

Bruxelas, 12 de setembro de 2022
(OR. en)

12302/22

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

**Dossiê interinstitucional:
2021/0106(COD)**

PARECER DO SERVIÇO JURÍDICO ¹

de:	Serviço Jurídico
Assunto:	Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial – Adequação dos artigos 114.º e 16.º do TFUE enquanto bases jurídicas para as disposições aplicáveis às autoridades policiais e judiciais

I. INTRODUÇÃO

1. O regulamento proposto estabelece regras harmonizadas para a colocação no mercado e a colocação em serviço de sistemas de inteligência artificial ("sistemas de IA") na União (a "proposta de regulamento")².

¹ O presente documento contém aconselhamento jurídico protegido nos termos do artigo 4.º, n.º 2, do Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão e não facultado ao público pelo Conselho da União Europeia. O Conselho reserva-se a faculdade de exercer todos os seus direitos em caso de publicação não autorizada.

² Doc. 8115/21.

2. Na reunião do Grupo das Telecomunicações e da Sociedade da Informação de 7 de abril de 2022, o Serviço Jurídico do Conselho ("SJC") interveio sobre a adequação das bases jurídicas duplas (artigos 16.º e 114.º do TFUE) do regulamento relativo aos sistemas de inteligência artificial ("sistemas de IA") que se propõe. As suas explicações confirmaram que os artigos 16.º e 114.º do TFUE constituem as bases jurídicas corretas da proposta e que o recurso ao artigo 87.º, n.º 2, do TFUE, em vez do artigo 114.º do TFUE, não é adequado. A pedido do Grupo, no presente parecer expõe-se por escrito e desenvolve-se a intervenção do representante do SJC na mesma reunião.
3. Os sistemas de IA são definidos no artigo 3.º, n.º 1, do regulamento proposto. Em geral, correspondem a certos tipos de software. O regulamento proposto aplica-se tanto aos fornecedores que colocam sistemas de IA no mercado como aos fornecedores que colocam sistemas de IA em serviço. Além disso, o regulamento proposto é igualmente aplicável aos utilizadores. Fornecedor pode ser uma pessoa singular ou coletiva, ou uma autoridade pública ou organismo que desenvolva um sistema de IA ou que tenha um sistema de IA desenvolvido com vista à sua colocação no mercado ou colocação em serviço sob o seu próprio nome ou marca. Utilizador pode ser uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que utilize, sob a sua autoridade, um sistema de IA.

4. De acordo com as definições constantes do artigo 3.º, as autoridades policiais e judiciais podem ser consideradas fornecedores e/ou utilizadores de um sistema de IA. Os sistemas de IA cuja finalidade prevista, tal como definida pelo fornecedor, seja a manutenção da ordem pública ou a administração da justiça, são classificados como de risco elevado nos termos do anexo III. Como tal, ficam obrigados ao cumprimento de requisitos essenciais (gestão de riscos, testagem, governação de dados, documentação técnica, transparência, supervisão humana, exatidão, solidez e cibersegurança) e de obrigações (como sistemas de gestão da qualidade, documentação técnica, avaliação da conformidade, medidas corretivas, dever de informação, obrigações dos importadores e distribuidores), bem como de normas e a submeter-se à avaliação da conformidade. Estas regras harmonizadas inspiram-se nas regras aplicáveis à segurança dos produtos estabelecidas na Diretiva 2006/42/CE (máquinas)³ e no Regulamento (CE) n.º 2017/745 (dispositivos médicos)⁴.
5. Refira-se que os sistemas de IA que envolvem a utilização de sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública pertencem à categoria de sistemas de IA proibidos. Há porém exceções a esta proibição da utilização de sistemas de IA está. Com efeito, a utilização de tais sistemas pode ou não ser autorizada pelos Estados-Membros. Se forem autorizados, ficam sujeitos a restrições e salvaguardas pormenorizadas, a fim de limitar a sua utilização ao estritamente necessário, com o objetivo de defender o direito fundamental à proteção dos dados pessoais. Tais restrições e salvaguardas estão previstas no regulamento proposto com base no artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE) e têm de ser complementadas pelo direito nacional. O artigo 5.º, n.º 1, alínea d), e n.ºs 2, 3 e 4 do regulamento proposto constitui uma *lex specialis* relativamente à Diretiva 2016/680 (Diretiva Proteção de Dados na Aplicação da Lei), que foi adotada com base no artigo 16.º, n.º 2, do TFUE.

³ Diretiva 2006/42/CE do Parlamento Europeu e do Conselho, de 17 de maio de 2006, relativa às máquinas e que altera a Diretiva 95/16/CE, JO L 157 de 9.6.2006, p. 24-86.

⁴ Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos, que altera a Diretiva 2001/83/CE, o Regulamento (CE) n.º 178/2002 e o Regulamento (CE) n.º 1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho JO L 117 de 5.5.2017, p. 1-175.

Em conformidade com o artigo 5.º, n.º 1, alínea d), os sistemas limitam-se aos seguintes objetivos:

- i) a investigação seletiva de potenciais vítimas específicas de crimes, nomeadamente crianças desaparecidas;
- ii) a prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de um ataque terrorista;
- iii) a deteção, localização, identificação ou instauração de ação penal relativamente a um infrator ou suspeito de uma infração penal referida no artigo 2.º, n.º 2, da Decisão relativa ao mandado de detenção europeu⁵ e punível no Estado-Membro em causa com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos e tal como definidas pela legislação desse Estado-Membro.

Nos termos do artigo 5.º, n.º 3, a utilização dessas tecnologias pelas autoridades policiais deve estar sujeita a autorização prévia de uma autoridade judicial ou administrativa. Contudo, numa situação de urgência devidamente justificada, a utilização do sistema pode ser iniciada sem autorização e esta pode ser solicitada durante ou após a utilização.

Nos termos do artigo 5.º, n.º 4, os Estados-Membros podem decidir autorizar a utilização de sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública e definir as regras pormenorizadas aplicáveis ao pedido, à emissão e ao exercício da autorização prévia, bem como para as correspondentes infrações penais.

6. As bases jurídicas do regulamento proposto são o artigo 16.º do TFUE (proteção de dados pessoais) e o artigo 114.º do TFUE (funcionamento do mercado interno). Por conseguinte, coloca-se a questão da adequação dessas bases jurídicas para as regras harmonizadas aplicáveis aos sistemas de IA fornecidos ou utilizados pelas autoridades policiais e judiciais.

⁵ Decisão-Quadro 2002/584/JAI do Conselho, de 13 de junho de 2002, relativa ao mandado de detenção europeu e aos processos de entrega entre os Estados-Membros, JO L 190 de 18.7.2002, p. 1.

7. O presente parecer incide, em primeiro lugar, sobre a adequação do artigo 114.º do TFUE enquanto base jurídica, no contexto específico das autoridades policiais mencionadas em várias disposições do regulamento proposto, ou seja, no que diz respeito aos sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público e aos sistemas de IA de risco elevado referidos no anexo III, ponto 6. O parecer aborda pois a questão de saber se o artigo 87.º, n.º 2, do TFUE (cooperação policial) não seria uma base jurídica mais adequada do que o artigo 114.º do TFUE (secção II) para abranger o fornecimento e a utilização de sistemas de IA pelas autoridades policiais. Por analogia, a conclusão da presente nota pode ser aplicada às autoridades judiciais referidas no anexo III, relativo aos sistemas de IA de risco elevado.
8. A presente nota analisa igualmente a adequação do artigo 16.º do TFUE enquanto base jurídica adicional e a aplicação dos Protocolos n.ºs 21 e 22 no contexto da utilização de sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública (secção III).

II. ADEQUAÇÃO DO ARTIGO 114.º DO TFUE ENQUANTO BASE JURÍDICA

9. De acordo com a jurisprudência constante, a base jurídica de um ato da União não depende da convicção de uma instituição quanto ao fim prosseguido, mas deve ser determinada de acordo com critérios objetivos suscetíveis de controlo jurisdicional, entre os quais figuram, nomeadamente, a finalidade e o conteúdo do ato. Se o exame de um ato demonstrar que este prossegue uma dupla finalidade ou que tem duas componentes e se uma destas finalidades ou componentes for identificável como principal ou preponderante, enquanto a outra é apenas acessória, esse ato deve ter por fundamento uma única base jurídica, a saber, a base jurídica exigida pela finalidade ou componente principal ou preponderante. Só excecionalmente, se se provar que persegue ao mesmo tempo vários objetivos, que se encontram ligados de forma indissociável, sem que um seja secundário e indireto relativamente ao outro, pode o ato fundamentar-se nas diferentes bases jurídicas correspondentes, a menos que essas bases jurídicas prescrevam procedimentos que sejam incompatíveis entre si. Assinale-se igualmente que o artigo 114.º, n.º 1, primeiro período, do TFUE deixa claro que as disposições do artigo se aplicam "[s]alvo disposição em contrário dos Tratados". Assim sendo, o recurso ao artigo 114.º do TFUE só se justifica se nenhuma disposição mais específica puder constituir a base jurídica para a adoção do ato em causa⁶. Se existir, no Tratado, uma disposição mais específica que possa constituir a base jurídica do ato em causa, este deve ser baseado nessa disposição⁷.

⁶ Parecer do SJC de 17 de maio de 2016, 9007/16, ponto 6.

⁷ Acórdão de 29 de abril de 2004, *Comissão /Conselho*, C-338/01, EU:C:2004:253, n.º 60.

A. OBJETIVO DO REGULAMENTO PROPOSTO

10. O regulamento proposto harmoniza a colocação no mercado, a colocação em serviço e a utilização de um determinado tipo de software (sistemas de IA). O facto de as autoridades públicas e os operadores privados poderem ser fornecedores ou utilizadores desses sistemas de IA não é, por si só, incompatível com a base jurídica do artigo 114.º do TFUE⁸.
11. Acresce que o facto de as autoridades policiais ou as pessoas que agem em seu nome poderem ser fornecedores ou utilizadores desses sistemas de IA não é suficiente para justificar o recurso à base jurídica do artigo 87.º do TFUE. Importa analisar a finalidade e o conteúdo do regulamento proposto para determinar se tal é necessário.
12. O regulamento proposto visa, em geral, nomeadamente no que diz respeito aos sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público e aos sistemas de IA de risco elevado, assegurar um nível de proteção elevado e coerente em toda a União, evitando simultaneamente que as divergências prejudiquem a livre circulação dos sistemas de IA e dos produtos e serviços conexos no mercado interno. O regulamento proposto estabelece obrigações uniformes para os operadores e garante a proteção uniforme das razões imperativas de interesse público e dos direitos das pessoas em todo o mercado interno (considerando 2). Mais concretamente, o regulamento proposto estabelece regras aplicáveis à colocação no mercado e à colocação em serviço de determinados sistemas de IA, garantindo assim o correto funcionamento do mercado interno e permitindo que esses sistemas beneficiem do princípio de livre circulação dos produtos e dos serviços (considerando 5). De um modo geral, a proposta procura estabelecer uma IA fiável desde a conceção, aplicável de forma generalizada, com um conjunto completo de regras para o desenvolvimento, a comercialização e a utilização de produtos, serviços e sistemas baseados na IA. Uma vez que a IA já se encontra num vasto número de serviços e produtos e que assim continuará a ser no futuro, a proposta segue uma lógica de mercado interno, estabelecendo um "quadro de segurança dos produtos" construído em torno de um conjunto de quatro categorias de risco. A proposta impõe requisitos para a entrada no mercado e a certificação de sistemas de IA de risco elevado através de um procedimento obrigatório de marcação CE.

⁸ Ver parecer do SJC (ST 11395/14, pontos 39 a 41) e precedentes como a Diretiva (UE) 2016/2102 e as Diretivas 2014/24/UE, 2014/25/UE e 2014/23/UE.

13. Nenhum dos objetivos declarados do regulamento proposto se refere à garantia de objetivos de segurança pública. Embora os objetivos de segurança pública devam ser alcançados indiretamente através do processo de harmonização da colocação no mercado/colocação em serviço/utilização de sistemas de IA pelas autoridades policiais, o Tribunal de Justiça⁹, interpretando o artigo 87.º, n.º 2, do TFUE à luz do artigo 67.º do TFUE, afirmou que, para que um ato da União, tendo em conta a sua finalidade e o seu conteúdo, se baseasse no primeiro artigo, devia estar diretamente relacionado com os objetivos estabelecidos no artigo 67.º do TFUE (ou seja, neste caso, a prevenção da criminalidade e a cooperação policial). No contexto do regulamento proposto fica esta interpretação excluída, uma vez que as únicas regras harmonizadas relativas à utilização desses sistemas pelas autoridades policiais são 1) regras de segurança dos produtos aplicáveis uniformemente a todos os fornecedores e utilizadores em relação à colocação no mercado/colocação em serviço ou utilização dos sistemas de IA ou 2) regras sobre a proteção de dados pessoais relativamente às quais foi aditado o artigo 16.º do TFUE (ver parte III infra) enquanto base jurídica.
14. Noutro processo¹⁰, apesar de o objetivo da alteração à diretiva relativa às armas de fogo ser o de garantir um nível mais elevado de segurança pública em relação à ameaça terrorista e a outras formas de criminalidade, o Tribunal de Justiça considerou que a harmonização dos aspetos relativos à segurança das mercadorias [era] um dos elementos essenciais para assegurar o bom funcionamento do mercado interno, uma vez que regulamentações díspares nesta matéria [eram] suscetíveis de criar obstáculos às trocas comerciais¹¹.

⁹ Acórdão de 6 de maio de 2014, *Comissão Europeia /Parlamento Europeu e Conselho da União Europeia*, C43/12, EU:C:2014:298.

¹⁰ Acórdão de 3 de dezembro de 2019, *República Checa/Parlamento Europeu*, C-482/17, EU:C:2019:1035.

¹¹ *Ibidem*, ponto 57: "*Ora, uma vez que a particularidade das armas de fogo consiste, contrariamente ao que alega a República da Polónia, na sua perigosidade não só para os utilizadores mas também para o grande público, como já salientou o Tribunal de Justiça no n.º 54 do Acórdão de 23 de janeiro de 2018, Buhagiar e o., C- 267/16, EU:C:2018:26, as considerações de segurança pública revelam-se, conforme recorda o quinto considerando da Diretiva 91/477, indispensáveis no âmbito de uma regulamentação sobre a aquisição e a detenção dessas mercadorias*". Ver também acórdão de 23 de janeiro de 2018, *Albert Buhagiar e outros/Ministro da Justiça*, C-267/16, EU:C:2018:26, n.º 54: "*A este respeito, importa observar que, tendo em conta o risco para a segurança das pessoas que as armas de fogo representam, a livre circulação destas armas só pôde ser atingida através de um enquadramento estrito das condições da sua transferência entre Estados- Membros, entre as quais figura o princípio da autorização prévia emitida pelos Estados- Membros em causa para uma transferência dessas mercadorias*".

15. Os objetivos do regulamento proposto, incluindo o artigo 5.º, n.º 1, alínea d), n.ºs 2, 3 e 4, relativo à utilização de sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública e as disposições relativas aos sistemas de IA de risco elevado a que se refere o anexo III, ponto 6, não estão diretamente ligados a um objetivo de segurança pública. Pelo contrário, a proposta responde às principais preocupações relacionadas com a forma como os sistemas de IA afetam a saúde, a segurança e os direitos fundamentais. Por conseguinte, as disposições pertinentes estão diretamente relacionadas com o objetivo de assegurar condições de concorrência equitativas na colocação no mercado/colocação em serviço ou utilização de sistemas de IA no mercado interno, protegendo simultaneamente a saúde, a segurança e os direitos fundamentais dos utilizadores.
16. Tendo em conta o que precede, o principal objetivo do regulamento proposto é melhorar o funcionamento do mercado interno, na aceção do artigo 114.º do TFUE, e os objetivos referidos no artigo 67.º do TFUE só estão ligados a esse objetivo principal de forma indireta e acessória.

B. CONTEÚDO DO REGULAMENTO PROPOSTO

17. O regulamento proposto contém essencialmente regras que determinam o que é necessário para colocar um produto específico (um software de IA) no mercado (ou para o colocar em serviço), de modo a garantir a sua segurança e a observância dos direitos fundamentais. Estabelece um conjunto completo de regras para o desenvolvimento, a comercialização e a utilização de produtos, serviços e sistemas baseados na IA. O regulamento proposto não obriga as autoridades policiais a utilizar um sistema de IA legalmente colocado no mercado, nem regula diretamente a forma como estas devem utilizar esse sistema de IA. Pelo contrário, delimita claramente as situações em que a utilização prevista é considerada de risco elevado pelo mero facto de serem as autoridades policiais ou judiciais a utilizar determinado sistema de IA.

18. Sucede que o artigo 29.º do regulamento proposto contém regras que estabelecem as condições de utilização de sistemas de IA de risco elevado, mas esta disposição não é específica ao setor, tem um âmbito limitado (principalmente no que diz respeito às instruções de utilização do produto) e está intrinsecamente ligada às obrigações impostas aos fornecedores de sistemas de IA pelo regulamento proposto. O referido artigo dá também aos Estados-Membros uma certa margem de manobra para preverem regras adicionais sobre a utilização de tais sistemas de IA de risco elevado. No que diz respeito aos sistemas de identificação biométrica à distância em "tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública (artigo 5.º), o regulamento proposto regula parcialmente a utilização desses sistemas do ponto de vista da proteção de dados, com base no artigo 16.º do TFUE (ver parte III infra).
19. Além disso, só os Estados-Membros podem decidir prever a possibilidade de autorizar total ou parcialmente a utilização desses sistemas de identificação biométrica à distância "em tempo real". As condições específicas dessa utilização continuam a ser estabelecidas no direito nacional, mas têm de respeitar os critérios e as salvaguardas gerais estabelecidos no regulamento: autorização judicial ou administrativa prévia, pedido, emissão e exercício da autorização prévia, bem como indicação das infrações penais em relação às quais esses sistemas podem ser utilizados.

20. Os sistemas de IA são um tipo específico de software. As regras harmonizadas aplicáveis à colocação no mercado ou à colocação em serviço/utilização de sistemas de IA são portanto regras harmonizadas semelhantes às da segurança dos produtos. Aplicam-se de forma uniforme, sem distinção entre utilizadores públicos e privados. Assim, de acordo com os considerandos pertinentes do regulamento proposto, deve ser assegurado um nível de proteção coerente e elevado em toda a União. Ao mesmo tempo, devem ser evitadas divergências que prejudiquem a livre circulação dos sistemas de IA e de produtos e serviços conexos no mercado interno. Tal objetivo pode ser alcançado estabelecendo obrigações uniformes para os operadores e garantindo a proteção uniforme das razões imperativas de interesse público e dos direitos das pessoas em todo o mercado interno, com base no artigo 114.º do TFUE¹².
21. O regulamento proposto contém várias referências à manutenção da ordem pública, à gestão do controlo das fronteiras e à administração da justiça no anexo III sobre os sistemas de IA de risco elevado (pontos 6, 7 e 8, respetivamente). Estas referências incluem uma enumeração pormenorizada e exaustiva correspondente ao artigo 6.º, n.º 2, para além de outros sistemas de risco elevado relacionados com os riscos dos produtos referidos no artigo 6.º, n.º 1, para a segurança. Com efeito, de acordo com o artigo 6.º, n.º 1, alguns sistemas de IA devem ser considerados de risco elevado por definição, devido à sua gravidade esperada e aos elevados riscos para os direitos fundamentais, a saúde e a segurança. Outros sistemas considerados de risco elevado e enumerados no anexo III são a educação, a gestão de infraestruturas críticas, o emprego, a identificação biométrica e a categorização, bem como o acesso a serviços públicos e privados essenciais.

¹² Como tal, é necessário adotar um quadro jurídico da União que estabeleça regras harmonizadas em matéria de inteligência artificial para promover o desenvolvimento, a utilização e a adoção da inteligência artificial no mercado interno e que, ao mesmo tempo, proporcione um nível elevado de proteção de interesses públicos, como a saúde e a segurança e a proteção dos direitos fundamentais, tal como são reconhecidos e protegidos pelo direito da União. Para alcançar esse objetivo, torna-se necessário estabelecer regras aplicáveis à colocação no mercado e à colocação em serviço de determinados sistemas de IA, garantindo assim o correto funcionamento do mercado interno e permitindo que esses sistemas beneficiem do princípio de livre circulação dos produtos e dos serviços (ver considerandos 2 e 5 da proposta).

22. No entanto, essas regras relativas aos sistemas de IA de risco elevado não determinam se as autoridades policiais e judiciais (ou as autoridades dos outros domínios identificados) devem ou não utilizar esses sistemas. O regulamento proposto só indiretamente produzirá os seus efeitos no desenvolvimento efetivo de sistemas de IA que possam ser utilizados pelas autoridades policiais e nos sistemas de IA utilizados atualmente e no futuro. Assim, as regras referem-se a sistemas de IA "*destinados a serem utilizados*" por essas autoridades (ver, por exemplo, artigos 3.º, ponto 12, 8.º n.º 2, e anexo III). A consequência de classificar um determinado sistema de IA como sendo de risco elevado é a aplicação de um conjunto específico de regras em matéria de gestão de riscos, governação de dados e especificações técnicas. Os utilizadores desses sistemas de IA de risco elevado são obrigados a respeitar as instruções de utilização, conservar registos e realizar avaliações de impacto sobre a proteção de dados.
23. Além disso, as obrigações dos utilizadores que não estejam relacionadas com as instruções de utilização podem ser estabelecidas no direito da União ou no direito nacional e não prejudicam o poder discricionário do utilizador para organizar os seus próprios recursos e atividades para efeitos de aplicação das medidas de supervisão humana indicadas pelo fornecedor (artigo 29.º, n.º 2, do regulamento proposto). Estas regras estabelecem salvaguardas adicionais em matéria de direitos fundamentais para os sistemas de IA de risco elevado.

24. Tendo em conta o que precede, importa salientar que o regulamento proposto não contém regras que visem permitir ou impedir que determinado sistema de IA de risco elevado colocado no mercado seja utilizado pelas autoridades policiais. Por efeito das regras propostas, será classificado de forma distinta (risco elevado) um sistema de IA desenvolvido ou utilizado pelas autoridades policiais em resultado da sua utilização prevista. Esta utilização seria regida pelo direito nacional e, em certa medida, decidida pelas próprias autoridades policiais. Com efeito, o regulamento proposto estabelece no artigo 29.º condições mínimas de utilização (limitadas às instruções de utilização) dos sistemas de IA de risco elevado, incluindo as enumeradas no anexo III, pontos 6, 7 e 8, que serão complementadas pelo direito nacional. Por conseguinte, deve ser feita uma distinção, em conformidade com a jurisprudência do Tribunal, entre, por um lado, o objetivo pretendido do regulamento proposto, que não é o de regulamentar a utilização de sistemas de IA pelas autoridades policiais, e, por outro, os efeitos que pode indiretamente produzir¹³, que são irrelevantes para efeitos da análise da adequação da base jurídica.
25. Os pontos 6, 7 e 8 (sobre a manutenção da ordem pública, a migração e a administração da justiça, respetivamente) não são predominantes entre os sistemas de IA de risco elevado. Com efeito, nos termos do regulamento proposto, um sistema de IA de risco elevado não tem necessariamente que estar enumerado no anexo III. A maioria dos sistemas de risco elevado está, de facto, enumerada genericamente no artigo 6.º, n.º 1, alíneas a) e b), do regulamento proposto (em relação à segurança dos produtos). Há outros sistemas de IA de risco elevado que são enumerados no anexo III, no qual se encontram os pontos 1 (identificação biométrica), 2 (infraestruturas críticas), 3 (educação e formação profissional) e 4 (emprego, gestão de trabalhadores e acesso ao emprego por conta própria), que dizem respeito a domínios diferentes da justiça e assuntos internos (JAI). Todos os utilizadores desses sistemas de IA de risco elevado estão sujeitos a um regime uniforme estabelecido não em função do seu estatuto específico (por exemplo, se são operadores económicos ou autoridades públicas), mas sim na perspetiva da proteção da saúde, da segurança e dos direitos fundamentais.

¹³ Ver acórdão do Tribunal de Justiça de 21 de junho de 2018, *República da Polónia/Parlamento Europeu e Conselho da União Europeia*, C-5/16, EU:C:2018:483, n.ºs 63 a 68, e acórdão do Tribunal de Justiça de 22 de junho de 2022, *Leistriz AG/LH*, C-534/20, EU:C:2022:495, n.º 28.

26. Por conseguinte, o regulamento proposto contém regras harmonizadas sobre a colocação no mercado, a colocação em serviço e a utilização de sistemas de IA, quer sejam utilizados por operadores privados quer por autoridades públicas, incluindo, a título acessório¹⁴, autoridades policiais e judiciais.
27. Para além da utilização de sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública, que obedece a regras específicas em matéria de tratamento de dados pessoais (ver parte III infra), o regulamento proposto não contém regras harmonizadas sobre a utilização de sistemas de IA de risco elevado. Como se esclareceu nos pontos 18 e 19 supra, a referência à utilização de sistemas de IA de risco elevado diz essencialmente respeito às instruções de utilização do produto (artigo 29.º) e está relacionada com as obrigações impostas aos fornecedores. Salientou-se já no ponto 22 que cabe ao direito nacional e às autoridades nacionais decidir se as autoridades policiais ou judiciais podem ou não utilizar sistema de IA de risco elevado legalmente colocados no mercado nos termos do regulamento proposto.
28. Por conseguinte, o artigo 87.º, n.º 2, do TFUE, em especial a alínea a), não constitui uma base jurídica adequada para o regulamento proposto. As regras da proposta não promovem nem impedem a recolha, o armazenamento, o tratamento, a análise nem o intercâmbio de informações pertinentes. Simplesmente, quando tais atividades forem realizadas por autoridades policiais, haverá que respeitar várias condições não específicas e harmonizadas para salvaguardar os direitos dos utilizadores. Do mesmo modo, entre os objetivos declarados do regulamento proposto não está o desenvolvimento de técnicas de investigação comuns. Os requisitos propostos relativos à utilização de sistemas de IA de risco elevado não são específicos ao domínio da JAI nem dizem respeito à cooperação policial *stricto sensu*, tal como é definida no TFUE.

¹⁴ Ver parecer do Tribunal de Justiça sobre a *Convenção de Istambul*, A-1/19, EU:C:2021:198, em especial os n.ºs 298 e 301.

29. No que diz respeito ao disposto no artigo 5.º, n.º 4, do regulamento proposto, os Estados-Membros podem ainda decidir autorizar a utilização de sistemas de identificação biométrica à distância em "tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública. Se assim o decidirem, os Estados-Membros têm o dever de estabelecer as regras de pormenor necessárias ao pedido, à emissão e ao exercício da autorização prévia, bem como as infrações penais conexas para cuja investigação ou repressão se autoriza a utilização¹⁵. Com base no resultado dos debates havidos no Conselho, estas regras propostas não teriam por consequência a atribuição de novas competências às respetivas autoridades nacionais. Pelo contrário, limita-se a utilização de mecanismos existentes ou de eventuais futuros mecanismos a fim de assegurar a defesa do direito à privacidade e a proteção dos dados pessoais.
30. À luz do que precede, o artigo 114.º do TFUE é a única base jurídica adequada para as regras harmonizadas sobre sistemas de IA de risco elevado, incluindo os utilizados pelas autoridades policiais e judiciais, e qualquer base jurídica JAI da parte III, título V, do TFUE, como o artigo 87.º do TFUE no que diz respeito a essas regras harmonizadas, não é justificada nem adequada.

¹⁵ É de salientar que o artigo 5.º, n.º 4, da proposta apresenta certas características semelhantes às do artigo 15.º, n.º 1, da Diretiva Privacidade Eletrónica 2002/58. Em especial, prevê a possibilidade de os Estados-Membros derrogarem determinadas proibições estabelecidas no direito da União. À luz da jurisprudência constante, as disposições nacionais destinadas a derrogar tal proibição ficarão necessariamente abrangidas pelo âmbito de aplicação do direito da União, o que, por sua vez, fará com que a Carta lhes seja aplicável.

III. ADEQUAÇÃO DO ARTIGO 16.º TFUE ENQUANTO BASE JURÍDICA ADICIONAL

31. O regulamento proposto inclui o artigo 16.º do TFUE como base jurídica, relativamente ao tratamento de dados pessoais no domínio da manutenção da ordem pública. Os considerandos 25 e 26 incluem uma referência ao artigo 6.º-A do Protocolo n.º 21 e ao artigo 2.º-A do Protocolo n.º 22 no que diz respeito ao tratamento de dados pessoais no domínio da prevenção da criminalidade. Na opinião da Comissão, o artigo 16.º do TFUE destina-se exclusivamente a servir de base jurídica para as disposições que impõem restrições ao tratamento de dados pessoais biométricos de forma complementar em comparação com a Diretiva 2016/680 (Diretiva Proteção de Dados na Aplicação da Lei). O artigo 5.º, n.º 1, alínea d), é formulado como uma proibição de princípio, à qual se aplica um conjunto de três exceções. Concretamente, é proibida a utilização de sistemas de identificação biométrica à distância em "tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública, a menos que tal seja estritamente necessário para a) realizar buscas seletivas de potenciais vítimas de crimes, b) prevenir um atentado terrorista iminente ou um atentado à integridade física/vida de uma pessoa, c) localizar ou identificar ou instaurar ação penal contra o autor ou suspeito de uma infração penal grave (com referência ao mandado de detenção europeu). No artigo 5.º, n.ºs 2, 3 e 4 impõem-se outros requisitos a esta utilização específica de sistemas de IA pelas autoridades policiais, nomeadamente, uma avaliação da necessidade e da proporcionalidade, uma autorização prévia (exceto em situações de emergência) e uma decisão dos Estados-Membros no sentido de autorizar ou não, a nível nacional, a utilização específica de ferramentas de IA nessas situações.
32. O artigo 5.º é uma disposição de pormenor que regula uma utilização específica de ferramentas de IA e que não só visa complementar o atual quadro legislativo da União (a Diretiva Proteção de Dados na Aplicação da Lei, ela própria baseada no artigo 16.º do TFUE), mas também exige um quadro de execução nacional.

33. Em essência, apesar de estar formulada como proibição, a regra específica do artigo 5.º pode ser descrita como estabelecendo um enquadramento rigoroso e excecional da vigilância generalizada de pessoas singulares, "em tempo real", por instrumentos de IA em espaços abertos, para efeitos da sua identificação. A proibição vai também além da simples utilização de câmaras para gravar e remete para a utilização de ferramentas de IA para o reconhecimento automatizado de sinais particulares humanos em espaços acessíveis ao público (como o rosto, mas também a marcha, as impressões digitais, o ADN, a voz, a digitação de teclado e outros sinais biométricos ou comportamentais). A proibição implica também uma captação e identificação concomitantes de pessoas mediante uma análise comparativa/verificação de dados. Além disso, há que apreciar a regra também tendo em conta o facto de poder igualmente ser permitida a identificação "em tempo real" por utilizadores privados em espaços públicos (para eventos como os jogos de futebol).
34. Os esclarecimentos adicionais prestados pela Comissão parecem indicar que, atualmente, nenhum ou talvez muito poucos Estados-Membros regulamentaram esta questão específica, com vista a permitir que as autoridades policiais utilizem ferramentas de IA na deteção "em tempo real" de pessoas em espaços públicos. No entanto, em termos práticos, embora não tenham sido apresentados elementos concretos que provem que as práticas e os instrumentos existentes terão de mudar, parece claro que as futuras técnicas de investigação, métodos forenses e regras em matéria de recolha de provas terão de integrar esta abordagem de proibição/exceção.
35. No que diz respeito à base jurídica, afigura-se que as disposições que impõem restrições ao tratamento de dados pessoais biométricos de forma complementar (em comparação com a Diretiva Proteção de Dados na Aplicação da Lei) têm por objetivo a proteção dos dados pessoais, estabelecendo salvaguardas adequadas. Tal objetivo está indissociavelmente ligado ao objetivo das disposições abrangidas pelo âmbito de aplicação do artigo 114.º TFUE, sem que um seja secundário e indireto em relação ao outro. O regulamento proposto visa estabelecer um quadro geral para os sistemas de IA seguindo uma abordagem baseada no risco. Neste contexto, a regulamentação horizontal dos sistemas de IA pode incluir salvaguardas rigorosas aplicáveis a este sistema específico de IA para a deteção em "tempo real". Por conseguinte, um sistema de IA específico que contenha salvaguardas adequadas em matéria de proteção de dados pessoais está indissociavelmente ligado ao objetivo geral de melhorar o funcionamento do mercado interno e não é secundário nem indireto em relação a este último. Assim sendo, o regulamento proposto deve reger-se por uma dupla base, em conformidade com a jurisprudência pertinente (ver ponto 9 supra).

36. No entanto, mantém-se a questão de saber que base jurídica deve ser utilizada para regulamentar o tratamento de dados pessoais para utilização dos sistemas referidos no artigo 5.º, n.º 1, alínea c), a n.º 4, do regulamento proposto. Com efeito, o artigo 87.º, n.º 2, alínea a), do TFUE, constitui uma base jurídica para as medidas tomadas pelos serviços policiais em matéria de prevenção, deteção e investigação de infrações penais, relativamente à recolha, ao armazenamento, ao tratamento, à análise e ao intercâmbio de informações pertinentes.
37. Como explicou o advogado-geral no Parecer PNR Canadá (A1/15), o artigo 16.º TFUE, por um lado, e os artigos 87.º, n.º 2, alínea a), e 82.º, n.º 1, alínea d), TFUE, por outro, não podem estabelecer entre si relações de tipo hierárquico "*lex generalis – lex specialis*"¹⁶. O artigo 16.º, n.º 2, do TFUE, é a única disposição aplicável às regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades policiais dos Estados-Membros no exercício de atividades de prevenção da criminalidade. O simples facto de o artigo 5.º remeter para a lista de crimes graves constante da Decisão-Quadro relativa ao mandado de detenção europeu não altera esta apreciação: a remissão não significa que esta decisão-quadro seja aplicável enquanto tal¹⁷. Trata-se apenas de uma técnica legislativa para enumerar crimes graves sem necessidade de criar um anexo separado.
38. Não deixa de ser verdade que a regra do artigo 5.º não é estabelecida como um meio de delimitar melhor as condições de aplicação dessas medidas relacionadas com a JAI, mas sim com vista a garantir que, no futuro, qualquer utilização da identificação biométrica "em tempo real" pelos sistemas de IA responda adequadamente às preocupações em matéria de direitos fundamentais e, principalmente, à necessidade de assegurar que os dados biométricos sejam recolhidos e tratados respeitando o direito à privacidade e aos dados pessoais.

A este respeito, o regulamento não pretende estabelecer um novo procedimento obrigatório específico da JAI, baseando-se antes em meios processuais já comprovados para garantir o respeito pelos direitos fundamentais.

¹⁶ Ver conclusões do advogado-geral P. Mengozzi, de 8 de setembro de 2016, *Projeto de acordo entre o Canadá e a União Europeia*, Processo 1/15, EU:C:2016:656, n.ºs 112 a 120.

¹⁷ A respeito da aplicação desta lista de crimes graves pelos Estados-Membros, veja-se o acórdão do Tribunal de Justiça de 27 de janeiro de 2022, *Liga dos Direitos Humanos/Conselho de Ministros*, C-817/19, EU:C:2022:65, n.ºs 150 a 152.

39. Se o artigo 16.º do TFUE for uma base jurídica adicional adequada, levantam-se questões quanto à aplicação dos artigos 6.º-A e 2.º-A dos Protocolos n.ºs 21 e 22, respetivamente. Como se expõe nos considerandos 25 e 26 da proposta, tal significa que, quando as autoridades policiais da Irlanda ou da Dinamarca utilizem sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para a prevenção da criminalidade, e não estando a Irlanda nem a Dinamarca vinculadas pelas regras correspondentes em matéria de cooperação policial ou de cooperação judiciária em matéria penal, estes dois Estados-Membros não estarão vinculados pelo artigo 5.º, n.º 1, alínea d), e n.ºs 2 e 3, do regulamento proposto. Não quer isto dizer que o artigo 5.º, n.º 1, alínea d), e n.ºs 2 e 3, contenha regras em matéria de cooperação policial, a exemplo de regras sobre a partilha de informações entre as autoridades policiais. Quer apenas dizer que o artigo 5.º, n.º 1, alínea d), e n.ºs 2 e 3, do regulamento proposto, à semelhança da Diretiva 2016/680 (Diretiva Proteção de Dados na Aplicação da Lei), que é *lex generalis* adotada com base no artigo 16.º do TFUE, regula o tratamento de dados pessoais biométricos no contexto específico dos sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para a prevenção da criminalidade, e nada mais. A proposta da Comissão a este respeito segue a abordagem adotada pelo legislador da União para a Diretiva Proteção de Dados na Aplicação da Lei e, como tal, confirma que, neste contexto, o recurso ao artigo 87.º, n.º 2, TFUE, não se justifica.
40. O aditamento do artigo 16.º TFUE ao artigo 114.º TFUE no caso em apreço justifica-se pelo facto de o artigo 5.º, n.º 1, alínea d), e n.ºs 2 e 3, ser o único que regula a utilização de um sistema de IA autorizado que interfere com o direito à proteção dos dados pessoais, que é *lex specialis* em relação ao quadro geral de proteção de dados. Tais regras de *lex specialis* em matéria de proteção de dados que afetam a utilização desses sistemas sensíveis de IA não podem ser consideradas secundárias nem indiretas em relação à base jurídica do mercado interno. Por conseguinte, o aditamento do artigo 16.º do TFUE como base jurídica é suficientemente justificado no regulamento proposto e o recurso ao artigo 87.º, n.º 2, alínea a), do TFUE não é adequado.

IV. CONCLUSÃO

41. À luz do que precede, o Serviço Jurídico do Conselho considera que:

- a) O recurso aos artigos 16.º e 114.º do TFUE como base jurídica para o regulamento proposto é justificado e adequado;
 - b) O recurso ao artigo 87.º, n.º 2, do TFUE ou a qualquer outra base jurídica no âmbito da JAI não é justificado nem adequado em relação às regras harmonizadas aplicáveis aos sistemas de IA que podem ser fornecidos ou utilizados pelas autoridades policiais ou judiciais.
-