COMISSÃO
EUROPEIA

Bruxelas, 19.2.2020
COM(2020) 64 final

RELATÓRIO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO E AO COMITÉ ECONÓMICO E SOCIAL EUROPEU

Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da Internet das coisas e da robótica

RELATÓRIO SOBRE AS IMPLICAÇÕES EM MATÉRIA DE SEGURANÇA E DE RESPONSABILIDADE DECORRENTES DA INTELIGÊNCIA ARTIFICIAL, DA INTERNET DAS COISAS E DA ROBÓTICA

1. Introdução

A inteligência artificial[1], a Internet das coisas[2] e a robótica criarão novas oportunidades e benefícios para a sociedade. A Comissão reconheceu a importância e o potencial destas tecnologias e a necessidade de investir significativamente nestes domínios[3], estando empenhada em tornar a Europa num líder mundial nos mesmos. Para tal, urge criar um quadro jurídico claro e previsível que dê resposta aos desafios tecnológicos.

1.1. Quadro vigente em matéria de segurança e de responsabilidade

O objetivo geral dos quadros jurídicos em matéria de segurança e de responsabilidade é assegurar que todos os produtos e serviços, incluindo os que integram novas tecnologias digitais, funcionam de forma segura, fiável e coerente e que os danos ocorridos são reparados de forma eficiente. A garantia de níveis elevados de segurança em todos os produtos e sistemas que integram novas tecnologias digitais e a existência de mecanismos sólidos de reparação de danos (ou seja, o quadro em matéria de responsabilidade) contribuem para uma melhor proteção dos consumidores. Além disso, promovem a confiança nestas tecnologias, uma condição prévia à sua adoção por parte da indústria e dos utilizadores. Por sua vez, isso favorecerá a competitividade da indústria europeia e contribuirá para a consecução dos objetivos da União[4]. A importância de um quadro claro em matéria de segurança e de responsabilidade, que vise assegurar a proteção dos consumidores e a segurança jurídica para as empresas, torna-se especialmente evidente perante a emergência de novas tecnologias como a inteligência artificial, a Internet das coisas e a robótica.

A União dispõe de um quadro regulamentar sólido e fiável em matéria de segurança e de responsabilidade pelos produtos, bem como de um conjunto sólido de normas de segurança, ambos complementados por legislação acional não harmonizada em matéria de responsabilidade. Em conjunto, estes instrumentos asseguram o bem-estar dos cidadãos no mercado único e incentivam a inovação e a adoção de tecnologias. No entanto, a inteligência artificial, a Internet das coisas e a robótica estão a transformar as características de muitos produtos e serviços.

A Comissão anunciou na sua Comunicação sobre a inteligência artificial para a Europa[5], adotada em 25 de abril de 2018, que publicaria um relatório de avaliação das implicações

---

1 O Grupo de Peritos de Alto Nível em Inteligência Artificial elaborou uma definição do conceito, disponível no seguinte endereço: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines.

2 A União Internacional das Telecomunicações incluiu uma definição de Internet das coisas na sua Recomendação ITU-T Y.2060, disponível no seguinte endereço: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060.

3 SWD(2016) 110, COM(2017) 9, COM(2018) 237 e COM(2018) 795.

4 http://ec.europa.eu/growth/industry/policy_pt.

5 https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=COM%3A2018%3A237%3AFIN.
O documento de trabalho dos serviços da Comissão que acompanha esta comunicação [SWD(2018) 137, disponível no endereço: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137]

para os quadros vigentes em matéria de segurança e de responsabilidade, decorrentes das novas tecnologias digitais. O presente relatório visa identificar e analisar as implicações mais abrangentes para os quadros regulamentares em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da Internet das coisas e da robótica, bem como eventuais lacunas dos mesmos. As orientações que constam do presente relatório, que acompanha o Livro Branco sobre a Inteligência Artificial, visam contribuir para o debate e fazem parte de um processo mais amplo de consulta das partes interessadas. A secção dedicada à segurança baseia-se na avaliação[6] da Diretiva Máquinas[7] e no trabalho com os grupos de peritos pertinentes neste domínio[8]. A secção dedicada à responsabilidade baseia-se na avaliação[9] da Diretiva Responsabilidade pelos Produtos[10], no contributo dos grupos de peritos pertinentes neste domínio[11] e em contactos com as partes interessadas. O objetivo do presente relatório não passa por apresentar uma panorâmica exaustiva das regras vigentes em matéria de segurança e de responsabilidade, mas antes por destacar as principais questões identificadas até à data.

1.2. Características da inteligência artificial, da Internet das coisas e da robótica

A inteligência artificial, a Internet das coisas e a robótica partilham muitas características. Todas estas tecnologias conseguem combinar **conectividade**, **autonomia** e **dependências de dados** para desempenharem tarefas com pouca ou nenhuma supervisão ou controlo humano. Os sistemas que integram inteligência artificial são também capazes de melhorar o seu próprio desempenho graças à aprendizagem com a experiência. A sua **complexidade** reflete-se, por um lado, na pluralidade de agentes económicos envolvidos na **cadeia de abastecimento** e, por outro, na multiplicidade de componentes, peças, *software*, sistemas e serviços que, em conjunto, dão forma aos novos ecossistemas tecnológicos, a que acresce a **abertura** destas tecnologias a atualizações de vária ordem após a sua colocação no mercado. As grandes quantidades de dados envolvidos, a dependência de algoritmos e a **opacidade** do processo decisório dos sistemas de inteligência artificial tornam mais difícil prever o comportamento de produtos com inteligência artificial e compreender as possíveis causas de um dano. Por último, a conectividade e a abertura podem igualmente expor produtos da Internet das coisas ou baseados na inteligência artificial a **ciberameaças**.

---

apresenta um primeiro levantamento dos desafios em matéria de responsabilidade surgidos no contexto das novas tecnologias digitais.

6 SWD(2018) 161 final.

7 Diretiva 2006/42/CE.

8 Rede de Segurança dos Consumidores, estabelecida pela Diretiva 2001/95/CE, relativa à segurança geral dos produtos, e grupos de peritos criados no âmbito da Diretiva 2006/42/CE, relativa às máquinas, e da Diretiva 2014/53/UE, relativa aos equipamentos de rádio, compostos por representantes dos Estados-Membros, da indústria e de outras partes interessadas, tais como associações de consumidores.

9 COM(2018) 246 final.

10 Diretiva 85/374/CEE.

11 O Grupo de Peritos em Responsabilidade e Novas Tecnologias foi criado para munir a Comissão de conhecimentos especializados sobre a aplicabilidade da Diretiva Responsabilidade pelos Produtos e das regras nacionais em matéria de responsabilidade civil e para a apoiar na elaboração de princípios orientadores de eventuais adaptações de atos legislativos em vigor relacionados com novas tecnologias. O grupo está dividido em dois subgrupos: o Subgrupo para a Responsabilidade pelos Produtos e o Subgrupo para as Novas Tecnologias. Consultar o seguinte endereço: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1.
O relatório *Liability for Artificial Intelligence and other emerging technologies*, elaborado pelo Subgrupo para as Novas Tecnologias, encontra-se disponível no seguinte endereço: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

1.3. Oportunidades criadas pela inteligência artificial, pela Internet das coisas e pela robótica

O aumento da confiança dos utilizadores e da aceitação social de novas tecnologias, a melhoria de produtos, processos e modelos empresariais e a contribuição para o aumento da eficiência dos fabricantes europeus são apenas algumas das oportunidades criadas pela inteligência artificial, pela Internet das coisas e pela robótica.

Além da produtividade e dos ganhos de eficiência, a inteligência artificial traz consigo a promessa de permitir aos seres humanos explorar níveis de conhecimento nunca alcançados, abrindo as portas a novas descobertas e ajudando a resolver alguns dos maiores desafios mundiais: do tratamento de doenças crónicas ao combate contra as alterações climáticas, passando pela previsão de surtos de doença, pela redução das taxas de mortalidade em acidentes de viação ou pela prevenção de ameaças à cibersegurança.

Estas tecnologias podem trazer muitos benefícios graças à melhoria da segurança dos produtos, tornando-os menos propensos a certos riscos. Por exemplo, a conectividade e a automatização dos veículos podem melhorar a segurança rodoviária, visto que a maioria dos acidentes de viação são causados por erro humano[12]. Além disso, os sistemas da Internet das coisas são concebidos para receber e processar grandes quantidades de dados provenientes de diversas fontes. Este aumento do nível de informação pode ser utilizado para que os produtos sejam capazes de se autoadaptar e, consequentemente, de se tornarem mais seguros. As novas tecnologias podem contribuir para uma maior eficácia na recolha de produtos, por exemplo, fazendo com que estes sejam capazes de avisar os utilizadores com o intuito de evitar problemas de segurança[13]. Se surgir um problema de segurança durante a utilização de um produto conectado, o produtor em causa pode comunicar diretamente com os utilizadores para os avisar sobre os riscos e, se possível, para resolver diretamente o problema, fornecendo, por exemplo, uma atualização de segurança. Um caso ilustrativo é o de um fabricante de telemóveis inteligentes que, durante a recolha de um dos seus produtos, em 2017, realizou uma atualização de *software* que reduziu a zero a capacidade da bateria dos telemóveis a recolher[14], para que os utilizadores cessassem a utilização desses aparelhos perigosos.

Além disso, as novas tecnologias podem contribuir para melhorar a rastreabilidade dos produtos. Por exemplo, as funções de conectividade da Internet das coisas podem permitir às empresas e às autoridades de fiscalização do mercado detetar produtos perigosos e identificar riscos nas cadeias de abastecimento[15].

Em paralelo com as oportunidades que podem gerar para a economia e a sociedade, a inteligência artificial, a Internet das coisas e a robótica podem igualmente comportar um risco associado de danos, materiais e imateriais, sobre interesses juridicamente protegidos. Esse risco aumentará à medida que os domínios de aplicação destas tecnologias se forem

---

[12] Estima-se que cerca de 90 % dos acidentes rodoviários são causados por erro humano. Ver relatório da Comissão intitulado «Salvar Vidas: reforçar a segurança dos veículos na UE» [COM(2016) 787 final].

[13] Por exemplo, o condutor de um automóvel pode receber um aviso para abrandar se tiver ocorrido um acidente na estrada.

[14] OCDE, «Measuring and maximising the impact of product recalls globally: OECD workshop report», *OECD Science, Technology and Industry Policy Papers*, n.º 56, OECD Publishing, Paris, 2018. Disponível no seguinte endereço: https://doi.org/10.1787/ab757416-en.

[15] OCDE, «Enhancing product recall effectiveness globally: OECD background report», *OECD Science, Technology and Industry Policy Papers*, n.º 58, OECD Publishing, Paris, 2018. Disponível no seguinte endereço: https://doi.org/10.1787/ef71935c-en.

alargando. Neste contexto, é essencial determinar se, e em que medida, o atual quadro jurídico em matéria de segurança e de responsabilidade continua a ser adequado para proteger os utilizadores.

2. Segurança

A Comissão declarou, na sua comunicação intitulada «Aumentar a confiança numa inteligência artificial centrada no ser humano», que ***os sistemas de IA*** [inteligência artificial] ***devem integrar mecanismos de proteção e de segurança desde a conceção para garantir que são comprovadamente seguros em todas as fases****, tendo em conta a* ***segurança física e mental*** *de todas as partes envolvidas*[16].

A análise da legislação da União em matéria de segurança dos produtos, apresentada na presente secção, visa examinar se o atual quadro legislativo da União contém os elementos necessários para assegurar que as novas tecnologias, em especial os sistemas de inteligência artificial, integram a proteção e a segurança desde a conceção.

O presente relatório incide principalmente na Diretiva Segurança Geral dos Produtos[17] e na legislação harmonizada no domínio dos produtos que segue as regras horizontais da «Nova Abordagem»[18] e/ou do «Novo Quadro Legislativo» (a seguir designado por «legislação» ou «quadro da União em matéria de segurança dos produtos»)[19]. As regras horizontais garantem a coerência entre as regras setoriais em matéria de segurança dos produtos.

A legislação da União em matéria de segurança dos produtos visa garantir que os produtos colocados no mercado da União cumprem elevados requisitos ambientais, sanitários e de segurança, e podem circular livremente em toda a União. A legislação setorial[20] é complementada pela Diretiva Segurança Geral dos Produtos[21], que obriga a que todos os bens de consumo, mesmo os não abrangidos pela legislação setorial da União, sejam seguros. As normas de segurança são complementadas pela fiscalização do mercado e pelos poderes conferidos às autoridades nacionais nos termos do Regulamento Fiscalização do Mercado[22] e da Diretiva Segurança Geral dos Produtos[23]. No domínio dos transportes, existem regras adicionais a nível nacional e da União, relativas à entrada em serviço de veículos a motor[24],

---

16 Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões — Aumentar a confiança numa inteligência artificial centrada no ser humano, Bruxelas, 8.4.2019 [COM(2019) 168 final].

17 Diretiva 2001/95/CE do Parlamento Europeu e do Conselho, de 3 de dezembro de 2001, relativa à segurança geral dos produtos (JO L 11 de 15.1.2002, p. 4).

18 JO C 136 de 4.6.1985, p. 1.

19 Regulamento (CE) n.º 765/2008 e Decisão n.º 768/2008/CE.

20 Este esquema não inclui a legislação da União em matéria de transportes e de automóveis.

21 Diretiva 2001/95/CE do Parlamento Europeu e do Conselho, de 3 de dezembro de 2001, relativa à segurança geral dos produtos (JO L 11 de 15.1.2002, p. 4).

22 Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, de 9 julho de 2008, que estabelece os requisitos de acreditação e fiscalização do mercado relativos à comercialização de produtos, e que revoga o Regulamento (CEE) n.º 339/93 (JO L 218 de 13.8.2008, p. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj) e, de 2021 em diante, Regulamento (UE) 2019/1020 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativo à fiscalização do mercado e à conformidade dos produtos e que altera a Diretiva 2004/42/CE e os Regulamentos (CE) n.º 765/2008 e (UE) n.º 305/2011 (JO L 169 de 25.6.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/1020/oj).

23 Artigo 8.º, n.º 1, alínea b), e n.º 3, da Diretiva Segurança Geral dos Produtos.

24 Por exemplo, a Diretiva 2007/46/CE, que estabelece um quadro para a homologação dos veículos a motor e seus reboques, e dos sistemas, componentes e unidades técnicas destinados a serem utilizados nesses

aeronaves ou navios, bem como regras claras relativas à segurança operacional, incluindo a atribuição de tarefas aos operadores e de funções de fiscalização às autoridades.

As normas europeias são igualmente um elemento essencial da legislação da União em matéria de segurança dos produtos. Dada a natureza global da digitalização e das novas tecnologias digitais, a cooperação internacional no domínio da normalização é particularmente importante para a competitividade da indústria europeia.

O quadro da União em matéria de segurança dos produtos foi, em grande parte, estabelecido antes da emergência de tecnologias digitais como a inteligência artificial, a Internet das coisas ou a robótica, pelo que nem sempre contém disposições explícitas relativas aos novos desafios e riscos a elas associados. No entanto, o facto de o atual quadro em matéria de segurança dos produtos ser neutro do ponto de vista tecnológico não impede que o mesmo se possa aplicar a produtos que incorporem estas tecnologias. Além disso, certos atos legislativos subsequentes que fazem parte do referido quadro, como os referentes aos dispositivos médicos ou ao setor dos automóveis, já foram redigidos tendo em conta alguns aspetos da emergência de tecnologias digitais, tais como as decisões automatizadas, o *software* como produto autónomo e a conectividade.

Lógica subjacente à atual legislação da União em matéria de segurança dos produtos[25]

As páginas que se seguem enumeram os desafios colocados pelas novas tecnologias digitais ao quadro da União em matéria de segurança dos produtos.

A **conectividade** é uma característica fundamental de cada vez mais produtos e serviços. Esta funcionalidade põe em causa o conceito tradicional de segurança, visto que pode comprometer direta e indiretamente a segurança dos produtos, quando os expõe à pirataria

veículos, e o Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, relativo à homologação e à fiscalização do mercado dos veículos a motor e seus reboques, e dos sistemas, componentes e unidades técnicas destinados a esses veículos, que altera os Regulamentos (CE) n.º 715/2007 e (CE) n.º 595/2009 e revoga a Diretiva 2007/46/CE.

[25] A figura apresentada não inclui os requisitos da legislação relativa ao ciclo de vida dos produtos, ou seja, à sua utilização e manutenção, e serve apenas para dar uma visão geral.

informática, abrindo caminho para ameaças à segurança do produto e afetando a segurança dos utilizadores.

A Islândia apresentou uma notificação no Sistema de Troca Rápida de Informação da UE, relativa a um relógio inteligente para crianças[26], que constitui um exemplo desta realidade. O produto em questão não causaria danos diretos às crianças que o usassem, mas, visto não cumprir um nível mínimo de segurança, poderia ser facilmente utilizado como um instrumento de acesso a essas crianças. Uma vez que uma das funções previstas do produto era manter as crianças seguras graças a um sistema de localização, os consumidores esperariam que este não colocasse ameaças passíveis de afetar a segurança dessas mesmas crianças, nomeadamente a possibilidade de estas serem localizadas e/ou contactadas por qualquer pessoa.

A Alemanha apresentou uma outra notificação ilustrativa desta questão, referente a um automóvel de passageiros[27]. O *software* do rádio do veículo pode ter determinadas falhas de segurança que permitem o acesso não autorizado de terceiros aos sistemas de controlo interligados do veículo. Se estas falhas de segurança do *software* fossem exploradas por um terceiro mal-intencionado, poderia ocorrer um acidente de viação.

As aplicações industriais também podem ser expostas a ciberameaças que afetem a segurança das pessoas em larga escala, se não cumprirem os níveis adequados de segurança. Tal seria o caso de ciberataques a um sistema de controlo crítico de uma instalação industrial, destinados a desencadear uma explosão suscetível de causar a perda de vidas.

De um modo geral, a legislação da União em matéria de segurança dos produtos não prevê requisitos essenciais obrigatórios especificamente destinados a combater ciberameaças que afetem a segurança dos utilizadores. No entanto, o Regulamento Dispositivos Médicos[28], a Diretiva Instrumentos de Medição[29], a Diretiva Equipamentos de Rádio[30] e a legislação relativa à homologação de veículos[31] incluem disposições relativas a aspetos de segurança. O Regulamento Cibersegurança[32] estabelece um enquadramento para a certificação voluntária da cibersegurança de produtos, serviços e processos das tecnologias da informação e da comunicação, ao passo que a legislação da União em matéria de segurança dos produtos estabelece requisitos obrigatórios.

Além disso, o risco de perda de conectividade das novas tecnologias digitais pode igualmente acarretar riscos de segurança. Por exemplo, se um alarme de incêndio conectado perder a sua ligação, pode não alertar o utilizador quando necessário.

Na atual legislação da União em matéria de segurança dos produtos, a segurança é um objetivo de ordem pública, cujo conceito se encontra associado à utilização do produto e aos riscos, por exemplo mecânicos, elétricos ou outros, que devem ser tidos em conta a fim de

[26] Notificação RAPEX da Islândia, publicada no sítio Web «Safety Gate» da UE (A12/0157/19).
[27] Notificação RAPEX da Alemanha, publicada no «Safety Gate» da UE (A12/1671/15).
[28] Regulamento (UE) 2017/745 relativo aos dispositivos médicos.
[29] Diretiva 2014/32/UE respeitante à disponibilização no mercado de instrumentos de medição.
[30] Diretiva 2014/53/UE respeitante à disponibilização de equipamentos de rádio.
[31] Diretiva 2007/46/CE que estabelece um quadro para a homologação dos veículos a motor e seus reboques, e dos sistemas, componentes e unidades técnicas destinados a serem utilizados nesses veículos. A diretiva será revogada e substituída pelo Regulamento (UE) 2018/858, relativo à homologação e à fiscalização do mercado dos veículos a motor e seus reboques, e dos sistemas, componentes e unidades técnicas destinados a esses veículos, que altera os Regulamentos (CE) n.º 715/2007 e (CE) n.º 595/2009 e revoga a Diretiva 2007/46/CE, com efeitos a partir de 1 de setembro de 2020.
[32] Regulamento (UE) 2019/881.

tornar o produto seguro. É importante ter em conta que, consoante o ato legislativo da União em matéria de segurança dos produtos, o conceito de utilização do produto abrange não só a utilização prevista, mas também a utilização previsível e, em alguns casos, como a Diretiva Máquinas[33], até mesmo uma má utilização, razoavelmente previsível, do produto.

O conceito de segurança consagrado na atual legislação da União em matéria de segurança dos produtos está em consonância com um conceito alargado de segurança que permita proteger consumidores e utilizadores. Assim, este conceito abrange a proteção contra todos os tipos de riscos associados aos produtos, não só de natureza mecânica, química ou elétrica, mas também ao nível da cibersegurança e da perda de conectividade dos dispositivos.

A este respeito, poderão ser equacionadas disposições explícitas a acrescentar ao conjunto de atos legislativos pertinentes da União, com vista a assegurar uma melhor proteção dos utilizadores e maior segurança jurídica.

A **autonomia**[34] é uma das principais características da inteligência artificial, cujos resultados não intencionais podem causar danos aos utilizadores e a pessoas expostas.

O quadro da União em matéria de segurança dos produtos já impõe aos produtores a obrigação de ter em conta, na avaliação dos riscos, a «utilização»[35] dada aos produtos ao longo da vida útil dos mesmos, o que abrange o futuro «comportamento» dos produtos com inteligência artificial, passível de ser determinado por antecipação durante a avaliação dos riscos realizada pelos fabricantes antes da colocação desses produtos no mercado. O quadro prevê igualmente que os fabricantes forneçam instruções e informações ou advertências de segurança aos utilizadores[36]. Neste contexto, a Diretiva Equipamentos de Rádio[37], por exemplo, exige que os fabricantes forneçam instruções que incluam as informações necessárias para a utilização dos equipamentos de rádio de acordo com os fins previstos.

Podem também surgir situações em que seja impossível determinar previamente, na totalidade, os resultados dos sistemas de inteligência artificial. Em tais casos, a avaliação dos riscos realizada antes da colocação do produto no mercado deixa de contemplar a utilização, o funcionamento ou o comportamento do mesmo. Sempre que a utilização do produto inicialmente prevista pelo fabricante é alterada[38] em resultado do comportamento autónomo,

---

33 Diretiva 2006/42/CE relativa às máquinas.

34 Embora os produtos com inteligência artificial possam agir de forma autónoma em função da leitura que fazem do meio em que se encontram, sem que sigam um conjunto predeterminado de instruções, o seu comportamento está limitado pelo objetivo que lhes foi atribuído e por outras escolhas de conceção determinantes tomadas por quem os desenvolveu.

35 De acordo com a legislação da União em matéria de segurança dos produtos, os produtores realizam a avaliação dos riscos com base na utilização prevista, na utilização previsível e na má utilização razoavelmente previsível do produto.

36 Decisão n.º 768/2008/CE do Parlamento Europeu e do Conselho, de 9 de julho de 2008, relativa a um quadro comum para a comercialização de produtos, e que revoga a Decisão 93/465/CEE (JO L 218 de 13.8.2008, p. 82). Anexo I, artigo R2, n.º 7: «*[o]s fabricantes devem assegurar que o produto é acompanhado de instruções e informações de segurança numa língua que possa ser facilmente compreendida pelos consumidores e outros utilizadores finais, de acordo com o que o Estado-Membro em questão decidir*».

37 Artigo 10.º, n.º 8, relativo às instruções para o utilizador final, e anexo VI, relativo à declaração UE de conformidade.

38 Por ora, o termo «autoaprendizagem» é usado no contexto da inteligência artificial sobretudo para indicar que as máquinas são capazes de aprender durante a fase de treino, não sendo, para já, necessário que o continuem a fazer depois de começarem a ser utilizadas. Pelo contrário, em especial no setor dos cuidados de saúde, as máquinas com inteligência artificial param de aprender, por norma, logo que a sua fase de treino é

ao ponto de afetar a conformidade com os requisitos de segurança, poderá ser necessário requerer uma nova avaliação do produto com autoaprendizagem[39].

Nos termos do atual quadro, os produtores que tomem conhecimento de que um produto apresenta riscos em termos de segurança ao longo do seu ciclo de vida já são obrigados a informar imediatamente as autoridades competentes e a tomar medidas no sentido de prevenir os riscos para os utilizadores[40].

Além da avaliação dos riscos realizada antes da colocação de um produto no mercado, pode efetuar-se outra avaliação dos riscos com exposição desse produto a alterações significativas ao longo da sua vida útil, por exemplo, a utilização para uma função diferente, não prevista pelo fabricante na avaliação dos riscos inicial. Essa avaliação deve incidir sobre o impacto na segurança causado pelo comportamento autónomo ao longo da vida útil do produto e ser realizada pelo agente económico adequado. Ademais, os atos legislativos pertinentes da União poderão incluir um reforço das obrigações dos fabricantes em matéria de instruções e advertências para os utilizadores.

A legislação em matéria de transportes já exige avaliações dos riscos semelhantes[41]. Por exemplo, a legislação relativa ao transporte ferroviário prevê que, se um veículo ferroviário for modificado após a sua certificação, o autor dessa modificação é obrigado a seguir um procedimento específico, estando definidos critérios claros para determinar se autoridade competente deve ser envolvida ou não nesse procedimento.

A função de autoaprendizagem dos produtos e sistemas dotados de inteligência artificial pode levar a que as máquinas tomem decisões que se desviam do inicialmente previsto pelos produtores e, consequentemente, daquilo que os utilizadores esperam. Esta situação levanta questões sobre o controlo humano e a possibilidade de as pessoas escolherem se, e de que modo, desejam delegar decisões em produtos e sistemas dotados de inteligência artificial, com vista a alcançar objetivos definidos por seres humanos[42]. A atual legislação da União em matéria de segurança dos produtos não se refere explicitamente à supervisão humana no contexto dos produtos e sistemas dotados de inteligência artificial com autoaprendizagem[43].

---

concluída com sucesso. Assim, no estado atual, o comportamento autónomo evidenciado por sistemas de inteligência artificial não implica que o produto desempenhe tarefas não previstas por quem o desenvolveu.

39 Em conformidade com o ponto 2.1 do «Guia Azul de 2016 sobre a Aplicação das Regras da UE em matéria de Produtos».

40 Artigo 5.º da Diretiva 2001/95/CE do Parlamento Europeu e do Conselho, de 3 de dezembro de 2001, relativa à segurança geral dos produtos.

41 O procedimento a seguir em caso de qualquer alteração do sistema ferroviário suscetível de ter impactos a nível da segurança (por exemplo alterações técnicas ou operacionais, ou ainda alterações organizativas que afetem os processos operacionais ou de manutenção) é descrito no anexo I do Regulamento de Execução (UE) 2015/1136 da Comissão (JO L 185 de 14.7.2015, p. 6).
Em caso de «alteração significativa», um «organismo de avaliação» independente (que pode ser a autoridade nacional de segurança ou outra autoridade competente em termos técnicos) deve apresentar um relatório de avaliação da segurança ao proponente da alteração.
Na sequência do processo de análise dos riscos, o proponente da alteração aplicará as medidas adequadas para atenuar os riscos (se o proponente for uma empresa ferroviária ou um gestor de infraestrutura, a aplicação do regulamento faz parte do seu sistema de gestão da segurança, cuja aplicação é, por sua vez, supervisionada pela autoridade nacional de segurança).

42 *Policy and Investment Recommendations for Trustworthy AI*, Grupo de Peritos de Alto Nível em Inteligência Artificial, junho de 2019.

43 Tal não exclui, no entanto, a necessidade de supervisão em situações específicas, decorrente de algumas das obrigações mais gerais aplicáveis à colocação do produto no mercado.

Os atos legislativos pertinentes da União poderão prever, como salvaguarda, requisitos específicos em termos de supervisão humana desde a fase de conceção até ao final do ciclo de vida de produtos e sistemas dotados de inteligência artificial.

O futuro «comportamento» das aplicações de inteligência artificial poderá dar origem a **riscos para a saúde mental**[44] dos utilizadores, decorrentes, por exemplo, da sua colaboração com robôs ou sistemas de inteligência artificial humanoides, em contexto doméstico ou profissional. Note-se, a este respeito, que, hoje em dia, o termo segurança se refere geralmente à perceção, por parte do utilizador, de ameaças físicas que possam advir das novas tecnologias digitais. Simultaneamente, o quadro jurídico da União define produtos seguros como aqueles que não apresentam riscos, ou que apresentam apenas riscos mínimos, para a segurança e a saúde das pessoas. É comummente aceite que a definição de saúde inclui o bem-estar físico e mental. Porém, os riscos para a saúde mental deverão estar explicitamente abrangidos pelo conceito de segurança dos produtos consagrado no quadro legislativo.

Por exemplo, as funções de autonomia não podem provocar ansiedade e desconforto excessivos durante períodos prolongados nem afetar a saúde mental. A este respeito, considera-se que os fatores que favorecem a sensação de segurança dos idosos[45] são os seguintes: manutenção de relações estáveis com o pessoal que presta cuidados de saúde, capacidade de decisão sobre as rotinas diárias e informação sobre estas últimas. Os fabricantes de robôs que interagem com idosos devem ter estes fatores em consideração, a fim de prevenirem os riscos para a saúde mental.

A este respeito, poderão ser equacionadas disposições explícitas, a acrescentar ao conjunto de atos legislativos pertinentes da União, que obriguem os produtores, por exemplo, de robôs humanoides providos de inteligência artificial a ter em conta os danos imateriais que os seus produtos podem causar nos utilizadores, em especial os mais vulneráveis, como os idosos integrados em ambientes de prestação de cuidados de saúde.

Outra característica essencial dos produtos e sistemas dotados de inteligência artificial é a **dependência de dados**. A exatidão e a pertinência dos dados são fatores essenciais para assegurar que os produtos e sistemas dotados de inteligência artificial tomam decisões em conformidade com o previsto pelo produtor.

A legislação da União em matéria de segurança dos produtos não se refere de forma explícita aos riscos para a segurança decorrentes de dados deficientes. No entanto, em função da «utilização» do produto, os produtores devem prever, durante as fases de conceção e ensaio, a exatidão e a pertinência dos dados para efeitos das funções de segurança.

Por exemplo, a capacidade de reconhecimento de um sistema concebido com inteligência artificial para detetar objetos específicos pode ser afetada por condições de iluminação deficiente, pelo que os responsáveis pela conceção devem incluir dados provenientes de ensaios do produto em condições normais e insuficientes de iluminação.

---

[44] Constituição da Organização Mundial de Saúde, primeiro ponto: *a saúde é um estado de completo bem-estar físico, mental e social, e não a mera ausência de doença ou enfermidade* (https://www.who.int/about/who-we-are/constitution).

[45] Akalin, N., Kristoffersson, A., Loutfi, A., «Evaluating the Sense of Safety and Security in Human–Robot Interaction with Older People», *Social Robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction*, Springer, julho de 2019, p. 237-264.

Um outro exemplo são os robôs agrícolas, como os utilizados na colheita de fruta, que são concebidos para detetar e localizar frutos maduros em árvores ou no solo. Embora os algoritmos desenvolvidos já apresentem taxas de sucesso na classificação superiores a 90 %, uma deficiência nos conjuntos de dados que alimentam esses algoritmos pode levar os robôs a tomarem más decisões e, consequentemente, a ferirem animais ou pessoas.

Neste cenário, coloca-se a questão de saber se a legislação da União em matéria de segurança dos produtos deve conter requisitos específicos relativos aos riscos para a segurança decorrentes de dados deficientes na fase de conceção, bem como a mecanismos destinados a assegurar a manutenção da qualidade dos dados ao longo da utilização dos produtos e sistemas com inteligência artificial.

A **opacidade** é outra característica essencial de alguns produtos e sistemas dotados de inteligência artificial, que pode resultar da capacidade destes melhorarem o seu desempenho graças à aprendizagem com a experiência. Os produtos e sistemas dotados de inteligência artificial podem apresentar diferentes níveis de opacidade, em função da abordagem metodológica escolhida. Essa opacidade pode dificultar a compreensão do processo de tomada de decisão do sistema (o chamado «efeito de caixa negra»). Talvez não seja necessário compreender todos os passos do processo decisório, mas, à medida que os algoritmos de inteligência artificial se tornam cada vez mais avançados e são utilizados em domínios críticos, é imperativo criar condições que permitam aos seres humanos compreender o que levou o sistema a tomar determinadas decisões algorítmicas. Isso seria particularmente importante para efeitos do mecanismo *ex post* de fiscalização, pois daria às autoridades a possibilidade de identificarem responsáveis pelos comportamentos e escolhas dos sistemas de inteligência artificial. A Comissão reconheceu igualmente essa importância na sua comunicação intitulada «Aumentar a confiança numa inteligência artificial centrada no ser humano»[46].

A legislação da União em matéria de segurança dos produtos não se refere de forma explícita aos riscos crescentes que decorrem da opacidade dos sistemas baseados em algoritmos, pelo que é necessário equacionar requisitos em matéria de transparência dos algoritmos, bem como de robustez, responsabilização e, quando pertinente, supervisão humana e resultados não enviesados[47], que serão particularmente importantes para efeitos do mecanismo *ex post* de fiscalização e para aumentar a confiança na utilização dessas tecnologias. Uma das formas de responder a este desafio seria impor aos responsáveis pelo desenvolvimento dos algoritmos a obrigação de divulgar os parâmetros de conceção e os metadados dos conjuntos de dados, em caso de acidente.

Entre os riscos adicionais suscetíveis de afetar a segurança encontram-se os decorrentes da **complexidade dos produtos e sistemas**, que resultam da variedade de componentes, dispositivos e produtos que podem estar integrados, influenciando-se mutuamente (por exemplo, os produtos que integram sistemas domésticos inteligentes).

O quadro jurídico da UE em matéria de segurança referido no início da presente secção[48] já aborda esta complexidade, nomeadamente, quando estabelece que os produtores realizam a

[46] https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top.

[47] Com base nos requisitos essenciais que o Grupo de Peritos de Alto Nível propôs nas suas «Orientações éticas para uma IA de confiança», disponíveis no seguinte endereço: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines.

[48] Regulamento (CE) n.º 765/2008, Decisão n.º 768/2008/CE e legislação setorial harmonizada em matéria de segurança dos produtos, por exemplo a Diretiva 2006/42/CE relativa às máquinas.

avaliação dos riscos tendo em conta a utilização prevista, a utilização previsível e, se aplicável, a má utilização razoavelmente previsível do produto.

Neste contexto, **se o produtor antecipar que o seu dispositivo será conectado e interagirá com outros dispositivos, tal deve ser tido em conta durante a avaliação dos riscos**. As utilizações, corretas e incorretas, são determinadas com base, por exemplo, na experiência de utilização anterior de produtos do mesmo tipo, em investigações de acidentes ou no conhecimento sobre o comportamento humano.

A complexidade dos sistemas é igualmente abordada de forma mais específica por legislação setorial em matéria de segurança, como o Regulamento Dispositivos Médicos, e, até certo ponto, pela legislação em matéria de segurança geral dos produtos[49]. Por exemplo, o fabricante de um dispositivo conectado, concebido para integrar sistemas domésticos inteligentes, deve ser razoavelmente capaz de prever que os seus produtos afetarão a segurança de outros produtos.

Adicionalmente, a legislação em matéria de transportes aborda a questão da complexidade a nível de sistemas. No caso dos automóveis, dos comboios e dos aviões, a homologação e a certificação são realizadas tanto a nível de cada componente individual como da totalidade do veículo ou aeronave. A adequação dos veículos à circulação rodoviária, a aeronavegabilidade e a interoperabilidade ferroviária são contempladas na avaliação da segurança. No setor dos transportes, os «sistemas» carecem de «autorização» por parte de uma autoridade, seja com base numa avaliação, por terceiros, da conformidade com requisitos técnicos claros, seja no seguimento da demonstração da forma como os riscos são tidos em consideração. A solução é, em geral, uma combinação dos níveis «produto» e «sistema».

A legislação da União em matéria de segurança dos produtos, incluindo a do setor dos transportes, já tem em conta, até certo ponto, a complexidade dos produtos e sistemas com vista a enfrentar os riscos suscetíveis de afetar a segurança dos utilizadores.

Os sistemas complexos envolvem frequentemente ***software***, um componente essencial de sistemas dotados de inteligência artificial. Em geral, o fabricante do produto final tem a obrigação de, no âmbito da avaliação inicial dos riscos, prever os riscos associados ao *software* integrado no produto em causa no momento da sua colocação no mercado.

Alguns atos legislativos da União em matéria de segurança dos produtos referem-se explicitamente ao *software* integrado em produtos. Por exemplo, a Diretiva Máquinas[50] exige que uma falha no suporte lógico (*software*) do sistema de comando não conduza a situações perigosas.

No contexto da legislação da União em matéria de segurança dos produtos, as atualizações de *software* podem ser comparadas a operações de manutenção por motivos de segurança, desde que não alterem significativamente um produto já colocado no mercado e não introduzam novos riscos não previstos na avaliação inicial dos riscos. Porém, se a atualização de *software* alterar significativamente o produto em que é descarregada, todo o produto pode ser considerado como sendo novo, devendo a sua conformidade com a legislação aplicável em

[49] O artigo 2.º da Diretiva Segurança Geral dos Produtos especifica que um produto seguro deve ter em conta «os efeitos sobre outros produtos quando for razoavelmente previsível a utilização do primeiro com os segundos».

[50] Anexo I, ponto 1.2.1, da Diretiva Máquinas.

matéria de segurança dos produtos ser reavaliada no momento em que a alteração se concretiza[51].

No que respeita ao *software* autónomo, que pode ser colocado separadamente no mercado ou carregado para um produto após a colocação deste no mercado, a legislação setorial harmonizada da União em matéria de segurança dos produtos não contém, regra geral, disposições específicas. No entanto, alguns atos legislativos da União abordam o *software* autónomo, como é o caso do Regulamento Dispositivos Médicos. Além disso, o *software* autónomo carregado em produtos conectados que comunicam por intermédio de determinados módulos de rádio[52] também pode ser regulado por atos delegados que completam a Diretiva Equipamentos de Rádio. Esta diretiva exige que certas classes ou categorias de equipamentos de rádio possuam funcionalidades que assegurem que o carregamento de *software* não põe em causa a sua conformidade[53].

Embora a legislação da União em matéria de segurança dos produtos tenha em conta os riscos decorrentes do *software* integrado num produto no momento da colocação deste no mercado, bem como de eventuais atualizações posteriores previstas pelo fabricante, poderá ser necessário incluir requisitos específicos e/ou explícitos relativos ao *software* autónomo (por exemplo, uma aplicação que possa ser descarregada). Deve ser dada especial atenção ao *software* autónomo que proporciona funcionalidades de segurança dos produtos e sistemas dotados de inteligência artificial.

Poderá ser necessário impor obrigações adicionais aos fabricantes para que estes incluam funcionalidades capazes de prevenir o carregamento de *software* com impacto na segurança ao longo da vida útil dos produtos com inteligência artificial.

Por último, as novas tecnologias digitais são afetadas pela **complexidade das cadeias de valor**. Note-se, porém, que esta complexidade não é nova nem foi suscitada exclusivamente pela emergência de tecnologias digitais como a inteligência artificial ou a Internet das coisas, sendo identificável, por exemplo, em produtos como os computadores e os robôs de serviço ou em sistemas de transporte.

No âmbito do quadro da União em matéria de segurança dos produtos, independentemente da complexidade da cadeia de valor, a responsabilidade pela segurança de um produto cabe ao produtor que o coloca no mercado. Essa responsabilidade do produtor abrange a segurança do produto final, incluindo as partes e componentes nele integradas, por exemplo o *software* instalado num computador.

Alguns atos da legislação da União em matéria de segurança dos produtos já contêm disposições que se referem explicitamente a situações em que vários agentes económicos intervêm num determinado produto antes de este ser colocado no mercado. A título de exemplo, a Diretiva Ascensores[54] exige que o agente económico responsável pela conceção e pelo fabrico do ascensor forneça à pessoa responsável pela instalação[55] «*toda a documentação e indicações necessárias para que esta última possa garantir que o ascensor seja corretamente instalado e ensaiado*». A Diretiva Máquinas exige que os fabricantes de

[51] Guia Azul de 2016 sobre a Aplicação das Regras da UE em matéria de Produtos.
[52] Módulos de rádio são dispositivos eletrónicos que possibilitam a transmissão e/ou receção de sinais de rádio (Wi-Fi, Bluetooth) entre dois dispositivos.
[53] Artigo 3.º, n.º 3, alínea i), da Diretiva Equipamentos de Rádio.
[54] Nos termos do artigo 16.º, n.º 2, da Diretiva 2014/33/UE.
[55] No âmbito da Diretiva 2014/33/UE, respeitante a ascensores, o instalador é equiparado ao fabricante e deve assumir a responsabilidade pela conceção, fabrico, instalação e colocação no mercado do ascensor.

equipamento forneçam ao operador informações sobre a montagem desse equipamento noutra máquina[56].

A legislação da União em matéria de segurança dos produtos tem em conta a complexidade das cadeias de valor, impondo obrigações a vários agentes económicos segundo o princípio da «responsabilidade partilhada».

Embora o regime vigente de responsabilidade do produtor pela segurança do produto final se tenha revelado adequado no contexto das atuais cadeias de valor complexas, a introdução de disposições que exijam especificamente a cooperação entre os agentes económicos envolvidos na cadeia de valor e os utilizadores poderá proporcionar segurança jurídica em cadeias de valor que, possivelmente, se tornarão cada vez mais complexas. Em particular, cada elemento da cadeia de valor com intervenção na segurança do produto (por exemplo os produtores de *software*), bem como os utilizadores (quando alteram um produto), deverá assumir a sua responsabilidade e facultar ao elemento seguinte as informações e medidas necessárias.

3. Responsabilidade

As disposições em matéria de segurança dos produtos e de responsabilidade pelos produtos acordadas a nível da União são dois mecanismos que se complementam com vista a alcançar o mesmo objetivo político de manter em funcionamento um mercado único de bens que garanta elevados níveis de segurança, ou seja, que minimize os riscos de danos para os utilizadores e permita indemnizá-los por danos resultantes de bens defeituosos.

A nível nacional, estas regras da União são complementadas por quadros não harmonizados em matéria de responsabilidade civil, que asseguram a indemnização de danos por diversas causas (tais como produtos e serviços) e abrangem as diferentes entidades que podem ser responsáveis pelos mesmos (tais como proprietários, operadores ou prestadores de serviços).

Embora a otimização das regras da União em matéria de segurança da inteligência artificial possa contribuir para evitar acidentes, estes podem acontecer, ainda assim. É neste contexto que assume importância a responsabilidade civil, cujas regras desempenham um papel duplo na sociedade: por um lado, asseguram que as vítimas de danos causados por outrem são indemnizadas e, por outro lado, oferecem incentivos económicos à parte responsável para que esta evite causar esses danos. As regras em matéria de responsabilidade devem proporcionar um equilíbrio entre a proteção dos cidadãos contra os danos e a abertura de um espaço de inovação para as empresas.

Os quadros em matéria de responsabilidade estabelecidos na União têm funcionado bem, estando assentes na aplicação paralela da Diretiva Responsabilidade pelos Produtos (Diretiva 85/374/CEE), que harmonizou a responsabilidade dos fabricantes de produtos defeituosos, e de outros regimes nacionais não harmonizados em matéria de responsabilidade.

A Diretiva Responsabilidade pelos Produtos proporciona um nível de proteção que os regimes nacionais de responsabilidade culposa não são, por si só, capazes de garantir, graças à criação de um sistema de responsabilidade objetiva do produtor por danos causados por um defeito nos seus produtos. No caso de danos físicos ou materiais, a parte lesada tem direito a

[56] Anexo I, ponto 1.7.4.2, da Diretiva Máquinas: «*[c]ada manual deve conter, se for caso disso, pelo menos as seguintes informações: i) instruções de montagem, instalação e ligação, incluindo desenhos, diagramas e meios de fixação e a designação do chassis ou da instalação em que a máquina se destina a ser montada*».

uma indemnização se provar a existência desses danos, do defeito do produto (ou seja, que este não proporcionou a segurança que o público pode legitimamente esperar) e de um nexo de causalidade entre ambos.

Os regimes nacionais não harmonizados preveem regras em matéria de responsabilidade culposa, de acordo com as quais as vítimas dos danos têm de provar a culpa da pessoa responsável, a existência dos danos e o nexo de causalidade entre a culpa e os danos, para conseguirem estabelecer o direito a indemnização. Além disso, os legisladores nacionais estabeleceram regimes de responsabilidade objetiva, no âmbito dos quais a responsabilidade por um risco é atribuída a determinada pessoa, sem que a vítima tenha de provar a culpa/defeito ou o nexo de causalidade entre a culpa/defeito e os danos.

Os regimes nacionais em matéria de responsabilidade conferem às vítimas de danos causados por produtos e serviços o direito a apresentar vários pedidos de indemnização paralelos, com base na responsabilidade culposa ou objetiva. Estas ações são frequentemente intentadas contra diferentes pessoas responsáveis e obedecem a condições diferentes.

A título de exemplo, uma vítima de um acidente de viação pode, tipicamente, intentar uma ação relativa à responsabilidade objetiva do proprietário do veículo (ou seja, o tomador do seguro de responsabilidade civil automóvel) e uma ação relativa à responsabilidade culposa do condutor, ambas ao abrigo do direito civil nacional, bem como uma ação contra o fabricante, ao abrigo da Diretiva Responsabilidade pelos Produtos, se o automóvel em causa tiver um defeito.

Em conformidade com as regras harmonizadas em matéria de seguro automóvel, a utilização do veículo deve ser objeto de um seguro[57] e, na prática, a seguradora é sempre o primeiro visado dos pedidos de indemnização por danos pessoais ou materiais. De acordo com estas regras, o seguro obrigatório indemniza a vítima e protege o segurado, que é responsável, nos termos das regras do direito civil nacional[58], por compensar os danos financeiros decorrentes do acidente automóvel. A Diretiva Responsabilidade pelos Produtos não obriga os produtores a contratar um seguro. No que respeita ao seguro automóvel, a legislação da União não estabelece um tratamento diferenciado para os veículos autónomos em relação aos veículos não autónomos. Todos os veículos, incluindo os autónomos, têm de estar cobertos por um seguro de responsabilidade civil automóvel contra terceiros, que é a forma mais simples de a pessoa lesada obter uma indemnização.

A contratação de seguros adequados pode atenuar as consequências negativas dos acidentes, garantindo que as vítimas são indemnizadas rapidamente. A existência de regras claras em matéria de responsabilidade ajuda as companhias de seguros a calcular os seus riscos e a solicitar o reembolso à parte responsável, em última instância, pelos danos. Por exemplo, se um acidente for causado por um defeito, a seguradora automóvel pode, depois de indemnizar a vítima, solicitar o reembolso ao fabricante.

No entanto, as características de novas tecnologias digitais como a inteligência artificial, a Internet das coisas e a robótica colocam desafios à aplicação de determinados aspetos dos quadros nacionais e da União em matéria de responsabilidade e podem reduzir a sua eficácia. Algumas destas características poderão dificultar a associação dos danos a um

[57] A harmonização relativa aos veículos automóveis foi introduzida pela Diretiva 2009/103/CE relativa ao seguro de responsabilidade civil que resulta da circulação de veículos automóveis e à fiscalização do cumprimento da obrigação de segurar esta responsabilidade.

[58] Na maioria dos Estados-Membros, a responsabilidade objetiva recai sobre a pessoa em cujo nome o veículo se encontra registado.

comportamento humano que justifique uma ação por responsabilidade culposa em conformidade com as regras nacionais. Significa isto que o processo de provar o direito a uma indemnização com base na legislação nacional em matéria de responsabilidade civil se poderá tornar difícil ou demasiado custoso, pelo que as vítimas poderão não ser devidamente indemnizadas. É importante que as vítimas de acidentes relacionados com produtos e serviços que utilizam novas tecnologias digitais, como a inteligência artificial, não beneficiem de um nível de proteção inferior ao das vítimas de acidentes relacionados com outros produtos e serviços semelhantes, em relação aos quais estas vítimas seriam indemnizadas nos termos da legislação nacional em matéria de responsabilidade civil. Essa disparidade poderia reduzir a aceitação social dessas novas tecnologias e criar resistência à sua utilização.

Será necessário determinar se as novas tecnologias poderão igualmente criar insegurança jurídica quanto à forma de aplicar a legislação em vigor (por exemplo, a forma como o conceito de culpa se aplicaria a danos causados pela inteligência artificial). Por sua vez, essa insegurança poderia desencorajar o investimento, bem como aumentar os custos de informação e de seguro para os produtores e outras empresas da cadeia de abastecimento, especialmente as PME europeias. Além disso, a eventual tentativa de resposta, por parte dos Estados-Membros, aos desafios enfrentados pelos respetivos quadros nacionais em matéria de responsabilidade poderá conduzir a uma fragmentação adicional, aumentando assim os custos da introdução no mercado único de soluções inovadoras no domínio da inteligência artificial e reduzindo o comércio transfronteiras nesse mercado. É importante que as empresas conheçam os seus riscos de responsabilidade ao longo da cadeia de valor e os consigam reduzir ou prevenir, e que contratem seguros eficazes contra os mesmos.

O presente capítulo explica de que modo as novas tecnologias desafiam os quadros vigentes e de que forma esses desafios poderão ser enfrentados. Além disso, alguns setores, como o dos cuidados de saúde, apresentam especificidades que podem merecer considerações adicionais.

Complexidade dos produtos, dos serviços e da cadeia de valor: a tecnologia e a indústria evoluíram drasticamente ao longo das últimas décadas. Em especial, a distinção entre produtos e serviços pode não ser tão evidente como no passado, estando os produtos e a prestação de serviços cada vez mais interligados. Embora os produtos e as cadeias de valor complexas não sejam uma novidade para a indústria europeia e para o seu modelo regulamentar, o *software* e a inteligência artificial merecem especial atenção no que diz respeito à responsabilidade pelos produtos. O *software* é um elemento essencial para o funcionamento de um grande número de produtos e pode afetar a sua segurança. Está habitualmente integrado nos produtos, mas pode também ser fornecido separadamente para permitir a utilização prevista daqueles. Um computador ou um telemóvel inteligente, por exemplo, seriam produtos sem utilização prática se não dispusessem de *software*. Significa isto que o *software* pode tornar um produto tangível defeituoso e causar danos físicos (ver caixa de texto dedicada ao *software* na secção sobre segurança), o que poderia conduzir à responsabilização do fabricante do produto nos termos da Diretiva Responsabilidade pelos Produtos.

No entanto, uma vez que o *software* surge em muitos tipos e formas, a sua classificação como serviço ou produto nem sempre é evidente. Assim, o *software* que controla o funcionamento de um produto tangível poderá ser considerado como parte ou componente desse produto, ao passo que a classificação de algumas formas de *software* autónomo poderá ser mais difícil.

Embora a definição de produto consagrada na Diretiva Responsabilidade pelos Produtos seja ampla, o seu âmbito poderá ser esclarecido para refletir melhor a complexidade das novas tecnologias e assegurar a possibilidade de indemnização de quaisquer danos causados por produtos defeituosos devido a *software* ou outras características digitais. Esta medida possibilitaria aos agentes económicos, por exemplo editores de *software*, determinar com maior certeza se poderiam ser considerados produtores nos termos da Diretiva Responsabilidade pelos Produtos.

As aplicações de inteligência artificial estão muitas vezes integradas em **complexos ambientes da Internet das coisas**, nos quais múltiplos dispositivos e serviços conectados interagem entre si. A combinação de diferentes componentes digitais num ecossistema complexo e a pluralidade de intervenientes podem dificultar a determinação da origem de eventuais danos e dos responsáveis pelos mesmos. Devido à complexidade destas tecnologias, pode ser muito difícil para as vítimas identificar a pessoa responsável e provar todas as condições necessárias para estabelecer o direito a indemnização, tal como exigido pela legislação nacional. Os custos destas competências especializadas podem ser economicamente proibitivos e desencorajar as vítimas de reclamarem o direito a indemnização.

Além disso, os produtos e serviços que dependem da inteligência artificial interagirão com tecnologias tradicionais, o que aumentará ainda mais a complexidade em termos de responsabilidade. Um exemplo desta situação são os automóveis autónomos, que partilharão as estradas com veículos tradicionais durante algum tempo. Alguns setores dos serviços (como a gestão de tráfego e os cuidados de saúde), em que sistemas de inteligência artificial parcialmente automatizados apoiarão a tomada de decisões por seres humanos, apresentarão níveis de complexidade semelhantes, em termos de interação entre os intervenientes.

De acordo com o relatório[59] elaborado pelo Subgrupo para as Novas Tecnologias do Grupo de Peritos em Responsabilidade e Novas Tecnologia, poderão ser equacionadas adaptações das legislações nacionais com vista a facilitar o ónus da prova para as vítimas de danos relacionados com a inteligência artificial. Por exemplo, o ónus da prova poderá ser associado ao cumprimento (por parte de um operador envolvido no caso) de obrigações específicas em matéria de cibersegurança ou de outras obrigações de segurança estabelecidas por lei: a falta de cumprimento dessas regras, pode dar lugar à reversão do ónus da prova no que respeita à culpa e ao nexo de causalidade.

A Comissão pretende saber se, e em que medida, poderá ser necessário atenuar as consequências da complexidade por via da atenuação/reversão do ónus da prova exigida pelas regras nacionais em matéria de responsabilidade no respeitante a danos causados pelo funcionamento de aplicações de inteligência artificial, recorrendo para tal a uma iniciativa a nível da UE.

No atinente à legislação da União, nos termos da Diretiva Responsabilidade pelos Produtos, um produto que não cumpra as regras de segurança obrigatórias é considerado defeituoso, independentemente da culpabilidade do produtor. Porém, pode igualmente haver motivos para ponderar formas de facilitar o ónus da prova para vítimas ao abrigo da diretiva, cuja aplicação depende das regras nacionais em matéria de elementos de prova e de estabelecimento do nexo de causalidade.

[59] Relatório *Liability for Artificial Intelligence and other emerging technologies*, disponível no seguinte endereço: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

Conectividade e abertura: no contexto atual, não é inteiramente claro o que podemos esperar em termos de segurança no respeitante a danos que resultem de violações da cibersegurança de produtos nem se esses danos seriam devidamente indemnizados nos termos da Diretiva Responsabilidade pelos Produtos.

As deficiências em termos de cibersegurança podem estar presentes desde o início, quando um produto é colocado em circulação, mas também podem surgir numa fase posterior, bem depois de o produto se encontrar no mercado.

Estabelecer obrigações claras em termos de cibersegurança nos quadros de responsabilidade culposa permite aos operadores determinar o que têm de fazer para evitar as consequências em matéria de responsabilidade.

Saber se um produtor poderia ter previsto certas alterações tendo em conta a utilização razoavelmente previsível do produto pode tornar-se uma questão mais proeminente no âmbito da Diretiva Responsabilidade pelos Produtos. Por exemplo, poderemos assistir a um aumento da utilização da «defesa com base no defeito tardio», segundo a qual um produtor não é responsável se o defeito não existir quando o produto é colocado em circulação, ou da «defesa com base no risco de desenvolvimento», segundo a qual seria impossível prever o defeito tendo em conta os conhecimentos mais avançados à data de desenvolvimento do produto. Além disso, a responsabilidade do produtor poderá ser reduzida se a parte lesada não tiver efetuado as atualizações de segurança necessárias, algo que poderá ser considerado como concorrência de culpa por parte da pessoa lesada. Uma vez que a noção de utilização razoavelmente previsível e as questões sobre a concorrência de culpa (como a omissão de uma atualização de segurança) se poderão tornar mais prevalentes, as pessoas lesadas poderão ter mais dificuldade em obter uma indemnização por danos causados por produtos defeituosos.

Autonomia e opacidade: as aplicações de inteligência artificial capazes de agir de forma autónoma realizam tarefas sem que todos os passos estejam predefinidos e com um nível mais baixo, ou eventualmente mesmo nulo, de controlo ou supervisão humana direta. Os algoritmos baseados em aprendizagem automática podem ser difíceis, se não impossíveis, de compreender (o chamado «efeito de caixa negra»).

Tal como a questão da complexidade, acima referida, o efeito de caixa negra patente em alguns sistemas de inteligência artificial poderá dificultar a obtenção de uma indemnização por danos causados por aplicações de inteligência artificial autónomas. A necessidade de compreender o algoritmo e conhecer os dados utilizados pelo sistema de inteligência artificial exige capacidade analítica e competências técnicas especializadas cujos custos poderão assumir valores proibitivos para as vítimas. Além disso, poderá ser impossível aceder ao algoritmo e aos dados sem a cooperação da parte potencialmente responsável. Na prática, isto poderá incapacitar as vítimas de apresentar um pedido de indemnização. Adicionalmente, não seria evidente como demonstrar a culpa de um sistema de inteligência artificial que agisse de forma autónoma, nem o que se entenderia como culpa de uma pessoa que agisse com base na utilização de inteligência artificial.

As legislações nacionais já integraram uma série de soluções para reduzir o ónus da prova para as vítimas em situações semelhantes.

A obrigação de os produtores assegurarem que todos os produtos colocados no mercado são seguros, ao longo de todo o seu ciclo de vida e em qualquer utilização razoavelmente previsível, permanece um princípio orientador das regras da União em matéria de segurança dos produtos e de responsabilidade pelos produtos. Significa isto que um fabricante terá de se certificar de que um produto que integra inteligência artificial respeita certos parâmetros de

segurança. As características da inteligência artificial não prejudicam o direito a esperar que os produtos cumpram determinados níveis de segurança, quer se trate de corta-relvas automáticos ou de robôs cirúrgicos.

A autonomia pode afetar a segurança de um produto, uma vez que pode alterar substancialmente as suas características, incluindo os seus dispositivos de segurança. Trata-se de saber em que condições as características da autoaprendizagem alargam a responsabilidade do produtor e em que medida o produtor previu determinadas alterações.

O conceito de «colocação em circulação», atualmente utilizado na Diretiva Responsabilidade pelos Produtos, poderá ser revisto, em estreita coordenação com alterações correspondentes no quadro da União em matéria de segurança, a fim de ter em conta que os produtos podem ser alterados e modificados. Esta revisão poderá igualmente ajudar a esclarecer quem é responsável por quaisquer alterações dos produtos.

De acordo com o relatório[60] elaborado pelo Subgrupo para as Novas Tecnologias do Grupo de Peritos em Responsabilidade e Novas Tecnologias, a operação de alguns dispositivos e serviços autónomos dotados de inteligência artificial poderá ter um perfil de risco específico em termos de responsabilidade, visto que estes podem causar danos significativos para interesses jurídicos essenciais, como o direito à vida, à saúde e à propriedade, e expor o público em geral a riscos. Tal poderá incidir principalmente em dispositivos dotados de inteligência artificial que circulam em espaços públicos (por exemplo veículos completamente autónomos, veículos aéreos não tripulados[61] e robôs de entrega de encomendas) ou em serviços que empregam inteligência artificial e que apresentem riscos semelhantes (por exemplo serviços de gestão de tráfego que orientam ou controlam veículos, ou serviços de gestão da distribuição de energia). Os desafios que a autonomia e a opacidade colocam às legislações nacionais em matéria de responsabilidade civil poderão ser resolvidos seguindo uma abordagem baseada nos riscos, de acordo com a qual os regimes de responsabilidade objetiva poderão assegurar que, sempre que um risco se concretize, a vítima seja indemnizada, independentemente da atribuição de culpa. Seria necessário avaliar cuidadosamente o impacto da escolha do responsável objetivo por tais operações no desenvolvimento e adoção da inteligência artificial, devendo equacionar-se uma abordagem baseada nos riscos.

No que diz respeito à operação de aplicações de inteligência artificial com um perfil de risco específico, a Comissão pretende saber se, e em que medida, será necessário introduzir a responsabilidade objetiva, tal como estabelecida nas legislações nacionais para riscos semelhantes a que o público se encontra exposto (por exemplo no respeitante à operação de veículos a motor, aeronaves ou centrais nucleares), com vista a permitir uma indemnização efetiva de eventuais vítimas. A Comissão está igualmente a recolher opiniões sobre a associação da responsabilidade objetiva a uma possível obrigação de contratar um seguro disponível, seguindo o exemplo da Diretiva Seguro Automóvel, para assim garantir que haja lugar a indemnização, independentemente da solvência da pessoa responsável, e ajudar a reduzir os custos dos danos.

[60] Relatório *Liability for Artificial Intelligence and other emerging technologies*, disponível no seguinte endereço: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

[61] Ver as referências a sistemas de aeronaves não tripuladas no Regulamento de Execução (UE) 2019/947 da Comissão, de 24 de maio de 2019, relativo às regras e aos procedimentos para a operação de aeronaves não tripuladas.

Quanto à operação das restantes aplicações de inteligência artificial, que constituirão a grande maioria, a Comissão está a ponderar a necessidade de adaptar o ónus da prova no que respeita ao nexo de causalidade e à culpa. Uma das questões assinaladas a este respeito no relatório[62] elaborado pelo Subgrupo para as Novas Tecnologias do Grupo de Peritos em Responsabilidade e Novas Tecnologias prende-se com os casos em que a parte potencialmente responsável não tenha mantido um registo dos dados pertinentes para determinar a responsabilidade ou em que não esteja disposta a partilhá-los com a vítima.

4. Conclusão

A emergência de novas tecnologias digitais como a inteligência artificial, a Internet das coisas e a robótica coloca novos desafios em termos de segurança dos produtos e de responsabilidade, como sejam a conectividade, a autonomia, a dependência de dados, a opacidade, a complexidade dos produtos e sistemas, as atualizações de *software* e uma maior complexidade da gestão da segurança e das cadeias de valor.

A atual legislação em matéria de segurança dos produtos contém uma série de lacunas que devem ser colmatadas, em especial na Diretiva Segurança Geral dos Produtos, na Diretiva Máquinas, na Diretiva Equipamentos de Rádio e no Novo Quadro Legislativo. O futuro trabalho de adaptação de diferentes atos legislativos incluídos neste quadro será levado a cabo de forma coerente e harmonizada.

Os novos desafios em termos de segurança criam também novos desafios em termos de responsabilidade. É necessário dar resposta a esses desafios relacionados com a responsabilidade para assegurar o mesmo nível de proteção que o proporcionado às vítimas das tecnologias tradicionais, mantendo simultaneamente o equilíbrio com as necessidades de inovação tecnológica. Tal contribuirá para criar confiança nestas novas tecnologias digitais e estabilidade de investimento.

Embora a atual legislação a nível nacional e da União em matéria de responsabilidade seja, em princípio, capaz de lidar com as novas tecnologias, a dimensão e o efeito combinado dos desafios colocados pela inteligência artificial poderão dificultar a indemnização das vítimas em todos os casos justificados[63]. Assim, ao abrigo das regras atuais, a repartição de custos em caso de danos pode ser injusta ou ineficaz. A fim de corrigir esta situação e eliminar potenciais incertezas patentes no quadro em vigor, poderão ser equacionados certos ajustamentos da Diretiva Responsabilidade pelos Produtos e dos regimes nacionais em matéria de responsabilidade, a realizar por intermédio de iniciativas adequadas da UE, assentes numa abordagem específica e baseada nos riscos, ou seja, que tenha em conta que as diferentes aplicações de inteligência artificial apresentam riscos diferentes.

[62] Relatório *Liability for Artificial Intelligence and other emerging technologies*, disponível no seguinte endereço: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

[63] Ver a página 3 do relatório elaborado pelo Subgrupo para as Novas Tecnologias e a recomendação política 27.2 do Grupo de Peritos de Alto Nível em Inteligência Artificial.