Questões ético-jurídicas relativas ao uso de apps geradoras de dados de mobilidade para vigilância epidemiológica da Covid-19. Uma perspetiva Europeia.

Alexandra Aragão,
Instituto Jurídico da Faculdade de Direito da
Universidade de Coimbra

O contexto: uso de aplicações móveis em situação de vigilância epidemiológica

Perante a catástrofe sanitária mundial provocada pelo novo vírus Corona, corre-se contra o tempo em busca de duas conquistas fundamentais para combater a Covid-19: vacinas e aplicações móveis de vigilância epidemiológica.

O que está em causa é a criação de aplicações móveis interoperáveis, que podem até recorrer a inteligência artificial, para criar uma rede de vigilância epidemiológica em toda a Europa para controlar a Covid-19.

O objetivo das presentes notas explicativas é contextualizar a Recomendação (UE) 2020/518 da Comissão Europeia, relativa a um conjunto de instrumentos comuns a nível da União com vista à utilização de tecnologias e dados para combater a crise da COVID-19 e sair da crise, nomeadamente no respeitante às aplicações móveis e à utilização de dados de mobilidade anonimizados, de 8 de abril de 2020[1] e apresentar os requisitos desejáveis das aplicações móveis interoperáveis na União Europeia destinadas à obtenção de dados de mobilidade anonimizados.

Um exemplo de uma aplicação deste tipo é a app *infopraia*[2] desenvolvida pela Agência Portuguesa do Ambiente originalmente para dar informações sobre a qualidade da água das praias e meteorologia nas zonas balneares. Na sequência do estado de emergência sanitária declarado em Portugal em 18 de março de 2020 a app foi adaptada para passar a fornecer informação sobre as condições de acesso às praias. Depois do fim do estado de emergência em 3 de maio, com o levantamento gradual das restrições à mobilidade individual, considerou-se prioritário regulamentar o acesso às praias, habitualmente sobrepovoadas em época balnear. Em maio de 2020 o relançamento da app *infopraia* com novas

[1] De agora em diante, abreviadamente *Recomendação app de mobilidade Covid-19* (https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2020.114.01.0007.01.POR&toc=OJ:L:2020:114:TOC).
[2] Disponível para download em https://play.google.com/store/apps/details?id=pt.apambiente.info_praia&hl=pt_PT

funcionalidades foi anunciado pelo Primeiro Ministro em conferência de imprensa. A app serve agora para dar informação sobre ocupação das praias sinalizando a maior ou menor afluência através de um semáforo virtual e indicando o limite de capacidade da praia com um semáforo vermelho. Apesar de a utilização da app não exigir registo, foi acusada de não garantir a privacidade de quem a usa pelo excesso de permissões solicitadas ao utilizador no momento da instalação: acesso a câmara, microfone e dados de localização. Dois dias depois de ter sido lançada a Agência Portuguesa do Ambiente reafirmou a segurança das condições de funcionamento.

Este é o contexto atual da discussão sobre o uso de apps geradoras de dados de mobilidade para vigilância epidemiológica. O que vamos fazer em seguida será analisar algumas questões ético-jurídicas relativas por um lado, ao potencial de benefícios para a saúde pública e o bem estar social e por outro, aos riscos individuais e coletivos associados às tecnologias digitais de comunicação e geolocalização.

Tecnologias para o bem estar em sociedades digitalizadas

Não exagera a Comissão quando considera que a União Europeia e os Estados membros estão a "enfrentar um desafio sem precedentes com impacto nos seus sistemas de saúde, no seu modo de vida, na sua estabilidade económica e nos seus valores"[3].

Um desafio de tamanha magnitude exige uma resposta à altura. Aplicações móveis[4] que produzem dados de mobilidade anonimizados e agregados para auxiliar as autoridades sanitárias e para as autoridades públicas competentes nos seus esforços de contenção da propagação do vírus, parecem ser a resposta que se necessitava.

As vantagens da utilização desses dados são compreender a forma como o vírus se propagará, avaliar a eficácia das medidas de distanciamento social, modelizar a dinâmica espacial das epidemias (limitações de deslocamentos, encerramentos de atividades não essenciais, confinamento total, etc.) e modelizar também os efeitos económicos da crise[5].

As vantagens para os cidadãos, da utilização de apps multifuncionais são igualmente significativas. As funções de autodiagnóstico e de controlo de sintomas, podem ser especialmente importantes para a estabilização emocional dos utilizadores infetados ou com receio de o estarem. As funções de alerta e de rastreio através de dados de proximidade (*bluetooth*) podem desempenhar um papel fundamental na identificação de contactos sociais. Os dados de mobilidade são úteis na escolha de trajetórias e destinos para evitar aglomerações de pessoas, permitindo a adoção de medidas de auto-proteção e comportamentos defensivos.

No final, toda a sociedade ganha com a interrupção das cadeias de transmissão e a limitação da propagação do vírus.

---

[3] *Recomendação app de mobilidade Covid-19.*

[4] A Comissão Europeia define *aplicações móveis*, como "os softwares de aplicação que funcionam em dispositivos inteligentes, nomeadamente telemóveis inteligentes, geralmente concebidos para uma interação abrangente e específica com recursos em linha, que tratam dados de proximidade e outras informações contextuais recolhidas por vários sensores presentes em qualquer dispositivo inteligente, e que são capazes de trocar informações através de várias interfaces de rede com outros dispositivos conectados". *Recomendação app de mobilidade Covid-19*

[5] *Recomendação app de mobilidade Covid-19.*

"As tecnologias digitais estão a mudar profundamente nossa vida quotidiana, a nossa maneira de trabalhar e de fazer negócios e a maneira como as pessoas viajam, comunicam e se relacionam. A comunicação digital, a interação nas redes sociais, o comércio eletrónico e as empresas digitais estão a transformar o nosso mundo"[6].

Com a tecnologia 5G, a automação, a internet das coisas e os sistemas baseados em inteligência artificial, aprendizagem de máquina e aprendizagem profunda[7] haverá um salto qualitativo[8] assinalável nas oportunidades de comunicação que contribuem para o desenvolvimento e o exercício das liberdades individuais. A figura ilustra o aumento das probabilidades de comunicação:

Fig. 1 Possibilidades de comunicação. Imagem adaptada a partir de *ITU Recommendation ITU-T Y.2060 (06/2012)*[9]

Nas palavras da Comissão, o volume de dados produzidos no mundo está a aumentar rapidamente, devendo passar de 33 zetabytes em 2018 para 175 zetabytes em 2025. Cada nova vaga de dados oferece à UE grandes oportunidades para se tornar líder mundial neste domínio. Além disso, o modo de armazenamento e de tratamento dos dados mudará radicalmente nos próximos cinco anos. Atualmente, 80 % do tratamento e da análise de dados ocorrem em centros de dados e instalações de computação centralizadas, e 20 % em objetos inteligentes conectados – nomeadamente automóveis, eletrodomésticos ou robôs de fabrico – e em instalações de computação próximas do utilizador («computação periférica»). Até 2025, é provável que estas proporções se invertam"[10].

---

[6] Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões *Construir o futuro digital da Europa* Bruxelas, 19.2.2020 COM(2020) 67 final, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:67:FIN).

[7] "O treino de um algoritmo de aprendizagem profunda para fins de classificação de objetos consiste na sua exposição a um grande volume de exemplos etiquetados (por exemplo, imagens), que estão categorizados de forma correta (por exemplo, imagens de aviões). Uma vez treinados, os algoritmos são capazes de classificar corretamente objetos que nunca viram, em alguns casos, com uma exatidão superior à dos seres humanos." Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões *Inteligência artificial para a Europa* Bruxelas, 25.4.2018 COM(2018) 237 final (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN).

[8] 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* Bruxelas 19.2.2020 COM(2020) 64 final (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0064) "AI, IoT e robótica compartilham muitas características. Eles podem combinar conectividade, autonomia e dependência de dados para executar tarefas com pouco ou nenhum controlo ou supervisão humana".

[9] International Telecommunication Union, *Next Generation Networks – Frameworks and functional architecture models Overview of the Internet of things* Recommendation ITU-T Y.2060 (06/2012) (https://www.itu.int/rec/T-REC-Y.2060-201206-I)

[10] Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões *Uma estratégia europeia para os dados,* Bruxelas, 19.2.2020 COM(2020) 66 final (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:66:FIN).

A incorporação de inteligência artificial ou IA nos dispositivos de comunicação de uso quotidiano representa outro avanço no potencial de contribuição das tecnologias digitais para a qualidade de vida.
A inteligência artificial são « sistemas de software (e eventualmente também de hardware) concebidos por seres humanos, que, tendo recebido um objetivo complexo, atuam na dimensão física ou digital percecionando o seu ambiente mediante a aquisição de dados, interpretando os dados estruturados ou não estruturados recolhidos, raciocinando sobre o conhecimento ou processando as informações resultantes desses dados e decidindo as melhores ações a adotar para atingir o objetivo estabelecido»[11].

Uma representação esquemática de um sistema de inteligência artificial ajuda a compreender o conceito pela desconstrução dos seus componentes:

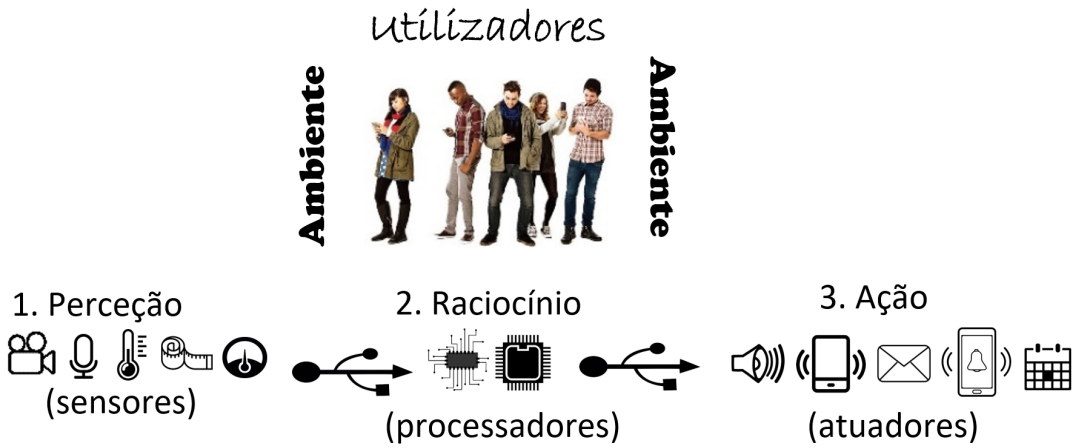

Fig. 2 Representação esquemática de um sistema de IA, adaptação do esquema desenvolvido pelo grupo independente de peritos de alto nível sobre a inteligência artificial [12]

Os sensores do sistema de IA são funcionalidades atualmente existentes em qualquer dispositivo de comunicação inteligente como um telemóvel, tablet ou computador. Podem ser câmaras, microfones, teclados, sítios web ou outros dispositivos de entrada de dados, bem como sensores de quantidades físicas (p. ex., sensores de temperatura, pressão, distância, força/binário ou sensores táteis).

Os atuadores podem ser sinais sonoros, vibração, envio de mensagens curtas (sms, tweets, etc.) ou e-mails, chamadas telefónicas para certos números, agendamento de eventos, ativação de alarmes ou outros dispositivos eletrónicos conectados, etc.

Desde secretárias virtuais a cirurgias assistidas por robots e veículos autónomos, vivemos numa época em que a automação passou a fazer parte do nosso dia a dia[13].
Com a chegada generalizada da quinta geração de redes de telecomunicações, ou tecnologia 5G, haverá impactes em muitos aspetos da vida dos cidadãos da União Europeia. Espera-se que além de oportunidades económicas, a transformação digital contribua para a transformação ecológica através da introdução de tecnologias digitais que usam 5G em

[11] Segundo o grupo independente de peritos de alto nível sobre a inteligência artificial criado pela Comissão Europeia em junho de 2018, "Uma definição de ia: principais capacidades e disciplinas científicas. Definição desenvolvida para efeitos dos documentos elaborados pelo grupo" (https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines).
[12] Adaptado de "Uma definição de ia: principais capacidades e disciplinas científicas" do Grupo independente de peritos de alto nível sobre a inteligência artificial (https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines).
[13] Susan Winterberg and Martin Lemos, *Automation: A Framework for a Sustainable Transition*, Business for Social Responsibility, April 2017 (https://www.bsr.org/reports/BSR_Automation_Sustainable_Jobs_Business_Transition.pdf).

domínios como os transportes, a energia, a indústria transformadora, a saúde, a agricultura e os meios de comunicação social[14].
Melhores serviços de saúde e bem-estar, melhoria das finanças pessoais, redução da pegada ambiental, acesso sem entraves a serviços públicos e privados, governação mais transparente, são alguns dos benefícios[15]
No domínio da saúde, o desenvolvimento de registos de saúde eletrónicos nacionais e a interoperabilidade transfronteiras dos dados de saúde permitirão o intercâmbio de resumos clínicos eletrónicos e de receitas eletrónicas entre os 22 Estados-Membros que participam na infraestrutura de serviços digitais de saúde em linha[16].
O cruzamento, através de repositórios federados, de tipos específicos de informações de saúde, tais como informações genómicas e imagens médicas digitais, significará um progresso assinalável a nível dos cuidados de saúde.
Em suma, a conectividade proporcionada pelo uso de novas tecnologias de comunicação comporta benefícios muito concretos para os cidadãos. A ponto de se poder afirmar que os telemóveis inteligentes deixaram de ser um luxo, para ser um bem essencial. Exemplificativamente, para cidadãos refugiados ou deslocados, o smartphone pode ser o seu bem mais precioso[17].

Aliás, desde 2012 que documentos das Nações Unidas afirmam a importância do direito de conexão à internet e a sua proteção como direito fundamental[18].

Portanto o "se" da aceitação das novas tecnologias de comunicação para alcançar os mais importantes desígnios sociais, como a proteção da saúde, não parece estar em discussão. Aquilo que está em causa são as condições de segurança na produção, acesso e utilização da informação produzida, processada, armazenada e transmitida. Quem, como, para quê e quando se deve aceder à informação?

Mais conectividade comporta maiores riscos

A par dos enormes benefícios de um futuro mais digital, a quantidade crescente de dados gerados pelos consumidores quando utilizam dispositivos de comunicação e serviços digitais

[14] Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões *Implantação segura de redes 5G na UE – Aplicação do conjunto de instrumentos da EU* Bruxelas, 29.1.2020 COM(2020) 50 final (https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0050&from=FR).
[15] Comunicação *Uma estratégia europeia para os dados* Bruxelas, 19.2.2020 (já citada).
[16] Comunicação *Uma estratégia europeia para os dados* Bruxelas, 19.2.2020 (já citada).
[17] Dois trabalhos jornalísticos dos jornais *Business Insider* e *The Economist* mostram porque os telemóveis são tão importantes para quem esteja na frágil situação de refugiado: https://www.businessinsider.com/why-so-many-refugees-have-smartphones-2016-5 . https://www.economist.com/international/2017/02/11/phones-are-now-indispensable-for-refugees.
[18] Num relatório apresentado em 2012, o Conselho de Direitos Humanos das Nações Unidas reconhece que a Internet é fundamental para o desenvolvimento e exercício de direitos humanos (United Nations Human Rights Council "the promotion, protection and enjoyment of human rights on the Internet" 5 july 2012 A/HRC/20/2 (https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A-HRC-20-2_en.pdf). Em 2016 defende a necessidade de promover, proteger e disfrutar de direitos humanos na Internet (Human Rights Council "the promotion, protection and enjoyment of human rights on the Internet" 27 June 2016 A/HRC/32/L.20 https://undocs.org/A/HRC/32/L.20), levando a que os meios de comunicação noticiassem que "as Nações Unidas consideram que a internet é um direito humano" (https://www.businessinsider.com/un-says-internet-access-is-a-human-right-2016-7). Entre 15 de junho e 3 de julho 2020 vai ser debatido um relatório sobre liberdade de expressão e opinião e a necessidade de combater a desinformmação sobre saúde pública (https://www.ohchr.org/_layouts/15/WopiFrame.aspx?sourcedoc=/Documents/Issues/Opinion/A_HRC_44_49_AdvanceEditedVersion.docx&action=default&DefaultItemOpen=1)

aumenta os riscos de discriminação, práticas desleais e efeitos de dependência. Quanto mais conectados estivermos, mais vulneráveis nos tornamos a ciberatividades maliciosas[19].
Apesar de a Comissão Europeia também desenvolver ações de diplomacia digital ou ciberdiplomacia[20] considera-se que apenas 13 dos 27 estados asseguram um nível adequado de proteção dos dados pessoais[21].
O futuro digital comporta riscos ambientais[22], riscos para a saúde física[23] ou para a saúde mental[24]. No presente texto referimo-nos apenas aos riscos resultantes da produção de dados pessoais e de localização por aplicações móveis ligadas a redes de vigilância epidemiológica.
Antes de mais, o risco mais grave é a cibercriminalidade entendida em sentido amplo, abrangendo tanto a *criminalidade clássica* agravada pela internet, como a *criminalidade digital* em sentido próprio.

A *criminalidade clássica*, pode ser facilitada pela identificabilidade pessoal (reconhecimento do rosto, nome, morada, profissão) ou pelo conhecimento da localização exata ou provável das pessoas através do smartphone. Ao poder conhecer ou prever a localização da pessoa a partir do conhecimento da morada, do local de trabalho, das rotinas, dos trajetos, dos horários habituais de permanência ou ausência em cada local, pode ocorrer um acréscimo de criminalidade, nomeadamente de crimes contra as pessoas (contra a vida, a integridade física, honra, a autodeterminação sexual), ou contra o património (furto do recheio da habitação, de viaturas ou de contas bancárias).

Mas a *criminalidade digital* será aquela que mais poderá aumentar. Referimo-nos aos crimes como a devassa ou violação de telecomunicações, resultantes do acesso e uso ilegal de informação pessoal como fotos, chaves digitais de identificação de cidadania, credenciais de acesso bancário, etc.. O acesso a estes dados pode permitir novos atos criminosos "clássicos" como ameaça, coação, sequestro, rapto, extorsão, corrupção, furto de valores, falsificação de documentos, etc.

Além disso, não podemos esquecer que mesmo sem configurar crime, existem muitas outras formas de acesso abusivo aos dados pessoais. Por exemplo, ao utilizar a internet para aceder a qualquer site em que o acesso é condicionado pela aceitação da instalação de *cookies.* Se o utilizador aceitar, os gestores do site passarão a ter acesso aos dados da navegação. Ficarão a saber que temas o utilizador pesquisou, que assuntos lhe interessam e o que provavelmente vai fazer a seguir. Saberão o que tenciona comprar, o que tenciona comer, que filmes tenciona ver, em quem tenciona votar, que doenças supõe padecer, até mesmo que crimes tenciona cometer. Em muitos casos, não é sequer necessário permitir a instalação de *cookies* para ter acesso a toda esta, e a muito mais informação. Se o utilizador tiver um perfil e

---

[19] Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões *Conectividade para um Mercado Único Digital Concorrencial - Rumo a uma Sociedade Europeia a Gigabits* (https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2016:0587:FIN:PT:PDF).
[20] Comunicação *Implantação segura de redes 5G na UE – Aplicação do conjunto de instrumentos da EU* (já citada).
[21] Comunicação *Uma estratégia europeia para os dados* Bruxelas, 19.2.2020 (já citada).
[22] Adam J. Vanbergen; Simon G. Potts, Alain Vian, E. Pascal Malkemper, Juliette Young, Thomas Tscheulin, "Risk to pollinators from anthropogenic electro-magnetic radiation (EMR): Evidence and knowledge gaps", *Science of The Total Environment*, Volume 695, 10 December 2019, 133833 (https://www.sciencedirect.com/science/article/pii/S0048969719337805)
[23] World Health Organization, *Establishing a dialogue on risks from electromagnetic fields*, 2002 (https://apps.who.int/iris/bitstream/handle/10665/42543/9241545712_eng.pdf?sequence=1&isAllowed=y&ua=1).
[24] World Health Organization, *Public health implications of excessive use of the Internet and other communication and gaming platforms*, 13 September 2018 (https://www.who.int/news-room/detail/13-09-2018-public-health-implications-of-excessive-use-of-the-internet-and-other-communication-and-gaming-platforms)

atividade nas redes sociais (como Facebook[25], Instagram[26] ou Twiter[27]), é fácil saber qual o seu círculo de amigos e inimigos, quais as suas preferências musicais ou clubísticas, quais as suas convicções ideológicas ou religiosas, quais as suas solidariedades ou hostilidades, quais os seus sonhos e ambições e até qual o seu estado de espírito em cada momento. Se tiver um perfil profissional (como Linked in[28], Xing[29], ou Jobcase[30]) saber-se-á qual o seu percurso académico e profissional, as suas competências, sucessos, promoções, transferências ou mudanças laborais.

Ou seja: os riscos decorrentes do uso de aplicações móveis ligadas a redes de vigilância epidemiológica são uma realidade comum a outras aplicações, plataformas ou serviços digitais que contenham ou possam aceder a informações pessoais, como o *Tinder*[31], o *Find my friends*[32] ou o *Snapchat*[33], todas elas já existentes, instaladas no mercado e com milhões de utilizadores.

Que direitos fundamentais estão aqui em causa? Vários. A liberdade de reunião (se a app for usada para detetar antecipadamente agrupamentos de pessoas); liberdade de iniciativa empresarial (se a app for usada para identificar atividades que estão a funcionar e ver quais poderiam estar abertas e quais deveriam estar fechadas); liberdade de deslocação (para sinalizar trajetos ou destinos desaconselháveis); intimidade da vida privada (se a app for usada para identificar comportamentos indesejáveis, nomeadamente de proximidade social); dignidade humana (se o confinamento puser em causa o acesso à alimentação ou outros direitos fundamentais); igualdade de tratamento e não discriminação (se a app for usada para obter informação pessoal sensível e houver acesso indevido por terceiros).

Mesmo usos bem intencionados e de boa fé dos dados fornecidos pelas apps que instalamos comportam o risco de criar uma sociedade orwelliana em que empresas vigiam potenciais clientes para lhes oferecer produtos ou serviços direcionados para os seus gostos ou necessidades; autoridades policiais vigiam os condutores para garantir a segurança rodoviária e autuar os infratores; entidades patronais vigiam os trabalhadores para monitorizar a segurança no trabalho e a produtividade laboral; diretores escolares vigiam os estudantes para prevenir violência e assédio na escola e assegurar o cumprimento das regras da biblioteca e da cantina; entidades financeiras vigiam os devedores para prevenir o sobre-endividamento e para acionar cobranças de créditos; autoridades sanitárias vigiam os infetados para acorrer às suas necessidades médicas e farmacêuticas e para evitar deslocações indesejadas.

O grande risco é o de as autoridades públicas (ou mesmo entidades privadas) levarem a cabo ações de vigilância massiva da população, e, tão mau ou pior ainda, o risco de vigilância discriminatória, abrangendo apenas certas minorias em função de critérios discriminatórios como os raciais, étnicos, etários, ideológicos, religiosos ou outros.

Mais ainda: se a app fornecer informação individual sobre a saúde do proprietário, que chegue ao conhecimento de terceiros pode conduzir a situações de discriminação *a*

[25] https://pt-pt.facebook.com/
[26] https://www.instagram.com/?hl=pt
[27] https://twitter.com/login?lang=pt
[28] https://pt.linkedin.com/
[29] https://www.xing.com/en
[30] https://www.jobcase.com/community/foryou
[31] https://tinder.com/
[32] https://apps.apple.com/us/app/find-my-friends/id466122094
[33] https://www.snapchat.com/

posteriori, mesmo após o fim da pandemia[34]. O utilizador que tenha estado infetado, poderá correr o risco, se essa informação cair nas mãos erradas, de ser discriminado no acesso ao emprego, ao consumo, aos transportes públicos, ao lazer, aos equipamentos coletivos, a seguros de habitação, a empréstimos bancários, ao arrendamento habitacional ou à obtenção de cuidados de saúde.

Por fim, se as aplicações móveis tiverem uma dimensão de inteligência artificial associada, os riscos poderão ser ainda maiores[35]. O uso de sistemas de inteligência artificial ("um conjunto de tecnologias que combinam dados, algoritmos e poder de computação"[36]) para a vigilância epidemiológica comporta riscos adicionais: tratando-se de sistemas baseados em "machine learning", a fiabilidade dos sistemas depende da disponibilidade de dados, pelo que há o risco de o sistema, numa fase inicial, cometer erros ou até incorrer no que se denomina injustiça algorítmica [37]. O risco da injustiça algorítmica está relacionado com a necessidade de um volume muito grande de dados para treinar os sistemas que aprendem através de correlações[38], o que pode conduzir a estigmatização de pessoas que partilham determinadas características, com base na perceção de uma relação entre estas características

[34] Idênticas discriminações chocantes existem igualmente em relação aos sobreviventes de cancro na contração de seguros e empréstimos.

[35] O risco de aplicações que utilizem IA é maior pela opacidade e imprevisibilidade da evolução dos sistemas de processamento dos dados recolhidos pelo sistema de IA. (Comunicação da Comissão *Inteligência artificial para a Europa*, já citada). A opacidade é outra característica principal de alguns produtos e sistemas baseados em IA que podem resultar da capacidade de melhorar seu desempenho aprendendo com a experiência. Dependendo da abordagem metodológica, os produtos e sistemas baseados em IA podem ser caracterizados por vários graus de opacidade. Isso pode levar a um processo de tomada de decisão do sistema difícil de rastrear ("efeito caixa preta"). Os humanos podem não precisar entender todas as etapas do processo de tomada de decisão, mas, à medida que os algoritmos de IA se tornam mais avançados e são implantados em domínios críticos, é decisivo que os humanos possam entender como as decisões algorítmicas do sistema foram alcançadas. (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.* Já citado).

[36] Livro branco *Sobre a inteligência artificial - Uma abordagem europeia virada para a excelência e a confiança*, Bruxelas, 19.2.2020 COM(2020) 65 final (https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_pt.pdf).

[37] Por exemplo se a função de autodiagnóstico conduzir a diagnósticos errados devido a enviesamento em função do género ou da raça, resultante de o algoritmo ter sido desenvolvido por programadores com determinado perfil ou pela utilização de uma população de teste com determinadas características. "Certos algoritmos de IA, quando utilizados para prever reincidência criminal, podem exibir enviesamento de género ou racial, demonstrando diferentes previsões de probabilidade de reincidência para mulheres vs homens ou para nacionais vs estrangeiros". Tolan S., Miron M., Gomez E. and Castillo C. "Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia", *Best Paper Award, International Conference on AI and Law,* 2019 (https://docplayer.net/131278107-Why-machine-learning-may-lead-to-unfairness-evidence-from-risk-assessment-for-juvenile-justice-in-catalonia.html).
"Alguns programas de IA para análise facial revelam enviesamento de género e racial, demonstrando poucos erros na determinação do género de homens de pele clara mas muitos erros na determinação d género de mulheres de pele mais escura". Joy Buolamwini, Timnit Gebru "Gender shades: intersectional accuracy disparities in commercial gender classification", *Proceedings of the 1st Conference on Fairness, Accountability and Transparency,* Proceedings of Machine Learning Research 81:77-91, 2018 (http://proceedings.mlr.press/v81/buolamwini18a.html).

[38] A obra *Algorithmic Fairness,* (the Public Policy Division of the Software & Information Industry Association, Siia Issue Brief 22, September 2016) (http://www.siia.net/Portals/0/pdf/Policy/Algorithmic%20Fairness%20Issue%20Brief.pdf) menciona, a título de exemplo, o bem conhecido e muito criticado estudo de Shai Danzigera, Jonathan Levav, e Liora Avnaim-intitulado *Extraneous factors in judicial decisions* que conclui, com base em análise estatísticas das sentenças, que as decisões dos juízes são influenciadas pelo almoço (Department of Management, Ben Gurion University of the Negev, Beer Sheva 84105, Israel; and Columbia Business School, Columbia University, New York, NY 10027
(http://houdekpetr.cz/!data/public_html/papers/economics_psychology/Danziger%20et%20al%202011.pdf).

e a doença[39]. Isto é o que se denomina enviesamento de máquina ou *machine bias*[40] e é ele que conduz à injustiça algorítmica.

Por tudo isso se compreende a preocupação da UE com a segurança dos sistemas e a confiança dos utilizadores[41].

A abordagem europeia: tecnologia digital de confiança

Ciente destes riscos, mas convicta dos benefícios, a Comissão Europeia apresentou em abril de 2020 um conjunto de princípios relativos às aplicações móveis de alerta e prevenção da COVID-19. Estes princípios não são novos, pelo contrário são comuns a muitas declarações semelhantes[42]. Sinteticamente, recomenda-se que as aplicações móveis:

- garantam o respeito pelos direitos fundamentais e a prevenção da estigmatização
- prefiram medidas menos intrusivas mas eficazes, como dados de proximidade para evitar o tratamento de dados sobre a localização ou os movimentos de pessoas
- usem tecnologias adequadas para estabelecer a proximidade dos dispositivos (por exemplo, *bluetooth* de baixo consumo de bateria e possibilidade de desligar)
- assegurem requisitos eficazes de cibersegurança
- suprimam dos dados pessoais após um período de 90 dias ou quando se declarar que a pandemia está sob controlo
- usem dados de proximidade anónimos em caso de infeção confirmada para alertar as pessoas que tenham estado em estreito contacto com a pessoa infetada
- assegurem transparência e confiabilidade nas aplicações.

---

[39] *Recomendação app de mobilidade Covid-19.*

[40] "Entende-se por enviesamento uma tendência parcial a favor ou contra uma pessoa, um objeto ou uma posição. Os enviesamentos podem surgir de muitas formas nos sistemas de IA. Por exemplo, nos sistemas de IA baseados em dados, como os produzidos por via da aprendizagem automática, o enviesamento na recolha de dados e na fase de treino pode levar um sistema de IA que apresenta enviesamentos. Na IA baseada na lógica, como os sistemas baseados em regras, podem surgir enviesamentos devido à forma como um engenheiro do conhecimento entenda as regras aplicáveis num determinado contexto. Também podem surgir enviesamentos devido à aprendizagem em linha e à adaptação através da interação. Podem ainda surgir através da personalização, que visa apresentar aos utilizadores recomendações ou fluxos de informações adaptadas aos seus gostos. Não estão necessariamente relacionados com preconceitos humanos ou uma recolha de dados baseada no ser humano. Podem ser suscitados, por exemplo, pelos contextos limitados em que um sistema é utilizado, não havendo nesse caso oportunidades de generalização para outros contextos. O enviesamento pode ser bom ou mau, intencional ou não intencional. Em alguns casos, o enviesamento pode causar resultados discriminatórios e/ou injustos, designados no presente documento por enviesamentos injustos". (*Orientações éticas para uma IA de confiança* Grupo de peritos de alto nível sobre a inteligência artificial criado pela Comissão Europeia em junho de 2018 (https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines)

[41] Livro Branco sobre a inteligência artificial: uma abordagem europeia virada para a excelência e a confiança Bruxelas, 19.2.2020 COM(2020) 65 final (https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_pt.pdf).

[42] Jessica Fjeld; Nele Achten; Hannah Hilligoss; Adam Christopher Nagy e Madhulika Srikumar analisam 36 documentos emanados por organizações da sociedade civil, por governos, por organização intergovernamentais, pelo setor privado e por atores multistakeholders. Da sua análise concluem que: 100% dos documentos analisados, estabelecendo princípios éticos do uso da IA incluem o princípio da justiça e não discriminação; 97% incluem o princípio da privacidade e imputabilidade (*accountability*); 94% incluem os princípios da transparência e explicabilidade; 81% incluem os princípios da segurança e asseguração; 78% incluem o princípio da responsabilidade profissional; 69% incluem o princípio do controlo humano da tecnologia e da promoção de valores humanos. (*Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI,* Research Publication No. 2020-1 January 15, 2020, https://cyber.harvard.edu/publication/2020/principled-ai ; https://ssrn.com/abstract=3518482).

O Grupo de peritos de alto nível sobre a inteligência artificial da União Europeia, elaborou uma lista de 133 questões de avaliação de uma IA de confiança[43] destinadas a ser respondidas pelas empresas que colocam no mercado produtos baseados em IA. As questões dividem-se por 7 categorias de preocupações éticas: ação e supervisão humanas, solidez técnica e segurança, privacidade e governação dos dados, transparência, diversidade, não discriminação e equidade, bem-estar societal e ambiental e responsabilização. Das 133 destacámos, exemplificativamente, as 36 mais significativas.

1. Ação e supervisão humanas

I. O sistema de IA interage com a tomada de decisões por utilizadores finais humanos (p. ex., recomendação de ações ou decisões a tomar, apresentação de opções)?

II. Nesses casos, existe algum risco de que o sistema de IA afete a autonomia humana interferindo com o processo decisório do utilizador final de uma forma não intencional?

III. Ponderou se o sistema de IA deveria comunicar aos utilizadores que uma decisão, um conteúdo, um conselho ou um resultado provém de uma decisão algorítmica?

IV. Caso o sistema de IA inclua um sistema de conversação automática (chat bot), os utilizadores finais humanos foram informados do facto de estarem a interagir com um agente não humano?

V. Adotou salvaguardas para evitar o excesso de confiança ou o excesso de dependência face ao sistema de IA nos processos de trabalho?

VI. Assegurou a existência de um «botão de paragem» ou um procedimento para abortar uma operação de forma segura, se necessário? Esse procedimento aborta o processo por completo, parcialmente ou delega o controlo num ser humano?

2. Solidez técnica e segurança

VII. Em particular, tomou em consideração diferentes tipos e naturezas de vulnerabilidades, como a poluição de dados, as infraestruturas físicas ou os ciberataques?

VIII. Ponderou a aquisição de uma apólice de seguro para cobrir eventuais danos causados pelo sistema de IA?

IX. Caso existam riscos de o sistema de IA causar danos, analisou a regulamentação em matéria de responsabilidade e de defesa do consumidor? De que modo teve essa regulamentação em conta?

X. Procedeu a uma estimativa do impacto provável de uma falha do seu sistema de IA que o leve a fornecer resultados incorretos, que o torne indisponível ou que o faça fornecer resultados inaceitáveis do ponto de vista societal (p. ex., práticas discriminatórias)?

XI. Tomou medidas para avaliar se são necessários dados adicionais, por exemplo para melhorar a exatidão ou eliminar os enviesamentos?

XII. Adotou formas de medir se o seu sistema está a produzir um número inaceitável de previsões incorretas?

3. Privacidade e governação dos dados

XIII. Tomou medidas para aumentar a privacidade, tais como a encriptação, a anonimização e a agregação?

XIV. Harmonizou o seu sistema com potenciais normas pertinentes (p. ex., ISO, IEEE) ou protocolos amplamente adotados para a sua gestão e governação quotidianas dos dados?

[43] *Orientações éticas para uma IA de confiança* Grupo de peritos de alto nível sobre a inteligência artificial (já citado).

XV. Garantiu que estas pessoas são qualificadas e necessitam de aceder aos dados, e que possuem as competências necessárias para compreender a política de proteção de dados ao pormenor?

XVI. Assegurou um mecanismo de supervisão para registar quando, onde, como, por quem e para que fim os dados foram acedidos?

4. Transparência

XVII. Métodos utilizados para testar e validar o sistema algorítmico: no caso de um sistema de IA baseado em regras, os cenários ou casos utilizados para o testar e validar devem ser documentados;

XVIII. Os resultados ou as decisões tomadas pelo algoritmo, bem como outras decisões potenciais que resultariam de casos diferentes (p. ex., para outros subgrupos de utilizadores) devem ser documentados.

XIX. Assegurou que uma explicação dos motivos por que um sistema fez determinada escolha que levou a um determinado resultado pode ser tornada compreensível para todos os utilizadores que desejem obter uma explicação?

XX. Criou mecanismos para informar os utilizadores acerca das razões e dos critérios subjacentes aos resultados do sistema de IA?

XXI. Comunicou também os riscos potenciais ou percecionados, tais como enviesamentos?

XXII. Em função do caso de utilização, refletiu sobre a psicologia humana e as potenciais limitações, como o risco de confusão, o enviesamento da confirmação ou a fadiga cognitiva?

XXIII. Comunicou claramente as características, as limitações e as potenciais insuficiências do sistema de IA:

XXIV. - em caso de desenvolvimento: a quem está a implantá-lo num produto ou serviço?

XXV. - em caso de implantação: ao utilizador final ou consumidor?

5. Diversidade, não discriminação e equidade

XXVI. Tomou em consideração a diversidade e a representatividade dos utilizadores nos dados?

XXVII. Em função do caso de utilização, assegurou a existência de um mecanismo para permitir que outros assinalem questões relacionadas com enviesamento, discriminação ou mau desempenho do sistema de IA?

XXVIII. Estabeleceu mecanismos para garantir a equidade dos seus sistemas de IA? Ponderou utilizar outros mecanismos possíveis?

XXIX. Avaliou se o sistema de IA pode ser utilizado por pessoas com necessidades especiais ou deficiência, ou pessoas em risco de exclusão? De que forma foi esta possibilidade incorporada na conceção do sistema e como é verificada?

XXX. A equipa envolvida na construção do sistema de IA é representativa do seu público-alvo de utilizadores? É representativa da população em geral, considerando também outros grupos que possam ser tangencialmente afetados?

XXXI. Avaliou se poderão existir pessoas ou grupos desproporcionadamente afetados pelas implicações negativas?

6. Bem-estar societal e ambiental

XXXII. Criou mecanismos para medir o impacto ambiental do desenvolvimento, da implantação e da utilização do sistema de IA (p. ex., energia utilizada pelo centro de dados, tipo de energia utilizada pelos centros de dados, etc.)?

XXXIII. Assegurou que o sistema de IA assinale claramente que a sua interação social é simulada e que não tem qualquer capacidade para «compreender» ou «sentir»?

XXXIV. Assegurou que os impactos sociais do sistema de IA são bem compreendidos? Por exemplo, avaliou se há risco de perda de postos de trabalho ou de perda de competências da mão de obra? Que medidas foram tomadas para combater tais riscos?

7. Responsabilização

XXV. Estão disponíveis processos para que terceiros (p. ex., fornecedores, consumidores, distribuidores/vendedores) ou trabalhadores comuniquem eventuais vulnerabilidades, riscos ou enviesamentos no sistema/aplicação de IA?

XXVI. Criou mecanismos para fornecer informações aos utilizadores (finais)/terceiros sobre as possibilidades de recurso?

É também possível apresentar as sete categorias de preocupações éticas graficamente para mostrar que todas têm idêntica importância.

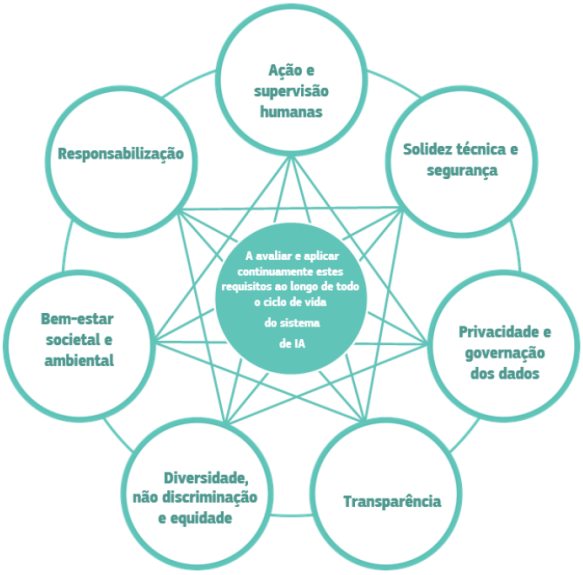

Figura 3. Interligação dos sete requisitos: todos têm igual importância e apoiam-se mutuamente, devendo ser aplicados e avaliados ao longo de todo o ciclo de vida de um sistema de IA[44]

De forma mais resumida, o Grupo de peritos de alto nível sobre a inteligência artificial na União Europeia, considera que uma IA de confiança tem três componentes:

1) deve ser ***legal***, garantindo o respeito de toda a legislação e regulamentação aplicáveis;

2) deve ser ***ética***, demonstrando respeito e garantindo a observância de princípios e valores éticos; e

3) deve ser ***sólida***, tanto do ponto de vista técnico como do ponto de vista social, uma vez que, mesmo com boas intenções, os sistemas de IA podem causar danos não intencionais. Uma IA de confiança diz respeito não só à fiabilidade do próprio sistema de IA, mas também à fiabilidade de todos os processos e intervenientes que fazem parte do ciclo de vida do sistema[45].

Em suma: a Europa digital deve refletir o melhor da Europa – aberta, justa, diversificada, democrática e confiante[46].

[44] *Orientações éticas para uma IA de confiança* Grupo de peritos de alto nível sobre a inteligência artificial (já citado).
[45] *Orientações éticas para uma IA de confiança* Grupo de peritos de alto nível sobre a inteligência artificial (já citado).
[46] Comunicação da Comissão *Construir o futuro digital da Europa* Bruxelas, 19.2.2020 COM(2020) 67 final, (já citado).

Reforçando a confiança: condições de utilização das tecnologias digitais

A transformação digital só pode funcionar se funcionar para todos e não apenas para uns poucos[47].

Os cidadãos devem ser empoderados para tomar as melhores decisões e garantir que todos beneficiam das vantagens da digitalização.

Numa época em que "o declínio dramático da confiança nas instituições, nos representantes políticos e nos meios de comunicação social"[48] é generalizado, para garantir a confiança, o mais importante é que os sistemas sejam concebidos com características que permitam responder com transparência a um conjunto de questões postas pelos cidadãos utilizadores. Essas questões são pelo menos quatro, e são respondidas pela Recomendação da Comissão Europeia relativa à utilização de tecnologias e dados para combater a crise da COVID-19:

Quem? As novas apps interoperáveis que venham a ser adotadas podem surgir por iniciativa do mercado ou dos Estados, mas carecem do consentimento ou aprovação dos Estados, pelo que se podem considerar, em qualquer caso, como sistemas de vigilância oficiais ou paraoficiais. As exigências técnicas e éticas são idênticas para as apps publicas e privadas. Todas elas devem dar todas as garantias de conseguir respeitar os requisitos regulamentares e éticos.

Como? Todo o sistema de vigilância epidemiológica assenta no pressuposto de que a adesão é facultativa[49]. Os vários serviços (como autodiagnóstico, notificações, alertas, conexão a serviços de telemedicina, dados de mobilidade, informações sobre trajetos ou aglomerações) não podem estar agregados, e dependentes de uma única adesão a tudo ou a nada. A adesão às funcionalidades ou serviços deve ser feita um a um (apenas informação, apenas diagnóstico, apenas georreferenciação, apenas acionamento de alertas, etc.). Os dados que são recolhidos pelo telemóvel são nele guardados e não serão enviados, a menos que o utilizador dê o seu consentimento e acione o envio a cada vez que pretender enviar os dados. É o cidadão que decide, livre e conscientemente se pretende enviar os seus dados que foram recolhidos pelo seu dispositivo de comunicação e nele armazenados. O sistema não poderá basear-se numa autorização única, mas antes cada envio exige uma atividade deliberada e uma autorização expressa do próprio utilizador.

Para quê? A aplicação deve servir apenas para vigilância da Covid-19 ou doenças similares que venham a surgir no futuro com idêntica gravidade, a menos que os cidadãos declarem voluntariamente pretender continuar a usar a app para outras doenças infetocontagiosas. Os dados devem ser acessíveis apenas para autoridades de saúde.

---

[47] Comunicação *Conectividade para um Mercado Único Digital Concorrencial - Rumo a uma Sociedade Europeia a Gigabits* (já citada).

[48] Parecer do Comité Económico e Social Europeu *Populismo e direitos fundamentais — zonas suburbanas e rurais* (parecer de iniciativa) (2020/C 97/07) Relatora: Karolina DRESZER-SMALEC Correlator: Jukka AHTELA Decisão da Plenária 20.2.2019 Adoção em plenária11.12.2019 (https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.C_.2020.097.01.0053.01.POR&toc=OJ:C:2020:097:FULL).

[49] Comunicação da Comissão *Orientações respeitantes a aplicações móveis de apoio à luta contra a pandemia de COVID-19 na perspetiva da proteção de dados* (2020/C 124 I/01) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29) "A confiança nelas depositadas é uma importante condição prévia do desenvolvimento, aceitação e utilização destas aplicações pelos cidadãos. As pessoas precisam de ter a certeza de que estas aplicações respeitam os direitos fundamentais e de que serão utilizadas apenas para os fins especificamente definidos, que não serão usadas para vigilância em larga escala e que os cidadãos manterão o controlo sobre os seus dados".

Quando? A aplicação funcionará apenas enquanto a epidemia durar. À medida que forem terminando as medidas de contenção da pandemia, a app deixará de funcionar sozinha, sendo todos os dados apagados e não será sequer necessário desinstalar a app no final.

Balanço e perspetivas futuras

Esta não será a primeira vez que os cidadãos da União Europeia beneficiam das vantagens de sistemas digitais com regras centralizadas.

O Sistema de Alerta Rápido para alimentos humanos e para animais — RASFF[50] — é uma ferramenta essencial para garantir o fluxo de informações para permitir uma reação rápida quando são detetados riscos para a saúde pública na cadeia alimentar. O RASFF permite partilhar informações sobre segurança alimentar de forma extremamente eficiente entre as autoridades nacionais de segurança alimentar dos 27 Estados-Membros da UE, a Comissão, a Agência Europeia da Segurança Alimentar, a Agência Espacial Europeia, a Noruega, Liechtenstein, Islândia e Suíça. As notificações urgentes são enviadas, recebidas e respondidas de forma eficiente a qualquer hora do dia ou da noite, sete dias por semana. As informações trocadas pelo RASFF podem levar à retirada de produtos do mercado. Graças ao RASFF, a UE possui um dos mais altos padrões de segurança alimentar do mundo.

A mesma coisa existe na União Europeia para os produtos de consumo destinados aos consumidores europeus[51]. O RAPEX[52] anuncia semanalmente os produtos perigosos encontrados no mercado europeu bem como as medidas tomadas, que podem ir desde alertas aos consumidores, até à recolha dos produtos e proibição de colocação de produtos similares no mercado.

No domínio das comunicações, os cidadãos europeus beneficiam da interoperabilidade telefónica desde que o Regulamento Europeu de 2015[53] acabou com os pagamentos de roaming nos telefonemas entre estados Membros a partir 15 de junho de 2017, ajudando assim a concretizar o mercado único digital. Este regime, que habitualmente toma a designação "roam-like-at-home", permite aos cidadãos usar o telemóvel em qualquer país da União como se estivessem no seu Estado de residência, sem quaisquer custos adicionais faturados pelos operadores móveis.

No domínio agrícola, a União Europeia já utiliza imagens de satélite para controlar as atividades agrícolas beneficiárias de apoios ou candidatas a fundos no âmbito da política agrícola comum para controlar o estado, os progressos e a conformidade das atividades agrícolas desenvolvidas no território dos Estados Membros. Em janeiro de 2020 o Tribunal de Contas[54] recomendou à Comissão Europeia a utilização dos mesmos procedimentos para monitorizar as mesmas exigências ambientais e climáticas.

---

[50] The Rapid Alert System for Food and Feed 2018 Annual Report https://ec.europa.eu/food/sites/food/files/safety/docs/rasff_annual_report_2018.pdf

[51] https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=SafeProductsOnline&lng=pt

[52] https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=main.listNotifications&lng=en

[53] Regulamento do Parlamento Europeu e do Conselho 2015/2120 de 25 de novembro de 2015.

[54] Tribunal de Contas Europeu, *Utilização de novas tecnologias de imagem no acompanhamento da Política Agrícola Comum: progresso constante em termos gerais, com maior lentidão no domínio do ambiente e do*

Os exemplos fornecidos são suficientes para demonstrar que as tecnologias digitais são uma alavanca fundamental da melhoria das condições de vida e parecem ser igualmente incontornáveis para ultrapassar a atual, ou futuras crises sanitárias.

Tal como a Comissão Europeia, pensamos que "como potentes facilitadores da transição para a sustentabilidade, as soluções digitais podem avançar na economia circular, apoiar a descarbonização de todos os setores e reduzir a pegada ambiental e social dos produtos colocados no mercado da UE. Por exemplo, setores-chave como agricultura de precisão, transporte e energia podem se beneficiar imensamente das soluções digitais na busca dos ambiciosos objetivos de sustentabilidade do Pacto Ecológico Europeu"[55].

É por tudo isto a União Europeia pretende modelar o seu futuro digital como uma sociedade aberta, democrática e sustentável: assegurar que as tecnologias de geolocalização e de comunicação digital garantem um ambiente confiável no qual os cidadãos têm poder de decisão sobre os dados que fornecem online e offline. O caminho europeu para a transformação digital pretende aprofundar os valores democráticos, respeitar os direitos fundamentais e contribuir para uma economia sustentável, neutra em termos de clima e eficiente em termos de recursos[56].

Em termos energéticos, a IA associada aos megadados pode servir para detetar as necessidades de energia com maior exatidão, possibilitando a criação de uma infraestrutura energética e a garantia de um consumo energético mais eficiente[57].

No setor dos transportes, transportes públicos inteligentes[58] ajudarão a minimizar a congestão rodoviária, otimizar a seleção de percursos, e reduzir o número mortes em acidentes rodoviários[59]. Podem também reforçar os esforços de descarbonização, reduzindo a pegada ambiental e permitindo que as pessoas com deficiência visual se tornem mais independentes[60]

É assim que a União Europeia pretende criar um espaço comum europeu de dados de saúde, essenciais para progredir nos domínios da prevenção, deteção e cura de doenças, bem como para tomar decisões informadas e fundamentadas com vista a melhorar a acessibilidade, a eficácia e a sustentabilidade dos sistemas de saúde. Mas a União pretende ir mais longe e criar também um espaço comum de dados financeiros, dados sobre as competências pessoais e empresariais e sobretudo dados industriais, da a agricultura, de mobilidade e de energia.

Por fim, pretende-se criar um espaço comum compreendendo igualmente dados do Pacto Ecológico Europeu, que permitam tirar partido dos dados para apoiar as ações prioritárias relativas às alterações climáticas, à economia circular, à poluição zero, à biodiversidade, à desflorestação e à garantia de cumprimento. Duas iniciativas concretas são «GreenData4All» (revisão da diretiva Inspire, que estabelece uma infraestrutura de informação geográfica na

---

clima Relatório Especial 4/2020 de 31.01.2020 (https://op.europa.eu/en/publication-detail/-/publication/06236121-43fd-11ea-b81b-01aa75ed71a1/language-en/format-HTML/source-115626237).

[55] Comunicação *Conectividade para um Mercado Único Digital Concorrencial - Rumo a uma Sociedade Europeia a Gigabits* (já citada).

[56] Comunicação da Comissão *Construir o futuro digital da Europa* Bruxelas, 19.2.2020 COM(2020) 67 final, (já citado).

[57] Ver, por exemplo, o projeto Encompass: http://www.encompass-project.eu/

[58] As novas soluções baseadas na IA ajudam a preparar as cidades para o futuro da mobilidade. Ver, por exemplo, o projeto financiado pela UE, denominado Fabulos: https://fabulos.eu/.

[59] *Orientações éticas para uma IA de confiança* Grupo de peritos de alto nível sobre a inteligência artificial (já citado).

[60]Ver, por exemplo, o projeto PRO4VIP, (http://www.euroblind.org/newsletter/2016/may-june/en/update-pro4vip-project) que tem como objetivos prioritários a mobilidade e a orientação de pessoas com dificuldade visuais ou combater ou cegueira, em especial devida ao envelhecimento.

União Europeia[61], e acesso à informação ambiental[62]) e «Destino Terra» (gémeo digital da Terra)[63]

Podemos portanto concluir que, graças às novas formas de comunicação e conetividade medida em gigabites, o mundo está a ficar cada vez mais pequeno, digital e sem fonteiras. Na sociedade, também ela cada vez mais digitalizada, a tecnologia está a contribuir para ganhos de bem estar tão significativos que já se fala do direito fundamental à internet.

Todas as condições estão reunidas para avançar, com segurança e confiança, para o futuro, *o nosso futuro* ***digital*** *comum*.

Referências

Buolamwini, Joy ; Gebru, Timnit "Gender shades: intersectional accuracy disparities in commercial gender classification", *Proceedings of the 1st Conference on Fairness, Accountability and Transparency,* Proceedings of Machine Learning Research 81:77-91, 2018 (http://proceedings.mlr.press/v81/buolamwini18a.html)

Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões *Inteligência artificial para a Europa* Bruxelas, 25.4.2018 COM(2018) 237 final (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN).

Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões *Uma estratégia europeia para os dados,* Bruxelas, 19.2.2020 COM(2020) 66 final (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:66:FIN).

Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões *Implantação segura de redes 5G na UE – Aplicação do conjunto de instrumentos da EU* Bruxelas, 29.1.2020 COM(2020) 50 final (https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0050&from=FR).

Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões *Construir o futuro digital da Europa* Bruxelas, 19.2.2020 COM(2020) 67 final (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:67:FIN).

Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões *Conectividade para um Mercado Único Digital Concorrencial - Rumo a uma Sociedade Europeia a Gigabits* (https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2016:0587:FIN:PT:PDF).

Comunicação da Comissão *Orientações respeitantes a aplicações móveis de apoio à luta contra a pandemia de COVID-19 na perspetiva da proteção de dados* (2020/C 124 I/01) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29)

Danzigera, Shai ; Levav, Jonathan ; Avnaim Liora *Extraneous factors in judicial decisions* Department of Management, Ben Gurion University of the Negev, Beer Sheva 84105, Israel; and Columbia Business School, Columbia University, New York, NY 10027 (http://houdekpetr.cz/!data/public_html/papers/economics_psychology/Danziger%20et%20al%202011.pdf).

Fjeld, Jessica; Achten, Nele; Hilligoss, Hannah; Nagy, Adam Christopher; Srikumar, Madhulika *Principled Artificial Intelligence: Mapping Consensus in Ethical and*

[61] Diretiva 2007/2/CE do Parlamento Europeu e do Conselho, de 14 de Março de 2007 (https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32007L0002).

[62] Diretiva 2003/4/CE, do Parlamento Europeu e do Conselho, de 28 de janeiro (https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32003L0004).

[63] https://ec.europa.eu/digital-single-market/en/news/convergent-use-high-performance-computing-cloud-data-and-artificial-intelligence-resources

Rights-based Approaches to Principles for AI, Research Publication No. 2020-1 January 15, 2020, https://cyber.harvard.edu/publication/2020/principled-ai ; https://ssrn.com/abstract=3518482).

Grupo de peritos de alto nível sobre a inteligência artificial criado pela Comissão Europeia em junho de 2018 *Orientações éticas para uma IA de confiança* (https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines)

Grupo independente de peritos de alto nível sobre a inteligência artificial criado pela Comissão Europeia em junho de 2018, "Uma definição de ia: principais capacidades e disciplinas científicas. Definição desenvolvida para efeitos dos documentos elaborados pelo grupo" (https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines).

International Telecommunication Union, *Next Generation Networks – Frameworks and functional architecture models Overview of the Internet of things* Recommendation ITU-T Y.2060 (06/2012) (https://www.itu.int/rec/T-REC-Y.2060-201206-I)

Livro branco *Sobre a inteligência artificial - Uma abordagem europeia virada para a excelência e a confiança*, Bruxelas, 19.2.2020 COM(2020) 65 final (https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_pt.pdf).

Livro Branco sobre a inteligência artificial: uma abordagem europeia virada para a excelência e a confiança Bruxelas, 19.2.2020 COM(2020) 65 final (https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_pt.pdf).

Parecer do Comité Económico e Social Europeu *Populismo e direitos fundamentais — zonas suburbanas e rurais* (parecer de iniciativa) (2020/C 97/07) Relatora: Karolina DRESZER-SMALEC Correlator: Jukka AHTELA Decisão da Plenária 20.2.2019 Adoção em plenária 11.12 (https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.C_.2020.097.01.0053.01.POR&toc=OJ:C:2020:097:FULL).

Parlamento Europeu e Conselho, Diretiva 2003/4/CE, de 28 de janeiro (https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32003L0004).

Parlamento Europeu e Conselho, Diretiva 2007/2/CE de 14 de Março de 2007 (https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32007L0002).

Public Policy Division of the Software & Information Industry Association, *Algorithmic Fairness,* Siia Issue Brief 22, September 2016. (http://www.siia.net/Portals/0/pdf/Policy/Algorithmic%20Fairness%20Issue%20Brief.pdf)

Recomendação (UE) 2020/518 da Comissão Europeia, de 8 de abril de 2020, relativa a um conjunto de instrumentos comuns a nível da União com vista à utilização de tecnologias e dados para combater a crise da COVID-19 e sair da crise, nomeadamente no respeitante às aplicações móveis e à utilização de dados de mobilidade anonimizados (https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2020.114.01.0007.01.POR&toc=OJ:L:2020:114:TOC).

Regulamento do Parlamento Europeu e do Conselho 2015/2120 de 25 de novembro de 2015.

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* Bruxelas 19.2.2020 COM(2020) 64 final (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0064)

Tolan, S.; Miron, M.; Gomez, E.; Castillo, C. "Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia", *Best Paper Award, International Conference on AI and Law,* 2019

(https://docplayer.net/131278107-Why-machine-learning-may-lead-to-unfairness-evidence-from-risk-assessment-for-juvenile-justice-in-catalonia.html).

Tribunal de Contas Europeu, *Utilização de novas tecnologias de imagem no acompanhamento da Política Agrícola Comum: progresso constante em termos gerais, com maior lentidão no domínio do ambiente e do clima* Relatório Especial 4/2020 de 31.01.2020 (https://op.europa.eu/en/publication-detail/-/publication/06236121-43fd-11ea-b81b-01aa75ed71a1/language-en/format-HTML/source-115626237).

United Nations Human Rights Council "The promotion, protection and enjoyment of human rights on the Internet" 27 June 2016 A/HRC/32/L.20 https://undocs.org/A/HRC/32/L.20)

United Nations Human Rights Council "The promotion, protection and enjoyment of human rights on the Internet" 5 july 2012 A/HRC/20/2 (https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A-HRC-20-2_en.pdf).

Vanbergen, Adam J.; Potts, Simon G. ; Vian, Alain; Malkemper E. Pascal; Young, Juliette ; Tscheulin, Thomas "Risk to pollinators from anthropogenic electro-magnetic radiation (EMR): Evidence and knowledge gaps", *Science of The Total Environment*, Volume 695, 10 December 2019, 133833 (https://www.sciencedirect.com/science/article/pii/S0048969719337805)

Winterberg, Susan; Lemos, Martin *Automation: A Framework for a Sustainable Transition*, Business for Social Responsibility, April 2017 (https://www.bsr.org/reports/BSR_Automation_Sustainable_Jobs_Business_Transition.pdf).

World Health Organization, *Establishing a dialogue on risks from electromagnetic fields*, 2002 (https://apps.who.int/iris/bitstream/handle/10665/42543/9241545712_eng.pdf?sequence=1&isAllowed=y&ua=1).

World Health Organization, *Public health implications of excessive use of the Internet and other communication and gaming platforms*, 13 September 2018 (https://www.who.int/news-room/detail/13-09-2018-public-health-implications-of-excessive-use-of-the-internet-and-other-communication-and-gaming-platforms)