Parlamento Europeu
2019-2024

Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos

2020/2016(INI)

8.6.2020

PROJETO DE 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: Tudor Ciuhodaru

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, nomeadamente os seus artigos 2.º e 6.º, e o Tratado sobre o Funcionamento da União Europeia,

– Tendo em conta a Carta dos Direitos Fundamentais da União Europeia,

– 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),

– Tendo em conta a Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, de 8 de abril de 2019, intitulada «Aumentar a confiança numa inteligência artificial centrada no ser humano[1],

– Tendo em conta o Livro Branco da Comissão, de 19 de fevereiro de 2020, sobre a inteligência artificial – Uma abordagem europeia virada para a excelência e a confiança[2],

– Tendo em conta a Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, de 19 de fevereiro de 2020, intitulada «Uma estratégia europeia para os dados»[3],

– 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)[4],

– 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[5],

---

[1] COM(2019)0168.
[2] COM(2020)0065.
[3] COM(2020)0066.
[4] JO L 119 de 4.5.2016, p. 1.
[5] JO L 119 de 4.5.2016, p. 89.

– 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[6],

– 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)[7],

– 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[8],

– 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 Assuntos Internos (A9-0000/2020),

A. Considerando que as tecnologias digitais em geral e a inteligência artificial (IA) em particular são extraordinariamente promissoras; que a IA é uma das tecnologias estratégicas do século XXI, na medida em que gera benefícios substanciais em termos de eficiência, precisão e comodidade, trazendo, assim, uma mudança positiva para a economia europeia; 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 dos seres humanos;

B. Considerando que o desenvolvimento da IA deve respeitar os valores em que a União assenta, em particular a dignidade humana, a liberdade, a democracia, a igualdade, o Estado de direito, os direitos humanos e os direitos fundamentais;

C. Considerando que sistemas de IA fiáveis devem ser responsáveis, concebidos para todos (incluindo as populações vulneráveis e marginalizadas), não discriminatórios, seguros e transparentes e respeitar a autonomia humana e os direitos fundamentais;

D. Considerando que a União, juntamente com os Estados-Membros, tem a responsabilidade crucial de assegurar que as escolhas estratégicas em matéria de desenvolvimento, implantação e utilização das aplicações de IA no domínio da justiça e da aplicação coerciva da lei sejam efetuadas de forma transparente, respeitem os princípios da necessidade e da proporcionalidade e garantam que as políticas e medidas

[6] JO L 295 de 21.11.2018, p. 39.
[7] JO L 201 de 31.7.2002, p. 37.
[8] JO L 135 de 24.5.2016, p. 53.

adotadas salvaguardem plenamente os direitos fundamentais na União;

E. Considerando que as aplicações de IA oferecem grandes oportunidades no domínio da aplicação coerciva da lei, permitindo nomeadamente melhorar os métodos de trabalho dos serviços policiais e das autoridades judiciais e combater mais eficazmente certos tipos de criminalidade, em particular a criminalidade financeira, o branqueamento de capitais e o financiamento do terrorismo, bem como certos tipos de cibercriminalidade;

F. 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;

G. Considerando que as aplicações de IA utilizadas pelos serviços policiais incluem aplicações como as tecnologias de reconhecimento facial, o reconhecimento automático de matrículas, a identificação de oradores, a identificação da fala, a 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 a identificação de ligações), a interceção da identidade internacional de assinante móvel (IMSI) e os 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 apresentam graus de fiabilidade e de precisão muito diferentes;

H. Considerando que as ferramentas e as aplicações IA são também utilizadas pelo poder judicial em todo o mundo, inclusivamente para a fixação de penas, o cálculo das probabilidades de reincidência e a determinação da liberdade condicional;

I. Considerando que a utilização da IA pelos serviços policiais comporta uma série de riscos potenciais, como a opacidade na tomada de decisões, diferentes tipos de discriminação e riscos para a proteção da privacidade e dos dados pessoais, a proteção da liberdade de expressão e de informação e a presunção de inocência;

J. Considerando que os sistemas de IA utilizados pelos serviços policiais também são vulneráveis a ataques por meio da IA; que os danos resultantes destas situações podem ser ainda mais importantes e podem causar danos exponencialmente maiores, tanto para indivíduos como para grupos;

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 aplicam-se 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;

2. Reafirma que todas as soluções de IA utilizadas pelos serviços policiais e pelo sistema judicial também devem respeitar plenamente os princípios da não discriminação, da liberdade de circulação, da presunção de inocência e do direito de defesa, da liberdade de expressão e de informação, da liberdade de reunião e de associação, da igualdade perante a lei e do direito à ação e a um tribunal imparcial;

3. Considera, a este respeito, que qualquer instrumento de IA desenvolvido ou utilizado

pelos serviços policiais ou pelo sistema judicial deve, no mínimo, ser seguro e adequado à sua finalidade, respeitar os princípios da equidade, da responsabilização, da transparência e da explicabilidade, e a sua implantação deve ser sujeita a uma verificação estrita da necessidade e da proporcionalidade;

4. Salienta a importância de impedir a vigilância em larga escala através de tecnologias de IA e de proibir as aplicações que possam viabilizar tal vigilância;

5. Salienta o potencial de preconceito e discriminação decorrente da utilização de aplicações de aprendizagem automática e de IA; 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;

6. Sublinha que muitas tecnologias de identificação baseadas em algoritmos identificam incorretamente um número desproporcionado de pessoas não brancas, crianças, idosos e mulheres;

7. Destaca a assimetria de poder entre os que desenvolvem e utilizam tecnologias de IA e aqueles que interagem e estão sujeitos a essas tecnologias;

8. Sublinha que os aspetos ligados à segurança e proteção dos sistemas de IA utilizados pelos serviços policiais devem ser cuidadosamente examinados e ser suficientemente sólidos e resilientes para prevenir consequências potencialmente catastróficas de ataques maliciosos contra sistemas de IA;

9. Considera necessário criar um regime claro e equitativo para a atribuição da responsabilidade jurídica pelas potenciais consequências negativas destas tecnologias digitais avançadas;

10. Sublinha que, em contextos judiciais e policiais, a decisão final deve ser sempre tomada por um ser humano, que pode ser responsabilizado pelas decisões adotadas, e deve ser prevista a possibilidade de recurso;

11. Solicita que os algoritmos sejam explicáveis e transparentes, a fim de garantir que o desenvolvimento, a implantação e a utilização de sistemas de IA no sistema judicial e nos serviços policiais respeitem os direitos fundamentais e sejam da confiança dos cidadãos, bem como de 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 que exista transparência em relação aos dados de base e ao modo como o sistema chega a uma determinada conclusão;

12. Apela a uma rastreabilidade dos sistemas de IA que defina as capacidades e os limites dos sistemas e permita identificar a origem dos elementos que determinam as decisões;

13. Solicita a realização de uma avaliação de impacto obrigatória dos direitos fundamentais antes da aplicação ou implantação de qualquer sistema de IA destinado aos serviços policiais ou ao sistema judicial, a fim de avaliar potenciais riscos para os direitos fundamentais;

14. Solicita a realização de auditorias periódicas e obrigatórias de todos os sistemas de IA utilizados pelos serviços policiais e pelo sistema judicial para testar e avaliar os sistemas algorítmicos, quando estiverem operacionais, a fim de detetar, investigar, diagnosticar e retificar quaisquer efeitos indesejáveis e adversos;

15. Solicita uma moratória sobre a implantação de sistemas de reconhecimento facial para fins policiais, até que as normas técnicas possam ser consideradas plenamente conformes aos direitos fundamentais, os resultados obtidos não sejam discriminatórios e exista confiança do público quanto à necessidade e à proporcionalidade da implantação dessas tecnologias;

16. Solicita aos Estados-Membros maior transparência geral e uma compreensão global da utilização das aplicações de IA na União, mediante uma repartição por autoridades policiais e judiciais dos Estados-Membros, tipos de ferramentas utilizadas, tipos de crime a que se aplicam e empresas que fornecem as ferramentas;

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

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.