BIG DATA E A PREVENÇÃO DE CRIMES: REFLEXOS DA VIGILÂNCIA NOS DIREITOS FUNDAMENTAIS E HUMANOS

BIG DATA AND CRIME PREVENTION: THE EFFECTS OF SURVEILLANCE ON FUNDAMENTAL AND HUMAN RIGHTS

Júlia Schmidt Kronbauer[1]

Luiza Berger von Ende[2]

Rafael Santos de Oliveira[3]

RESUMO

A expansão da internet e o desenvolvimento tecnológico tornaram reais as suposições cinematográficas para o século XXI que previam a capacidade de prevenção de crimes utilizando a tecnologia. Isso se deu, a nível mundial, a partir do 11 de Setembro de 2001, quando se instaurou a guerra ao terror, a qual inaugurou a era da utilização de dados pessoais em prol da segurança pública. Nesse sentido, o presente trabalho propõe-se a investigar as implicações do tratamento massivo de dados sob o pretexto da prevenção de crimes em relação aos direitos fundamentais e humanos. Para tanto, utiliza o método de abordagem dedutivo e os métodos de procedimento funcionalista e monográfico no estudo dos agentes responsáveis pelo tratamento e da maneira como é feito, bem como a efetividade de tal prevenção criminal e as implicações do tema nos direitos fundamentais e humanos. Resulta da pesquisa que a vigilância ocorre em uma parceria de empresas digitais e agências governamentais, e que se torna difícil evitá-la tanto por óbices impostos na regulamentação quanto pela crença na imparcialidade algorítmica. Ademais, que os conceitos de criminoso e terrorista são arbitrários e abrem margem para uma discriminação setorizada e violadora de direitos civis. Por fim, a vigilância e o tratamento de dados a nível nacional e internacional com o pretexto da prevenção de crimes se mostra inefetiva para o fim a que se propõe e viola a privacidade, a segurança e a liberdade dos cidadãos.

Palavras-chave: algoritmos; big data; guerra ao terror; prevenção de crimes; vigilância.

ABSTRACT

The expansion of the internet and the technological development turned the cinematographic suppositions for the 21st century, that predicted the capability of preventing crimes utilizing

[1] Autora. Graduanda em Direito pela Universidade Federal de Santa Maria (UFSM). Pesquisadora do Centro de Estudos e Pesquisas em Direito e Internet da UFSM (CEPEDI). Currículo Lattes: http://lattes.cnpq.br/1449532117977804. Bolsista Pró-Revistas. Endereço eletrônico: julia.schmidt.k@gmail.com

[2] Autora. Graduanda em Direito pela Universidade Federal de Santa Maria (UFSM). Pesquisadora do Centro de Estudos e Pesquisas em Direito e Internet da UFSM (CEPEDI). Bolsista PROBIC/FAPERGS. Estudante do Curso Técnico em Informática do Colégio Politécnico da UFSM. Currículo Lattes: lattes.cnpq.br/3314168049325773. Endereço eletrônico: luiza.bergerv@gmail.com.

[3] Orientador. 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. Currículo Lattes: http://lattes.cnpq.br/9933895574541972. Endereço eletrônico: advrso@gmail.com.

technology, real. This happened, on an international level, as of September 11th of 2001, when the war on terror was initiated, which inaugurated the era of using personal data to benefit public safety. Hence, the present paper aims to investigate the implications that the massive data treatment under the pretext of crime prevention have on the fundamental and human rights. For that matter, the deductive approach method and the functionalist and monographical procedure methods were used to study the agents responsible for the data treatment and the way that it is done, as well as the effectiveness of such criminal prevention and the implications of this subject on the fundamental and human rights. The research results show that surveillance occurs in a partnership between digital companies and governmental agencies, and that it is difficult to avoid surveillance, not only because of obstacles created by its regulamentation, but also due to the belief in algorithmic neutrality. Furthermore, the results show that the definition of criminal and of terrorist are arbitrary and allow for a sectorized discrimination that violates civil rights. Finally, surveillance and data treatment, on national and international level, with the pretext of crime prevention shows itself as ineffective to its attributed end and violates the privacy, the safety, and the freedom of the citizens.
Keywords: algorithms; big data; war on terror; crime prevention; surveillance.

1 INTRODUÇÃO

Longa-metragem de Spielberg, Minority Report[4] fantasia o ano de 2054 repleto de inovações tecnológicas, com carros autônomos, *outdoors* de publicidade direcionados especialmente para cada pessoa e, ainda, um sistema de previsão de crimes futuros. Esse programa contava com a mais desenvolvida tecnologia, capaz de exibir dados de um futuro que, evidentemente, ainda não havia ocorrido, mas estaria fadado para tanto. A partir dessas informações, a Divisão de Pré-Crime da Polícia de Washington tinha o poder de evitar que os crimes previstos ocorressem, prendendo o criminoso imediatamente antes do momento que realizaria o crime. O sucesso do projeto era celebrado, ostentando uma queda da taxa de homicídios da região para zero.

A trama se desenvolve a partir de quando se planeja a expansão do projeto, com a sua implementação a nível federal, e um agente jurídico faz uma visita in loco a fim de verificar o funcionamento do sistema. O cético representante do Procurador da República passa a questionar a acurácia e confiabilidade dos resultados das previsões, sugerindo a possibilidade de existirem brechas no sistema - as quais são negadas veementemente pelo departamento. O ponto-chave se dá quando John Anderton, o policial chefe da Divisão de Pré-Crime, outrora contrariado pelas interferências federais no seu trabalho, é indicado pelo sistema que tanto

[4] MINORITY Report. Direção: Steven Spielberg. Produção: Gerald R. Molen, Bonnie Curtis, Walter F. Parkes e Jan de Bont. Estados Unidos: 20th Century Fox, DreamWorks e SKG, 2002. Netflix.

defendia como o futuro perpetrador de um assassinato cuja vítima ele sequer conhece, suscitando um dilema sobre o qual o filme se desenrola.

Muitos dos futurismos preconizados pelo filme em 2002 já existem em 2021 (ainda que a obra não tenha sido capaz de antecipar a existência de cenários como a computação em nuvem, limitação que é revelada nos pen-drives de vidro do tamanho de uma folha de papel que o departamento de polícia necessitava utilizar para visualizar os vídeos dos crimes de uma tela para outra), tais como o reconhecimento da identidade a partir da íris, o direcionamento e personalização de anúncios com base nas experiências de cada pessoa e, também, a utilização de *softwares* que permitem a direção automatizada de veículos. Fora isso, e, mais importante, a ideia que ocupa o próprio cerne da obra é, de alguma maneira, realidade - isto é, a utilização de dados com a finalidade de prevenir crimes. Esse fato se evidencia em razão da coleta e utilização do *big data* e de algoritmos por parte de agências de inteligência de governos ao redor do mundo a partir, especialmente, do atentado de 11 de Setembro de 2001 nos Estados Unidos, sob o pretexto da guerra ao terror.

Na maior parte das vezes, entretanto, essa interceptação informacional ocorreu de forma oculta, atingindo também os dados de cidadãos que sequer tinham contato com qualquer transgressão da lei, sem que se soubesse. Isso foi trazido à tona a partir de 2013 por Edward Snowden, ex-analista da CIA que protagonizou um dos mais importantes vazamentos do governo estadunidense, expondo que a National Security Agency (NSA) [Agência de Segurança Nacional] mantinha o registro de dados dos cidadãos não somente norte-americanos, mas de fora do país, desde décadas anteriores e por tempo indeterminado, dados os quais foram e ainda eram obtidos sem a necessidade de mandados judiciais e que poderiam ser tratados e acessados a qualquer momento.[5]

O pretexto dessa extração e tratamento massivo de dados, conforme a NSA, seria a segurança dos cidadãos, com a premissa de que poder-se-ia evitar a ocorrência de atos terroristas a partir da análise dos rastros de dados deixados pelos futuros criminosos na internet e em outras telecomunicações. Por outro lado, a falta de transparência e de explicações sobre tamanha vigilância desencadeou preocupações quanto à privacidade e à liberdade das pessoas às quais se referiam os dados - vale dizer, uma parte significativa da população mundial. Tendo em mente todo esse contexto, emerge o questionamento: quais as

[5] 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.

implicações do tratamento massivo de dados sob o pretexto da prevenção de crimes em relação aos direitos fundamentais e humanos?

A presente pesquisa, então, objetiva investigar as relações entre a utilização de dados pessoais e tecnologia e a prevenção de crimes nos direitos fundamentais e humanos; especificamente, compreender como se dá a extração e tratamento de dados, o uso das tecnologias e a atuação das instituições públicas e privadas, bem como investigar a efetividade da intencionada prevenção e em que ponto esse cenário se relaciona com os direitos humanos e fundamentais dos cidadãos. Para tanto, utiliza o método de abordagem dedutivo, que consiste na aplicação de premissas gerais sobre dados pessoais e direitos humanos no caso específico da prevenção de crimes por meios tecnológico-informacionais, e os métodos de procedimento funcionalista e monográfico, sendo que o primeiro se dá com a compreensão dos elementos supramencionados (como a tecnologia, os dados e os atores públicos e privados) e o papel que desempenham nesse cenário de antecipação criminosa a partir de informações, e o segundo se vale do estudo de casos representativos de outros semelhantes, que possibilitam o devido entendimento do fenômeno. As técnicas de pesquisa empregadas são a bibliográfica e documental.

2 OS AGENTES E A UTILIZAÇÃO DO BIG DATA E DO DATA MINING NA PREVENÇÃO DE CRIMES

A expansão e a popularização da internet no planeta a partir da década de 90 gerou um grande aumento na produção e circulação de dados em rede, especialmente após o marco da Web 2.0, quando os internautas, até então apenas receptores de conteúdo, passaram também a ser produtores das informações. Desde então - e graças, ainda, ao barateamento das tecnologias de armazenamento e aumento do poder computacional geral - os dados e metadados que circulam na rede são continuamente armazenados por instituições públicas e privadas que fazem parte do intercâmbio de dados.

A esse cenário de grande quantidade de informações existentes na internet se dá o nome de *big data*, o qual pode ser traduzido na prática de coletar e armazenar vários tipos de dados. Isso guarda relação intrínseca com a mineração de dados, que consiste na extração de

informações úteis a partir desse emaranhado desordenado.[6] Este processo é feito por algoritmos computacionais, capazes de realizar a operação de correlação de dados e identificação de padrões de maneira célere. Um dos mais importantes usos dessa tecnologia se dá na realização de um perfil para cada usuário da internet, identificando seu histórico, sua rede de contatos e suas preferências, o que permite a previsão comportamental dessa grande massa de internautas.

A realização de perfis é especialmente utilizada nas plataformas de internet, como redes sociais e mecanismos de busca, para realizar o direcionamento de conteúdo e de anúncios de maneira personalizada a cada usuário. A primeira finalidade da prática é fazer com que o usuário receba informações mais relevantes a si, considerando seus interesses, e que permaneça mais tempo conectado à plataforma; a segunda, consequentemente, é apresentar anúncios publicitários que tenham mais probabilidade de surtir efeito para cada pessoa, sendo essa a maior fonte de renda das plataformas digitais na atualidade. Por isso, as instituições privadas digitais são a maior fonte de dados comportamentais na internet.

É importante, nesse sentido, atentar para o ensinamento da matemática Cathy O'Neil[7], que revela que a tecnologia não pode ser tida como neutra, e que os modelos computacionais (entre eles, os algoritmos de realização de perfis) carregam vieses e opiniões de quem os programou. Assim, ainda que a correlação realizada por uma máquina possa parecer imparcial, ou que apenas está desvendando informações verídicas e precisas a partir de pistas deixadas na internet, esse procedimento é guiado a partir dos interesses da empresa dona do algoritmo, a qual, sob o pretexto de proteção de propriedade intelectual e segredos empresariais, não dá transparência ao seu código ou sequer explicações sobre seu funcionamento, de modo que não é informado às pessoas atingidas pelo tratamento dos dados o porquê de se ter chegado àquele resultado. Isto é, caso o algoritmo, a partir da mineração de dados, informe, sem que seja informado explicitamente por determinada pessoa, que ela tem certas características - que faz parte de certo grupo religioso, que tenha certos hábitos ou que estejam em certa faixa de renda - é difícil e até mesmo impossível, certas vezes, que se compreenda a lógica por trás dessa inferência. Contudo, o senso comum e as instituições creem de olhos fechados nessa decisão.

---

[6] SCHNEIER, Bruce. **Data and Goliath:** the hidden battles to collect your data and control your world. New York: W. W. Norton, 2015. p. 39.

[7] O'NEIL, Cathy. **Armas de Destruição Matemática:** como o Big Data aumenta a desigualdade e ameaça a democracia. Tradução Rafael Abraham. Santo André: Rua do Sabão, 2020.

Isso é especialmente relevante quando se analisa o fato de que instituições públicas fazem parcerias com o setor privado com o objetivo de realizar trocas informacionais, e que muitas agências governamentais buscam a prevenção de crimes a partir dos rastros pessoais deixados na internet. Nos Estados Unidos, por exemplo, revelou-se que a Agência de Segurança Nacional, por meio de parcerias consensuais e até mesmo de interceptações sigilosas arbitrárias, utilizava dados pessoais de posse de grandes corporações digitais e empresas de telecomunicação - dispensando a necessidade de mandados judiciais - os quais eram tratados em projetos secretos com objetivos turvos.[8] À vista disso, a vigilância estadunidense ganha destaque no cenário internacional, cujos motivos são apontados por Schneier:

> Os Estados Unidos têm a rede de vigilância mais ampla do mundo porque tem três vantagens. Têm um orçamento de inteligência maior do que o resto do mundo combinado. A fiação física da Internet faz com que grande parte do tráfego mundial atravesse as fronteiras dos EUA, até mesmo o tráfego entre dois outros países. E quase todas as maiores e mais populares empresas de hardware, software e Internet do mundo estão sediadas nos Estados Unidos e sujeitas às suas leis. É a hegemonia.[9]

Assim, o país que sedia grande parte das maiores corporações digitais da atualidade é o mesmo que encontra óbices na publicação de legislações que limitem tanto o poder corporativo quanto o poder governamental sobre dados de cidadãos, sejam estadunidenses, sejam estrangeiros.[10] A partir dessa e de outras atitudes, cria-se no ideário comum, fortemente incentivado pelas empresas e agências governamentais, a ideia que a evolução da tecnologia implica necessariamente maior vigilância; entretanto, conforme Shoshana Zuboff[11], não passa de um mito, visto que é de interesse de tais instituições que se naturalize a invasão da privacidade e a comercialização e a utilização arbitrária de dados pessoais sem o consentimento dos titulares. Portanto, a vigilância constante nas redes de internet não é

---

[8] 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.

[9] Tradução livre de "The US has the most extensive surveillance network in the world because it has three advantages. It has a larger intelligence budget than the rest of the world combined. The Internet's physical wiring causes much of the world's traffic to cross US borders, even traffic between two other countries. And almost all of the world's largest and most popular hardware, software and Internet companies are based in the US and subject to its laws. It's the hegemon". SCHNEIER, Bruce. **Data and Goliath:** the hidden battles to collect your data and control your world. New York: W. W. Norton, 2015. p. 76.

[10] SCHNEIER, Bruce. **Data and Goliath:** the hidden battles to collect your data and control your world. New York: W. W. Norton, 2015. p. 94.

[11] 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, 2020.

necessária para seu funcionamento, mas, sim, para um projeto de instituições públicas e privadas.

Nesse sentido, o dataísmo preconizado por Harari[12] já abre espaço para sua consolidação no século XXI, visto que é largamente difundido e aceito que a atuação algorítmica é inevitável e benéfica, inclusive vencendo a capacidade humana por revelar padrões invisíveis aos olhos destes últimos. Ocorre que, muitas vezes, os padrões permanecem invisíveis às pessoas simplesmente porque não sustentam, de fato, nexo causal entre eles: a mineração de dados ignora a cientificidade requerida em uma análise estatística séria e correta, feita por seres humanos.[13] Dessa forma, infere conclusões que, apesar de atraentes, são falhas e discriminatórias, não obstante sejam utilizadas pelas empresas para traçar perfis e pelos governos para identificar criminosos e terroristas.

Pelo exposto, é possível traçar o caminho percorrido por empresas digitais e instituições públicas, as quais, em especial nos Estados Unidos, utilizam a previsão comportamental feita a partir dos rastros digitais de internautas com a finalidade de prever comportamentos criminosos. Importa mencionar que o referido país que ostenta o título de líder de vigilância não é o único, e que incentiva outras nações, pela guerra ao terror, a fazerem o mesmo. É assim que a tecnologia se alia a dispositivos jurídicos e políticas governamentais em prol de uma suposta prevenção criminal, cujas balizas e efetividade são abordadas no tópico a seguir.

3 A PREVENÇÃO DE CRIMES COMO JUSTIFICATIVA DA VIGILÂNCIA E SUA RELAÇÃO COM DIREITOS HUMANOS FUNDAMENTAIS

Hodiernamente, ao redor do mundo, existem diversos dispositivos legais que se propõem a combater e prevenir o terrorismo, como a Resolução 1.566 do Conselho de Segurança da ONU e, também, a Lei Antiterrorismo do ordenamento jurídico pátrio. Entretanto, a definição de terrorismo exposta por essas legislações é ampla e imprecisa, o que faz com que esse termo possa ser utilizado como um instrumento político.[14]

---

[12] HARARI, Yuval Noah. **Homo Deus:** uma breve história do amanhã. São Paulo: Companhia das Letras, 2016.
[13] 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.
[14] BASTOS, Bruna. **Os Caminhos do Terrorismo e da Desumanização:** por uma cooperação internacional. Cruz Alta: Ilustração, 2021. pp. 39-40.

A figura do terrorista, então, muito se assemelha à figura do inimigo, apresentada pelo jurista argentino Eugenio Raúl Zaffaroni. Ambos conceitos partem de uma definição imprecisa e até mesmo genérica, que possuem o decisionismo por parte do Estado como pressuposto imprescindível para preencher seus vazios. Dessa maneira, cria-se um ambiente propício ao autoritarismo estatal, já que o terrorista, ou o inimigo, acaba sendo um elemento politicamente assinalado[15], podendo servir como fachada para elencar determinadas pessoas ou grupos de pessoas como inimigas da população civil.

Além disso, outro problema encontrado referente à questão da guerra ao terror é a dificuldade de identificar o terrorista e diferenciá-lo dos demais integrantes da sociedade civil. Isso porque presume-se que o terrorista, ou inimigo, oculta-se entre os cidadãos e precisa, então, ser identificado e individualizado para, somente em um momento posterior, ser neutralizado. O problema é que a sua identificação, impossível de ser realizada *ab initio*, pressupõe a investigação de toda a população civil e, consequentemente, a invasão de privacidade de todos os cidadãos. Em suma, outorga-se ao Estado o direito de limitar as garantias e liberdades da população para cumprir com o objetivo de identificar e conter os terroristas e demais inimigos.[16]

Tais impactos negativos advindos da guerra ao terror vêm contaminando ordenamentos jurídicos ao redor do mundo através de dispositivos como a supramencionada Lei Antiterrorismo (Lei nº 13.260/2016)[17], de âmbito nacional. Com o objetivo de prevenir ataques terroristas, a lei chega a punir até mesmo atos preparatórios do terrorismo, enumerados em rol exemplificativo em seu art. 5º. Afinal, ao analisar os artigos dessa Lei conjuntamente com o contexto sócio-político já apresentado, percebe-se que a referida norma tipifica a punição de atos indeterminados de preparação a um crime de definição demasiadamente ampla, ou seja, cria uma oportunidade para que injustiças e arbitrariedades ocorram na aplicação da lei, tanto por parte de julgadores, quanto por parte de autoridades policiais.

---

[15] ZAFFARONI, Raúl. **O Inimigo no Direito Penal**. Rio de Janeiro: Editora Revan, 2007. p. 142.
[16] ZAFFARONI, Raúl. **O Inimigo no Direito Penal**. Rio de Janeiro: Editora Revan, 2007. p. 117.
[17] 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.

No mesmo sentido, o governo de Nova Gales do Sul, na Austrália, em 2008, sob o pretexto de contra-atacar o terrorismo, aumentou os poderes discrecionários da polícia ao permitir a condenação de indivíduos por associação. A partir de 2016, as autoridades policiais também ganharam a faculdade de prender pessoas maiores de 14 anos por duas semanas, sem qualquer acusação e sem que elas tivessem como contatar um advogado, parentes ou amigos. Eventualmente, essas novas condutas permitidas por lei com a justificativa de acabar com o terrorismo também começaram a ser aplicadas na prevenção de outros tipos de crimes, invertendo o princípio de presunção da inocência, ignorando o princípio do contraditório e da ampla defesa, e condenando e aprisionando cidadãos com base em meros rumores e suspeitas. [18]

É evidente, diante ao exposto, que legislações que objetivam a prevenção de crimes - principalmente dos crimes de terrorismo - acabam por inverter o processo penal, limitando garantias processuais, violando direitos fundamentais e, consequentemente, ameaçando as diretrizes e princípios de um Estado Democrático de Direito. Ressalta-se, ainda, que a incorporação dessa espécie de dispositivos legais oportuniza atuações arbitrárias e injustas por parte de autoridades policiais, que podem ser motivadas não somente por equívocos, mas também por interesses políticos e intenções discriminatórias.

Dessa forma, a supostamente inovadora ambição de prever e prevenir a ocorrência de crimes acaba seguindo o absurdo caminho dos legisladores da Roma Antiga, que, ao criar a *lex Julia* contra crimes de lesa-majestade, chegavam a apenar a posse e fabricação de tela púrpura, já que o objeto poderia ser utilizado na preparação de um magnicídio[19] . A diferença reside, essencialmente, nos meios e nas ferramentas de investigação utilizados para identificar as supostas ameaças terroristas. Para vencer a guerra ao terror, busca-se desenvolver estratégias e novos mecanismos tecnológicos que acabam por suprimir as garantias do Estado de Direito, promovendo restrições à liberdade com o intuito de aperfeiçoar as estratégias preditivas de catalogação para neutralizar possíveis riscos[20].

Trata-se da *surveillance* e do *big data*, utilizados como ferramentas de investigação para conseguir a identificação de possíveis inimigos ou terroristas, através da constante

---

[18] 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: 03 out. 2021. p. 4.

[19] ZAFFARONI, Raúl. **O Inimigo no Direito Penal**. Rio de Janeiro: Editora Revan, 2007. p. 117.

[20] 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. p. 85

vigilância de toda a população e do constante e indiscriminado armazenamento de dados dos usuários de *internet*. Essas tecnologias, no entanto, colocam a população em risco em frente a abusos de autoridade[21], visto que, como argumenta Schneier[22], com uma quantidade suficiente de dados sobre alguma pessoa, não importa quem seja, pode-se acusá-la de algum crime, o que faz com que qualquer pessoa possa ser condenada por desrespeitar as leis caso alguma autoridade resolva tê-la como alvo.

Dessa maneira, é evidente que essas ferramentas de investigação facilitam a perseguição política de determinados indivíduos ou grupos, já que seu uso é extremamente apropriado para identificar pessoas de determinada religião, de determinado posicionamento político, que fazem parte de certas organizações ou sociedades, que participam de protestos ou manifestações e, enfim, pessoas classificadas como dissidentes políticos[23]. Depois dessa identificação, governos interessados em realizar um rígido controle social, como a China, podem facilmente tomar as medidas autoritárias que desejarem para satisfazer seus interesses políticos.

Ao mesmo tempo em que, de forma colateral, apresentam ameaças aos direitos fundamentais e liberdades civis dos cidadãos, a vigilância em massa e a prospecção de dados não têm demonstrado serem eficazes para o fim a que se propõem, ou seja, para identificar ameaças terroristas. Pelo contrário, muitas vezes, pessoas inocentes acabam tendo seus direitos e liberdades civis violados por erros dos algoritmos do sistema de alerta, que podem identificar indivíduos como perigosos por causa de postagens humorísticas ou pelo uso de determinadas palavras-chave catalogadas no sistema como suspeitas, sem que o contexto geral da mensagem seja interpretado pelo algoritmo. É importante ressaltar que tais identificações equivocadas são ainda mais recorrentes em pessoas que fazem parte de grupos marginalizados, já propensos a serem vigiados com maior escrutínio pelas autoridades.

Concomitantemente, as ameaças terroristas de verdade, infelizmente, não estão sendo neutralizadas. Foi este o caso do atentado que ocorreu na maratona de Boston, em 2013, depois que medidas de *surveillance* já tinham sido adotadas nos Estados Unidos, mas que, mesmo assim, não foi previsto e muito menos evitado.

---

[21] SCHNEIER, Bruce. **Data and Goliath:** the hidden battles to collect your data and control your world. New York: W. W. Norton, 2015. p. 109.
[22] SCHNEIER, Bruce. **Data and Goliath:** the hidden battles to collect your data and control your world. New York: W. W. Norton, 2015. p. 108.
[23] SCHNEIER, Bruce. **Data and Goliath:** the hidden battles to collect your data and control your world. New York: W. W. Norton, 2015. p. 164.

Portanto, evidencia-se que a limitação de garantias processuais e a tipificação de atos preparatórios, com o objetivo de prevenir crimes em geral, mas mais especificamente o terrorismo, são flagrantes ameaças ao Estado Democrático de Direito. A criação dessas leis instala e legitima um regime de *surveillance*, que não é eficaz ao fim a que se propõe e, ainda, provoca reiteradas e constantes violações à privacidade dos indivíduos, bem como a demais direitos fundamentais e liberdades civis.

4 CONSIDERAÇÕES FINAIS

Diante do exposto, tal como em Minority Report, não há de se depositar confiança cega em um sistema que age conforme interesses enviesados e causa danos irreparáveis aos direitos de toda a coletividade. Apesar da difundida crença de que atuação algorítmica é superior à capacidade humana, os mecanismos e as ferramentas tecnológicas que se propõem a usar os rastros digitais dos internautas para realizar uma suposição comportamental e prever comportamentos criminosos são sujeitos a inúmeras falhas que, muitas vezes, não podem ser compreendidas nem mesmo pelos desenvolvedores dos algoritmos, já que a linha de raciocínio seguida pela máquina, muitas vezes, carece de transparência. Tais falhas, que podem ser provocadas tanto pela maneira com que o algoritmo foi desenvolvido, quanto adquiridas através do aprendizado de máquina, podem levar a resultados falaciosos e discriminatórios, que causam grave dano aos direitos humanos e fundamentais da população.

Outrossim, mesmo que os sistemas de predição comportamental e prevenção de crimes fossem aperfeiçoados ao máximo, através do aprimoramento das operações de tratamento de dados e dos mecanismos de vigilância em massa, esse mesmo sistema, criado com boas intenções, poderia acabar sendo utilizado para satisfazer interesses políticos de um determinado grupo que se encontra no poder. Ao permitir a fácil e rápida identificação de pessoas que pertencem a determinada religião ou que se identificam com determinada posição política, essas ferramentas facilitam a perseguição de dissidentes políticos e qualquer outro setor da população elencado como indesejável por aqueles que estão no poder, o que se configura como um flagrante ameaça não somente aos direitos fundamentais e às liberdades civis da população, como também à própria estrutura do Estado Democrático de Direito.

Dessa forma, sob o pretexto de prevenir a ocorrência de crimes - mais especificamente, a ocorrência de atos terroristas -, instaura-se um regime de *surveillance* que

apresenta diversos pontos negativos, como os já elencados anteriormente, e que, ao mesmo tempo, não demonstra ser eficaz ao fim a que se propõe. Além disso, com o objetivo de eliminar um inimigo abstrato preventivamente, são criados dispositivos legais que tipificam atos preparatórios e, com isso, acabam limitando garantias processuais, ignorando princípios do ordenamento jurídico e até mesmo invertendo o processo penal.

No final, com base no equivocado entendimento de que reiteradas violações ao direito à privacidade dos indivíduos - o que, consequentemente, resulta na violação de demais direitos humanos e liberdades civis, como exposto anteriormente - são necessárias para a promoção da segurança pública e nacional, legisla-se no sentido de autorizar e legitimar condutas autoritárias por parte do Estado. Entretanto, o que se percebe é que tais violações não servem para a efetivação de um bem maior e a relativização dos pilares do Estado Democrático de Direito tende a levá-lo à sua própria extinção antes de qualquer vitória em uma guerra ao terror.

REFERÊNCIAS

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

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

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.

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: 03 out. 2021.

MINORITY Report. Direção: Steven Spielberg. Produção: Gerald R. Molen, Bonnie Curtis, Walter F. Parkes e Jan de Bont. Estados Unidos: 20th Century Fox, DreamWorks e SKG, 2002.

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.

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.

ZAFFARONI, 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, 2020.