MONÇÕES
Revista de Relações Internacionais da UFGD
ISSN 2316-8323

DIREITOS HUMANOS, INTELIGÊNCIA ARTIFICIAL E PRIVACIDADE

JOÃO FRANCISCO CASSINO
Mestrando em Ciências Humanas e Sociais pela UFABC e Especialista em Relações Internacionais pela Universidade de Brasília (UnB).

RODOLFO DA SILVA AVELINO
Doutorando em Ciências Humanas e Sociais pela UFABC e Mestre em TV Digital pela Universidade Estadual Paulista (UNESP); Professor do Insper.

SÉRGIO AMADEU DA SILVEIRA
Doutor e Mestre em Ciência Política pela Universidade de São Paulo (USP); Professor Associado da Universidade Federal do ABC (UFABC).

RESUMO: Este texto trata dos riscos e implicações da inteligência artificial e dos algoritmos para os objetivos contidos na Declaração Universal dos Direitos Humanos. Nesse sentido, as perspectivas de James Der Derian, Frank Pasquale, David Chandler, Shoshana Zuboff, Philip N. Howard e Nick Srnicek foram mobilizadas para a compreensão da atual fase do capitalismo global, do mercado de captura e o processamento em massa de dados pessoais. Diversos casos descritos indicam que a privacidade é cada vez menos respeitada enquanto as empresas protegem seus segredos competitivos com patentes, códigos fechados e acordos de confidencialidade. Técnicas de Big Data e algoritmos em rede podem ser utilizados para melhorar e agilizar a administração pública, mas também resultam em novas práticas discriminatórias que violam o direito à privacidade, à liberdade de expressão e à justiça. Grupos étnicos e raciais, mulheres e comunidade LGBT já sofrem com decisões tomadas por sistemas computacionais autômatos que levam à segregação e ao preconceito.

PALAVRAS-CHAVE: Direitos Humanos; Algoritmos; Privacidade.

HUMAN RIGHTS, ARTIFICIAL INTELLIGENCE AND PRIVACY

ABSTRACT: This text presents risks and implications of artificial intelligence and algorithms for the goals contained in the Universal Declaration of Human Rights. In this sense, the perspectives of James Der Derian, Frank Pasquale, David Chandler, Shoshana Zuboff, Philip N. Howard and Nick Srnicek have been mobilized to understand the current phase of global capitalism, the market of capture and of mass processing of personal data. Several cases described indicate that privacy is less and less respected as companies protect their competitive secrets with patents, closed codes and confidentiality agreements. Big Data techniques and network algorithms can be used to improve and streamline public administration, but also result in new discriminatory practices that violate the right to privacy, freedom of expression and justice. Ethnic and racial groups, women and the LGBT community already suffer from decisions made by automated computer systems that lead to segregation and prejudice.

KEYWORDS: Human rights; Algorithms; Privacy.

1. Introdução

A Declaração Universal dos Direitos Humanos completou 70 anos em 2018. Foram enormes os avanços obtidos desde que foi adotada pela Assembleia Geral da Organização das Nações Unidas (ONU). No entanto, novos desafios aos direitos humanos surgiram com a expansão da Inteligência Artificial, com a automação e com a mediação social dos algoritmos. As implicações dessas tecnologias no cenário político, econômico e social contemporâneo, seus tipos principais, a nova escala das violações de direitos praticados a partir das tecnologias de rastreamento, intrusão, interceptação e coleta de informações promovida por estados nacionais e por grandes corporações que atuam em âmbito planetário são os temas que serão tratados neste artigo. Os riscos à democracia, à liberdade de expressão, de perseguição de minorias, de grupos políticos e de violação de privacidade atingiram um novo patamar, sem precedentes na História. Se os Estados nacionais sempre lançaram mão de espionagem para controle de inimigos internos e externos e se as corporações sempre tentaram obter o máximo de informações sobre seus clientes para melhor direcionamento de negócios, com o atual estágio do desenvolvimento das Tecnologias de Comunicação e Informação, o indivíduo, que sempre foi muito frágil à ação desses poderes, agora tem pouca chance de defesa e de prevenção contra esses mecanismos, que funcionam em amplitude global.

O Conselho de Direitos Humanos da ONU já se manifestou quanto à promoção, à proteção e ao usufruto da Internet com a resolução de 27 de junho de 2016 (A/HRC/32/L.20), com a qual reconhece que: *"a privacidade online é importante para a realização do direito da liberdade de expressão e para assegurar opiniões sem interferência e para o direito à liberdade de pacífica reunião ou associação".* A resolução também se preocupa com a violação de diretos humanos e de liberdades fundamentais na Internet e com a impunidade para tais abusos, mas o texto não aprofunda sobre os perigos provenientes das tecnologias de Inteligência Artificial. Perigos, como por exemplo, o risco de limitação da presunção da autonomia do indivíduo a partir do uso direcionado de seus dados pessoais, mesmo que tenham sido fornecidos voluntariamente pelo cidadão ou pelo consumidor.

O espaço cibernético é um elemento novo e decisivo do contexto político mundial, como escreveu o teórico das Relações Internacionais Joseph Nye Jr. na

publicação *Cyberpower* (2010). Para ele, o ciberespaço reduz diferenciais de poder entre atores, o que seria um bom exemplo da difusão de poder que caracteriza a política global no Século XXI. Nye Jr. complementa ao afirmar que as assimetrias de vulnerabilidade a partir das redes implica que atores menores têm mais capacidade de exercer poder no ciberespaço do que em outros domínios da política mundial, como a força da guerra ou a influência econômica e cultural. Nye Jr. não cita claramente, mas torna-se evidente a necessidade de defesa de cada um desses atores contra os sistemas de vigilância permanentes viabilizados pela Internet, cuja intencionalidade das práticas fica óbvia como no caso Snowden, que será tratado adiante.

A "paranoia da espionagem", explicitada pelo pesquisador James Der Derian no texto *Antidiplomacy: Spies, Terror, Speed, and War (*1992), é reforçada pelas burocracias e pelos sistemas de inteligência militar, que, com as redes de coleta de informação ameaçam as fronteiras geopolíticas tradicionais, tornando-se mais difícil distinguir entre o "eu" e o "outro" (o inimigo), de separar o que é "interno" do que é "externo". Der Derian escreve que a espionagem contemporânea é compreendida como sinônimo do "poder da informação". Assim, inspirado em Paul Virilo, pensa a vigilância e a guerra como uma função da "velocidade". Especificamente, percebe a necessidade de captação das informações em tempo real que estão em todo o lugar. Para Der Derian, a espionagem é onipresente e o poder crescentemente vigilante. Destaque-se que essas afirmações não consideravam o enorme poder da Agência de Segurança Nacional[1] (NSA). Se o espião (fonte dos serviços de inteligência) precisa de indistinção e de sua não-identidade para ter garantida sua segurança, nada melhor que o anonimato da Internet e a captura de informações à distância, sem a presença física do agente secreto. Em outro artigo mais recente, *Critical Encounters in International Relations* (2009, p. 72-73), Der Derian chega a questionar se a "condição pós-moderna", cunhada por Lyotard e identificada pelo trabalho de Foucault, Deuleuze e outros, já não teria sido suplantada pela "condição virtual" da comunicação instantânea, da onipresença das imagens, dos fluxos de capitais e da velocidade videográfica da guerra, fazendo da soberania estatal uma transitoriedade, um fenômeno tecnologicamente transitório. Ressalte-se que o

[1]*National Security Agency – Departament of Defense – USA.*

pensamento de Der Derian é fortemente influenciado por Foucault, o que garante embasamento para questionar escolas tradicionais das Relações Internacionais nascidas da teoria realista (*ibid.*, p. 70).

A queda da União Soviética e do bloco socialista europeu, no início do anos 1990, fez com que os campos das Relações Internacionais e da Ciência Política passassem por uma ebulição teórica para que se explicasse a nova ordem mundial surgida no pós-Guerra Fria, que variou do otimismo do "Fim da História" (com a vitória definitiva das democracias de mercado) de Francis Fukuyama ao pessimismo do "Choque de Civilizações" (os novos conflitos culturais e religiosos) de Samuel P. Huntington. Da mesma forma, o conceito de *"segurança nacional"* passou por severa avaliação. Nesse contexto, os estudos *críticos de segurança* são um bom alicerce teórico para compreender como as tecnologias algorítmicas afetam os Estados Nacionais e os Direitos Humanos, pois, como explicam Keith Krause e Michel C. Williams (1997, p. 52), o coração dos estudos críticos de segurança é a orientação para a prática e para a superação de desafios com abordagens alternativas ao neorrealismo e ao neoliberalismo.

2. A nova escala das violações

Com a expansão das redes sociais *online* operadas por sistemas algorítmicos, uma série de tecnologias de modulação de comportamento passaram a interferir na condutas das pessoas a partir da coleta, processamento e análise, nem sempre autorizadas, de dados pessoais, em especial, dos comportamentos e atitudes que as pessoas realizam na Internet. Segundo o próprio Facebook sua plataforma envolve mais de 2 bilhões de usuários (2018). A pesquisa do Comitê Gestor da Internet no Brasil, com amostra de 25 mil entrevistados acima de 10 anos, em 2017, indica que 74% dos brasileiros com acesso à Internet acessam as redes sociais *online*. Diante dessa utilização intensa das redes de relacionamento, as teorias behavioristas alcançaram um novo patamar e estão sendo amplamente aplicadas pelas próprias plataformas, agências de *marketing* e de inteligência.

O texto *Psychological Targeting as an Effective Approach to Digital Mass Persuasion* sugere um tamanho de escala em que pesquisas psicométricas podem

ser realizadas. Antes da Internet e, principalmente, antes das redes sociais, a observação massiva de pessoas e o acompanhamento constante das suas ações era muito difícil. As pesquisas de laboratório mostram que esses apelos persuasivos são mais eficazes em influenciar o comportamento quando são adaptados às características psicológicas únicas dos indivíduos (Kosinski, 2016). Com a programação de algoritmos que seguem milhares de perfis de usuários das redes sociais *online* é possível definir os traços principais de personalidade de cada uma delas, como a pesquisa nos relata:

> Aproveitando a avaliação dos traços psicológicos das pegadas digitais, realizamos três experimentos do mundo real que alcançaram mais de 3,7 milhões de pessoas. Nossas experiências demonstram que o direcionamento de pessoas com apelos persuasivos adaptados a seus perfis psicológicos pode ser usado para influenciar seu comportamento conforme medido por cliques e conversões. [As taxas de cliques (CTRs) são uma métrica de marketing digital comumente usada que quantifica o número de cliques em relação ao número de vezes que o anúncio foi exibido. A taxa de conversão é uma métrica de marketing que reflete o número de conversões, como downloads de aplicativos ou compras em lojas on-line, em relação ao número de vezes que o anúncio foi exibido.] Os experimentos foram executados usando publicidade no Facebook, um comportamento típico plataforma de segmentação. (Matz, Kosinski, Nave, Stillwell, 2017, p.2, tradução livre[2])

O escândalo da empresa Cambridge Analytica (CA), agência de *marketing* que se vangloriava de ter sido responsável pela vitória de Donald Trump e pela aprovação da saída do Reino Unido da União Europeia (Brexit), ocorreu quando a imprensa internacional tomou conhecimento da violação massiva da privacidade dos usuários do Facebook promovida pela empresa (GUIMÓN, 2018, online). A CA aplicou técnicas psicométricas somadas ao cruzamento de dados geográficos sem

[2] Trecho original em inglês: *Capitalizing on the assessment of psychological traits from digital footprints, we conducted three real-world experiments that reached more than 3.7 million people. Our experiments demonstrate that targeting people with persuasive appeals tailored to their psychological profiles can be used to influence their behavior as measured by clicks and conversions. [Click-through rates (CTRs) are a commonly used digital marketing metric that quantifies the number of clicks relative to number of times the ad was shown. Conversion rate is a marketing metric that reflects number of conversions, such as app downloads or online store purchases, relative to the number of times the ad was shown.] The experiments were run using Facebook advertising, a typical behavioral targeting platform. (MATZ, S. C. et al. Psychological targeting as an effective approach to digital mass persuasion. Proceedings of the national academy of sciences, v. 114, n. 48, p. 12714-12719, 2017)*

autorização de milhões de usuários do Facebook para persuadi-los a votar de um determinado modo. A partir de um questionário respondido por alguns milhares de usuários do Facebook, a personalidade de cada um deles foi categorizado por uma das empresas ligadas a CA. Em seguida, passou a acompanhar a navegação no Facebook desses usuários. Utilizando algoritmos de aprendizagem de máquina (*machine learning*) estabeleceu um padrão de como cada tipo de personalidade clicava em determinados *links*, memes e postagens na rede social. A violação massiva de privacidade e do direito a não ser vigiado ocorre quando a CA ocorre quando os algoritmos de aprendizagem passam a acompanhar a navegação e a clicagem de mais de 70 milhões de norte-americanos com a finalidade de traçar o perfil psicométrico de cada um deles.

A gigantesca escala transnacional das violações de direitos humanos pela Internet também foi demonstrada pelo ex-analista de inteligência da *National Security Agency* (NSA), Edward Snowden, em 2013. O que ficou evidente é que as empresas de tecnologia com sede nos Estados Unidos possuem uma cumplicidade ambígua com a NSA que as utiliza para coletar dados de seus usuários em diversos países no mundo. O pesquisador David Lyon compreende que a vigilância se deslocou em direção ao *Big Data*. Nesse cenário, três questões são qualitativamente novas: primeiro, a vigilância consegue ser interconectada e quase permanente, ubíqua; segundo, a vigilância assume a perspectiva da descoberta de padrões, o que irá justificar o acesso sem precedentes aos dados de todos; terceiro, o uso do *Big Data* exige uma mudança ética e nas definições de privacidade para que possam retomar seu sentido diante dessas tecnologias (LYON, 2014, online).

3. Inteligência Artificial, *Big Data* e Algoritmos

Como tantas outras expressões comumente no mundo digital, o termo “Inteligência Artificial” não tem uma definição precisa, podendo variar para quem o utiliza. De acordo com Biddle (2018), trata-se de um conceito abrangente de subconjuntos, sendo um deles o “aprendizado de máquina” (*machine learning*). Como o nome sugere, seu objetivo principal é permitir que os computadores “aprendam sozinhos” e se tornem mais eficientes. Domingos (2017) informa que o

"aprendizado de máquina" abrange vários termos: reconhecimento de padrões, modelagem estatística, mineração de dados, descoberta de conhecimento, análise preditiva, ciência de dados, sistemas adaptativos e *deep learning*, dentre outros.

"*Big Data*" é outro conceito que permite várias interpretações, mas na maioria dos casos é o nome dado para o armazenamento, integração, processamento e tratamento destas gigantescas bases de dados geradas cotidianamente pela sociedade global conectada. Que bases são essas? Suas buscas no Google, sua atividade no Facebook e outras redes sociais, sua atividade bancária – extrato de conta-corrente e da fatura do cartão de crédito, os arquivos da câmera de segurança do seu condomínio, a declaração de Imposto de Renda, o registro dos medicamentos comprados em drogarias, o prontuário médico *online*, os filmes assistidos na Netflix ou outro serviço de *streaming*, seus e-mails, as músicas ouvidas no Spotify, os vídeos assistidos no YouTube. Enfim, toda e qualquer atividade na Internet que possa ser registrada e armazenada.

Como explica o professor de direito norte-americano Frank Pasquale, em seu livro *The Black Box Society*, o *Big Data* permite o funcionamento de um complexo padrão de técnicas de reconhecimento e análise de massivos volumes de dados que buscam racionalizar decisões e substituir intermediários. Neste contexto, as corporações que exploram o *Big Data* buscam capturar e integrar os dados de todas as pessoas físicas e jurídicas que estão na rede. Os dados são a matéria-prima valiosa, sem a qual não é possível realizar análises de tendências e predições. As cidadãs e os cidadãos podem pensar que ao ceder seus dados pessoais para as grandes plataformas e aos aplicativos tecnológicos terão no máximo o recebimento de propagandas indesejadas na Internet, conhecidas pelo nome de *spam*, mas, na verdade, tornam-se extremamente vulneráveis, uma vez que perdem a capacidade de controlar as informações sobre sua vida, história, interesses, percepções e desejos. Ao mesmo tempo que a privacidade é colocada em xeque pela captura massiva de dados, as corporações ocultam seus *softwares* e algoritmos por meio de códigos fechados, classificam trabalhos inovadores como confidenciais, registram patentes, assinam acordos de não-divulgação e aplicam regras de mordaça (PASQUALE, 2015, p. 03). O sigilo nos negócios é apresentado como indispensável para Wall Street e para o Vale do Silício, mas mulheres e homens que têm toda a sua atividade *online* gravada não conhecem as implicações sociais das práticas

invisíveis de como suas informações pessoais são classificadas e tratadas. As corporações alegam que a opacidade é a forma de se proteger diante de seus competidores. Pasquale escreve que *"o dinheiro está em busca do reconhecimento de padrões – quer juntar os pontos do comportamento passado para prever o futuro"* (*Ibid.,* p. 19). Os dados pessoais são a principal fonte de lucros para as corporações do *Big Data* que tomam decisões cruciais sobre como classificar e hierarquizar os indivíduos a partir de algoritmos fechados cuja a observação não permite saber o que fazem. Frank Pasquale alerta que essas corporações possuem técnicas de ofuscação para manter a opacidade de seus algoritmos e tecnologias.

Chandler (2015, p. 845) vê o *Big Data* como uma ferramenta de empoderamento, de capacidade de construir sociedades autogovernáveis e autorreproduzíveis. Funciona de uma forma diferente do que ocorreu com o modernismo pós-revolução industrial. Modelos de governança do tipo *Top-Down* ou o entendimento de causa-e-efeito para intervenções de políticas públicas são substituídos pela metodologia de gestão automatizada e centralizada da "autogovernança" do *Big Data*. Tal fenômeno é denominado por Chandler como a chegada de um mundo Pós-Humano, governado por uma realidade relacional e que elimina consequências indesejáveis. Se já vivemos ou não em um mundo "Pós-Humano" é um questionamento que exigirá estudos, pesquisas e reflexões aprofundadas no campo das Relações Internacionais.

Como argumenta a pesquisadora Shoshana Zuboff, *Big Data* não é uma tecnologia ou efeito tecnológico inevitável. Não é um processo autônomo, sua origem é plenamente social. Ela chama essa nova lógica de acumulação, que troca dados pessoais por dinheiro, de *Capitalismo de Vigilância*, do qual o *Big Data* é tanto uma condição como uma expressão (ZUBOFF, 2015, p. 77). Uma empresa como o Google não questiona se pode fotografar casas para sua base de dados. Simplesmente faz o que quer. Se processada, leva seus adversários à exaustão judicial ou eventualmente paga valores insignificantes se comparados ao retorno financeiro. Zuboff diz ainda que essa combinação de dados, extração e análise são a chave para a nova lógica de acumulação. As receitas dependem de ativos de dados apropriados por meio de operações automatizadas onipresentes. Esses ativos constituem uma nova classe: os *Ativos de Vigilância*, que é o que atrai os investimentos no *Capitalismo de Vigilância*. (*Ibid.,* p. 81) Trata-se de um regime

institucional em rede, ubíquo, que grava, modifica e torna mercadoria a experiência diária, de torradeiras a corpos, da comunicação ao pensamento, sempre com uma visão para estabelecer novos caminhos de "monetização" e lucros. Um poder soberano que aniquila a liberdade alcançada pelo mando da lei, que elimina a necessidade de contratos, de governança e o dinamismo da democracia de mercado. O Capitalismo de Vigilância estabelece uma nova forma de poder na qual os contratos e a força da lei são suplantados por recompensas e punições de um novo tipo de "mão invisível" (*Ibid.,* p. 82). O Capitalismo de Vigilância não elimina o direito de privacidade, mas o redistribui. Ao invés de ser um direito de todos, concentra-o nas empresas, que invoca tal direito como forma de legitimação para manter obscuras as operações de vigilância.

Em síntese, os subconjuntos *machine learning*, mineração de dados e *Big Data,* foram as técnicas que tornaram possível o que tem se chamado de Inteligência Artificial. De acordo com Sugomori (2016), esse novo método é uma ferramenta potente em comparação às abordagens anteriores que dependiam de informações fornecidas por seres humanos. Agora, as gigantescas bases de dados disponíveis são os insumos para classificação automatizada e criação de padrões. E com o reconhecimento de padrões, torna-se factível oferecer previsões para condutas semelhantes no futuro. Tais modelos preditivos são parametrizáveis e melhoram progressivamente de maneira automática.

O poder das empresas que controlam essas tecnologias fez com que o autor Philip N. Howard publicasse o livro *Pax Technica: How the Internet of Things May Set Us Free or Lock Us UP*, no qual explica conflitos políticos e de competição, domésticos ou globais, que ocorrem por meio das Tecnologias da Informação. Ele considera que já vivemos uma *Pax Technica*, um momento histórico em que arranjos políticos, econômicos e culturais de instituições sociais e de dispositivos conectados em rede unem firmemente governos e indústrias em pactos de defesa mútua, delineando colaborações, definindo padrões e explorando dados. A *Pax Technica* já teria substituído a *Pax Americana,* inaugurada no pós-Segunda Guerra Mundial, pois, de acordo com Howard, os EUA já perderam o controle da era digital. O país não seria mais a fonte primária de inovação em redes digitais e nem o mais importante construtor de infraestrutura de comunicação e informação. Se há 20 anos não haviam dúvidas de que os EUA eram o nó central na rede de desenvolvimento

tecnológico e do fluxo global de informações, este foi um estado temporário, superado. (HOWARD, 2015, p. 14)

Há um profundo debate no campo das Relações Internacionais de que se, no mundo pós-Guerra Fria, os Estados Unidos da América são o poder dominante ou se vivemos em um mundo multipolar, no qual convivem e disputam diferentes tipos de atores que projetam diferentes tipos de poder. Howard questiona quem tem esse poder e o que significa exercer esse poder. Para ele, nos dias atuais, quem projeta as novas tecnologias de informação, produz as mídias digitais e define os padrões da Internet tem grande influência e força para manipular a opinião pública. Os EUA seguem sendo um importante ator, seja pela tecnologia oriunda do *Silicon Alley*, pela capacidade de monitoração da Internet da Agência de Segurança Nacional (NSA) ou pela ascendência governamental sobre organizações como a *Internet Society* ou a *International Corporation for Assigned Names and Numbers* (ICANN). Mas há o crescimento tecnológico chinês, que tem o controle direto de seus usuários de sistemas, que exporta *hardware* para outros países e amplia sua rede de infraestrutura. E existem também os que Howard chama de "insurgentes tecnológicos", como o *Pirate Bay* e o *Wikileaks*, os *hackers* e os que denunciaram – e denunciam – segredos governamentais na rede (*Ibid.,* p. 13). Em muitos países do mundo, a política mudou radicalmente após a chegada da Internet – da profusão de *blogs* até o vazamento de vídeos de denúncias de violência policial, que se espalham de maneira viral. Talvez seja um exagero do autor falar em *Pax Technica*, mas, no mínimo, a proposição é sintomática dos problemas que os estados nacionais estão enfrentando com as inovações das tecnologias informacionais e que influenciam a política, a economia e a cultura.

Nick Srnicek, no livro *Platform Capitalism*, também aponta significativas mudanças da sociedade atual em comparação com a sociedade industrial do pós-Guerra. A capacidade de extrair dados para a inteligência dos negócios, da produção ao consumo, era bem limitada no capitalismo do mundo industrial. Já no cenário dominado pelas plataformas digitais e pelas tecnologias cibernéticas, a extração de dados está no DNA dos modelos de negócio. As plataformas, amplamente utilizadas e cada vez mais presentes em versões para celulares, coletam todos os dados possíveis dos seus usuários e dos dispositivos que utilizam com a finalidade de aprimorar as informações armazenadas e gerar receitas. O capitalismo do Século

XXI encontrou um novo material para se apropriar: os dados pessoais, afirma Srnicek. As plataformas digitais têm se tornado crescentemente o modo dominante de organizar os negócios e de monopolizar informações, analisá-las, usá-las e vendê-las.

4. Tipos de Violações de Direitos

As tecnologias mediadas por algoritmos têm a capacidade de infringir artigos da Declaração Universal dos Direitos Humanos, o que permite identificar tipos das principais violações. São exemplos o Artigo 7º (contra qualquer discriminação), o Artigo 10º (julgamento por tribunal independente), o Artigo 12º (privacidade e direito a intimidade) e o Artigo 19º (que garante o direito de liberdade de expressão e de opinião).

Imagine um veículo voador não tripulado, um *drone*, armado de mísseis *hellfire*, sobrevoando uma área civil de um país islâmico. O autômato persegue das alturas um determinado sujeito, previamente escolhido. Não conhece seu nome, mas vem há tempos observando seu padrão de comportamento, seu padrão biológico, seu peso estimado, sua altura aproximada, os locais por onde circula, os tipos de pessoas com quem conversa, hábitos e horários. Um algoritmo analisa e um *software* armazena todas as informações capturadas pelo olho mecânico e compara com parâmetros do que seria o padrão comportamental de um militante terrorista. Um sistema de pontuação, um *ranking*. O *drone* também observa o terreno, o número de pessoas no entorno do perseguido, quais os equipamentos em volta – se há prédios, fábricas, escolas, hospitais, estabelecimentos comerciais, conjuntos residenciais. Se a pontuação do possível militante atinge um número pré-definido no *ranking* e dadas as condições ideais ambientais, como boa visibilidade e pouca gente próxima, o robô assassino libera automaticamente seu míssil de fogo infernal dos céus e explode a vítima. Uma decisão autônoma, sem interveniência humana. Sem culpas ou ressentimentos por vidas aniquiladas ou danos colaterais. O que parece cena de um filme de ficção científica é a nova fronteira da pesquisa militar tecnológica dos Estados Unidos da América, conforme demonstra Grégoire Chamayou em seu livro *Teoria do Drone*. O pesquisador e filósofo escreve que, por

enquanto, os *drones* são controlados a distância, por operadores humanos, por princípio de telecomando.

Os exércitos não contam ainda com robôs letais autônomos, mas existem vários projetos nesse sentido. Um exemplo é o robô russo FEDOR (*Final Experimental Demonstration Object Research*), um humanoide projetado para substituir seres humanos em locais de alto risco, como em operações de resgate e em missões espaciais, desenvolvido pela Fundação de Estudos Avançados (FPI) do governo russo. Dentre suas habilidades, o FEDOR pode disparar armas de fogo com as mãos esquerda e direita, o que fez com a mídia internacional comparasse o autômato com o ciborgue do filme o *Exterminador do Futuro*, estrelado por Arnold Schwarzenegger na década de 1980. Não é difícil de imaginar que, em poucos anos, projetos similares serão utilizados em palcos de guerras. *"Quem dominar a Inteligência Artificial, dominará o mundo"*, disse o presidente da Federação Russa, Vladimir Putin, em evento público em setembro de 2017, divulgado pelo *site* RT.com.

O Artigo 10° da Declaração Universal dos Direitos Humanos manifesta: *"Toda a pessoa tem direito, em plena igualdade, a que a sua causa seja equitativa e publicamente julgada por um tribunal independente e imparcial que decida dos seus direitos e obrigações ou das razões de qualquer acusação em matéria penal que contra ela seja deduzida".* Um *software* que decide executar alguém, seja de um *drone* assassino ou de um robô pistoleiro, viola o princípio inscrito no Artigo 10º, pois o sistema computacional decretou sua eliminação física sem que um tribunal humano lhe oferecesse qualquer chance de defesa.

A situação torna-se mais preocupante se observarmos a concertação de esforços entre estados nacionais e instituições privadas para adaptar os desafios globais às exigências e aos limites da soberania estatal, como escreveu James Der Derian, em seu livro *Virtuous War*. Nesse trabalho, o autor revelou com profundidade a emergência de uma nova aliança virtual entre a indústria militar e as redes de entretenimento e de mídia. Em março de 2018, foi divulgado, pela BBC, um acordo entre o Google e o Pentágono para a desenvolver soluções de inteligência artificial para os *drones* dos EUA, o que confirma a estreita ligação das empresas de tecnologia da informação com o aparato militar do Estado norte-americano, conforme já descrito por Der Derian. Na primeira fase do projeto, o Google colaborará com um processo de análise automatizada da imensa quantidade de

filmagens coletadas diariamente pelos objetos voadores. Uma quantidade tão vasta de dados que é praticamente impossível ser aproveitada com eficiência por olhos humanos.

O combate ao terrorismo também é preocupação da Comissão Europeia, que tem exigido dos grandes serviços de Internet para que atuem contra a propagação de conteúdos extremistas na Rede Mundial de Computadores, conforme noticiou o jornal *El País*, em março de 2017. Os primeiros minutos após a publicação são considerados vitais para barrar a difusão de vídeos, áudios, imagens e textos. A instituição quer que as principais plataformas apaguem este tipo de conteúdo em, no máximo, uma hora depois de notificadas pelas autoridades policiais. Extinguir esses materiais só é possível com algoritmos capazes de reconhecer, rastrear e eliminar os conteúdos dentre as milhares de contas de cada serviço. Se há quase uma unanimidade quanto a necessidade de bloquear a propagação de filmagens de decapitações e de torturas executadas por organizações como o Estado Islâmico, há que se reconhecer que a tecnologia utilizada para combater este tipo de mensagem pode ser também aplicada na censura de qualquer tipo de informação indesejada. Tal prática pode levar a violação do Artigo 19° da Declaração Universal dos Direitos Humanos: *"Todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e ideias por qualquer meio de expressão".* Movimentos sociais, reivindicatórios, políticos, religiosos ou de qualquer outra natureza podem ser facilmente removidos por ferir interesses dos controladores dessas plataformas ou dos governos nacionais, que podem usar seu poder para pressionar as corporações para cercear o direito de expressão.

Um grupo de físicos da Universidade de Miami tenta criar um modelo matemático para filtrar o universo das mensagens *online* pró-terrorismo. O trabalho é feito via mineração de dados extraídos da rede social russa Vkontakte, buscando identificar simpatizantes de grupos radicais. O resultado da pesquisa foi publicado pela revista *Science*, em 2016. Da mesma forma, os algoritmos de redes sociais como o Facebook têm a capacidade de rotular seus usuários por preferência política: liberais, moderados ou conservadores, no caso da política interna dos Estados Unidos, publicou o jornal *NY Times*, em 2016. A dedução é baseada na atividade do usuário: as páginas que ele visita e as publicações que ele "curte". Se

alguém “curtir” a página de Donald Trump possivelmente será rotulado como conservador. Mesmo que a pessoa prefira são se vincular a conteúdos políticos de qualquer natureza, a rede social poderá classificá-la politicamente analisando os perfis de outras pessoas do seu círculo e que têm gostos e comportamentos similares.

O Centro de Investigações Sociológicas (CIS), em 2016, na Espanha, fez uma pesquisa com 2.500 pessoas, publicada no *El País*, quando perguntou peso e altura dos eleitores homens e mulheres. Com isso, criaram uma fórmula para estimar a preferência eleitoral de acordo com as características físicas dos votantes. Um exemplo: pessoas de esquerda teriam mais sobrepeso e altura média menor do que as de direita, mais magras e altas. Em democracias, essas rotulações políticas podem gerar pouco ou nenhum problema, mas em estados autoritários, totalitários, em situações de golpe de Estado ou de guerra civil, podem custar a vida ou a liberdade de alguém.

Análises algorítmicas já são usadas para justificar prisões. Em 2013, policiais de Wisconsin, EUA, prenderam um homem que dirigia um carro usado em uma troca de tiros. Na sentença que o levou a cadeia, o juiz responsável pelo caso citou que o criminoso era de alta probabilidade de reincidência conforme previsão de um programa de computador chamado COMPAS, utilizado para avaliação de riscos. O caso saiu em matéria do *NY Times*, em outubro de 2017. Por se tratar de um *software* proprietário não é possível saber como exatamente o programa funciona e o fabricante se recusou a divulgar seu código-fonte.

A cidade de Chicago, EUA, desde 2015, criou a Lista de Assuntos Estratégicos (do inglês: *Strategic Subject List*), que tem por objetivo classificar quais cidadãos têm mais probabilidade de envolvimento em atividades criminosas. A listagem é montada por um algoritmo não-publico, que pontua as chances de um indivíduo se envolver em um tiroteio como agressor ou mesmo como vítima. O sistema de pontos calcula e localiza em uma escala de 0 (risco extremamente baixo) até 500 (risco extremamente alto). A lista é publicada *online*, mas sem o nome das pessoas. Mesmo assim, pode-se questionar se a ferramenta não viola o direito de presunção de inocência. Não é possível ter certeza de que os dados completos dessa lista – ou de similares – não vazem. Se os nomes das pessoas com alta pontuação forem, por qualquer razão, acidentalmente ou não, divulgados ao público

é certo que elas serão punidas, ficando estigmatizadas, rotuladas, por crimes que não cometeram. O sistema de Chicago tem a preocupação de não incluir cor/raça ou sexo como um dos oito atributos que compõem o *ranking*. Porém, se essa lista for cruzada com outras bases de dados usando as técnicas de *Big Data* será muito simples complementar estes campos que podem ser usados como forma de reforçar preconceitos.

Preconceito contra mulheres, negros, LGBT ou qualquer outro grupo é uma violação do Artigo 7° da Declaração Universal dos Direitos Humanos: *"Todos são iguais perante a lei e, sem distinção, têm direito a igual protecção da lei. Todos têm direito a protecção igual contra qualquer discriminação que viole a presente Declaração e contra qualquer incitamento a tal discriminação"*. Mas podem as fórmulas, as equações matemáticas e os algoritmos serem preconceituosos? Laurie Penny, jornalista e ativista feminista de Londres, em artigo que publicou no jornal britânico *The Guardian,* afirma que robôs (Inteligência Artificial) são racistas e sexistas tanto quanto as pessoas que os criaram. São muitos os exemplos que podem ser usados para sustentar essa opinião. Os *softwares* de reconhecimento facial, cada vez mais utilizados para combater o crime e o terrorismo, funcionam melhor com rostos caucasianos, com pessoas brancas. Tal falha é chamada de "Biometria Imperfeita" pelo estudo "*O Alinhamento Perpétuo – Reconhecimento Facial Policial Não-Regulamentado na América*", produzido pelo Centro de Privacidade & Tecnologia da *Georgetown Law*. Algoritmos desenvolvidos majoritariamente por engenheiros homens e brancos e que fracassam ao discernir as faces de afrodescendentes podem levar à detenção e à culpabilização de inocentes.

A pesquisadora negra Joy Buolamwini, do *MIT Media Lab* e fundadora da organização Liga da Justiça Algorítmica[3], realizou um experimento ao trabalhar com robôs que usam visão computadorizada para detectar seres humanos. Após sucessivos problemas de reconhecimento facial, ela usou uma máscara branca, de plástico duro, não flexível, para interagir com as máquinas. Surpreendeu-se quando obteve melhores resultados do que com sua face verdadeira. Em entrevista ao *The Guardian*, Buolamwini explicou que a razão disso ocorrer é que os algoritmos são

[3] Algorithmic Justice League - https://www.ajlunited.org

sistemas projetados e treinados com rostos brancos, apesar do impacto do uso dessa tecnologia se dar em populações etnicamente diversas.

O aplicativo *Google Photos*, que organiza álbuns digitais *online*, foi alvo de um caso de grande repercussão na mídia, em 2015. Um usuário descobriu que o programa etiquetava automaticamente seus amigos negros como gorilas. A Inteligência Artificial do Google não era capaz de diferenciar humanos de pele escura de chimpanzés e outros tipos de macacos. O episódio fez com que a empresa se desculpasse publicamente. Em janeiro de 2018, três anos depois, a revista *Wired* testou o algoritmo, que estava "cego" para símios, apresentando "nenhum resultado" para buscas. Ou seja, para evitar o erro, a empresa passou a impedir a marcação automática para este tipo de animal.

Em 2016, nova polêmica ocorreu quando um jovem internauta divulgou um vídeo mostrando as diferenças ao procurar, utilizando o buscador do Google, as palavras-chave "três adolescentes negros" e depois "três adolescentes brancos". Na primeira busca apareciam fotos de fichas criminais, caras fechadas e ameaçadoras, de presidiários negros trajados de roupa laranja. Na segunda busca surgiam moços brancos e moças louras, felizes, sorridentes, abraçados uns aos outros, bem vestidos com roupas coloridas, festivas, segurando bolas de futebol e de basquete. A matéria foi publicada no *El País*, em junho de 2016.

Não são somente as minorias étnicas que podem ser vítimas de perseguição algorítmica. Em 2017, a comunidade LGBT acusou o YouTube de filtrar conteúdos de relacionamentos de pessoas de mesmo sexo, publicou o *The Guardian*. Esses vídeos seriam considerados "potencialmente inapropriados" e colocados em modo restrito, ficando escondidos na plataforma. Outro exemplo, mais grave, é de um *software* experimental da Universidade de Stanford, EUA, que seria supostamente capaz de diferenciar pessoas homossexuais e heterossexuais de acordo com suas características faciais. Para realização do estudo foram utilizadas 35 mil fotos de norte-americanos brancos, obtidas em um site de relacionamento. O nível de acerto seria de 81% para pessoas do gênero masculino e de 74% de gênero feminino. As características faciais adotadas incluíam características fixas (como o formato do nariz, por exemplo) e transitórias (como higiene pessoal). O estudo foi publicado pelo *Journal of Personality and Social Psychology*.

Relatório publicado pela Associação Internacional de *Gays*, Lésbicas, Bissexuais, Transexuais e Intersexuais (www.ilga.org), em 2017, informa que existem no mundo 72 países que criminalizam as relações homoafetivas e em oito deles a pena pode ser a morte. O que aconteceria se países como Irã, Arábia Saudita, Iêmen e Sudão resolvessem utilizar o *software* da Universidade de Stanford como forma de comprovar o "crime de homossexualismo"?

Países do Oriente Médio já utilizam esse tipo de tecnologia como forma de repressão. Em outubro de 2017, um palestino foi detido por causa de um erro de tradução do Facebook. Profissional de construção civil, ele publicou uma foto de si próprio junto a uma escavadeira e escreveu "bom dia", em árabe. O sistema de tradução da rede social reproduziu a expressão em hebraico "ataquem-nos" e em inglês "machuquem-nos" (*hurt them*). Foi o suficiente para que a polícia de Israel realizasse uma operação para prender o trabalhador, noticiou o *El País*.

Na mesma época, o site norte-americano ProPublica.org provou que o Facebook permitia habilitar propagandas para impulsionar conteúdos para grupos antissemitas. Ao pagar US$ 30,00, tiveram acesso aos tópicos "odiadores de judeus", "como queimar judeus" e "história de como os judeus arruinaram o mundo". A rede social aprovou os tópicos em 15 minutos. Depois de contactada pela equipe do ProPublica, a empresa eliminou a existência dessas categorias.

Algoritmos também pode atuar de forma sexista, estereotipando as mulheres. Pesquisadores da Universidade da Virgínia (ZHAO, WANG, YASKAR, ORDONEZ e CHENG), EUA, descobriram que objetos típicos de serviços de cozinha, como faca, garfo e colher, são associados por alguns *softwares* de I.A. ao sexo feminino, enquanto objetos de recreação como raquete de tênis, motocicleta e barco são vinculados aos homens.

Um artigo no jornal *NY Times*, de agosto de 2015, mostra que os *softwares* dos aparelhos de ar condicionado são baseados nas taxas metabólicas de homens adultos, a partir de uma fórmula criada nos anos 1960. O resultado é conforto ambiental para eles, mas uma temperatura fria demais para as mulheres, que acabam tendo que trabalhar agasalhadas.

O aplicativo de relacionamentos Tinder criou uma versão secreta de seu serviço, o TinderSelect, apenas para uso de pessoas de "boa aparência". Não se sabe os critérios da ferramenta para definir como são escolhidos os participantes,

como calcula quão desejável, quão atraente, é cada um. O conceito “atraente”, por si, é discriminatório, sexista, independente do que o sistema defina como padrão. A notícia foi publicada na Folha de S.Paulo, em março de 2017.

As corporações dizem que imperfeições biométricas, falhas de reconhecimento facial, categorizações equivocadas, erros de tradução, falhas e demais descalabros algorítmicos podem ser resolvidos com o avanço da tecnologia. E, para tanto, elas precisam captar cada vez mais dados, mais informações, da sociedade como um todo. Quanto menos privacidade melhor seria a experiência dos usuários nos serviços de *Big Data* ofertados, como se isso não fosse a base do Capitalismo de Vigilância.

A violação de privacidade ataca o Artigo 12° da Declaração Universal dos Direitos Humanos: *“Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei”*.

Todos os exemplos citados até agora podem ser considerados como violação de privacidade e como infrações ao Artigo 12º. Porém, é importante ressaltar um caso emblemático, ocorrido em 2010, que demonstra os riscos que a coleta massiva de dados promovida pelas corporações gera para os cidadãos. A autoridade de proteção de dados da Alemanha [4] exigiu uma auditoria sobre as informações coletadas pelo serviço de mapeamento de ruas chamado *Google Street View*. Lançado em 2007, o procedimento da coleta é feito por carros equipados com câmeras e outros dispositivos tecnológicos que percorrem as vias públicas das cidades fotografando-as detalhadamente para depois associá-las ao mapa de cada localidade. Os veículos utilizados pelo Google tinham antenas instaladas capazes de capturar dados de redes wi-fi, domésticas e corporativas, e utilizar esses dados em seus serviços de localização. A empresa publicou em seu *blog* oficial, em 27 de abril de 2010, que recolhia nomes de redes (SSIDs) e números de identificação (*Mac Addresses*) de aparelhos de rede como roteadores, mas não guardava os dados que passavam por essas redes. Porém, em 14 de maio, após confrontado pela autoridade alemã, o Google fez uma nova publicação, na qual admitiu que por

[4] Die Landesbeauftragte für den Datenschutz Nordrhein- Westfalen - www.ldi.nrw.de

engano havia incluído um código em seu *software* que coletava exemplos de dados que trafegavam pelas redes wi-fi, mas que nunca haviam utilizado essas informações nos produtos da empresa. Um pedaço de código, legado de um projeto experimental, havia sido reutilizado para programar os carros do *Street View*. Esta teria sido a origem do erro que levou à captura de dados pessoais. *"Tão logo fomos avisados do problema, nós alteramos nossos veículos do Street View e segregamos os dados de nossa rede, que desconectamos para fazê-la inacessível. Apagaremos os dados tão logo seja possível (...)"*, registrou o Google em seu *blog*. Em síntese, a empresa equipou seus veículos com antenas e com um *software* capaz de recolher e armazenar dados técnicos e pessoais de redes wi-fi de cada residência nas ruas por onde passou. O procedimento durou, pelo menos, de 2007 a 2010, quando a prática foi questionada pelo governo alemão. Em sua defesa, a corporação disse que se tratava de um erro, de um acidente.

De maneira mais explícita, o Governo da República Popular da China não tem constrangimentos em usar o *Big Data* para analisar as informações de seus cidadãos na Internet. Em seu *blog Copy From China*, o jornalista Felipe Zmoginski escreve que o país asiático pretende criar um "sistema de crédito social", com o qual irá pontuar cada indivíduo, premiando pessoas "bem-comportadas" e punindo "desordeiros". A empresa Sesame Credit, subsidiária do grupo Alibaba, conduz um projeto piloto, desde 2014, pelo qual analisa o comportamento *online* de voluntários que trocam seus dados pessoais por descontos em produtos diversos, como empréstimos bancários. Zmoginski diz que não há transparência no sistema, mas aparentemente quem gasta dinheiro com videogames costuma receber menos pontos de quem compra livros ou fraldas para bebê. A implantação plena do sistema está prevista para 2020 e a adesão será obrigatória para todos os chineses. Haverá cruzamento de dados de comércio eletrônico, da autoridade fiscal e de boletins de ocorrência. Fazer barulho após 22 horas, fumar em local proibido, atrasar o pagamento da conta de luz ou dirigir bêbado fará com que se perca pontos sociais. Se relacionar com quem tem pontuação baixa ou alta também poderá influenciar na posição de cada pessoa no *ranking*. Enquanto ainda funciona como um serviço privado, em sua página de Internet, www.creditsesame.com, a empresa vende seu serviço justificando que *"a diferença entre uma boa pontuação de crédito e uma má pode significar milhares de dólares e mesmo um impacto na capacidade de obter um*

empréstimo". Curiosamente, ao mesmo tempo em que classifica e categoriza seus clientes, a Credit Sesame afirma que a privacidade é de alta prioridade para a empresa. Que utiliza o método mais poderoso de criptografia disponível e que as informações do usuário são visíveis apenas para ele mesmo. Que os dados não são vendidos ou compartilhados com terceiros, com patrocinadores ou com empregados.

5. Conclusão

Os casos aqui relatados demonstram que as tecnologias cibernéticas, apropriadas ou desenvolvidas pelas corporações capitalistas, estão servindo à violação e ao enfraquecimento de importantes princípios da Declaração Universal de Direitos Humanos. A intensa competição entre empresas levou a estruturação de um mercado informacional baseado principalmente na coleta, armazenamento e venda de dados pessoais, processados e reunidos em amostras ou em estado bruto. A atual economia informacional pode ser compreendida como um Capitalismo de Plataforma (Srnicek) que é um Capitalismo de Vigilância (Zuboff).

Além disso, essas atividades são operadas por actantes, *softwares*, algoritmos e tecnologias de tratamento de grandes bases de dados que permitem realizar predições com a finalidade de influenciar decisões privadas e públicas. Confirmando a análise de Der Derian, poderosos estados nacionais, articulando suas corporações de tecnologia e entretenimento, passam a ampliar as ações de vigilância sobre cidadãos, adentrando em espaços privados altamente reveladores da personalidade, comportamento, interesse e desejo das pessoas.

Por fim, a inteligência artificial, em especial, os algoritmos de *machine learning,* que tantos benefícios pode trazer para a educação, saúde, gestão pública e de negócios, organização de cidades, simultaneamente está abrindo caminho para a proliferação de aparelhos de segurança e de ação militar autômatos, sem a necessidade da mediação humana. Essa nova fase da prática estatal da violência, seja para o controle social ou para a guerra, implica que a Declaração Universal dos Direitos Humanos seja +defendida e ampliada para que possamos conter as nefastas tendências de dominação opressiva e assimetrias inaceitáveis em nosso cotidiano.

Referências Bibliográficas

BELLUCKAUG, Pam. *Chilly at Work? Office Formula Was Devised for Men.* Site: NYTimes.com, em 3 de agosto de 2015. Disponível em: <https://www.nytimes.com/2015/08/04/science/chilly-at-work-a-decades-old-formula-may-be-to-blame.html>. Acesso em 5 de abril de 2017.

CHAMAYOU, Grégoire. *Teoria do Drone.* SP, Cosac Naify, 2015.

CHANDLER, David. *A world without causation: Big data and the coming of age of posthumanism*. Millennium, v. 43, n. 3, p. 833-851, 2015.

CHICAGO DATA PORTAL. Site Oficial da Cidade de Chicago. *Strategic Subject List. Disponível em: <https://data.cityofchicago.org/Public-Safety/Strategic-Subject-List/4aki-r3np>. Acesso em: 5 de abril de 2018.*

Data collected by Google cars. Site: Google Europe Blog, em 27 de abril de 2010. Disponível em: <https://europe.googleblog.com/2010/04/data-collected-by-google-cars.html>. Acesso em 5 de abril de 2018.

DER DERIAN, James. *Antidiplomacy: spies, terror, speed, and war. Blackwell*, 1992.

DER DERIAN, James. *Critical encounters in international relations.* International Social Science Journal, v. 59, n. 191, p. 69-73, 2008.

DER DERIAN, James. *Virtuous War: Mapping the Military-Industrial-Media-Entertainment-Network.* 2nd ed. Taylor & Francis e-Library, 2009.

DOMINGOS, Pedro. *O algoritmo mestre.* São Paulo: Novatec. 2017.

FUNDAÇÃO DE ESTUDOS AVANÇADOS (FPI). Site Oficial do Governo da Federação Russa, em 13 de outubro de 2017. *Disponível em:* <http://fpi.gov.ru/press/media/razrabotchik_robota_fedora_rasskazal_o_pyati_svoih_slozhneyshih_zadacha h>. Acesso em: 2 de abril de 2018.

GARVIE, Clare; BEDOYA, Alvaro; FRANKIE, Jonathan. *The Perpetual Line-up*

Unregulated Police Face Recognition in America. Center on Privacy & Technology at Georgetown Law, em 18 de outubro de 2016. *Disponível em: <www.perpetuallineup.org>*. Acesso em: 5 de abril de 2018.

GUIMÓN, Pablo. Christopher Wylie: *"O 'Brexit' não teria acontecido sem a Cambridge Analytica".* Internacional. EL PAÍS Brasil. 18/04/2018. Disponível: https://brasil.elpais.com/brasil/2018/03/26/internacional/1522058765_703094.html Acesso 05/10/2018.

HOWARD, Philip N. *Pax Technica: How the Internet of things may set us free or lock us up.* Yale University Press, 2015.

HUNT, Elle. *LGBT community anger over YouTube restrictions which make their videos invisible*. Site: TheGuardian.com, em 20 de março de 2017. Disponível em: <https://www.theguardian.com/technology/2017/mar/20/lgbt-community-anger-over-youtube-restrictions-which-make-their-videos-invisible>. Acesso em 5 de abril de 2018.

ISRANI, Ellora Thadaney. *When an Algorithm Helps Send You to Prison.* Site: NYTimes.com, em 26 de outubro de 2017. *Disponível em:* <https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html>. Acesso em: 2 de abril de 2018.

JOHNSON, N.F.; ZHENG, M.; VOROBYEVA, Y.; GABRIEL, A.; QI, H.; VELASQUEZ, N.; MANRIQUE, P.; JOHNSON, D.; RESTREPO, E.; SONG, C.; WUCHTY, S. *New online ecology of adversarial aggregates: ISIS and beyond .* Science (Magazine), Vol 352, Issue 6292 , em 17 de junho de 2016. *Disponível em:* <http://science.sciencemag.org/content/352/6292/1459>. Acesso em: 2 de abril de 2018.

KELION, Leo. *Google tech used by Pentagon 'to analyse drone videos'*. Site: BBC.com, em 7 de março de 2018. *Disponível em:* <http://www.bbc.com/news/technology-43316667> Acesso em: 2 de abril de 2018.

KOSINSKI, Michal et al. *Mining big data to extract patterns and predict real-life outcomes*. Psychological methods, v. 21, n. 4, p. 493, 2016.

KOSINSKI, Michal; WANG, Yilun. *Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation From Facial Images.* Journal of Personality and Social Psychology. February 2018, Vol. 114, Issue 2, P. 246-257. Stanford Graduate School of Business. *Disponível em:* <https://www.gsb.stanford.edu/faculty-research/publications/deep-neural-networks-are-more-accurate-humans-detecting-sexual>. Acesso em: 5 de abril de 2018.

LLANERAS, Kiko. *Dime cuánto mides y te diré a quién votas.* Site: ElPais.com, em 23 de junho de 2017. Disponível em: <https://politica.elpais.com/politica/2017/06/23/ratio/1498207330_149656.html>. Acesso em: 2 de abril de 2018.

LYON, David. *Surveillance, Snowden, and big data: Capacities, consequences, critique*. Big Data & Society, v. 1, n. 2, 2014. Disponível: http://journals.sagepub.com/doi/pdf/10.1177/2053951714541861 Acesso em: 10/05/2018.

MATZ, S. C. et al. *Psychological targeting as an effective approach to digital mass persuasion.* Proceedings of the national academy of sciences, v. 114, n. 48, p. 12714-12719, 2017.

MERRILLAUG, Jeremy B. *Liberal, Moderate or Conservative? See How Facebook Labels You*. Site: NYTimes.com, em 23 de agosto de 2016. *Disponível em:* <https://www.nytimes.com/2016/08/24/us/politics/facebook-ads-politics.html>. Acesso em: 2 de abril de 2018.

NYE JR, Joseph S. *Cyberpower.* Harvard Univ Cambridge, MA, Belfer Center for Science and International Affairs, 2010.

PASQUALE, Frank. *The black box society: The secret algorithms that control money and information*. Harvard University Press, 2015.

PENNY, Laurie. *Robots are racist and sexist. Just like the people who created them.* Site: TheGuardian.com, em 20 de abril de 2017. *Disponível em: <https://www.theguardian.com/commentisfree/2017/apr/20/robots-racist-sexist-people-machines-ai-language>. Acesso em: 5 de abril de 2018.*

PEREDA, Cristina F. *¿Google es racista?: Un joven demuestra en un vídeo las diferencias al buscar "tres adolescentes negros" y "tres adolescentes blancos"*. Site: ElPais.com, em 10 de junho de 2016. Disponível em <https://elpais.com/internacional/2016/06/10/estados_unidos/1465577075_876238.html>. Acesso em 5 de abril de 2018.

SÁNCHEZ, Álvaro. *Los gigantes de Internet tendrán una hora para borrar contenidos terroristas. Site: ElPais.com, em 1º de março de 2017. Disponível em: <https://elpais.com/internacional/2018/03/01/actualidad/1519898000_774757.html>. Acesso em: 2 de abril de 2018.*

SANZ, Juan Carlos. *Un palestino detenido por un error de traducción de Facebook*. Site: ElPais.com, em 25 de outubro de 2017. Disponível em: <https://elpais.com/internacional/2017/10/24/mundo_global/1508864861_586037.html>. Acesso em 5 de abril de 2018.

SILVEIRA, Sérgio Amadeu da. *Tudo sobre tod@s: Redes digitais, privacidade e venda de dados pessoais.* Ebook Kindle, 2017.

SIMONITE, Tom. *When It Comes to Gorillas, Google Photos Remains Blind.* Site: Wired.com, em 11 de janeiro de 2018. Disponível em: <https://www.wired.com/story/when-it-comes-to-gorillas-google-photos-remains-blind>. Acesso em 5 de abril de 2018.

SRNICEK, Nick; DE SUTTER, Laurent. *Platform Capitalism*. Cambridge, UK; Malden, MA: Polity, 2017.

Tinder tem versão secreta só para pessoas bonitas e celebridades, diz site. Site: Folha de S.Paulo, em 8 de março de 2017. Disponível em: <http://www1.folha.uol.com.br/tec/2017/03/1864670-tinder-tem-versao-secreta-so-para-pessoas-bonitas-e-celebridades.shtml>. Acesso em 5 de abril de 2018.

TOBIN, Ariana; ANGWIN, Julia; VARNER, Madeleine. *Facebook Enabled Advertisers to Reach 'Jew Haters'*. Site: ProPublica.org, em 14 de setembro de 2017. Disponível em: <https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters>. Acesso em 5 de abril de 2018.

TUCKER, Ian. *Interview: 'A white mask worked better': why algorithms are not colour blind.* Site: TheGuardian.com, em 28 de maio de 2017. *Disponível em:*

<https://www.theguardian.com/technology/2017/may/28/joy-buolamwini-when-algorithms-are-racist-facial-recognition-bias>. Acesso em: 5 de abril de 2018.

UNITED NATIONS GENERAL ASSEMBLY. Human Rights Council. *A/HRC/32/L.20 – Draft Resolution/Decision: The Promotion, Protection And Enjoyment Of Human Rights On The Internet.*, 2016.

VIRILIO, Paul; PACIORNIK, Celso Mauro; DOS SANTOS, Laymert Garcia. *Velocidade e política*. Estação Liberdade, 1996.

WiFi data collection: An update. Site: Google Europe Blog, em 14 de maio de 2010. Disponível em: <https://europe.googleblog.com/2010/05/wifi-data-collection-update.html>. Acesso em 5 de abril de 2018.

'Whoever leads in AI will rule the world': Putin to Russian children on Knowledge Day. Site: RT.com, em 1º de setembro de 2017. *Disponível em:* <https://www.rt.com/news/401731-ai-rule-world-putin>. Acesso em: 2 de abril de 2018.

ZHAO, Jieyu; WANG, Tianlu; YATSKAR, Mark; ORDONEZ, Vicente; CHENG, Kai-Wei. *Men Also Like Shopping: Reducing Gender Bias Amplification using Corpus-level Constraints.* University of Virginia, 2017. Disponível em: <http://www.cs.virginia.edu/~kc2wc/publications/ZWYOC.html>. Acesso em 5 de abril de 2018.

ZMOGINSKI, Felipe. *Sistema de crédito social chinês revela uso autoritário da tecnologia.* Site: Blog Copy From China - Blogosfera UOL, em 28 de março de 2018. Disponível em: <https://copyfromchina.blogosfera.uol.com.br/2018/03/28/na-china-pontuacao-de-comportamento-beira-o-autoritarismo/>. Acesso em 5 de abril de 2018.

ZUBOFF, Shoshana, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization, em* 4 de abril de 2015. Journal of Information Technology (2015) 30, 75–89.