ISSN 2238-9121

INTELIGÊNCIA ARTIFICIAL E PREVENÇÃO DE CRIMES: DA GUERRA AO TERROR À *SURVEILLANCE*

ARTIFICIAL INTELLIGENCE AND CRIME PREVENTION: FROM THE WAR ON TERROR TO SURVEILLANCE

Luiza Berger von Ende[1]
Júlia Schmidt Kronbauer[2]
Rafael Santos de Oliveira[3]

RESUMO

Em um contexto de *surveillance*, big data e guerra ao terror pós 11 de Setembro, este trabalho objetiva compreender que riscos são oferecidos aos direitos humanos fundamentais pelo uso da inteligência artificial no tratamento de dados com o pretexto de combater o terrorismo. Utiliza-se o método de abordagem dedutivo e os de procedimento monográfico e funcionalista para investigar o papel da inteligência artificial na guerra ao terror, examinar o tratamento conferido ao terrorismo pelo ordenamento jurídico nacional e internacional e compreender a eficiência do emprego dessa tecnologia para o fim a que se propõe e os reflexos causados por este fenômeno nos direitos fundamentais e humanos. Depreende-se que, a partir de parcerias público-privadas na troca de informações, faz-se o tratamento massivo de dados pessoais que identificam padrões e realizam previsões comportamentais da população; esse prognóstico, então, é utilizado para identificar possíveis terroristas. Entretanto, o conceito de terrorismo é bastante impreciso, abrindo espaço para servir como instrumento político e justificativa para a invasão da privacidade de todos os cidadãos, com a criação de leis penais autoritárias que ameaçam liberdades civis. Por fim, não somente a *surveillance* se mostra inefetiva para evitar o terrorismo como também acarreta a discriminação de grupos da sociedade, a violação de direitos políticos e o próprio ataque ao Estado Democrático de Direito, que é submetido a um estado de exceção permanente.

Palavras-chave: *big data*; direitos fundamentais e humanos; terrorismo; vigilância.

ABSTRACT

In the context of surveillance, Big Data, and the war on terror after September, 11th, this paper aims to comprehend the risks that the use of artificial intelligence in the treatment of data, with the pretext of ending terrorism, presents to the fundamental and human rights. The deductive method of approach, as well as the monographical and functionalist methods of procedure are used to investigate the role that artificial intelligence has in the war on terror, to examine the treatment that national and international legal systems give to terrorism, and to comprehend the efficiency of the use of this technology to its established goal and its effects on the fundamental and human rights. It is surmised that, through public-private partnerships in the exchange of information, a massive treatment of personal data is carried out, identifying patterns and making comportamental

[1] Bolsista CAPES. Mestranda do Programa de Pós-Graduação em Direito da Universidade Federal de Santa Maria (PPGD/UFSM). Bacharel em Direito pela UFSM. Pesquisadora do Centro de Estudos e Pesquisas em Direito e Internet (CEPEDI/UFSM). E-mail: luizabergerv@gmail.com.
[2] Mestranda do Programa de Pós-Graduação em Direito da Universidade Federal de Santa Maria (PPGD/UFSM). Bacharel em Direito pela UFSM. Pesquisadora do Centro de Estudos e Pesquisas em Direito e Internet (CEPEDI/UFSM). E-mail: julia.schmidt.k@gmail.com.
[3] Doutor em Direito pela Universidade Federal de Santa Catarina. Professor Associado I no Departamento de Direito da Universidade Federal de Santa Maria, em regime de dedicação exclusiva, e no Programa de Pós-Graduação em Direito da UFSM. Coordenador do CEPEDI/UFSM. E-mail: rafael.oliveira@ufsm.br.

predictions about the population; this prognostic is then utilized to identify possible terrorists. However, the definition of terrorism is rather imprecise, which allows it to be used as a political instrument and as a reason for the invasion of privacy of all citizens, with the creation of authoritarian criminal laws that threaten civil liberties. Finally, not only does surveillance show itself as ineffective to prevent terrorism, but it can also entail the discrimination of certain social groups, the violation of political rights, and an attack against the democratic constitucional state, which is subjected to a permament state of emergency.

Keywords: big data; fundamental and human rights; terrorism; surveillance.

INTRODUÇÃO

Desde a Revolução Industrial, há o receio generalizado de que os seres humanos serão substituídos por máquinas. Os Ludistas, naquela época, revoltaram-se contra a troca da mão de obra humana pela tecnologia, destruindo os instrumentos de trabalho em protesto. Hoje, o temor se torna ainda mais fundado à medida que novos sistemas tecnológicos chegam cada vez mais próximos a simular a inteligência humana, sendo capazes de realizar tarefas cognitivas, com a vantagem de fazê-las muito mais rápido. Há mesmo quem disserte sobre a possibilidade de um paradigma de dataísmo no futuro, no qual o controle dos recursos e da vida terrestre como um todo seria exercido por um super-algoritmo[4].

De imediato, elucide-se que a inteligência artificial (IA) - nome dado de forma genérica à tecnologia capaz de, e. g., criar imagens, traduzir textos e realizar reconhecimento facial - muito embora apresente engenhosas funcionalidades, ainda não deve causar preocupação por substituir de forma completa os seres humanos. Tendo em vista que sua "inteligência" é por demais específica, ou seja, que esses programas são capazes de realizar tarefas em prol de um objetivo bastante estreito, ainda não foi alcançada uma inteligência artificial geral capaz de realizar as mais diversas operações. O matemático David Sumpter[5] até mesmo compara a inteligência de uma máquina à de uma mera bactéria, incapaz de realizar atividades para as quais não foi intensamente treinada.

Não obstante, o nível de desenvolvimento da IA atual é capaz, sim, de realizar tarefas expressivas, como o tratamento de dados e a elaboração de previsões a partir dos padrões neles examinados. Assim, grandes empresas digitais utilizam essas predições com

[4] HARARI, Yuval Noah. **Homo Deus:** uma breve história do amanhã. São Paulo: Companhia das Letras, 2016.
[5] SUMPTER, David. **Dominados pelos Números:** do Facebook e Google às fake news – os algoritmos que controlam nossa vida. Tradução Anna Maria Sotero, Marcello Neto. Rio de Janeiro: Bertrand Brasil, 2019.

o fim de realizar o direcionamento personalizado de anúncios para cada internauta; instituições financeiras calculam a probabilidade de um potencial cliente quitar a dívida de um empréstimo; e empresas selecionam candidatos sob medida para uma vaga de emprego ofertada, dentre milhares de currículos submetidos. Para que tais tratamentos e prognósticos sejam executáveis, é necessário que esteja à disposição do programa uma quantidade significativa de dados a serem analisados, a qual se consubstancia no fenômeno do *big data*. Ele representa, em primeiro lugar, a existência desses dados circulando em rede, em especial a rede mundial de computadores; em segundo lugar, o *big data* implica o armazenamento de toda essa quantidade de dados[6], o que é possível devido aos recursos computacionais de acumulação informacional de grandes empresas e governos.

A primeira etapa, isto é, a circulação dos dados, é fomentada, principalmente, pela facilidade de produção de conteúdo na internet pelos próprios usuários; a segunda - o armazenamento - ademais dos interesses privados, foi impulsionada após 11 de Setembro de 2001, quando, nos Estados Unidos, aviões colidiram com os prédios do World Trade Center e provocaram milhares de mortes no mais famoso atentado terrorista da história. Em resposta, o país inaugurou uma guerra ao terror, não apenas de caráter militar, como também informacional. Entre as medidas adotadas estava a elaboração de normas internas que legalizaram a coleta e o tratamento de dados pelas instituições governamentais estadunidenses de forma irrestrita, culminando, assim, em uma constante e sorrateira vigilância - o que se entende por *surveillance*.

Ocorre que a capacidade de espionagem do país não se restringiu somente ao território norte-americano. Particularmente após as revelações feitas pelo ex-analista de dados da CIA Edward Snowden, descobriu-se que a interceptação de dados de cidadãos estadunidenses e estrangeiros, seu armazenamento por tempo indefinido e sua utilização para propósitos sigilosos eram práticas comuns da Agência de Segurança Nacional dos EUA[7], cujo episódio de maior comento no Brasil ocorreu quando da descoberta de coleta indevida de dados telefônicos da então Presidenta da República Dilma Rousseff. Os dados eram utilizados pela inteligência norte-americana com a justificativa da prevenção do terrorismo, alegadamente, pois a tecnologia da Agência seria capaz de identificar padrões de dados que revelassem a premeditação e organização de futuros ataques terroristas.

Nesse cenário de vigilância constante e de promessas de prevenção de crimes pelo

[6] SCHNEIER, Bruce. **Data and Goliath:** the hidden battles to collect your data and control your world. New York: W. W. Norton, 2015.
[7] SNOWDEN, Edward. **Eterna Vigilância:** Como montei e desvendei o maior sistema de espionagem do mundo. Tradução Sandra Martha Dolinski. São Paulo: Planeta do Brasil, 2019.

uso da inteligência artificial que se estende até os tempos hodiernos, propõe-se a seguinte questão: que riscos para os direitos fundamentais e humanos podem ser causados a partir do uso da IA no contexto de *surveillance* sob o pretexto da prevenção do terrorismo? O presente trabalho utiliza o método de abordagem dedutivo para compreender os reflexos da vigilância de dados e o uso da inteligência artificial quando usados com a justificativa da prevenção do terrorismo. Sob o método de procedimento funcionalista, a primeira seção trata de compreender como atua a IA em um contexto de *big data* em prol da vigilância, bem como o papel de atores públicos e privados para entender como ocorre a elaboração e do funcionamento das estruturas tecnológicas que sustentam a guerra informacional ao terror e a *surveillance*. Na segunda parte, enfrenta-se a forma com que o terrorismo é tratado no ordenamento jurídico nacional e internacional, tecendo entendimentos sobre os reflexos nos direitos humanos e fundamentais, bem como no Estado Democrático de Direito. Por fim, o terceiro tópico investiga a efetividade da vigilância por meio da IA para o combate ao terror e o impacto desse cenário nos direitos da população. Estes dois últimos itens empregam o método monográfico pelo estudo de casos suficientemente representativos de outros semelhantes que permitam a generalização e um entendimento amplo sobre o fenômeno. As técnicas de pesquisa foram a bibliográfica, pelo estudo de livros e artigos científicos sobre a temática, bem como a documental, no exame de relatórios e normas nacionais e estrangeiras.

1 O PAPEL DA INTELIGÊNCIA ARTIFICIAL E DO *BIG DATA* NA GUERRA AO TERROR

De forma sucinta, é possível afirmar que a inteligência artificial, considerando a abordagem do aprendizado de máquina ou aprendizado profundo, é um algoritmo - isto é, uma sequência de código lógica e finita com o objetivo de solucionar um problema - que confere maior grau de autonomia para que o próprio programa tome decisões, ancoradas tanto na programação prévia quanto nos dados de treinamento que recebe. A mais exitosa abordagem do aprendizado de máquina hoje é a rede neural, que permite que o computador descubra como atingir o objetivo desejado a partir de seus próprios métodos, com mínima interferência humana na programação. O sucesso dessa perspectiva se dá em

razão de que seus combustíveis se encontram de forma abundante no ambiente digital: grande poder computacional e uma vasta quantidade de dados[8].

Esse gigante volume de dados que alimenta as inteligências artificiais advém do fenômeno do *big data*, definido pelo criptógrafo e especialista em cibersegurança Bruce Schneier[9] como a prática geral de coletar e armazenar todos os tipos de dados. Foi a partir da popularização da internet e, posteriormente, da segunda geração da Web, que, além de receptores, os internautas passaram a ser produtores de conteúdo[10], desencadeando o fenômeno. A explosão das redes sociais, de sites de negócios e plataformas de busca continua a gerar um tráfego de dados gigantesco, em que os mais de 5,3 bilhões de usuários da internet passam, em média, quase 7 horas diárias utilizando a rede mundial de computadores[11] e produzindo dados e metadados em todas as operações.

Diante da abundância informacional, dados que eram inicialmente utilizados para simples melhoria técnica nas plataformas passaram a ser vistos como renda em potencial para as empresas digitais. Como descrito por Zuboff[12], assim foi construída a era do capitalismo de vigilância, em que a experiência humana nas plataformas da internet é capturada e armazenada pelas companhias, as quais utilizam programas computacionais, algoritmos preditivos e inteligência artificial para correlacionar esses dados e obter padrões que permitam prever o comportamento futuro de cada internauta-cidadão. Essa previsão, então, é vendida a anunciantes, e transformou-se na principal fonte de renda de gigantes digitais como Google, Amazon e Facebook. Assiste razão a Zuboff quando contesta a legitimidade da coleta dos dados e dos fins aos quais se destinam, os quais geralmente desprezam a privacidade e a autonomia dos indivíduos.

Portanto, é das plataformas a origem da maior parte da vigilância como se conhece hoje, e, cada vez mais, se torna impossível não se submeter a ela: os serviços digitais, dominados por um grupo muito seleto e poderoso de empresas, são, mais do que nunca, indispensáveis para a vida em sociedade. Assim, solicitar a própria exclusão digital não é uma opção viável, e escolher entre duas grandes empresas capitalistas de vigilância não

[8] LEE, Kai-Fu. **Inteligência Artificial:** como os robôs estão mudando o mundo, a forma como amamos, nos comunicamos e vivemos. Tradução Marcelo Barbão. Rio de Janeiro: Globo Livros, 2019.
[9] SCHNEIER, Bruce. **Data and Goliath:** the hidden battles to collect your data and control your world. New York: W. W. Norton, 2015.
[10] MAGRANI, Eduardo. **A Internet das Coisas.** Rio de Janeiro: FGV Editora, 2018.
[11] WE ARE SOCIAL; HOOTSUITE. Digital 2024 Global Overview Report: the essential guide to the world's connected behaviours. **We Are Social,** 2024. Disponível em: https://wearesocial.com/uk/blog/2024/01/digital-2024. Acesso em: 18 out. 2024.
[12] ZUBOFF, Shoshana. A Era do Capitalismo de Vigilância: a luta por um futuro humano na nova fronteira do poder. Tradução George Schlesinger. Rio de Janeiro: Intrínseca, 2021.

torna mais livre o internauta ou melhor tutela seus dados, pois a vigilância permanece no mesmo vigor[13].

Nesse sentido, é uma prática recorrente ao redor do planeta que instituições governamentais realizem parcerias com o setor privado para transacionar dados, de forma que a vigilância pública seja diretamente interligada com a privada. Embora isso aconteça em vários países, é interessante destacar o pioneirismo dos Estados Unidos na corrida da *surveillance*, uma vez que é sede de muitas das maiores empresas da internet do mundo, que as suas instituições dispõem de bastante tecnologia e recursos para a inteligência e a segurança nacional e que foi o país que instaurou a guerra ao terror a partir do atentado das Torres Gêmeas. Desde então, diversos projetos e legislações foram implementados para promover a segurança e o combate ao terrorismo, como o Patriot Act, com a premissa de que, pela vigilância, surgiriam indícios de futuros atos de terrorismo para que pudessem ser tomadas medidas antecipatórias que impedissem a concretização do ato criminoso. O resultado dessa parceria público-privada de intercâmbio de dados é que se torna muito difícil que se elaborem leis, especialmente nos EUA, para barrar a vigilância corporativa, visto que o próprio governo é beneficiado por ela[14].

A despeito da cooperação para a troca voluntária de informações, as instituições governamentais daquele país frequentemente subvertem o acordo e obtêm dados de maneira a invadir sistemas e recolher materiais de forma autoritária. Ao inserir *backdoors* nos produtos comercializados por empresas privadas, inclusive de menor porte, agências estatais invadem de maneira arbitrária a coleta e armazenamento de dados das corporações, canalizando o material obtido diretamente para sua utilização[15]. Isso veio à tona e fomentou intensa preocupação a contar das revelações sobre as práticas da Agência de Segurança Nacional dos EUA feitas pelo ex-analista de dados que trabalhou na instituição, Edward Snowden, as quais exibiram as práticas autoritárias da Agência. A instituição mantinha o registro de dados de cidadãos norte-americanos e estrangeiros armazenados desde longa data e por tempo indeterminado, realizando tratamento computacional e até mesmo investigações a partir dos dados[16].

[13] SCHNEIER, Bruce. **Data and Goliath:** the hidden battles to collect your data and control your world. New York: W. W. Norton, 2015.
[14] SCHNEIER, Bruce. **Data and Goliath:** the hidden battles to collect your data and control your world. New York: W. W. Norton, 2015.
[15] SCHNEIER, Bruce. **Data and Goliath:** the hidden battles to collect your data and control your world. New York: W. W. Norton, 2015.
[16] SNOWDEN, Edward. **Eterna Vigilância:** Como montei e desvendei o maior sistema de espionagem do mundo. Tradução Sandra Martha Dolinski. São Paulo: Planeta do Brasil, 2019.

Há quem defenda que a vigilância é inerente à tecnologia, e que os benefícios oferecidos em troca da espionagem são uma troca justa e inevitável. Entretanto, não passa de um mito: é possível existir tecnologia sem *surveillance*, e o capitalismo de vigilância foi elaborado intencionalmente por quem detém o poder da informação[17]. Assim, é imprescindível que sejam observados princípios basilares dos direitos humanos e fundamentais em todas as etapas do funcionamento e utilização das plataformas e serviços digitais (mas também analógicos) que coletem e utilizem dados pessoais.

Importa mencionar que, em que pese existam recentes leis de proteção a dados pessoais - como a General Data Protection Regulation (GDPR) da União Europeia, de 2016, e a Lei Geral de Proteção de Dados Pessoais brasileira (LGPD - Lei n. 13.709/2018) - não é possível afirmar que, por si só, conferem enfrentamento suficiente à coleta e tratamento indiscriminado e arbitrário dessas informações. Notam-se dificuldades na efetiva investigação e responsabilização de corporações privadas, que são a fonte principal das informações utilizadas por agências governamentais, ainda que ambas as leis tenham entrado em vigor[18].

Além disso, há um ponto chave que falta nesse cenário: a cientificidade e veracidade do resultado da correlação e do tratamento de dados. Veja-se que os algoritmos das corporações que realizam essas tarefas são protegidos por patentes e leis de propriedade intelectual, o que não permite que se compreenda como o algoritmo chegou a uma decisão a partir da correlação dos dados; e que, partindo desse ponto, estão livres para fazerem inferências que afetarão a vida dos cidadãos e a segurança pública, identificando possíveis criminosos com base nos rastros digitais deixados por internautas nos sites da Web. Ocorre, ainda, que estas correlações computacionais são essencialmente diferentes de estudos estatísticos propriamente ditos, pois estes últimos têm uma metodologia de obtenção de estatística rígida e amparada por teorias vastamente testadas. Em outras palavras, não somente porque dois eventos ocorrem simultaneamente é que eles estão interligados, e a falta de rigor da análise feita a partir do *big data*, muitas vezes, ignora esse parâmetro[19]. Assim, grande parte das correlações que são feitas para

[17] ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância:** a luta por um futuro humano na nova fronteira do poder. Tradução George Schlesinger. Rio de Janeiro: Intrínseca, 2021.
[18] ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância:** a luta por um futuro humano na nova fronteira do poder. Tradução George Schlesinger. Rio de Janeiro: Intrínseca, 2021.
[19] LINDOSO, Maria Cristine Branco. Discriminação de gênero em processos decisórios automatizados. Dissertação (Mestrado em Direito) - Programa de Pós-Graduação em Direito, Universidade de Brasília. Brasília, 2019.

identificar possíveis criminosos e terroristas são, na verdade, falsas, o que é certamente capaz de causar violações a direitos humanos e fundamentais.

Esse cenário ainda é intensificado por um senso comum que aceita a utopia da imparcialidade algorítmica, a qual imagina que, por se tratarem de operações realizadas por máquinas, sem sentimentos ou preconceitos humanos, seriam necessariamente imparciais e justas. Sem embargo, algoritmos e IAs - por mais autônomas que sejam - têm pontos cegos que "refletem o julgamento e as prioridades de seus criadores"[20], de modo algum podendo ser escusadas ao agir reproduzindo vieses e discriminações.

Depreende-se, portanto, que a IA é nutrida pelas bases de dados de empresas privadas, que também é utilizada por governos. Ambos os atores realizam correlações entre dados pessoais e realizam predições comportamentais, estes últimos com o objetivo explícito de combater o terrorismo, mas sem que o resultado desse tratamento seja, necessariamente, verídico, em razão da falta de cientificidade dos frutos do tratamento de dados. Assim, muitas correlações incorretas acabam pondo em risco direitos da população a nível nacional e internacional. Em vista disso, na sequência, abordam-se os reflexos da *surveillance* nos direitos fundamentais e humanos, discorrendo sobre a pertinência da prática para, de fato, atuar na prevenção criminal e terrorista.

2 O TRATAMENTO JURÍDICO DA AMEAÇA ABSTRATA DO TERRORISMO

Baseado no entendimento dos interesses públicos e privados no emprego da IA para a prevenção do terrorismo, é preciso perceber de que forma essa conjuntura relaciona-se com os direitos fundamentais e humanos, tanto a nível nacional quanto internacional. Assim, é necessário o exame de como ordenamentos jurídicos compreendem o terrorismo e em que medida atingem outras problemáticas ao lidarem com a segurança nacional e os dados da população mundial.

Apesar de existirem diversos dispositivos legislativos que se propõem a combater a prática criminosa, como a nacional Lei Antiterrorismo (Lei n. 13.260/2016) e a Resolução 1.566 do Conselho de Segurança da ONU, os conceitos de terrorismo - e, consequentemente, de terrorista - neles apresentados são muito amplos e imprecisos. Isso faz com que se abra espaço para a utilização indiscriminada do termo, que pode até

[20] O'NEIL, Cathy. **Algoritmos de Destruição em Massa:** como o Big Data aumenta a desigualdade e ameaça a democracia. Tradução Rafael Abraham. Santo André: Rua do Sabão, 2020. p. 34.

mesmo ser utilizado como um instrumento político[21]. Assim, a definição de terrorista assemelha-se muito à de inimigo, desenvolvido por Zaffaroni: ambas são conceituações amplas, que incentivam e até mesmo necessitam da permeação do decisionismo para preencher seus vazios e, portanto, não são figuras onticamente impostas nem dados de fato que se impõem ao direito, mas, sim, elementos politicamente assinalados[22]. Em suma, a identificação do terrorista, ou do inimigo, é "vazia de conteúdo, que o poder pode preencher a seu bel prazer, porque sempre necessita ter um inimigo"[23].

Outro problema criado pela implantação desse conceito vago no ordenamento jurídico é a dificuldade para diferenciar os inimigos do restante da população civil, já que se argumenta que aqueles que devem ser combatidos pelo Direito Penal ocultam-se entre a população[24]. Dessa maneira, quando se propõe a neutralização desses indivíduos, pressupõe-se, em primeiro lugar, a necessidade de sua individualização e identificação dentro da sociedade. Tal exigência, por sua vez, apenas pode ser suprida através da investigação e, consequentemente, da invasão à privacidade de todos os cidadãos.

Dessa forma, a guerra contra o terrorismo não somente cria uma ameaça abstrata que pode ser utilizada como pretexto para elencar determinadas pessoas como inimigas da população civil, de acordo com o interesse de determinadas pessoas que estão no poder, mas também aprova e justifica os meios necessários de violação da privacidade para que isso ocorra. Os mecanismos legislativos aprovados em nome da guerra ao terror culminam, então, em um ambiente jurídico propício ao autoritarismo estatal:

> Quando autorizam invasões de domicílio, revistas de pessoas, veículos automotores e residências, investigações e registros de comunicações de toda índole, detenções de suspeitos etc., mas apenas de suspeitos de terrorismo, sabe-se que será impossível evitar que as agências policiais utilizem estas faculdades cada vez que o julgarem conveniente, bastando-lhes alegar que o fazem por suspeita de terrorismo e que, por acaso, acharam cigarros de maconha, dinheiro não declarado ou uma carteira roubada. Tudo isso contando com agências executivas e políticas não deterioradas, pois do contrário sabe-se perfeitamente que esses elementos declararão ter encontrado as coisas por acaso, sempre que não tiverem chegado a um acordo extorsivo com o infrator. Com essas medidas, abre-se um amplo campo para a corrupção, a tortura, as vinganças pessoais, os

[21] BASTOS, Bruna. **Os Caminhos do Terrorismo e da Desumanização:** por uma cooperação internacional. Cruz Alta: Ilustração, 2021.
[22] ZAFFARONI, Eugenio Raúl. **O Inimigo no Direito Penal.** Rio de Janeiro: Editora Revan, 2007.
[23] ZAFFARONI, Eugenio Raúl. **O Inimigo no Direito Penal.** Rio de Janeiro: Editora Revan, 2007. p. 142.
[24] ZAFFARONI, Eugenio Raúl. **O Inimigo no Direito Penal.** Rio de Janeiro: Editora Revan, 2007.

> assédios sexuais, a chantagem e a perseguição política de dissidentes, antipáticos ou indisciplinados[25].

O extrato de Zaffaroni mostra que a guerra ao terror faz com que sejam criadas leis penais e processuais autoritárias, que violam os direitos humanos e fundamentais e as liberdades civis, objetivando neutralizar o terrorismo. Ao redor do mundo, políticos promulgam legislações que possuem o intuito de antecipar e prevenir ameaças e ataques terroristas através da análise de dados da população, priorizando uma suposta efetivação da segurança pública em detrimento dos princípios e garantias constitucionais.

Tal pretensão está presente na legislação russa e francesa. A Lei Federal nº 242-FZ, da Rússia, ampliou a capacidade de intervenção estatal nos dados das grandes empresas da internet, possibilitando a interceptação de dados pelo governo russo. Igualmente, na França, mudanças na legislação de segurança na internet permitiram que os órgãos de inteligência franceses pudessem grampear telefones, interceptar comunicações eletrônicas e também todas as informações de usuários de empresas de internet[26].

O ordenamento jurídico pátrio também produziu legislações semelhantes, como a Lei Antiterrorismo, que pune a realização de atos preparatórios de terrorismo, bem como "receber, prover, oferecer, obter, guardar, manter em depósito, solicitar, investir, de qualquer modo, direta ou indiretamente, recursos, ativos, bens, direitos, valores ou serviços de qualquer natureza, para o planejamento, a preparação ou a execução"[27] dos crimes previstos na lei. No que tange à investigação de tais delitos, o diploma referencia a Lei nº 12.850/2013, que prevê, entre outros meios de obtenção de prova, a interceptação de comunicações telefônicas e telemáticas e o acesso a dados cadastrais constantes de bancos de dados públicos ou privados e a informações eleitorais ou comerciais[28].

---

[25] ZAFFARONI, Eugenio Raúl. **O Inimigo no Direito Penal.** Rio de Janeiro: Editora Revan, 2007. p. 119.

[26] MORAIS, José Luis Bolzan de. O fim da geografia institucional do Estado. A "crise" do Estado de Direito!. In: MORAIS, José Luis Bolzan de (Org.). **Estado & Constituição:** o "fim" do Estado de Direito. Florianópolis: Tirant Lo Blanch, 2018.

[27] BRASIL. Lei n. 13.260, de 16 de março de 2016. Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis n º 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013. Brasília: **Diário Oficial da União**, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm. Acesso em: 22 jul. 2021. s. p.

[28] BRASIL. Lei n. 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Brasília: **Diário Oficial da União**, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12850.htm. Acesso em: 21 set. 2021.

Assim, a Lei Antiterrorismo permite, na verdade, a invasão à privacidade de indivíduos com o intuito (ou pretexto) de investigar atos preparatórios - de rol exemplificativo, ou seja, não delimitados ou especificados - de um crime de definição ampla (ou genérica). É evidente a maneira que o dispositivo legal em questão abre margem para atuações arbitrárias e injustas de autoridades policiais, bem como oportuniza a manifestação de comportamentos autoritários e discriminatórios por parte do Estado. Ou seja, o advento de legislações como as supramencionadas cria condições de possibilidade para a instrumentalização do Direito como fato legitimador de condutas intervencionistas e violentas, com a prerrogativa de um combate a movimentos terroristas, mas que, muitas vezes, são meramente uma fachada para a satisfação de outros interesses políticos[29].

Além disso, é importante destacar que o medo generalizado - instituído pela existência do terrorismo e reforçado pela espetacularização e pelo sensacionalismo midiático - faz com que certa parcela da população aceite, voluntariamente, a instauração de um regime de *surveillance*. Isso porque busca-se difundir o entendimento de que violações dos direitos humanos e de liberdades civis são necessárias para evitar e combater um mal maior. Em nome da segurança, é instalado, apoiado e legitimado um regime de exceção que não é mais excepcional, mas permanente através de leis como as citadas.

Dessa forma, através de legislações de controle e de coleta e uso de dados por parte dos Estados, busca-se identificar possíveis ameaças terroristas e prevenir ataques. Entretanto, como é impossível saber *ab initio* quem é o inimigo/terrorista, é preciso acessar e analisar os dados de todos os indivíduos. Essa análise da população em geral, por sua vez, só pode ser feita através de ferramentas de inteligência artificial, que filtram termos e códigos e apontam padrões de entre usuários, com o intuito de realizar predições comportamentais. O problema é que essas tecnologias são propensas a falhas e vieses e, além disso, muitas vezes, possuem processos de decisão opacos, produzindo resultados que não podem ser explicados nem pelos próprios desenvolvedores dos algoritmos.

3 A EFETIFIDADE DA *SURVEILLANCE* COMO MEDIDA PARA EVITAR O TERRORISMO E EFEITOS DO TRATAMENTO DE DADOS SOBRE OS DIREITOS HUMANOS E FUNDAMENTAIS

[29] BASTOS, Bruna. **Os Caminhos do Terrorismo e da Desumanização:** por uma cooperação internacional. Cruz Alta: Ilustração, 2021.

Quando se debruça mais especificamente sobre a questão da *surveillance* e do *big data* como ferramentas de investigação para identificar ameaças terroristas, tem-se que, com suficientes dados pessoais e comportamentais coletados de uma determinada pessoa, não importa quem ela seja, ela pode ser acusada e considerada culpada de algum crime ou infração penal. Isso porque, tal como a definição de terrorismo, o conceito do que é errado também é arbitrário e pode mudar rapidamente de acordo com quem está no poder de decidir a respeito de tais conceitos – o que pode, inclusive, resultar na categorização e discriminação de determinados setores da população[30].

Ademais, é difícil estabelecer padrões entre os atos de terrorismo, o que é essencial para cumprir o propósito de prevenir ameaças. Essa dificuldade existe devido ao fato de que cada ataque é único e, também, porque são raros os indivíduos que praticam condutas como essa - o que faz com que a sua identificação tenha um impacto desproporcional nos critérios de identificação de outros prováveis terroristas[31].

Culmina-se, assim, em estratégias de detecção inefetivas, as quais, além de todo o exposto, promovem a crença em estereótipos ofensivos, que maculam a ordem e a harmonia social. Entretanto, os frutos dessa guerra não se resumem à discriminação praticada pela sociedade civil, mas também acabam permitindo e até mesmo legitimando a discriminação por parte das instituições:

> A vigilância em massa e a prospecção de dados são muito mais adequadas para tarefas de discriminação populacional: achar pessoas com certas crenças políticas, pessoas que são amigas de certos indivíduos, pessoas que fazem parte de sociedades secretas, e pessoas que atendem a certos encontros e comícios. [...] Além disso, sob uma lei autoritária, os inevitáveis alarmes falsos são um problema menor; denunciar pessoas inocentes por sedição instala medo na população[32].

[30] SCHNEIER, Bruce. **Data and Goliath:** the hidden battles to collect your data and control your world. New York: W. W. Norton, 2015.
[31] SCHNEIER, Bruce. **Data and Goliath:** the hidden battles to collect your data and control your world. New York: W. W. Norton, 2015.
[32] SCHNEIER, Bruce. **Data and Goliath:** the hidden battles to collect your data and control your world. New York: W. W. Norton, 2015. p. 164. Tradução livre de "Mass surveillance and data mining are much more suitable for tasks of population discrimination: finding people with certain political beliefs, people who are friends with certain individuals, people who are members of secret societies, and people who attend certain meetings and rallies. Those are all individuals of interest to a government intent on social control like China. The reason data mining works to find them is that, like credit card and fraudsters, political dissidents are likely to share a well-defined profile. Additionally, under authoritarian rule the inevitable false alarms are less of a problem; charging innocent people with sedition instills fear in the populace."

Dessa forma, não existem razões científicas que levem à conclusão de que dados irrelevantes sobre pessoas inocentes facilitem a detecção de terroristas. No entanto, existem inúmeras evidências dos danos que a constante violação à privacidade de cada um pode causar aos direitos da população em geral, especialmente aos direitos de grupos marginalizados e já propensos a serem vigiados com maior escrutínio pelas autoridades[33].

Tal fenômeno pôde ser claramente percebido no Japão, através do vazamento de documentos do Departamento de Polícia de Tokyo (MPD), em 2010. Os documentos revelavam a vigilância que o órgão exercia sobre a comunidade muçulmana da cidade, tendo perfis completos e detalhados de seus membros com informações bancárias, movimentação doméstica, histórico de trabalho, amizades, afiliações com mesquitas e histórico de passaportes. Não somente isso, mas o MPD também monitorava lugares religiosos, restaurantes da comunidade e organizações de caridade islâmicas. Tal vigilância estatal, motivada por razões religiosas e étnicas, é flagrantemente discriminatória e, também, caracteriza-se como uma clara violação do direito humano à privacidade[34].

Outros casos que já ocorreram, a título exemplificativo da perigosa abrangência do conceito de terrorismo e do uso da vigilância em massa da população, são documentados pela obra Sujeito a Termos e Condições[35]. O documentário apresenta, entre outros, o caso de um estudante que foi interrogado, em sua escola, pelo Serviço Secreto dos Estados Unidos em decorrência de uma postagem que fez em uma rede social. O estudante, ingenuamente preocupado com o então Presidente estadunidense Barack Obama, publicou que Obama deveria tomar cuidado com possíveis homens-bomba, o que foi interpretado pelo sistema digital de alerta do FBI como sendo uma ameaça ao presidente. Também são apresentados casos de pessoas que foram presas para serem impedidas de realizarem protestos e manifestações em geral, tendo suas liberdades civis violadas. Algumas das manifestações mencionadas foram efetivamente planejadas, mas outras foram simplesmente discutidas de forma hipotética em redes sociais e ligações telefônicas. De qualquer forma, os possíveis participantes foram detidos, com a justificativa de que, em um futuro próximo, possivelmente perturbariam a paz social[36].

[33] SCHNEIER, Bruce. **Data and Goliath:** the hidden battles to collect your data and control your world. New York: W. W. Norton, 2015.
[34] MANTELLO, Peter. The machine that ate bad people. **Big Data & Society**, dez. 2016. Disponível em: https://journals.sagepub.com/doi/pdf/10.1177/2053951716682538. Acesso em: 20 set. 2021.
[35] SUJEITO a Termos e Condições. Direção: Cullen Hoback. Produção: Cullen Hoback, Nitin Khanna e John Ramos. Estados Unidos: Variance Films e Hyrax Films, 2013.
[36] SUJEITO a Termos e Condições. Direção: Cullen Hoback. Produção: Cullen Hoback, Nitin Khanna e John Ramos. Estados Unidos: Variance Films e Hyrax Films, 2013.

Com isso, percebe-se que, apesar de surgirem cada vez mais legislações que elencam a vigilância em massa e a prospecção de dados como importantes armas na batalha contra ameaças terroristas, elas não têm se demonstrado eficazes ao fim a que se propõem. Inocentes acabam sofrendo graves repressões por erros advindos dos sistemas de alerta ou por interesses políticos de um determinado grupo e, ao mesmo tempo, os reais ataques terroristas - como o ocorrido na Maratona de Boston, em 2013 - não são evitados.

Além disso, embora seja possível argumentar que as falhas apresentadas pelas tecnologias em questão podem ser corrigidas, que a IA pode ser aperfeiçoada e que a supervisão humana dos resultados apresentados garantiriam uma maior efetividade dos métodos de prevenção do terrorismo e acabariam com os impactos negativos existentes, a verdade é que isso não é necessariamente verdade. Afinal, o aperfeiçoamento das tecnologias de *surveillance* também significa o aperfeiçoamento de tecnologias que facilitam perseguições políticas e práticas discriminatórias deliberadas. A decisão de utilizar tais ferramentas de modo ético, respeitando os direitos humanos, ficaria exclusivamente nas mãos do indivíduo ou do grupo que se encontra em seu domínio. Em outras palavras, "concede-se ao poder a faculdade de estabelecer até que ponto será necessário limitar os direitos para exercer um poder que está em suas próprias mãos"[37].

Dessa forma, a instauração de um regime de *surveillance*, respaldado pela legislação e executado através de ferramentas de IA, não encontra mais as instituições político-jurídicas como limites e tampouco é balizado pelos sistemas de garantias que buscam efetivar os direitos fundamentais, já que a própria legislação entende que eles devem ser relativizados. Consequentemente, "o Estado de Direito é submetido ao medo e à urgência e, com isso, admite sua própria redução" (MORAIS, 2018, p. 94), dando lugar a práticas de promoção da segurança pública que não são eficazes ao fim a que se propõem e, ainda, provocam reiteradas e constantes violações à privacidade dos indivíduos, bem como a demais direitos fundamentais e liberdades civis conquistados através dos anos.

CONCLUSÃO

Tal como toda invenção humana, a inteligência artificial não tem valor inerente: ao mesmo tempo em que facilita o trabalho de várias organizações, também atua na invasiva previsão comportamental e identificação de possíveis criminosos partindo de matérias-

[37] ZAFFARONI, Eugenio Raúl. **O Inimigo no Direito Penal.** Rio de Janeiro: Editora Revan, 2007. p. 192.

primas informacionais fruto da violação da privacidade de bilhões de pessoas, sem que suas predições sejam cientificamente respaldadas. Esse cenário, capitaneado por detentores de poder corporativo e estatal, foi instaurado pela guerra ao terror pelos Estados Unidos, cuja justificativa de prevenir atos terroristas, elevando a segurança como direito supremo, coloca em xeque outras garantias de cidadãos de todo o mundo desde o momento da coleta de dados até as medidas adotadas após o resultado do tratamento algorítmico.

Para além da busca por um criminoso pela detecção de padrões de comportamento dos internautas-cidadãos, diversas normas nacionais e estrangeiras se dedicam ao tema do terrorismo, sem, contudo, estabelecer uma definição precisa do termo que permita, de fato, a identificação inequívoca das atitudes tomadas por terroristas. Decorre disso a possibilidade de atribuição da condição de inimigo a um indivíduo ou grupo que se mostre oportuno a quem detém o poder, de forma a corromper os dispositivos normativos para fins políticos. Portanto, a *surveillance* e o tratamento de dados advindo dela oferecem os meios necessários para distinguir, entre a população geral, críticos, manifestantes, ativistas, pessoas de certas origens étnicas, nacionais, religiosas ou culturais e quaisquer outras características inconvenientes à manutenção da ordem desejada pelo poder.

A realização desse tipo de vigilância e arbitrariedade utiliza o escudo da tecnologia, acreditada imparcial, neutra e justa, para perpetuar violações de direitos especialmente em direção a pessoas já marginalizadas na sociedade. A falta de escrutínio, publicidade e explicação das razões e dos métodos usados pela IA empregada por corporações e instituições governamentais que identifica criminosos e terroristas esconde a falta de indícios suficientemente probatórios de qualquer transgressão, que, todavia, são o bastante para motivar intervenções institucionais na vida das pessoas-alvo do algoritmo.

Outrossim, mesmo quando utilizada com a mais bem-intencionada das intenções, é possível que mecanismos de inteligência artificial cometam equívocos em seus resultados e, consequentemente, causem graves danos aos direitos humanos e fundamentais da população. Isso porque os algoritmos podem partir de falsos pressupostos e vieses discriminatórios que foram inseridos no seu banco de dados, no seu desenvolvimento ou até mesmo adquiridos através do aprendizado de máquina — processo muitas vezes inexplicável pelos próprios desenvolvedores de algoritmos de retroalimentação. Afinal, ao analisar dados da realidade humana sem a utilização de um pensamento crítico, chega-se a conclusões que perpetuam injustiças e preconceitos existentes.

Portanto, depreende-se que o uso da inteligência artificial para realizar o tratamento de dados coletados pela *surveillance* com o objetivo de evitar crimes e o

terrorismo não só é inefetiva como também viola direitos humanos fundamentais em seu processo. É assim que a guerra ao terror se transveste de promoção da segurança nacional para mascarar a violação da privacidade, a discriminação e a erosão de direitos políticos, bem como para legitimar um estado de exceção permanente que esfacela o Estado Democrático de Direito e admite medidas invasivas e autoritárias para combater um mal que sequer tem definição.

REFERÊNCIAS

BASTOS, Bruna. **Os Caminhos do Terrorismo e da Desumanização:** por uma cooperação internacional. Cruz Alta: Ilustração, 2021.

BRASIL. Lei n. 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Brasília: **Diário Oficial da União,** 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12850.htm. Acesso em: 21 set. 2021.

BRASIL. Lei n. 13.260, de 16 de março de 2016. Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis n º 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013. Brasília: **Diário Oficial da União,** 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm. Acesso em: 22 jul. 2021.

HARARI, Yuval Noah. **Homo Deus:** uma breve história do amanhã. São Paulo: Companhia das Letras, 2016.

LEE, Kai-Fu. **Inteligência Artificial:** como os robôs estão mudando o mundo, a forma como amamos, nos comunicamos e vivemos. Tradução Marcelo Barbão. Rio de Janeiro: Globo Livros, 2019.

LINDOSO, Maria Cristine Branco. **Discriminação de gênero em processos decisórios automatizados.** Dissertação (Mestrado em Direito) - Programa de Pós-Graduação em Direito, Universidade de Brasília. Brasília, 2019.

MAGRANI, Eduardo. **A Internet das Coisas.** Rio de Janeiro: FGV Editora, 2018.

MANTELLO, Peter. The machine that ate bad people. **Big Data & Society,** dez. 2016. Disponível em: https://journals.sagepub.com/doi/pdf/10.1177/2053951716682538. Acesso em: 20 set. 2021.

MORAIS, José Luis Bolzan de. O fim da geografia institucional do Estado. A "crise" do Estado de Direito!. In: MORAIS, José Luis Bolzan de (Org.). **Estado & Constituição:** o "fim" do Estado de Direito. Florianópolis: Tirant Lo Blanch, 2018.

O'NEIL, Cathy. **Algoritmos de Destruição em Massa:** como o Big Data aumenta a desigualdade e ameaça a democracia. Tradução Rafael Abraham. Santo André: Rua do Sabão, 2020.

SCHNEIER, Bruce. **Data and Goliath:** the hidden battles to collect your data and control your world. New York: W. W. Norton, 2015.

SNOWDEN, Edward. **Eterna Vigilância:** Como montei e desvendei o maior sistema de espionagem do mundo. Tradução Sandra Martha Dolinski. São Paulo: Planeta do Brasil, 2019.

SUJEITO a Termos e Condições. Direção: Cullen Hoback. Produção: Cullen Hoback, Nitin Khanna e John Ramos. Estados Unidos: Variance Films e Hyrax Films, 2013.

SUMPTER, David. **Dominados pelos Números:** do Facebook e Google às fake news – os algoritmos que controlam nossa vida. Tradução Anna Maria Sotero, Marcello Neto. Rio de Janeiro: Bertrand Brasil, 2019.

WE ARE SOCIAL; HOOTSUITE. Digital 2024 Global Overview Report: the essential guide to the world's connected behaviours**. We Are Social,** 2024. Disponível em: https://wearesocial.com/uk/blog/2024/01/digital-2024. Acesso em: 18 out. 2024.

ZAFFARONI, Eugenio Raúl. **O Inimigo no Direito Penal.** Rio de Janeiro: Editora Revan, 2007.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância:** a luta por um futuro humano na nova fronteira do poder. Tradução George Schlesinger. Rio de Janeiro: Intrínseca, 2021.