A PROPOSTA REGULATÓRIA DA UNIÃO EUROPEIA PARA A *INTELIGÊNCIA ARTIFICIAL* (2ª. parte) – Sistemas de "risco inaceitável"

Demócrito Reinaldo Filho
Desembargador do TJPE

A *Comissão Europeia*, braço executivo da União Europeia, apresentou no dia 21 de abril deste ano a sua proposta para regulamentação das tecnologias de *inteligência artificial* (IA)[1]. A proposta, que recebeu o nome de *Artificial Intelligence Act*[2], tem uma abordagem regulatória calcada na **hierarquização dos riscos** oferecidos por sistemas e tecnologias que usam IA[3]. Ao fazer a apresentação da proposta de regulamento, a Comissária Europeia para a Economia e Sociedade Digital, Margrethe Vestager, foi enfática ao afirmar que as regras da Comissão Europeia baniriam "os sistemas de IA considerados uma clara

---

[1] **Inteligência artificial** (por vezes mencionada pela sigla em português **IA** ou pela sigla em inglês **AI** - *artificial intelligence*) é a inteligência similar à humana exibida por sistemas de *software*, além de também ser um campo de estudo acadêmico.

[2] O nome completo atribuído à proposta legislativa é: *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS*. Cópia em PDF da proposta de regulação pode ser obtida em: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence

[3] Para melhor compreensão do modelo regulatório baseado nos riscos oferecidos pelos sistemas de IA, sugerimos a leitura de nosso primeiro artigo sobre a proposta de Regulamento da Comissão Europeia. Ele serve de introdução ao tema da regulação da inteligência artificial na UE e é a primeira parte de nossa análise sobre o Regulamento. Sua leitura é fundamental para a compreensão do escopo e objetivo do Regulamento. O titulo do primeiro artigo é: *A PROPOSTA REGULATÓRIA DA UNIÃO EUROPEIA PARA A INTELIGÊNCIA ARTIFICIAL (1ª. parte) – A hierarquização dos riscos*.

ameaça à segurança, meios de subsistência e direitos das pessoas"[4].

Segundo essa visão regulatória baseada nos riscos (*risk-based regulatory approach*), as restrições e exigências aumentam conforme maiores sejam os riscos que os sistemas de IA possam oferecer a direitos e garantias fundamentais dos indivíduos. Os níveis de regulação são diferentes de acordo com os riscos, variam conforme os riscos que os sistemas de IA possam apresentar a valores da sociedade e direitos das pessoas.

Nessa acepção, a proposta classifica os sistemas de IA em três diferentes patamares de risco: os de "risco inaceitável" (*unacceptable risk*), os de "risco elevado" (*high-risk*) e os de "risco limitado" (*limited risk*) ou de "risco mínimo" (*minimal risk*). O desenvolvimento e utilização de sistemas que apresentem "risco inaceitável" são completamente vedados, em razão do elevado potencial de vulneração de direitos fundamentais.

O Título II da Proposta de Regulamento descreve as "práticas de inteligência artificial proibidas" (*prohibited artificial intelligence practices*), assim consideradas aquelas que gerem "riscos inaceitáveis" de vulneração à saúde, segurança e direitos fundamentais das pessoais. Seguindo a abordagem baseada na *hierarquização dos riscos* criados pelos sistemas de IA, a norma regulamentar fornece uma lista de práticas consideradas inaceitáveis por violar princípios e direitos fundamentais da pessoa humana. Na categoria de práticas ou sistemas de IA inaceitáveis, encontram-se as seguintes:

a) o emprego de "técnicas subliminares além da consciência de uma pessoa", suficiente a

[4] Ver reportagem da BBC, publicada em 21.04.21, acessível em: https://www.bbc.com/news/technology-56830779.

distorcer o seu comportamento de maneira a causar-lhe dano físico ou psicológico (art. 5°., 1, *a*)[5];

b) exploração de vulnerabilidades de um grupo específico de pessoas, que, devido à idade ou deficiência física ou mental (como crianças, idosos ou pessoas com deficiência), possam ter seu comportamento distorcido de maneira a causar-lhes dano físico ou psicológico (art. 5°., 1, *b*)[6].

Como se observa, o Regulamento procura banir do mercado todos os sistemas artificialmente inteligentes que possam "manipular o comportamento humano". Nessa categoria estariam incluídos, por exemplo, brinquedos com assistentes de voz que podem "encorajar comportamentos perigosos" por parte de crianças ou adolescentes ou quaisquer outros equipamentos artificialmente inteligentes que comprometam o discernimento e a "livre vontade" dos usuários.

---

[5] Na redação original (em inglês):
"Article 5
1. The following artificial intelligence practices shall be prohibited:
(a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm; […}".

[6] Na redação original (em inglês):
"Article 5
1. The following artificial intelligence practices shall be prohibited: […]
(b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm; […].

Sistemas de pontuação social (*social scoring*)

Além de sistemas que induzam ou manipulem o comportamento das pessoas, por meio do uso de técnicas subliminares não percebidas pela consciência ou da exploração de vulnerabilidades causadas pela idade ou deficiências fisiológicas, o regulamento ainda coloca na categoria de "práticas de inteligência artificial proibidas" os programas e algoritmos utilizados por autoridades governamentais para "pontuação social" (*social scoring*). Segundo o art. 5º., 1., c, (i) e (ii), ficam vedados os sistemas utilizados para "avaliação ou classificação da *confiabilidade* de pessoas físicas durante um certo período de tempo com base no comportamento social ou características pessoais ou de personalidade conhecidas ou possíveis de serem previstas, com a pontuação social resultando em:

> (i) tratamento prejudicial ou desfavorável de certas pessoas naturais ou grupos de pessoas em contextos sociais que não estão relacionados com os contextos nos quais os dados foram originalmente gerados ou coletados;
>
> (ii) tratamento prejudicial ou desfavorável de certas pessoas ou grupos de pessoas que são injustificados ou desproporcionais aos seus comportamentos ou sua gravidade"[7].

[7] Na redação original (em inglês):
"Article 5
1. The following artificial intelligence practices shall be prohibited:
(c) the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or

Nesse ponto, o Regulamento bane a utilização de sistemas equivalentes ao "crédito social" chinês. Como se sabe, o Governo da China desenvolveu ao longo dos últimos anos o maior e mais eficiente aparato tecnológico para monitoramento digital, o chamado sistema de "crédito social". Por meio dele, consegue vigiar o comportamento de cada um do seu quase 1,4 bilhão de cidadãos. O sistema de "crédito social" chinês permite valorização e avaliação exaustiva das pessoas, atribuindo pontuação que gera uma espécie de ranking entre os chineses. Dependendo da quantidade de pontos que a pessoa atingir, pode ser punida ou recompensada[8]. Cada indivíduo é avaliado por sua conduta social e a vida cotidiana das pessoas é vigiada constantemente, em todos os aspectos. Atividades nas redes sociais são vigiadas, para censurar críticas ao regime. Quem transita pela rua também é vigiado. Um sistema de 200 milhões de câmeras de vigilância, dotadas de inteligência artificial, controla o movimento das pessoas. Drones também são utilizados para vigiar espaços públicos. Os provedores de serviços na Internet e de telefonia celular são obrigados a compartilhar os dados de seus usuários com os serviços de segurança do Governo. Na China não há nenhum momento da

---

predicted personal or personality characteristics, with the social score leading to either or both of the following:
(i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;
(ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity;

[8] Se a pontuação for boa, a pessoa recebe algumas recompensas sociais, como ter direito a matricular um filho numa boa escola. Já uma pontuação baixa pode impedir que uma pessoa se matricule na escola de sua preferência, que seja contratada para uma boa vaga de emprego ou impedida de viajar, por exemplo. Em 2018, segundo relatório divulgado pelo Centro de Informação do Crédito Público Nacional da China, 23 milhões de pessoas foram impedidas de viajar devido à pontuação baixa. Ver notícia publicada em 27.01.20, acessível em: https://www.poder360.com.br/internacional/entenda-o-sistema-de-credito-social-planejado-pela-china/

vida cotidiana que não esteja submetido a observação. Cada atividade é controlada. O Estado chinês sabe onde cada cidadão está, com quem se encontra, o que faz, o que compra, o que procura e para onde se dirige[9].

Ao estabelecer impedimento a sistemas de avaliação ou classificação da "confiabilidade" das pessoas, a partir do comportamento social ou características pessoais ou de personalidade conhecidas ou preditivas, a Comissão Europeia repudia o modelo adotado no conhecido "Sistema de Crédito Social" (SCS) chinês. A Comissão Europeia "envia uma clara mensagem à China de que o sistema de 'crédito social' é incompatível com democracias liberais", afirma Maroussia Lévesque, pesquisadora do *Berkman Klein Center* da Universidade Harvard[10].

A utilização de sistemas de pontuação por parte de governos é tida por inaceitável por conta do extremo risco que representa não somente para as pessoas mas para a sociedade de um modo geral. A utilização desses sistemas de controle comportamental por parte de governos viola direitos e garantias fundamentais das sociedades democráticas e é um primeiro passo para a construção de regime autoritário de vigilância (*authoritarian surveillance*).

Sistemas de vigilância biométrica

A proposta de Regulamento também veda a utilização por órgãos do Poder Público de sistemas de

---

[9] Conforme artigo de nossa autoria, publicado em março de 2020, sob o título "Como os países asiáticos utilizam a tecnologia para combater a epidemia do coronavírus - A transição do capitalismo de vigilância para a vigilância totalitária?", acessível em: https://jus.com.br/artigos/80616/como-os-paises-asiaticos-utilizam-a-tecnologia-para-combater-a-epidemia-do-coronavirus

[10] Conforme notícia publicada no site Politico, em 21.04.21, acessível em: https://www.politico.eu/article/europe-throws-down-gauntlet-on-ai-with-new-rulebook/

identificação biométrica remota[11] (como, p. ex., reconhecimento facial) em espaços públicos, salvo exceções previstas em lei. Em princípio, os sistemas de identificação biométrica de forma remota são vedados, em razão dos riscos inaceitáveis de violação a direitos fundamentais, só sendo admitidos nas seguintes situações: a) para busca de vítimas de crimes e crianças desaparecidas; b) para reprimir ameaça séria e iminente à vida ou integridade física de uma pessoa ou para prevenir ataques terroristas; c) para localizar indivíduos que tenham praticado crimes graves (art. 5°., 1, d)[12]. Somente delitos graves podem justificar a utilização de sistemas de IA de identificação biométrica para encontrar criminosos.

Essas três situações admitidas como exceções são rigidamente definidas e reguladas, a exemplo dos demais sistemas de "alto risco". Nessas situações excepcionais, o uso dos sistemas de identificação biométrica remota fica sujeito a prévio procedimento de avaliação e contínua fiscalização, para garantir o respeito aos direitos

---

[11] Nos termos da definição contida no art. 3°. (item 36), sistemas de identificação biométrica remota (*remote biometric identification system*) são os que permitem identificação de pessoas naturais a distância por meio da comparação dos dados biométricos da pessoa contidos em uma base de dados.

[12] Conforme o art. 5°., 1, d, de seguinte redação (no original, em inglês):
"Article 5
1. The following artificial intelligence practices shall be prohibited: […]
(d) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:
(i) the targeted search for specific potential victims of crime, including missing children;
(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;
(iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA62 and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State."

fundamentais das pessoas. A fim de garantir que esses sistemas sejam usados de maneira responsável e proporcional às situações de excepcionalidade, o Regulamento prevê que certos elementos devem ser levados em conta, nomeadamente no que diz respeito à natureza da situação que deu origem ao pedido, além da seriedade, probabilidade e gravidade do dano resultante pela não utilização da identificação biométrica, bem como as consequências da utilização para os direitos e liberdades das pessoas envolvidas (art. 5°., d)[13]. Além disso, a utilização do sistema fica sujeita a limites adequados de tempo e espaço, atendendo nomeadamente às provas ou indicações relativas às ameaças, às vítimas ou ao autor. O banco de dados de referência de pessoas deve ser apropriado para cada caso de uso em cada uma dessas três situações excepcionais[14].

Mesmo nesses casos, é exigida autorização judicial ou de autoridade administrativa competente, que deve avaliar se o uso do sistema de identificação

---

[13] Conforme o art. 5°., 2, de seguinte redação (no original, em inglês):
"Article 5
[...]
2. The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall take into account the following elements:
(a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;
(b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.
In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations."

[14] Conforme o art. 5°., 2, parte final, de seguinte redação (no original, em inglês):
"Article 5
"In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations."

biométrica remota é necessário e proporcional para atender à situação de excepcionalidade (uma das três especificadas no art. 5°., n.° 1, alínea d)[15]. Somente em casos de urgência, o uso do sistema pode ser iniciado antes da obtenção da autorização judicial ou administrativa. Em tais hipóteses de urgência, o uso deve ser restrito ao mínimo absolutamente necessário e estar sujeito a salvaguardas e condições adequadas, predispostas na legislação interna dos Estados-membros, devendo a autoridade policial obter a autorização o mais rapidamente possível, apresentando as razões de não ter podido fazê-lo mais cedo[16].

O uso de sistemas de reconhecimento facial para vigilância em massa, em locais públicos, já tem sido vedado por diversos países (alguns integrantes da UE), por se tratar de tecnologia particularmente intrusiva, que pode afetar a vida privada de grande parcela da população e submeter as pessoas a uma constante vigilância, o que indiretamente pode dissuadi-las do exercício de liberdades individuais.

---

[15] Conforme o art. 5°., 3, de seguinte redação (no original, em inglês):
"Article 5
[...]
3. As regards paragraphs 1, point (d) and 2, each individual use for the purpose of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 4. However, in a duly justified situation of urgency, the use of the system may be commenced without an authorisation and the authorisation may be requested only during or after the use.
The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2."

[16] Conforme "Considerando" n. 21.

Em junho de 2020, a IBM anunciou que não mais iria pesquisar e desenvolver tecnologias de reconhecimento facial, alegando riscos à privacidade das pessoas e possíveis injustiças na utilização por forças policiais. Em carta ao Congresso dos EUA, o presidente da empresa afirmou que se opõe ao uso da tecnologia para monitoramento e vigilância em massa[17]. No dia seguinte foi a vez de a Amazon anunciar moratória de um ano para uso do seu software de reconhecimento facial "Rekognition", por autoridades policiais. A Amazon afirmou que vai aguardará as autoridades regulamentarem o uso da tecnologia, cuja utilização ficará limitada a organizações civis para resgate de vítimas de tráfico de pessoas ou crianças desaparecidas[18].

Ao fazer a apresentação da proposta de regulamento da Comissão Europeia, a Comissária Europeia para a Economia e Sociedade Digital, Margrethe Vestager, afirmou ser importante a proibição do uso de reconhecimento facial para identificar pessoas em tempo real no meio de uma multidão, pois "não há espaço para a vigilância em massa em nossa sociedade"[19].

Recife, 17 de maio de 2021.

---

[17] Ver notícia publicada no site G1, em 09.06.20, acessível em: https://g1.globo.com/economia/tecnologia/noticia/2020/06/09/ibm-encerra-area-de-pesquisa-em-reconhecimento-facial-e-pede-reforma-da-policia.ghtml

[18] Ver notícia publicada no site G1, em 10.06.20, acessível em: https://g1.globo.com/economia/tecnologia/noticia/2020/06/10/amazon-proibe-uso-de-sua-tecnologia-de-reconhecimento-facial-pela-policia-por-um-ano.ghtml

[19] Conforme notícia publicada no site Politico, em 21.04.21, acessível em: https://www.politico.eu/article/europe-throws-down-gauntlet-on-ai-with-new-rulebook/