fundamentais: privacidade, proteção de dados, não discriminação, segurança e aplicação da lei[7],

– Tendo em conta a audição realizada na Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos (LIBE), em 20 de fevereiro de 2020, sobre a inteligência artificial no domínio do Direito penal e a respetiva utilização pelas autoridades policiais e judiciárias em matéria penal,

– Tendo em conta o relato da missão da Comissão LIBE nos Estados Unidos efetuada em fevereiro de 2020,

– Tendo em conta o artigo 54.º do seu Regimento,

– Tendo em conta os pareceres da Comissão do Mercado Interno e da Proteção dos Consumidores e da Comissão dos Assuntos Jurídicos,

– Tendo em conta o relatório da Comissão das Liberdades Cívicas, da Justiça e dos

[2] JO L 119 de 4.5.2016, p. 89.
[3] JO L 295 de 21.11.2018, p. 39.
[4] JO L 201 de 31.7.2002, p. 37.
[5] JO L 135 de 24.5.2016, p. 53.
[6] Textos Aprovados, P9_TA(2020)0173.
[7] JO C 263 de 25.7.2018, p. 82.

Assuntos Internos (A9-0232/2021),

A. Considerando que as tecnologias digitais, em geral, e a proliferação do tratamento e da análise de dados possibilitados pela inteligência artificial (IA), em particular, são extraordinariamente promissoras, embora acarretem riscos; que, nos últimos anos, se verificaram grandes avanços no desenvolvimento da IA, fazendo desta uma das tecnologias estratégicas do século XXI, com potencial para gerar benefícios substanciais em termos de eficiência, precisão e comodidade, trazendo, assim, uma mudança positiva para a sociedade, mas também sérios riscos para os direitos fundamentais e para as democracias alicerçadas no Estado de Direito; que a IA não deve ser vista como um fim em si, mas como um instrumento ao serviço das pessoas, com o objetivo último de aumentar o bem-estar, as capacidades e a segurança dos seres humanos;

B. Considerando que, não obstante os progressos contínuos a nível da velocidade de processamento e da capacidade de memória, não existem ainda programas capazes de igualar a flexibilidade humana no que se refere a domínios mais amplos ou a tarefas que exijam a compreensão do contexto ou uma análise crítica; que algumas aplicações de IA alcançaram, na execução de determinadas tarefas específicas (através de aplicações tecnológicas inovadoras para o domínio jurídico, por exemplo), níveis de desempenho semelhantes aos de peritos e profissionais humanos, sendo capazes de gerar resultados a uma velocidade excecionalmente elevada e a uma escala muito mais vasta;

C. Considerando que em alguns países, inclusive em vários Estados-Membros, o recurso a aplicações de IA, ou a sistemas integrados de IA, pelas autoridades policiais e pelo sistema judicial é maior do que noutros, o que se fica, em parte, a dever à falta de regulamentação e a diferenças regulamentares que possibilitam ou interditam a utilização de IA para determinadas finalidades; que a crescente utilização da IA no domínio do Direito penal se baseia em promessas segundo as quais diminuirá o crime e conduzirá a decisões mais objetivas; que, no entanto, estas promessas nem sempre são verdadeiras;

D. Considerando que os direitos e as liberdades fundamentais consignados na Carta devem ser garantidos ao longo de todo o ciclo de vida da IA e respetivas tecnologias, nomeadamente no momento da conceção, do desenvolvimento, da implantação e utilização, e devem ser tidos em conta no quadro da aplicação da lei em todas as circunstâncias;

E. Considerando que a tecnologia de IA deve ser desenvolvida de forma antropocêntrica, ser digna de confiança pública e estar sempre ao serviço dos seres humanos; que os sistemas de IA devem garantir que são concebidos de modo a que possam ser sempre desligados por um operador humano;

F. Considerando que os sistemas de IA devem ser concebidos para proteção e benefício de todos os membros da sociedade (tendo, nomeadamente, em conta as populações vulneráveis e marginalizadas na sua conceção), ser não discriminatórios e seguros, e que as suas decisões devem ser explicáveis e transparentes, respeitar a autonomia humana e os direitos fundamentais, por forma a serem fiáveis, tal como descrito nas Orientações éticas para uma IA de confiança do Grupo de peritos de Alto Nível sobre a Inteligência Artificial;

G. Considerando que a União, juntamente com os Estados-Membros, tem a responsabilidade fundamental de garantir que as decisões relativas ao ciclo de vida e à utilização de aplicações de IA no domínio da justiça e da aplicação da lei sejam tomadas de forma transparente, salvaguardando na íntegra os direitos fundamentais e, em particular, não perpetuem a discriminação, a parcialidade ou os preconceitos, onde quer que existam; que as opções políticas pertinentes devem respeitar os princípios da necessidade e da proporcionalidade, de modo a garantir a constitucionalidade e um sistema judicial equitativo e humano;

H. Considerando que as aplicações de IA podem criar grandes oportunidades no domínio da execução da lei, em particular na melhoria dos métodos de trabalho das autoridades policiais e judiciais, assim como no combate mais eficiente a certos tipos de crime, designadamente a criminalidade financeira, o branqueamento de capitais e o financiamento do terrorismo, o abuso sexual em linha e a exploração de crianças, bem como certos tipos de cibercrime, contribuindo, assim, para a segurança e a proteção dos cidadãos da UE, ao mesmo tempo que podem implicar riscos significativos para os direitos fundamentais das pessoas; que um recurso generalizado à IA para efeitos de vigilância em larga escala seria desproporcionado;

I. Considerando que o desenvolvimento e o funcionamento de sistemas de IA para as autoridades policiais e judiciárias implica um contributo de múltiplas pessoas, organizações, componentes de máquinas, algoritmos de programas informáticos e utilizadores humanos, em ambientes muitas vezes complexos e difíceis; que as aplicações da IA pelas autoridades policiais e judiciárias se encontram em fases de desenvolvimento distintas, que vão desde a conceptualização através de criação de protótipos, passando, ainda, pela avaliação ou pela utilização pós-aprovação; que poderão surgir, no futuro, novas possibilidades de utilização, à medida que aumenta a maturidade das tecnologia, graças à investigação científica em curso a nível mundial;

J. Considerando que é necessário um modelo claro para a atribuição de responsabilidade jurídica pelos potenciais efeitos nocivos dos sistemas de IA no domínio do Direito penal; que as disposições regulamentares neste domínio devem sempre manter a responsabilidade humana e ter como objetivo, acima de tudo, evitar quaisquer efeitos nocivos;

K. Considerando que, em última análise, cabe aos Estados-Membros garantir o pleno respeito dos direitos fundamentais sempre que sejam utilizados sistemas de IA no domínio da aplicação da lei e do poder judicial;

L. Considerando que a relação entre a proteção dos direitos fundamentais e a eficácia do policiamento tem de constituir sempre um elemento fundamental das discussões sobre o eventual recurso à IA pelos serviços policiais e como é que tal deve ser feito, atendendo a que essas decisões podem ter consequências duradouras para a vida e a liberdade dos indivíduos; que tal é particularmente importante, visto que a IA pode vir a tornar-se uma parte permanente do ecossistema da nossa justiça penal, ao proporcionar assistência e análise em matéria de investigação;

M. Considerando que a IA é utilizada pelas autoridades policiais em programas informáticos como as tecnologias de reconhecimento facial, nomeadamente para

procurar suspeitos em bases de dados e identificar vítimas de tráfico de seres humanos ou de exploração sexual e abuso de menores, no reconhecimento automático de matrículas, na identificação de pessoas pela voz, no reconhecimento da fala, na leitura labial, nas escutas (ou seja, algoritmos de deteção de disparos), na investigação e na análise autónomas de bases de dados identificadas, nas previsões (previsão policial e análise de locais de criminalidade), nas ferramentas de deteção de comportamentos, as ferramentas avançadas de autópsia virtual, para ajudar a determinar a causa da morte, nos instrumentos autónomos para detetar fraudes financeiras e o financiamento do terrorismo, na monitorização das redes sociais (extração e recolha de dados para a identificação de ligações) e nos sistemas de vigilância automatizada que integram diferentes possibilidades de deteção (como a deteção de batimentos cardíacos e as câmaras térmicas); que as aplicações atrás referidas, a par de potenciais ou futuras aplicações da tecnologia de IA no âmbito da aplicação da lei, podem ter graus de fiabilidade e precisão muito variados e um impacto na proteção dos direitos fundamentais e na dinâmica dos sistemas de justiça criminal; que muitas dessas ferramentas são utilizadas em países terceiros, mas seriam ilegais nos termos do quadro legislativo e da jurisprudência da União em matéria de proteção de dados; que a utilização rotineira de algoritmos, ainda que com uma taxa reduzida de falsos positivos, pode conduzir a que o número de alertas falsos ultrapasse, de longe, o de alertas corretos;

N. Considerando que as ferramentas e as aplicações IA são também utilizadas pelo poder judicial em vários países do mundo, inclusivamente para sustentar decisões sobre a prisão preventiva, sentenças, o cálculo das probabilidades de reincidência e a determinação da liberdade condicional, a resolução de litígios em linha, a gestão da jurisprudência e a disponibilização de um acesso facilitado à justiça; que tal conduziu a uma distorção e diminuição das oportunidades dadas às pessoas de cor e a outras minorias; que, atualmente na UE, com exceção de alguns Estados-Membros, a sua utilização se limita principalmente a processos civis;

O. Considerando que a utilização da IA pelas autoridades policiais implica uma série de riscos potencialmente elevados e, em alguns casos, inaceitáveis, para a proteção dos direitos fundamentais dos indivíduos, designadamente decisões opacas, diferentes tipos de discriminação e erros inerentes ao algoritmo subjacente, que podem ser reforçados por ciclos de resposta, bem como riscos para a proteção da privacidade e dos dados pessoais, a proteção da liberdade de expressão e de informação, a presunção de inocência, o direito a um recurso efetivo e a um julgamento justo, bem como riscos para a liberdade e a segurança das pessoas;

P. Considerando que os sistemas de IA utilizados pelos serviços policiais e pelo poder judicial também são vulneráveis a ataques por meio da IA ou à contaminação de dados, através da qual se procede deliberadamente à inclusão de um conjunto de dados incorreto, para produzir resultados tendenciosos; que os danos resultantes destas situações podem ser ainda mais importantes e causar danos exponencialmente maiores, tanto a nível individual, como coletivo;

Q. Considerando que a utilização da IA no domínio da aplicação da lei e do poder judicial não deve ser encarada como uma mera viabilidade técnica, mas sim como uma decisão política relativa à conceção e aos objetivos da aplicação da lei e dos sistemas de justiça

penal; que o Direito penal moderno e liberal assenta na ideia de que as autoridades estatais reagem a um crime após este ter sido cometido, sem partir do princípio que as pessoas são perigosas e precisam de ser constantemente monitorizadas de modo a evitar quaisquer eventuais ilícitos; que as técnicas de vigilância baseadas na IA desafiam profundamente esta abordagem e tornam urgente que os legisladores de todo o mundo avaliem de forma exaustiva as consequências decorrentes da autorização da implantação de tecnologias que diminuem o papel dos seres humanos na aplicação da lei e nas decisões de justiça;

1. Reitera que, na medida em que o tratamento de grandes quantidades de dados é a base da IA, o direito à proteção da vida privada e o direito à proteção dos dados pessoais se aplicam a todos os domínios da IA e que o quadro jurídico da União em matéria de proteção dos dados e da privacidade deve ser plenamente respeitado; recorda, por conseguinte, que a UE já definiu normas de proteção de dados no quadro da aplicação da lei que constituem os alicerces de qualquer regulamentação futura no domínio da IA para utilização pelas autoridades policiais e pelo poder judicial; recorda que o tratamento de dados pessoais deve ser lícito e justo, as finalidades do tratamento devem ser especificadas, explícitas e legítimas, o tratamento deve ser adequado, pertinente e não excessivo em relação à finalidade para a qual é tratado, deve ser exato, atualizado e os dados inexatos devem, a menos que sejam aplicáveis restrições, ser retificados ou apagados, que os dados não devem ser conservados mais tempo do que o necessário, devem ser definidos prazos claros e adequados para o apagamento ou para a revisão periódica da necessidade de conservação desses dados, que deve ser efetuada de forma segura; sublinha igualmente que deve ser evitada a eventual identificação de pessoas através de uma aplicação de IA que utilize dados previamente anonimizados;

2. Reafirma que todas as soluções policiais e judiciais baseadas na inteligência artificial devem também ser utilizadas no pleno respeito pela dignidade humana, pelos princípios da não discriminação, da liberdade de circulação, da presunção de inocência e do direito de defesa, incluindo o direito ao silêncio, a liberdade de expressão e o livre acesso à informação, a liberdade de reunião e a liberdade de associação, a igualdade perante a lei, o princípio da igualdade das partes e o direito a um recurso efetivo e a um julgamento justo, em conformidade com a Carta dos Direitos Fundamentais e a Convenção Europeia dos Direitos do Homem; salienta que deve ser proibida toda e qualquer utilização de IA que seja incompatível com os direitos fundamentais;

3. Reconhece que a rapidez com que as aplicações de IA estão a ser desenvolvidas em todo o mundo não permite uma listagem exaustiva das aplicações e, por conseguinte, exige um modelo de governação claro e coerente que garanta, tanto os direitos fundamentais dos indivíduos, como a clareza jurídica para os criadores, tendo em conta a evolução permanente da tecnologia; considera, no entanto, tendo em conta o papel e a responsabilidade das autoridades policiais e judiciais e o impacto das decisões que tomam para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou de execução de sanções penais, que o recurso a aplicações de IA tem de ser classificada como de alto risco nos casos em que possa vir a afetar significativamente a vida das pessoas;

4. Entende, neste contexto, que quaisquer instrumentos de IA desenvolvidos ou utilizados pelas autoridades policiais ou judiciais devem, no mínimo, ser seguros, robustos, fiáveis

e adequados ao fim a que se destinam, respeitar os princípios de equidade, da minimização dos dados, da responsabilização, da transparência, da não discriminação e da explicabilidade, e que o seu desenvolvimento, implantação e utilização devem ser sujeitos a uma avaliação dos riscos e a testes rigorosos de necessidade e proporcionalidade, em que as salvaguardas devem ser proporcionais aos riscos identificados; destaca que a confiança dos cidadãos na utilização da IA desenvolvida, implantada e utilizada na UE depende do pleno cumprimento desses critérios;

5. Reconhece o contributo positivo de certos tipos de aplicações de IA para o trabalho das autoridades policiais e judiciais em toda a União; salienta, designadamente, a melhoria da gestão da jurisprudência, tornada possível por ferramentas que permitem opções de pesquisa adicionais; considera que existe uma série de outras utilizações potenciais da IA para a aplicação da lei e para o sistema judicial que poderiam ser exploradas tendo em conta os cinco princípios da Carta Europeia de Ética. sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu Ambiente, adotada pela CEPEJ, prestando especial atenção às «utilizações a considerar com a reserva mais extrema», identificadas pela CEPEJ;

6. Sublinha que qualquer tecnologia pode ser desviada dos seus propósitos, pelo que se impõe um controlo democrático rigoroso e uma supervisão independente de qualquer tecnologia que seja utilizada pelas autoridades policiais e judiciais, especialmente as que possam ser desviadas para a vigilância ou a elaboração de perfis em larga escala; observa, por conseguinte, com grande preocupação, o potencial de determinadas tecnologias de IA utilizadas pelas autoridades policiais para efeitos de vigilância em larga escala; destaca o requisito legal de impedir a vigilância em larga escala através de tecnologias de IA, que, por definição, não é consentânea com os princípios da necessidade e da proporcionalidade, e de proibir a utilização de aplicações que possam resultar na vigilância em larga escala;

7. Salienta que a abordagem adotada em alguns países terceiros relativamente ao desenvolvimento, implantação e utilização de tecnologias de vigilância em larga escala interfere desproporcionadamente com os direitos fundamentais, pelo que não deve ser seguida pela UE; realça, por conseguinte, que as salvaguardas contra a utilização abusiva de tecnologias de IA por parte das autoridades policiais e judiciais também têm de ser regulamentadas de modo uniforme em toda a União;

8. Salienta o potencial de parcialidade e discriminação resultante da utilização de aplicações de IA, tais como a aprendizagem automática, incluindo dos algoritmos em que tais aplicações se baseiam; observa que os preconceitos podem ser inerentes a conjuntos de dados de base, especialmente quando são utilizados dados históricos, inseridos pelos criadores dos algoritmos ou gerados quando os sistemas são aplicados em situações reais; destaca que os resultados das aplicações de IA são necessariamente influenciados pela qualidade dos dados utilizados e que esses preconceitos inerentes tendem a aumentar gradualmente, a perpetuar e a ampliar a discriminação existente, em particular para pessoas pertencentes a certos grupos étnicos ou certas comunidades racializadas;

9. Sublinha que muitas das tecnologias de identificação baseadas em algoritmos atualmente em uso cometem um número desproporcionado de erros de identificação e

categorização e são, portanto, prejudiciais para as pessoas racializadas, pessoas de certas comunidades étnicas, pessoas LGBTI, crianças e idosos, e mulheres; relembra que as pessoas têm, não só o direito de ser corretamente identificadas, como também o de nem sequer serem identificadas, a menos que tal seja exigido por lei, por razões imperiosas e legítimas de interesse público; salienta que as previsões da IA baseadas nas características de um grupo específico de pessoas acabam por amplificar e reproduzir as formas de discriminação existentes; considera que devem ser envidados esforços importantes para evitar a discriminação e a parcialidade automatizadas; requer fortes salvaguardas adicionais quando as autoridades policiais ou judiciais utilizam sistemas de AI em tarefas relacionadas com menores;

10. Destaca a assimetria de poder entre os que utilizam tecnologias de IA e aqueles que lhes estão sujeitos; salienta que é imperativo que a utilização de IA pelas autoridades policiais e judiciais não se torne um fator de desigualdade, divisão social ou exclusão; sublinha o impacto da utilização de ferramentas de IA nos direitos de defesa dos suspeitos, a dificuldade em obter informações significativas sobre o seu funcionamento e a consequente dificuldade em contestar os seus resultados em tribunal, em particular por indivíduos sob investigação;

11. Toma nota dos riscos relacionados, em particular, com as fugas de dados, as violações da segurança dos dados e o acesso não autorizado a dados pessoais e outras informações relacionadas, por exemplo, com investigações criminais ou processos judiciais tratados por sistemas de IA; sublinha que os aspetos ligados à segurança e proteção dos sistemas de IA utilizados pelas autoridades policiais e judiciais devem ser cuidadosamente examinados e ser suficientemente sólidos e resistentes para prevenir consequências potencialmente catastróficas de ataques maliciosos contra sistemas de IA; salienta a importância da segurança desde a conceção, bem como da supervisão humana específica antes de operar determinadas aplicações críticas e, por conseguinte, insta as autoridades policiais e judiciais a utilizarem apenas aplicações de IA que respeitem o princípio da privacidade e da proteção de dados desde a conceção, a fim de evitar o desvirtuamento das funções;

12. Destaca que nenhum sistema de IA deve poder causar danos à integridade física de seres humanos, nem atribuir direitos ou impor obrigações jurídicas às pessoas;

13. Reconhece os desafios à correta determinação da responsabilidade jurídica e da responsabilização por danos potenciais, dada a complexidade do desenvolvimento e funcionamento dos sistemas de IA; considera necessário criar um regime claro e justo para a atribuição da responsabilidade jurídica pelas potenciais consequências negativas destas tecnologias digitais avançadas; sublinha, no entanto, que o objetivo primordial tem de ser o de evitar a todo o transe que se produzam essas consequências; apela, por conseguinte, à aplicação do princípio da precaução em todas as aplicações da IA no contexto da aplicação da lei; sublinha que a responsabilidade jurídica e a responsabilização devem caber sempre a uma pessoa singular ou coletiva, que tem de ser sempre identificada no que toca às decisões tomadas com o apoio da IA; salienta, por conseguinte, a necessidade de garantir a transparência das estruturas empresariais que produzem e gerem sistemas de IA;

14. Considera essencial, tanto para a eficácia do exercício dos direitos de defesa, como para

a transparência dos sistemas nacionais de justiça penal, que um quadro jurídico específico, claro e preciso regule as condições, modalidades e consequências da utilização de instrumentos de IA no âmbito da aplicação da lei e do poder judicial, bem como os direitos das pessoas visadas e procedimentos de reclamação e reparação eficazes e facilmente disponíveis, designadamente o recurso judicial; sublinha o direito de as partes num processo penal terem acesso ao processo de recolha de dados e às avaliações conexas efetuadas ou obtidas através da utilização de aplicações de IA; sublinha a necessidade de as autoridades de execução envolvidas na cooperação judiciária, ao decidirem sobre um pedido de extradição (ou de entrega) para outro Estado-Membro ou país terceiro, avaliarem se a utilização de instrumentos de IA no país requerente pode comprometer manifestamente o direito fundamental a um julgamento justo; insta a Comissão a facultar orientações sobre a forma de realizar essa avaliação no contexto da cooperação judiciária em matéria penal; insiste que os Estados-Membros, em conformidade com a legislação aplicável, devem garantir que as pessoas sejam informadas se forem sujeitas à utilização de aplicações de IA pelas autoridades policiais ou judiciais;

15. Assinala, contudo, que se os humanos se basearem exclusivamente nos dados, perfis e recomendações gerados pelas máquinas, não serão capazes de levar a cabo uma avaliação independente; salienta as consequências potencialmente graves, mormente no domínio da aplicação da lei e da justiça, quando as pessoas confiam excessivamente na natureza aparentemente objetiva e científica dos instrumentos de IA e não consideram a possibilidade de os seus resultados serem incorretos, incompletos, irrelevantes ou discriminatórios; destaca que cumpre evitar uma confiança excessiva nos resultados fornecidos pelos sistemas de IA e salienta a necessidade de as autoridades reforçarem a confiança e os conhecimentos necessários para desafiar ou anular uma recomendação algorítmica; considera importante ter expectativas realistas sobre tais soluções tecnológicas e não prometer soluções de aplicação da lei perfeitas e a deteção de todas as infrações cometidas;

16. Sublinha que, em contextos judiciais e policiais, toda e qualquer decisão judicial ou similar deve ser sempre tomada por um ser humano, que pode ser responsabilizado pelas decisões tomadas; considera que as pessoas sujeitas a sistemas alimentados por IA têm de poder recorrer a medidas corretivas; recorda que, ao abrigo do Direito da UE, uma pessoa tem o direito de não ser objeto de uma decisão que produza efeitos jurídicos que lhe digam respeito ou que a afete de forma significativa, caso se baseie exclusivamente no tratamento automatizado de dados; sublinha ainda que o processo de decisão individual automatizado não se deve basear em categorias particulares de dados pessoais, a menos que estejam em vigor medidas adequadas para salvaguardar os direitos e liberdades da pessoa em causa e os seus legítimos interesses; destaca que o Direito da UE proíbe a definição de perfis que conduza à discriminação de pessoas singulares com base em categorias particulares de dados pessoais; relembra que as decisões no domínio da aplicação coerciva da lei são, quase sempre, decisões que acarretam um efeito jurídico para a pessoa em causa, em virtude da natureza executória das autoridades policiais e das respetivas ações; salienta que a utilização de IA pode influenciar as decisões humanas e ter impacto em todas as fases do processo penal; considera, por conseguinte, que as autoridades que utilizam sistemas de IA devem respeitar normas jurídicas extremamente elevadas e assegurar a intervenção humana, especialmente na análise dos dados provenientes desses sistemas; requer, portanto, que

seja mantido a poder discricionário soberano dos juízes e a tomada de decisões numa base casuística; apela à proibição do uso de IA e das tecnologias relacionadas para propor decisões judiciais;

17. Apela à explicabilidade, à transparência, à rastreabilidade algorítmica e à verificação, como parte necessária da supervisão, de molde a garantir que o desenvolvimento, a implantação e a utilização de sistemas de IA pelas autoridades policiais e judiciais respeitem os direitos fundamentais e sejam da confiança dos cidadãos, bem como a assegurar que os resultados gerados pelos algoritmos de IA possam ser compreensíveis para os utilizadores e para os que estão sujeitos a esses sistemas, e a que haja efetivamente transparência em relação aos dados de base e ao modo como o sistema chega a uma determinada conclusão; salienta que, para assegurar a transparência técnica, a robustez e a exatidão, esses instrumentos e sistemas só devem poder ser adquiridos pelas autoridades policiais ou judiciais da União cujos algoritmos e cuja lógica sejam auditáveis e acessíveis, pelo menos, à polícia e ao sistema judicial, bem como aos auditores independentes, de molde a permitir a sua avaliação, auditoria e controlo, e não devem ser fechados ou rotulados como propriedade exclusiva pelos vendedores; assinala, além disso, que deve ser fornecida documentação em linguagem clara e inteligível sobre a natureza do serviço, as ferramentas desenvolvidas, o desempenho e as condições em que se pode esperar que funcionem e os riscos que possam acarretar; apela, por conseguinte, às autoridades judiciais e policiais para usarem de uma transparência proactiva e total sobre as empresas privadas que lhes fornecem sistemas de AI para fins de aplicação da lei e judiciais; recomenda, por conseguinte, a utilização de programas informáticos abertos, sempre que possível;

18. Incentiva as autoridades policiais e judiciais a identificarem e avaliarem os domínios em que algumas soluções de IA personalizadas possam ser benéficas e a procederem ao intercâmbio de boas práticas em matéria de implantação da IA; apela à adoção pelos Estados-Membros e pelas agências da UE de processos adequados de contratação pública para sistemas de IA quando utilizados num contexto policial ou judicial, a fim de assegurar a sua conformidade com os direitos fundamentais e a legislação aplicável, incluindo a garantia de que a documentação e os algoritmos de *software* estão disponíveis e acessíveis às autoridades competentes e às autoridades de supervisão para efeitos de revisão; solicita, em particular, regras vinculativas que exijam a divulgação pública das parcerias público-privadas, dos contratos e aquisições, bem como do objetivo para o qual são adquiridos; salienta que cumpre facultar o financiamento necessário às autoridades, bem como dotá-las dos conhecimentos especializados necessários para assegurar o pleno cumprimento dos requisitos éticos, jurídicos e técnicos associados à implantação da IA;

19. Apela rastreabilidade dos sistemas de IA e do processo decisório que delineia as suas funções, define as capacidades e limitações dos sistemas e acompanha a origem dos atributos definidores de uma decisão, através de documentação obrigatória; sublinha a importância de manter uma documentação completa dos dados de formação, do seu contexto, da finalidade, da exatidão e dos efeitos secundários, bem como do seu tratamento por parte de quem cria e concebe algoritmos e da respetiva conformidade com os direitos fundamentais; destaca que deve ser sempre possível reduzir a computação de qualquer sistema de IA a uma forma compreensível para os seres humanos;

20. Solicita uma avaliação de impacto obrigatória dos direitos fundamentais antes da aplicação ou implantação de qualquer sistema de IA destinado às autoridades policiais ou judiciais, a fim de avaliar potenciais riscos para os direitos fundamentais; relembra que uma avaliação prévia do impacto na proteção de dados para todos os tipos de tratamento é obrigatória, em particular para os que utilizem novas tecnologias, sempre que o tratamento seja suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares, e considera que é esse o caso no que se refere a todas as tecnologias de IA para fins policiais e judiciais; destaca os conhecimentos especializados das autoridades de proteção de dados e das agências dos direitos fundamentais na avaliação destes sistemas; realça que estas avaliações de impacto em matéria de direitos fundamentais devem ser realizadas de uma forma tão aberta quanto possível e com a participação ativa da sociedade civil; solicita que as avaliações de impacto definam também claramente as salvaguardas necessárias para fazer face aos riscos identificados e que sejam tornadas públicas, na medida do possível, antes da implantação de qualquer sistema de IA;

21. Salienta que só através de uma boa gestão da inteligência artificial europeia, bem como de uma avaliação independente, será possível a tão necessária aplicação dos princípios dos direitos fundamentais; solicita a realização de auditorias periódicas obrigatórias de todos os sistemas de IA utilizados pelas autoridades policiais e judiciais por uma autoridade independente, sempre que exista o potencial de afetar significativamente a vida das pessoas, para testar e avaliar os sistemas algorítmicos, o seu contexto, a finalidade, a exatidão, o desempenho e a escala, e, uma vez em funcionamento, para detetar, investigar, diagnosticar e retificar quaisquer efeitos indesejados e adversos e para assegurar que os sistemas de IA estão a funcionar como pretendido; apela, por conseguinte, a um quadro institucional claro para este efeito, que inclua uma supervisão regulamentar e controlo adequados, de molde a garantir a plena aplicação e um debate democrático plenamente informado sobre a necessidade e a proporcionalidade da IA no domínio da justiça penal; sublinha que os resultados dessas auditorias devem ser disponibilizados em registos públicos, para que os cidadãos saibam se estão a ser implantados sistemas de IA e quais as medidas tomadas para corrigir violações de direitos fundamentais;

22. Salienta que os conjuntos de dados e os sistemas algorítmicos utilizados ao efetuar classificações, avaliações e previsões durante as várias fases do tratamento de dados no âmbito do desenvolvimento de IA e de tecnologias conexas também podem levar a um tratamento diferenciado e à discriminação direta e indireta de grupos de pessoas, em particular porque os dados utilizados na formação de algoritmos de policiamento preditivo refletem as prioridades de vigilância em vigor e, consequentemente, podem acabar por reproduzir e amplificar os preconceitos correntes; salienta, portanto, que as tecnologias da IA, especialmente quando utilizadas para fins policiais e judiciais, requerem investigação e contributos interdisciplinares, nomeadamente nos domínios da ciência e dos estudos tecnológicos, estudos críticos sobre a raça, estudos sobre deficiência e outras disciplinas ligadas ao contexto social, incluindo a forma como a diferença é construída, o trabalho de classificação e as respetivas consequências; destaca, por conseguinte, a necessidade de investir sistematicamente na integração dessas disciplinas no estudo e na investigação da IA a todos os níveis; salienta também que é importante que as equipas que concebem, desenvolvem, testam, mantêm, implantam e adquirem estes sistemas de IA para as autoridades policiais e judiciais,

representem, sempre que possível, a diversidade da sociedade em geral como um meio não técnico para reduzir os riscos de discriminação;

23. Destaca que uma responsabilização e responsabilidade adequadas exigem uma formação especializada considerável, sobretudo das autoridades policiais e judiciais, no que diz respeito às normas éticas, aos perigos potenciais, às limitações e à correta utilização da tecnologia de IA; salienta que importa velar por que os decisores beneficiem de uma formação profissional adaptada e disponham das qualificações adequadas sobre os riscos de parcialidade, uma vez que os conjuntos de dados podem basear-se em dados discriminatórios e assentes em preconceitos; apoia a criação de iniciativas de sensibilização e educativas, para garantir que que quem faz parte das autoridades policiais ou judiciais está ciente e compreende as limitações, as capacidades e os riscos associados aos sistemas de IA, mormente o risco de preconceito resultante da automatização; recorda que a inclusão na formação em IA de conjuntos de dados de casos de racismo por parte das forças policiais no exercício das suas funções conduzirá inevitavelmente a preconceitos racistas nos resultados, nas pontuações e recomendações geradas pela IA; reitera, por conseguinte, o seu apelo aos Estados-Membros para que promovam políticas contra a discriminação em todos os domínios e desenvolvam planos de ação nacionais contra o racismo nos domínios do policiamento e do sistema judicial;

24. Observa que o policiamento preditivo é uma das aplicações de IA utilizadas pelas autoridades policiais, mas adverte que, embora o policiamento preditivo possa analisar os conjuntos de dados fornecidos para a identificação de padrões e correlações, não pode dar resposta ao problema da causalidade e não pode fazer previsões fiáveis sobre o comportamento individual, pelo que não pode constituir a única base para uma intervenção; salienta que várias cidades dos Estados Unidos puseram termo à utilização de sistemas de previsão policial após auditorias; relembra que durante a missão da Comissão LIBE aos Estados Unidos, em fevereiro de 2020, os deputados ao Parlamento foram informados pelos departamentos de polícia de Nova Iorque e de Cambridge/Massachusetts que haviam gradualmente posto fim aos seus programas de previsão policial, devido à falta de eficácia, ao impacto discriminatório e a falhas práticas, optando, antes, pelo policiamento de proximidade; relembra que o policiamento de proximidade conduziu a uma diminuição das taxas de criminalidade; opõe-se, por conseguinte, à utilização da IA pelas autoridades policiais para fazer previsões comportamentais sobre indivíduos ou grupos com base em dados históricos e comportamentos passados, pertença a grupos, localização ou quaisquer outras características semelhantes, tentando, assim, identificar pessoas suscetíveis de cometer um crime;

25. Regista os diferentes tipos de utilização do reconhecimento facial, tais como, entre outros, a verificação/autenticação (ou seja, a correspondência entre um rosto ao vivo e uma fotografia num documento de identificação, por exemplo, no caso das fronteiras inteligentes), a identificação (ou seja, a correspondência entre uma fotografia e uma base de dados de fotografias) e a deteção (isto é, deteção de rostos em tempo real a partir de fontes como imagens de CCTV, e correspondência desses rostos com bases de dados, por exemplo, no caso de vigilância em tempo real), cada um dos quais tem diferentes implicações para a proteção dos direitos fundamentais; está firmemente convicto de que a implantação de sistemas de reconhecimento facial pelas autoridades policiais deve ser limitada a fins claramente justificados, no pleno respeito dos

princípios da proporcionalidade e da necessidade, bem como da lei aplicável; reitera que a utilização de tecnologia de reconhecimento facial tem, no mínimo, de cumprir os requisitos de minimização dos dados, exatidão dos dados, limitação do armazenamento, segurança dos dados e responsabilização, devendo também ser lícita, equitativa e transparente e prosseguir uma finalidade específica, explícita e legítima que seja claramente identificada no Direito da União ou dos Estados-Membros; entende que os sistemas de verificação e autenticação só podem continuar a ser implantados e utilizados com êxito se os seus efeitos adversos puderem ser atenuados e se os critérios acima referidos forem cumpridos;

26. Apela, além disso, à proibição permanente do recurso a análises automatizadas e/ou do reconhecimento em espaços acessíveis ao público de outras características humanas, tais como o andar, as impressões digitais, o ADN, a voz e outros sinais biométricos e comportamentais;

27. Solicita, contudo, uma moratória à implantação de sistemas de reconhecimento facial para fins de aplicação da lei destinados à identificação, a menos que sejam estritamente utilizados para efeitos de identificação de vítimas de crime, até que as normas técnicas possam ser consideradas plenamente conformes com os direitos fundamentais, os resultados obtidos não sejam tendenciosos e discriminatórios, o quadro jurídico preveja salvaguardas rigorosas contra a utilização indevida e um controlo e supervisão democráticos rigorosos, e existam provas empíricas da necessidade e proporcionalidade da implantação de tais tecnologias; faz notar que, nos casos em que os critérios acima referidos não sejam cumpridos, os sistemas não devem ser utilizados ou implantados;

28. Manifesta profunda preocupação com o recurso, pelas autoridades policiais e pelos serviços de informação, a bases de dados privadas de reconhecimento facial como a *Clearview AI*, uma base de dados com mais de rês mil milhões de imagens, inclusive de cidadãos da UE, que foram recolhidas ilegalmente de redes sociais e outras partes da Internet; insta os Estados-Membros a obrigarem as autoridades policiais a divulgarem se estão a utilizar a tecnologia *Clearview AI* ou tecnologias equivalentes de outros prestadores; recorda o parecer do Comité Europeu para a Proteção de Dados (CEPD), segundo o qual é provável que a utilização de um serviço como a *Clearview AI* pelas autoridades policiais não seja compatível com o regime de proteção de dados da UE; insta a Comissão a proibir a utilização de bases de dados privadas de reconhecimento facial no domínio da aplicação da lei;

29. Toma nota do estudo de viabilidade da Comissão sobre as possíveis alterações à Decisão Prüm[8], incluindo no que se refere ao reconhecimento facial; observa que os resultados de investigações anteriores indicam que nenhum novo identificador potencial, como o reconhecimento da íris ou o reconhecimento facial, será tão fiável, em contexto forense, como o ADN ou as impressões digitais; relembra à Comissão que toda e qualquer proposta legislativa deve ser devidamente fundamentada e respeitar o princípio da proporcionalidade; urge a Comissão a não alargar o quadro da Decisão Prüm, a menos que existam provas científicas sólidas da fiabilidade do reconhecimento facial num contexto forense comparável com o ADN ou as impressões digitais, depois

[8] Decisão 2008/615/JAI do Conselho, de 23 de junho de 2008, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiras. JO L 210 de 6.8.2008, p. 1.

de ter realizado uma avaliação de impacto completa, e tendo em conta as recomendações da Autoridade Europeia para a Proteção de Dados (AEPD) e do CEPD;

30. Destaca que a utilização de dados biométricos está mais amplamente relacionada com o princípio do direito à dignidade humana, que constitui a base de todos os direitos fundamentais garantidos pela Carta; Considera que a utilização e a recolha de quaisquer dados biométricos para fins de identificação à distância, por exemplo, através de reconhecimento facial em espaços públicos, bem como em cancelas de controlo automatizado de fronteiras utilizadas em controlo fronteiriços nos aeroportos, podem acarretar riscos específicos para os direitos fundamentais, cujas implicações podem variar consideravelmente em função da finalidade, do contexto e do âmbito da utilização; salienta ainda a validade científica contestada da tecnologia de reconhecimento, designadamente de câmaras que detetam movimentos oculares e alterações na dimensão da pupila, num contexto policial; entende que o uso da identificação biométrica nos contextos policial e judicial deve ser sempre considerada de «alto risco» e, por conseguinte, sujeita a requisitos adicionais, de acordo com as recomendações do Grupo de Peritos de Alto Nível sobre IA da Comissão;

31. Manifesta a sua profunda preocupação com projetos de investigação financiados pelo Horizonte 2020 que implantam inteligência artificial nas fronteiras externas, como o projeto iBorderCtrl, um «sistema inteligente de deteção de mentiras» que traça o perfil dos viajantes com base numa entrevista automatizada por computador realizada, antes da viagem, com recurso à câmara Web do viajante, bem como uma análise de 38 pequenos gestos, baseada em inteligência artificial e testada na Hungria, na Letónia e na Grécia; exorta a Comissão a aplicar, através de medidas legislativas e não legislativas, e, recorrendo, se necessário, a processos por infração, uma proibição de todo e qualquer tratamento biométrico, inclusive o reconhecimento facial, para efeitos de aplicação da lei, que resulte numa vigilância em larga escala nos espaços acessíveis ao público; insta ainda a Comissão a pôr termo à investigação ou à implantação de soluções ou de programas biométricos sempre que tal possa contribuir para uma vigilância indiscriminada nos espaços públicos; salienta, neste contexto, que deve ser dada especial atenção, e aplicado um quadro rigoroso, à utilização de veículos aéreos não tripulados em operações policiais;

32. Apoia as recomendações do Grupo de Peritos de Alto Nível sobre IA da Comissão que advoga a proibição da pontuação em larga escala das pessoas recorrendo à IA; considera que qualquer forma de pontuação normativa dos indivíduos realizada em larga escala pelas autoridades públicas, em especial as autoridades policiais e judiciais, redunda numa perda de autonomia, compromete o princípio da não discriminação e não pode ser considerada em sintonia com os direitos fundamentais, em particular a dignidade humana, tal como codificada na legislação da UE;

33. Apela a uma maior transparência geral, de molde a permitir uma compreensão abrangente da utilização das aplicações de IA na União; solicita que os Estados-Membros forneçam informações completas sobre os instrumentos utilizados pelas suas autoridades policiais e judiciais, os tipos de instrumentos utilizados, os fins para que são utilizados, os tipos de crime a que são aplicados e os nomes das empresas ou organizações que desenvolveram esses instrumentos; exorta todas as autoridades policiais e judiciais a informarem o público e a garantirem também uma transparência

suficiente no que se refere à utilização que fazem da IA e de tecnologias conexas no desempenho das respetivas competências, designadamente mediante a divulgação das taxas de falsos positivos e de falsos negativos da tecnologia em causa; solicita que a Comissão compile e atualize as informações num único local; exorta a Comissão a publicar e atualizar igualmente informações sobre a utilização da IA pelas agências da União responsáveis pelas funções policiais e judiciais; insta o CEPD a avaliar a legalidade destas tecnologias e das aplicações de IA utilizadas pelas autoridades policiais e judiciais;

34. Recorda que as aplicações de IA, mormente aplicações utilizadas pelas autoridades policiais e judiciais, estão a ser desenvolvidas a nível mundial e a um ritmo acelerado; urge todas as partes interessadas europeias, incluindo os Estados-Membros e a Comissão, a garantirem, através da cooperação internacional, o envolvimento de parceiros fora da UE, para melhorar as normas a nível internacional e encontrar um quadro jurídico e ético comum e complementar para a utilização da IA, em particular para as autoridades policiais e judiciais, que respeite plenamente a Carta, o acervo europeu em matéria de proteção de dados e; de uma maneira geral, os direitos humanos;

35. Insta a Agência dos Direitos Fundamentais da UE, em colaboração com o CEPD e a AEPD, a elaborar orientações, recomendações e boas práticas abrangentes, com o intuito de especificar melhor os critérios e as condições para o desenvolvimento, a utilização e a implantação de aplicações e soluções de IA a utilizar pelas autoridades policiais e judiciais; compromete-se a realizar um estudo sobre a aplicação da Diretiva relativa à proteção de dados na aplicação da lei[9], por forma a identificar o modo como a proteção dos dados pessoais foi assegurada nas atividades de tratamento levadas a cabo pelas autoridades policiais e judiciais, em especial no âmbito do desenvolvimento ou da implantação de novas tecnologias; insta, além disso, a Comissão a ponderar a necessidade de uma ação legislativa específica para definir melhor os critérios e as condições para o desenvolvimento, a utilização e a implantação de aplicações e soluções de IA por parte das autoridades policiais e judiciais;

36. Encarrega o seu Presidente de transmitir a presente resolução ao Conselho e à Comissão.

[9] Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho, JO L 119 de 4.5.2016, p. 89.

EXPOSIÇÃO DE MOTIVOS

A inteligência artificial (IA) é uma das tecnologias estratégicas do século XXI, na medida em que gera benefícios substanciais em termos de eficiência, precisão e comodidade, contribuindo de forma positiva para a economia europeia. Entre outros aspetos, as aplicações de IA melhoraram os cuidados de saúde, aumentaram a eficiência da agricultura, contribuíram para a atenuação das alterações climáticas e para a adaptação aos seus efeitos e melhoraram a eficiência da produção.

A IA é uma das principais prioridades da atual Comissão. A Presidente da Comissão, Ursula von der Leyen, anunciou, nas suas orientações políticas, uma abordagem europeia coordenada sobre as implicações humanas e éticas da IA, bem como uma reflexão sobre a melhor utilização de grandes volumes de dados para promover a inovação. O reconhecimento da IA como questão a tratar a nível da UE foi acompanhado de uma reflexão sobre a forma de garantir a confiança nas tecnologias de IA e de velar por que a IA não comprometa os direitos fundamentais na UE.

No entanto, o Parlamento Europeu debruçou-se sobre a IA vários anos antes de a Comissão ter decidido fazer dela uma das suas principais prioridades. Várias resoluções sobre megadados, robótica e inteligência artificial, aprovadas pelo Parlamento desde 2016, demonstram a importância atribuída a este tema pelo Parlamento. As resoluções examinaram as diferentes implicações da IA e a forma como afeta o bem-estar, a educação, a tecnologia, os direitos legais e fundamentais, bem como a indústria em geral. Estas resoluções sublinharam a necessidade de adotar uma abordagem «centrada no ser humano», baseada no respeito dos direitos fundamentais, nomeadamente a Carta da UE e o quadro da UE em matéria de proteção de dados.

Tendo em conta que «a IA é um conjunto de tecnologias que combinam dados, algoritmos e capacidade computacional», os «progressos em computação e a cada vez maior disponibilidade de dados são, por conseguinte, os principais motores do atual impulso da IA»[1]. A questão central prende-se com o facto de a IA se basear na recolha, na análise e na acumulação recorrente de grandes quantidades de dados, incluindo dados pessoais, provenientes de várias fontes, os quais são objeto de um tratamento automatizado por algoritmos informáticos e técnicas avançadas de tratamento de dados. Estas técnicas utilizam tanto dados armazenados como dados transmitidos em fluxo, a fim de gerar certas correlações, tendências e padrões (análise de megadados). Os dados utilizados pela IA não provêm apenas dos indivíduos; as aplicações de IA utilizam sobretudo dados provenientes da indústria, das empresas e do setor público, tratados para uma série de finalidades diferentes. Mesmo que os dados utilizados pelas aplicações de IA possam, por vezes, ser dados não pessoais, as atividades de IA implicam, em muitos casos, o tratamento de dados pessoais, dado que as atividades de IA conduzem frequentemente a decisões automatizadas com efeitos diretos nos indivíduos. Estas características da IA exigem, por conseguinte, que se preste especial atenção, neste domínio, ao respeito dos princípios básicos da proteção de dados e da privacidade.

A IA oferece igualmente grandes oportunidades no domínio da aplicação coerciva da lei e da justiça penal, permitindo nomeadamente melhorar os métodos de trabalho dos serviços policiais e das autoridades judiciais e combater mais eficazmente certos tipos de criminalidade, em particular nos domínios da criminalidade financeira, do branqueamento de capitais e do

[1] COM(2020) 65 final.

financiamento do terrorismo, bem como certos tipos de cibercriminalidade. Neste setor, as aplicações de IA incluem, por exemplo, as tecnologias de reconhecimento facial, o reconhecimento automático de matrículas, a identificação de oradores, a identificação da fala, tecnologias de leitura dos lábios, a vigilância auditiva (ou seja, algoritmos de deteção de disparos), a investigação e a análise autónomas de bases de dados identificadas, as previsões (previsão policial e análise de focos de criminalidade), as ferramentas de deteção de comportamentos, as ferramentas autónomas para detetar fraudes financeiras e o financiamento do terrorismo, a monitorização das redes sociais (extração e recolha de dados para identificar ligações), a interceção da IMSI e os sistemas de vigilância automatizada que integram diferentes possibilidades de deteção (como a deteção de batimentos cardíacos e as câmaras térmicas). No sistema judicial, as ferramentas de IA podem ser utilizadas para calcular as probabilidades de reincidência e para determinar a liberdade condicional ou a pena.

Não obstante os benefícios que a IA traz, o facto é que comporta simultaneamente uma série de riscos potenciais, como a opacidade na tomada de decisões, diferentes tipos de discriminação, a intrusão na vida privada e desafios para garantir a proteção dos dados pessoais, a dignidade humana e a liberdade de expressão e de informação. Estes riscos potenciais são ainda mais graves no setor da aplicação coerciva da lei e da justiça penal, uma vez que podem afetar a presunção de inocência e os direitos fundamentais à liberdade e à segurança do indivíduo, bem como a vias de recurso efetivas e a um julgamento justo.

O presente relatório procura abordar as questões suscitadas pela utilização da IA no direito penal e a sua utilização pelas autoridades policiais e judiciárias em matéria penal. Embora reconheça as oportunidades e vantagens que a IA pode proporcionar, também sublinha os riscos e as consequências importantes que pode comportar.

O relatório salienta a necessidade de respeitar plenamente os direitos fundamentais consagrados na Carta dos Direitos Fundamentais da União Europeia e na legislação da União em matéria de proteção da vida privada e de proteção dos dados, nomeadamente a Diretiva (UE) 2016/680 (Diretiva Cooperação Policial), bem como de respeitar vários princípios fundamentais no ciclo de vida da IA, como a explicabilidade e a transparência dos algoritmos, a rastreabilidade e a realização de avaliações de impacto obrigatórias sobre os direitos fundamentais antes da aplicação ou implementação de qualquer sistema de IA e de auditorias obrigatórias. Todos estes requisitos são necessários não apenas para garantir a legalidade dos sistemas de IA, mas também para obter a confiança das pessoas no que se refere à utilização desses sistemas pelas autoridades policiais e judiciárias.

Por último, o relator solicita uma moratória para a implantação de sistemas de reconhecimento facial para fins policiais. O estado de avanço destas tecnologias e o seu importante impacto nos direitos fundamentais exigem um debate profundo e aberto na sociedade, a fim de examinar as diferentes questões que se colocam e a justificação para a sua implantação.

3.9.2020

PARECER DA COMISSÃO DO MERCADO INTERNO E DA PROTEÇÃO DOS CONSUMIDORES

dirigido à Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos

sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais
(2020/2016(INI))

Relator de parecer: Marcel Kolaja

SUGESTÕES

A Comissão do Mercado Interno e da Proteção dos Consumidores insta a Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos, competente quanto à matéria de fundo, a incorporar as seguintes sugestões na proposta de resolução que aprovar:

A. Considerando que, face aos benefícios potenciais para a sociedade decorrentes da inteligência artificial e aos riscos inerentes, o funcionamento do mercado único digital deve ser melhorado mercê do reforço da segurança jurídica para os fornecedores de IA, bem como da confiança e da segurança dos consumidores, melhorando as garantias de proteção do Estado de direito e dos direitos fundamentais, em particular o direito à privacidade e à proteção dos dados pessoais, o direito à igualdade e à não discriminação, o direito a uma boa administração, o direito a um julgamento justo e o direito a um nível elevado de proteção dos consumidores; que é necessária uma abordagem europeia comum em relação à IA e ao regulamento para a sua utilização em matéria penal pela polícia e pelos serviços responsáveis pela aplicação da lei, a fim de evitar a fragmentação no mercado único;

B. Considerando que as autoridades policiais e judiciárias utilizam frequentemente a inteligência artificial, a título experimental ou habitual, com diferentes tipos de utilizações, consequências e riscos que incluem, nomeadamente, sistemas de reconhecimento facial, perfis de ADN, cartografia preditiva da criminalidade, extração de dados de telemóveis, motores avançados de pesquisa de jurisprudência, resolução de litígios em linha e aprendizagem automática para a administração da justiça;

C. Considerando que a utilização de IA pode representar uma mudança de paradigma na administração da justiça penal;

D. Considerando que, de acordo com o relatório da Agência dos Direitos Fundamentais, ainda existem poucas informações disponíveis sobre a eventual utilização ou a

experimentação de tecnologias de reconhecimento facial nos Estados-Membros[1];

E. Considerando que, nos Estados-Membros em que estava disponível alguma informação sobre a utilização de tecnologias de reconhecimento facial, as autoridades responsáveis pela proteção de dados consideraram que a utilização dessas tecnologias não respeitava a legislação em matéria de proteção de dados e carecia de base jurídica para a sua implantação;

F. Considerando que a União pode fazer a diferença no mercado interno se reformar os procedimentos de contratação pública, por forma a que os governos respeitem, nas suas ações e comportamentos, objetivos políticos secundários, como a proteção de dados e a não discriminação;

G. Considerando que pode existir discriminação nos processos de tomada de decisões baseados em algoritmos durante a fase de conceção, teste e implementação, devido aos enviesamentos presentes nos conjuntos de dados ou nos algoritmos;

H. Considerando que o desenvolvimento técnico e a aplicação da IA devem basear-se em princípios para garantir o respeito pelos direitos humanos e pelos direitos fundamentais;

I. Considerando que, em 4 de dezembro de 2018, a Comissão Europeia para a Eficiência da Justiça do Conselho da Europa publicou a carta ética para a utilização de inteligência artificial nos sistemas judiciais, que estabelece princípios éticos para a utilização de IA nos sistemas judiciais;

J. Considerando que determinadas utilizações de tecnologias baseadas na IA são particularmente sensíveis e vulneráveis em relação a abusos, o que levou recentemente algumas empresas tecnológicas a decidirem deixar de disponibilizar software ligado a essas tecnologias;

1. Considera que a IA utilizada pelas autoridades policiais e judiciárias tem de ser, regra geral, classificada como de alto risco e tratada com o máximo cuidado e os mais elevados padrões de proteção de dados, tendo em conta o papel destas autoridades na defesa do interesse público, bem como a natureza das suas responsabilidades; entende que existe uma necessidade urgente de um quadro regulamentar comum europeu aplicável à IA no mercado interno; considera que a UE deve assumir a liderança na adoção de regulamentação a nível da União, nomeadamente em matéria de contratos públicos, com base em regras claras, nos direitos fundamentais e em princípios éticos, bem como no desenvolvimento e na utilização de IA, de modo a garantir o mesmo nível elevado de proteção dos consumidores e normas setoriais uniformes em toda a UE, a fim de permitir um melhor funcionamento do mercado interno, incentivando simultaneamente a inovação e promovendo a segurança jurídica para as empresas, especialmente as PME; insta a Comissão a examinar a aplicação da legislação existente antes de iniciar novas propostas legislativas;

2. Reconhece que a utilização da IA no domínio da justiça pode ajudar a melhorar a

[1] Agência dos Direitos Fundamentais da União Europeia: Facial recognition technology: fundamental rights considerations in the context of law enforcement (FRA Focus), 27 de novembro de 2019 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

eficiência e a qualidade dos processos; salienta, neste contexto, que é necessário respeitar, em especial, as regras estabelecidas na Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal;

3. Exorta a Comissão a avaliar a tecnologia de IA disponível no mercado e o nível de utilização pelas autoridades policiais e judiciais em cada país;

4. Salienta que a IA deve ajudar a aliviar a carga administrativa que recai sobre as autoridades públicas e a melhorar a eficiência dos seus processos decisórios e que os sistemas de IA devem estar sempre sujeitos a supervisão, colaboração e coordenação humanas; a este respeito, sublinha que os seres humanos devem ser sempre responsáveis, em última instância, por quaisquer decisões em matéria penal; salienta a importância de dispor de conjuntos de dados exatos, quando estes são utilizados para apoiar processos relacionados com a administração pública em linha e a tomada de decisões administrativas em toda a União;

5. Salienta a importância de viabilizar a inovação, a transparência, a rastreabilidade e a verificação; salienta que a IA de fonte aberta poderia contribuir para este objetivo, reforçando simultaneamente a cooperação e promovendo uma cultura de intercâmbio de ideias e de experiências relacionadas com a utilização e a criação de algoritmos;

6. Considera que os instrumentos de IA utilizados em matéria penal pela polícia e pelos serviços responsáveis pela aplicação da lei devem ser colocados à disposição como software de fonte aberta, sempre que possível no âmbito do procedimento de contratação pública, em conformidade com a legislação aplicável, nomeadamente a Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao direitos de autor e aos direitos conexos no mercado único digital, e que a documentação relativa ao software e os algoritmos devem ser acessíveis, permitindo, assim, que as autoridades competentes examinem a forma como o sistema de IA chegou a uma determinada conclusão; salienta que uma auditoria sobre os direitos fundamentais deve fazer parte integrante de uma avaliação prévia da conformidade; considera que, a par da garantia do respeito do direito e dos valores da UE e das normas aplicáveis em matéria de proteção de dados, e sem pôr em risco as investigações ou as ações penais, os algoritmos explicáveis e imparciais que respeitem a obrigação de transparência suficiente, bem como a utilização de dados abertos para formação em conformidade com a legislação aplicável, incluindo a Diretiva (UE) 2019/1024 relativa aos dados abertos e à reutilização de informações do setor público sem prejuízo do Regulamento (UE) 2016/679, são essenciais para garantir que as empresas e os cidadãos, incluindo os consumidores, possam confiar e beneficiar de serviços públicos de melhor qualidade, acessíveis, não discriminatórios e fiáveis a um custo justo;

7. Salienta que a recolha de dados e vigilância de pessoas com base na IA devem estar circunscritas a pessoas suspeitas da prática de crimes e a casos de vigilância aprovada por um tribunal, em conformidade com a legislação nacional aplicável, tendo em conta o respeito pela vida privada e a presunção de inocência, incluindo de outros utilizadores e consumidores que possam ser inadvertidamente afetados por esses sistemas e práticas; salienta que, nos casos em que o processo de tomada de decisão é assistido por cálculos estatísticos, importa velar por que os decisores beneficiem de uma formação

profissional adaptada e disponham das qualificações adequadas sobre os riscos de enviesamento, uma vez que os conjuntos de dados podem basear-se em dados discriminatórios e assentes em preconceitos; salienta, a este respeito, a importância da qualidade dos algoritmos e dos dados originais e recorda que a utilização da IA deve basear-se no princípio da não discriminação na introdução e análise de dados; solicita que os procedimentos de adjudicação de contratos contenham salvaguardas contra eventuais enviesamentos; apela ao intercâmbio de informações e de boas práticas sobre a aplicação de técnicas e instrumentos com base na IA pelas autoridades judiciais e policiais nos Estados-Membros, a fim de evitar uma abordagem fragmentada no mercado único e assegurar a proteção dos consumidores e dos cidadãos em toda a União;

8. Insiste em que os Estados-Membros, em conformidade com o direito penal aplicável, devem assegurar que os cidadãos e os consumidores são informados quando estão sujeitos à utilização de IA e que lhes sejam disponibilizados procedimentos de reclamação e recurso simples, eficazes e de fácil acesso, incluindo recurso por via judicial, para que possam defender eficazmente os seus direitos;

9. Recorda o elevado risco ligado a determinados tipos de IA, incluindo as tecnologias de reconhecimento facial em espaços públicos, a deteção automática de comportamentos, a definição de perfis para dividir as pessoas em categorias de risco nas fronteiras, a deteção e o reconhecimento biométricos para vigilância em larga escala, a pontuação em massa dos cidadãos e o policiamento preditivo, e insta a Comissão a regulamentar a contratação pública e a respetiva utilização para eliminar o risco de abuso; congratula-se, neste contexto, com os trabalhos em curso da Comissão destinados a avaliar a utilização de tecnologias biométricas, a ponderar opções regulamentares, incluindo uma abordagem baseada no risco e a proibição destas tecnologias em circunstâncias específicas, bem como a introdução das salvaguardas necessárias sempre que a sua utilização se justifique;

10. Realça que a capacidade discricionária soberana dos juízes e a tomada de decisões caso a caso têm de ser mantidas para evitar a normalização de decisões baseadas em cálculos puramente estatísticos.

INFORMAÇÕES SOBRE A APROVAÇÃO NA COMISSÃO ENCARREGADA DE EMITIR PARECER

Data de aprovação	3.9.2020
Resultado da votação final	+: 40 –: 4 0: 0
Deputados presentes no momento da votação final	Alex Agius Saliba, Andrus Ansip, Alessandra Basso, Brando Benifei, Adam Bielan, Hynek Blaško, Biljana Borzan, Vlad-Marius Botoş, Markus Buchheit, Dita Charanzová, Deirdre Clune, David Cormand, Petra De Sutter, Carlo Fidanza, Evelyne Gebhardt, Sandro Gozi, Maria Grapini, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Marcel Kolaja, Kateřina Konečná, Andrey Kovatchev, Jean-Lin Lacapelle, Maria-Manuel Leitão-Marques, Morten Løkkegaard, Adriana Maldonado López, Antonius Manders, Beata Mazurek, Leszek Miller, Dan-Ştefan Motreanu, Kris Peeters, Anne-Sophie Pelletier, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Kim Van Sparrentak, Marion Walsmann, Marco Zullo
Suplentes presentes no momento da votação final	Maria da Graça Carvalho, Anna Cavazzini, Krzysztof Hetman

VOTAÇÃO NOMINAL FINAL NA COMISSÃO ENCARREGADA DE EMITIR PARECER

40	+
PPE	Maria da Graça Carvalho, Deirdre Clune, Krzysztof Hetman, Arba Kokalari, Andrey Kovatchev, Antonius Manders, Dan-Ştefan Motreanu, Kris Peeters, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Marion Walsmann
S&D	Alex Agius Saliba, Brando Benifei, Biljana Borzan, Evelyne Gebhardt, Maria Grapini, Maria-Manuel Leitão-Marques, Adriana Maldonado López, Leszek Miller, Christel Schaldemose
RENEW	Andrus Ansip, Vlad-Marius Botoş, Dita Charanzová, Sandro Gozi, Svenja Hahn, Morten Løkkegaard
ID	Hynek Blaško
GREENS/EFA	Anna Cavazzini, David Cormand, Petra De Sutter, Marcel Kolaja, Kim Van Sparrentak
ECR	Adam Bielan, Carlo Fidanza, Eugen Jurzyca, Beata Mazurek
EUL/NGL	Kateřina Konečná, Anne-Sophie Pelletier
NI	Marco Zullo

4	-
ID	Alessandra Basso, Markus Buchheit, Virginie Joron, Jean-Lin Lacapelle

0	0

Legenda dos símbolos utilizados:
+ : votos a favor
- : votos contra
0 : abstenções

15.9.2020

PARECER DA COMISSÃO DOS ASSUNTOS JURÍDICOS

dirigido à Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos

sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais
(2020/2016(INI))

Relator de parecer: Angel Dzhambazki

SUGESTÕES

A Comissão dos Assuntos Jurídicos insta a Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos, competente quanto à matéria de fundo, a incorporar as seguintes sugestões na proposta de resolução que aprovar:

A. Considerando que o direito a um processo justo é um direito fundamental e juridicamente vinculativo consagrado na Carta dos Direitos Fundamentais da União Europeia e na Convenção Europeia dos Direitos do Homem para efeitos de aplicação da lei; considerando que o mesmo se aplica ao longo de todo o processo penal, incluindo no domínio da aplicação da lei, e que a sua salvaguarda exclui, em todas as fases do processo, a adoção de medidas, incluindo medidas técnicas, cuja consequência direta ou indireta seja privar os direitos de defesa da sua essência; considerando que as garantias associadas a este princípio – nomeadamente as de «tribunal independente», «igualdade perante a lei» e presunção de inocência – são mais rigorosas no domínio do direito penal; considerando que estes direitos têm de ser respeitados em todas as circunstâncias, nomeadamente no contexto da utilização da inteligência artificial (IA), especialmente tendo em conta que as tecnologias baseadas em IA podem ter um impacto nos vários direitos humanos;

B. Considerando que a proteção dos dados pessoais – em conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD)[1] e outra legislação pertinente, se for caso disso – é aplicável em qualquer altura;

C. Considerando que a IA e as tecnologias conexas, incluindo as suas capacidades de autoaprendizagem, implicam sempre um certo nível de intervenção humana;

D. Considerando que a IA tem potencial para se tornar uma componente permanente dos

[1] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (JO L 119 de 4.5.2016, p. 1).

sistemas de direito penal;

E. Considerando que a IA e as tecnologias conexas são uma prioridade para a União, tendo em conta os avanços rápidos no setor tecnológico e a importância de estar vigilante quanto ao seu impacto atual e futuro no sistema único europeu de direitos de propriedade intelectual; considerando que vários setores já estão a aplicar a IA e tecnologias conexas, como a robótica, os transportes e os cuidados de saúde, para citar apenas alguns setores;

F. Considerando que as tecnologias como a IA e as conexas poderiam ser utilizadas no domínio do direito penal com o objetivo de reduzir as taxas de criminalidade, facilitar determinados procedimentos através da sua utilização na análise de dados estatísticos no âmbito da análise e da prevenção da criminalidade e na deteção e investigação de processos penais; considerando que a União deve continuar a desenvolver as suas capacidades relativamente ao software, ao armazenamento de dados e às tecnologias de IA, a fim de melhorar as insuficiências no que se refere à proteção de dados e à privacidade;

G. Considerando que estas tecnologias podem ser utilizadas para criar bases de dados estatísticos anonimizadas que ajudem as autoridades, o meio académico e os legisladores a analisar os números e a conceber eficazmente políticas para prevenir a criminalidade e ajudar os delinquentes a reintegrarem-se com êxito na sociedade;

H. Considerando que o quadro jurídico da IA e a sua aplicação ao direito penal devem incluir medidas legislativas sempre que necessário, começando com medidas obrigatórias para evitar práticas que ponham em causa os direitos e as liberdades fundamentais;

I. Considerando que, devido ao caráter intrinsecamente opaco dos sistemas de IA, os novos instrumentos utilizados nos contextos da justiça penal podem entrar em conflito com algumas liberdades fundamentais;

J. Considerando que os eventuais riscos associados à aplicação de sistemas de IA em questões de justiça penal devem ser evitados e atenuados, a fim de salvaguardar os direitos fundamentais dos suspeitos e arguidos em processos penais;

1. Salienta a importância crucial de avaliar devidamente os riscos da utilização de sistemas de IA, tais como a discriminação e as violações da privacidade, e de ponderar todas as implicações éticas e operacionais da utilização da IA e das tecnologias conexas na nossa sociedade – em particular, pelas autoridades estatais, a polícia e as autoridades judiciais nos sistemas de justiça penal – e ainda a responsabilidade e as questões probatórias no caso de potenciais erros associados ao funcionamento dos sistemas de IA; considera que é necessário um quadro regulamentar claro para definir limites e proporcionar as salvaguardas necessárias; considera que os princípios éticos – como os estabelecidos na Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu Ambiente, do Conselho da Europa – devem ser tidos em conta e respeitados pelas entidades públicas e privadas responsáveis pela conceção e desenvolvimento iniciais dos instrumentos e serviços de IA, de modo a que todas as partes interessadas da área social possam dispor de informações completas sobre as estruturas empresariais das empresas que produzem programas de IA; salienta a importância do fator humano, que

tem de ser sempre o decisor final na utilização de software baseado na tecnologia da IA e no sistema penal, seja na aplicação da lei pela polícia ou na justiça penal; reitera que o software de reconhecimento biométrico só deve ser utilizado em situações em que se justifique claramente;

2. Salienta a necessidade de estabelecer e manter um equilíbrio entre a utilização dos sistemas de IA nos processos penais e o respeito de todos os direitos fundamentais e garantias processuais previstos no direito europeu e internacional;

3. Salienta a importância de a IA ser utilizada no devido respeito dos princípios do Estado de direito e da independência do poder judicial no processo de tomada de decisão;

4. Insta a Comissão a clarificar melhor as regras relativas à proteção e partilha dos dados recolhidos através da IA e das tecnologias conexas pelas autoridades autorizadas a recolher e/ou tratar esses dados — incluindo dados não pessoais e anonimizados que permitam identificar direta ou indiretamente pessoas – respeitando plenamente o RGPD e a Diretiva Privacidade Eletrónica[2]; sublinha, além disso, que o direito a um julgamento justo deve abranger o direito dos cidadãos e litigantes de acederem a esses dados – em especial, quando recolhidos a partir dos seus dispositivos ou equipamentos pessoais – em conformidade com o RGPD, mas também para efeitos do seu direito de defesa, logo que a sua responsabilidade jurídica seja invocada;

5. Sublinha a importância de aumentar a transparência dos sistemas de IA utilizados em questões de justiça penal, a fim de permitir a supervisão judicial e de garantir que os criadores de IA e tecnologias conexas providenciem um nível suficiente de transparência dos algoritmos e das decisões algorítmicas para benefício das autoridades competentes e dos cidadãos; salienta o direito geral de as partes terem acesso a processos relativos à recolha de dados, às avaliações de prognóstico utilizadas para a prevenção da criminalidade, à catalogação e avaliação de provas criminais e para determinar se um suspeito pode constituir um perigo para a sociedade se não for restringido pela legislação da UE em vigor, como a Diretiva (UE) 2016/680[3]; além disso, sublinha a importância de ter acesso aos resultados elaborados ou obtidos através dos instrumentos de IA e, em última análise, de definir a responsabilidade pelos procedimentos de notificação e o papel da IA e das tecnologias conexas em matéria penal, em particular, no que diz respeito à análise de grandes quantidades de provas em investigações criminais e à identificação de suspeitos ou vítimas de crimes; recorda a importância das questões relacionadas com a governação, os direitos fundamentais e as garantias processuais, a não discriminação, a responsabilização, a transparência, a imparcialidade, a equidade e a integridade intelectual da IA e das tecnologias conexas, salientando simultaneamente a necessidade de assegurar a supervisão humana em todas as circunstâncias; insiste em que as autoridades judiciais têm de ser obrigadas a justificar as suas decisões, nomeadamente quando utilizarem elementos de prova fornecidos por tecnologias assistidas pela IA, que exigem um nível elevado de controlo

[2] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (JO L 201 de 31.7.2002, p. 37).
[3] Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados (JO L 119 de 4.5.2016, p. 89).

judicial e critérios de admissibilidade rigorosos – em conformidade com a sua resolução sobre a robótica[4], de 16 de fevereiro de 2017, que salienta que deve ser sempre possível apresentar a fundamentação subjacente a qualquer decisão tomada com o auxílio da IA que possa ter impacto na vida de uma ou mais pessoas; recorda a distinção entre a utilização da IA e das tecnologias conexas na prevenção da criminalidade e na justiça penal; salienta que as tecnologias de IA devem imperativamente desempenhar sempre um papel secundário;

6. Recorda que as utilizações abusivas mais graves da IA e das tecnologias conexas – como a vigilância em larga escala, a definição de perfis e os programas de previsão policial, que podem avaliar onde é provável a ocorrência de crimes, onde é provável localizar os suspeitos de crimes, as possibilidades de vitimização, a vulnerabilidade, a notificação de pessoas desaparecidas ou se alguém é vítima ou autor de violência doméstica ou dum delito sexual – e as violações dos direitos processuais podem ser cometidas pelas autoridades públicas que atuam no domínio da aplicação da lei;

7. Sublinha a importância de utilizar os dados autogerados na recolha e análise de elementos de prova; recorda que tanto na prevenção da criminalidade como na justiça penal, os erros ou a possível utilização abusiva da análise de dados de entrada e saída, bem como a sua interpretação, podem estar enraizados no fator humano envolvido, pelo que exorta a uma abordagem cautelosa aquando da análise da eficácia e adequação da utilização das tecnologias de IA em todos os processos decisórios;

8. Exorta todas as autoridades públicas competentes – em especial, as autoridades de aplicação da lei como as autoridades policiais e judiciárias – a informarem o público acerca disto e a garantirem uma transparência suficiente no que se refere à sua utilização da IA e de tecnologias conexas ao desempenharem as suas competências, sobretudo no âmbito da justiça penal;

9. Considera essencial que a aplicação de sistemas de IA no contexto dum processo penal assegure o respeito dos princípios fundamentais do processo penal – incluindo o direito a um julgamento justo, o princípio da presunção de inocência e o direito a um recurso efetivo – e também o acompanhamento e o controlo independente dos sistemas decisórios automatizados;

10. Sublinha a importância do princípio do controlo humano e da verificação dos resultados elaborados ou obtidos através dos instrumentos de IA; recorda a importância das questões relacionadas com a governação, a transparência, a explicação e a responsabilização, a fim de garantir o respeito dos direitos fundamentais e evitar potenciais falhas na IA;

11. Salienta a sua abordagem cautelosa relativamente à utilização de software de reconhecimento biométrico; realça a ambiguidade resultante duma insuficiência inerente no que se refere à proteção de dados e às violações da privacidade dos dados; observa com preocupação a acumulação de dados pessoais dos cidadãos na União Europeia por países estrangeiros, através de criadores e fornecedores do setor privado;

[4] Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (JO C 252 de 18.7.2018, p. 239).

12. Recorda que – em conformidade com as atuais regras da UE em matéria de proteção de dados e com a Carta dos Direitos Fundamentais da União Europeia – a IA só pode ser utilizada para fins de reconhecimento biométrico à distância quando essa utilização for devidamente justificada, proporcionada e sujeita a salvaguardas adequadas; saúda as recomendações do Grupo de peritos de alto nível sobre a inteligência artificial da Comissão, no sentido duma utilização proporcionada, ponderada e baseada nos riscos da tecnologia de reconhecimento biométrico, em conformidade com a legislação relativa à proteção dos dados pessoais; propõe que a aplicação dessa tecnologia tenha de ser claramente justificada ao abrigo da legislação em vigor e sugere que a Comissão avalie a forma de incorporar essas recomendações de forma eficaz, em particular, no que respeita ao direito à privacidade e à proteção dos dados pessoais;

13. Acredita firmemente que as decisões tomadas pela IA ou pelas tecnologias conexas – especialmente nos domínios da justiça e da aplicação da lei – que tenham um impacto direto e significativo nos direitos e obrigações das pessoas singulares ou coletivas devem ser sujeitas a uma verificação humana rigorosa e a um processo equitativo;

14. Considera necessário analisar se é conveniente que as decisões de aplicação da lei sejam parcialmente delegáveis na IA e, em caso afirmativo, em que condições e em que medida pode ser autorizada essa utilização da IA; considera que a IA e as tecnologias conexas que podem substituir as decisões das autoridades públicas devem ser tratadas com a máxima precaução; salienta a necessidade de conceber princípios éticos sólidos e códigos de conduta específicos com vista à conceção e utilização da IA para ajudar as autoridades responsáveis pela aplicação da lei e as autoridades judiciais, caso as decisões em matéria de aplicação da lei sejam delegadas na IA; remete para o trabalho em curso na Comissão dos Assuntos Jurídicos.

INFORMAÇÕES SOBRE A APROVAÇÃO NA COMISSÃO ENCARREGADA DE EMITIR PARECER

Data de aprovação	10.9.2020
Resultado da votação final	+: 22 –: 3 0: 0
Deputados presentes no momento da votação final	Manon Aubry, Gunnar Beck, Geoffroy Didier, Angel Dzhambazki, Ibán García Del Blanco, Jean-Paul Garraud, Esteban González Pons, Mislav Kolakušić, Gilles Lebreton, Karen Melchior, Jiří Pospíšil, Franco Roberti, Marcos Ros Sempere, Liesje Schreinemacher, Stéphane Séjourné, Raffaele Stancanelli, Marie Toussaint, Adrián Vázquez Lázara, Axel Voss, Marion Walsmann, Tiemo Wölken, Lara Wolters, Javier Zarzalejos
Suplentes presentes no momento da votação final	Heidi Hautala, Emil Radev

VOTAÇÃO NOMINAL FINAL NA COMISSÃO ENCARREGADA DE EMITIR PARECER

22	+
PPE	Geoffroy Didier, Esteban González Pons, Jiří Pospíšil, Emil Radev, Axel Voss, Marion Walsmann, Javier Zarzalejos
S&D	Ibán García Del Blanco, Franco Roberti, Marcos Ros Sempere, Tiemo Wölken, Lara Wolters
RENEW	Karen Melchior, Liesje Schreinemacher, Stéphane Séjourné, Adrián Vázquez Lázara
ID	Gunnar Beck, Jean-Paul Garraud, Gilles Lebreton
ECR	Angel Dzhambazki, Raffaele Stancanelli
NI	Mislav Kolakušić

3	-
VERTS/ALE	Heidi Hautala, Marie Toussaint
GUE/NGL	Manon Aubry

0	0

Legenda dos símbolos utilizados:
+ : votos a favor
- : votos contra
0 : abstenções

INFORMAÇÕES SOBRE A APROVAÇÃO
NA COMISSÃO COMPETENTE QUANTO À MATÉRIA DE FUNDO

Data de aprovação	29.6.2021
Resultado da votação final	+: 36 –: 24 0: 6
Deputados presentes no momento da votação final	Magdalena Adamowicz, Konstantinos Arvanitis, Malik Azmani, Katarina Barley, Pernando Barrena Arza, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Patrick Breyer, Saskia Bricmont, Joachim Stanisław Brudziński, Jorge Buxadé Villalba, Damien Carême, Caterina Chinnici, Marcel de Graaff, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Laura Ferrara, Nicolaus Fest, Jean-Paul Garraud, Maria Grapini, Sylvie Guillaume, Andrzej Halicki, Evin Incir, Sophia in ‘t Veld, Patryk Jaki, Marina Kaljurand, Fabienne Keller, Peter Kofod, Łukasz Kohut, Moritz Körner, Alice Kuhnke, Jeroen Lenaers, Juan Fernando López Aguilar, Lukas Mandl, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Paulo Rangel, Terry Reintke, Diana Riba i Giner, Ralf Seekatz, Michal Šimečka, Birgit Sippel, Sara Skyttedal, Martin Sonneborn, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Tomas Tobé, Dragoş Tudorache, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Elissavet Vozemberg-Vrionidi, Jadwiga Wiśniewska, Elena Yoncheva, Javier Zarzalejos
Suplentes presentes no momento da votação final	Tanja Fajon, Miguel Urbán Crespo

VOTAÇÃO NOMINAL FINAL NA COMISSÃO COMPETENTE QUANTO À MATÉRIA DE FUNDO

36	**+**
NI	Laura Ferrara, Martin Sonneborn
Renew	Malik Azmani, Anna Júlia Donáth, Sophia in ‘t Veld, Fabienne Keller, Moritz Körner, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu, Dragoş Tudorache
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Tanja Fajon, Maria Grapini, Sylvie Guillaume, Evin Incir, Marina Kaljurand, Łukasz Kohut, Juan Fernando López Aguilar, Javier Moreno Sánchez, Birgit Sippel, Bettina Vollath, Elena Yoncheva
The Left	Konstantinos Arvanitis, Pernando Barrena Arza, Cornelia Ernst, Miguel Urbán Crespo
Verts/ALE	Patrick Breyer, Saskia Bricmont, Damien Carême, Alice Kuhnke, Terry Reintke, Diana Riba i Giner, Tineke Strik
24	**-**
ID	Nicolas Bay, Nicolaus Fest, Jean-Paul Garraud, Marcel de Graaff, Peter Kofod, Annalisa Tardino, Tom Vandendriessche
NI	Milan Uhrík
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Lena Düpont, Andrzej Halicki, Jeroen Lenaers, Lukas Mandl, Roberta Metsola, Nadine Morano, Paulo Rangel, Ralf Seekatz, Sara Skyttedal, Tomas Tobé, Elissavet Vozemberg-Vrionidi, Javier Zarzalejos
6	**0**
ECR	Joachim Stanisław Brudziński, Jorge Buxadé Villalba, Patryk Jaki, Nicola Procaccini, Jadwiga Wiśniewska
PPE	Emil Radev

Legenda dos símbolos utilizados:
+ : votos a favor
- : votos contra
0 : abstenções