Revista Jurídica unicuritiba

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

DESGLOBALIZAÇÃO E IA: MORTE DA INTERNET GLOBALIZADA, AUMENTO DAS TECNO-AUTOCRACIAS E FIM DA ERA DA AUTORREGULAÇÃO

DEGLOBALIZATION AND AI: THE DEATH OF THE GLOBALIZED INTERNET, THE RISE OF TECHNO-AUTOCRACIES AND THE END OF THE ERA OF SELF-REGULATION

PAOLA CANTARINI[1]
Professora universitária, PhD em Direito, Filosofia (PUC-SP) e em Filosofia do Direito (Unisalento); Pós-Doutorado em Direito, Filosofia e Sociologia (FDUSP, PUCSP-TIDD, EGS, Universidade de Coimbra/CES, IEA/USP). Pesquisadora do IEA/projeto UAI, e em pós-doutorado na USP/RP em IA. Presidente e Pesquisadora no EthikAI – ethics as a service . Membro da Comissão da Criança e do Adolescente e da Comissão de Proteção de Dados da OABSP e de IA da OAB/Santo Amaro.

RESUMO: O presente artigo visa, pois, trazer reflexões críticas, acerca da questão da vigilância relacionada ao big data, com base em autores como Foucault e seus estudos de sociedade da normalização, disciplina e regulamentação, sua evolução nas obras de Deleuze e de Byung-Chun Han, com a perspectiva da sociedade de controle e do panóptico digital, e David Lyon, conjugando-se tal temática à questão do fim da era da autorregulação quanto à IA, a batalha pela supremacia tecnológica e os desafios envolvendo os três principais modelos de países, quais sejam, EUA, China e EU. O artigo também trará uma abordagem crítica e interdisciplinar acerca de questões interligadas como o fim da internet globalizada e o surgimento de uma verdadeira balkanização da internet e da economia digital.

Objetivos: Visa-se aprofundar questões fundamentais, em uma abordagem crítica e interdisciplinar acerca de mitos, objetivos, desafios e oportunidades com relação à temática da IA, em específico acerca dos principais modelos regulatórios existentes, e temáticas relacionadas, como a balkanização da internet e da economia digital, o fim da era da autorregulação, e a batalhas pela supremacia tecnológica, associadas a temática do aumento da vigilância, caracterizada agora como em massa e com uso do big data.

[1] Este texto faz parte das pesquisas desenvolvidas em sede de pós-doutorado na USP/RP em IA com bolsa Fapesp.

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

Metodologia: A metodologia e as técnicas de investigação combinarão a investigação teórica, relacionando-se com a metodologia de Michel Foucault denominada de "teatro filosófico", buscando-se uma visão interdisciplinar e holística, e uma epistemologia multifacetada.

Resultados: Buscou-se contribuir para o entendimento acerca dos três principais modelos regulatórios de IA, quais sejam EUA, EU e China, trazendo suas características e os desafios futuros em torno de problemáticas como da corrida em prol do desenvolvimento e da regulação da IA, bem como acerca de um necessário equilíbrio entre de um lado a busca da inovação, não como um direito absoluto, mas de forma a ser compatibilizada com uma proteção adequada e sistêmica de direitos potencialmente afetados pela tecnologia.

Contribuições: O artigo ressalta a importância de uma abordagem crítica, interdisciplinar e holística acerca da temática da IA em geral, assim como no tocante aos temas do panóptico digital, da vigilância digital, relacionados por sua vez com os conceitos de supremacia tecnológica e diversas perspectivas em torno de modelos regulatórios, visando-se desafiar mitos e dogmas como o da existência de um necessário trade-off entre regulação da tecnologia e a inovação, enfatizando a importância de se evitar abordagens utópicas e também distópicas.

Palavras-Chave: inteligência artificial; direitos fundamentais; panóptico digital; vigilância digital; supremacia tecnológica; modelos regulatórios.

***ABSTRACT**: This article aims to provide critical reflections on the issue of surveillance related to big data, based on authors such as Foucault and his studies of the society of normalization, discipline and regulation, its evolution in the works of Deleuze and Byung-Chun Han, with the perspective of the society of control and the digital panopticon, and David Lyon, combining this theme with the question of the end of the era of self-regulation in relation to AI, the battle for technological supremacy and the challenges involving the three main country models, namely the USA, China and the EU. The article will also take a critical and interdisciplinary approach to interconnected issues such as the end of the globalized internet and the emergence of a true balkanization of the internet and the digital economy.*

***Objectives:** The aim is to delve into fundamental issues, in a critical and interdisciplinary approach to myths, objectives, challenges and opportunities in relation to the theme of AI, specifically in relation to the main existing regulatory models, and related themes, such as the balkanization of the internet and the digital economy, the end of the era of self-regulation, and the battles for technological supremacy, associated with the theme of increased surveillance, now characterized as mass and with the use of big data.*

***Methodology:** The methodology and research techniques will combine theoretical research with Michel Foucault's "philosophical theater" methodology, seeking an interdisciplinary and holistic vision and a multifaceted epistemology.*

***Results:** The aim was to contribute to an understanding of the three main AI regulatory models, namely the US, the EU and China, bringing out their characteristics and the future challenges surrounding issues such as the race to develop and regulate AI, as*

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

well as the necessary balance between, on the one hand, the pursuit of innovation, not as an absolute right, but in a way that is compatible with adequate and systemic protection of rights potentially affected by the technology.

Contributions: *The article highlights the importance of a critical, interdisciplinary and holistic approach to the subject of AI in general, as well as to the themes of the digital panopticon, digital surveillance, related in turn to the concepts of technological supremacy and various perspectives on regulatory models, with the aim of challenging myths and dogmas such as the existence of a necessary trade-off between regulating technology and innovation, emphasizing the importance of avoiding utopian and dystopian approaches.*

Keywords: *Artificial intelligence; Fundamental rights; Digital panopticon; Digital surveillance; Technological supremacy; Regulatory models*

1 BATALHA PELA SUPREMACIA TECNOLÓGICA, MODELOS REGULATÓRIOS EM JOGO E FIM DA INTERNET GLOBAL

Em tempos de batalha pela supremacia tecnológica, fala-se agora não apenas em uma corrida em prol do desenvolvimento da IA pelos países mas também em prol da regulamentação da tecnologia, tendo sido abandonado o discurso pela maioria dos principais players de que não é necessária a regulamentação da IA, contudo, abrindo-se novas dinâmicas nesta seara, com novos desafios por parte de empresas de tecnologia que operam globalmente, já que há diversos modelos regulatórios em jogo e em rota de colisão, com destaque para os sistemas americano, chinês e europeu. Aponta-se para verdadeiras batalhas verticais interseccionais na evolução da economia digital, apostando-se no fim da internet globalizada, e no surgimento de nichos regionais específicos, com a fragmentação da internet global em uma "splinternet", ou seja, diversas "internetes paralelas", controladas por diferentes governos, a exemplo das americana e chinesa, como destaca o relatório de 2022 do Council on Foreign Relations, ao afirmar que "a era da internet global acabou" (https://www.cfr.org/annual-report-2022).

Ao mesmo tempo que é apontada a divisão de estratégias de IA diversas entre EUA, China e EU, com uma evolução de tal conflito de modo contínuo, aposta-se no declínio do modelo regulatório americano**,** baseado no mercado, já que o próprio país estaria se afastando dele, adotando uma postura, de um lado mais reguladora, e de outro mais de intervenção do Estado, ou seja, aproximando-se tanto do sistema

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

europeu como do chinês, além das críticas da população a questões que envolvem moderação de conteúdo, discursos de ódio, e da mudança de mindset das próprias empresas de tecnologia que cada vez mais admitem que a regulamentação é necessária, reconhecendo-se que a era da autorregulação acabou.

Tal dinâmica acaba por desafiar as premissas de uma internet global, ocorrendo um processo de fragmentação, desmembramento e desacoplamento gradual da economia digital global, reduzindo-se as chances de cooperação global, dando ensejo a se postular por uma desglobalização, a exemplo da conduta da China de bloquear acesso a vários sites estrangeiros e dos EUA de limitar a capacidade de operação de softwares americanos, como os do Google, com restrições de uso em telefones fabricados pela empresa chinesa Huawei.

Por outro lado, haveria uma certa aproximação do modelo regulatório americano ao chinês, com a mudança de postura após o acirramento da guerra tecnológica entre os países, já que haveria uma verdadeira balkanização da internet e da economia digital, apostando-se em um fortalecimento do modelo regulatório estatal chinês como marco para a economia digital.

Uma das questões centrais quando se aponta para a necessidade de regular a IA, tanto via heterorregulação como via sandbox ou autorregulação regulada é atingir um grau de conformidade e maturidade em nível internacional, a exemplo do que ocorre na área de proteção de dados, sendo um requisito da União Europeia e do Brasil para a transferência internacional de dados, bem como vem sendo destacada tal necessidade no âmbito da temática do sandbox regulatório, em especial nos documentos da lavra da OCDE. É o que dispõe também a lei americana denominada “Clarifying Lawful Overseas Use of Data Act” (CLOUD Act) de 2018, autorizando o governo americano a firmar acordos bilaterais de compartilhamento de dados com países que são certificados como tendo proteções adequadas para privacidade e liberdades civis.

Contudo, verifica-se que no âmbito da IA há uma competição regulatória entre 3 principais modalidades distintas de abordagem, considerando-se EUA, EU e China, e as empresas em algum momento terão que realizar escolhas no sentido de fazer uma opção por qual caminho tomar, sendo em muitos casos incompatível a observância do conjunto de perspectivas simultaneamente, já que se fundam em premissas e valores diversos. De um lado temos as políticas americanas com base no "America First" e de outro lado a agenda “Made in China 2025”, apostando-se na

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

corrida armamentista com base principalmente na autossuficiência tecnológica em áreas consideradas essenciais e críticas, como IA, semicondutores, computação em nuvem e baterias, em direção ao protecionismo tecnológico ou nacionalismo digital, com a majoração do papel do Estado na economia digital, por meio de subsídios estatais na área tecnológica, podendo dar ensejo ao que se denomina de “tecno-nacionalismo” global.

Como terceira opção regulatória temos a União Europeia vocacionada a uma proteção mais robusta de direitos, em uma abordagem orientada a direitos, se contrapondo ao modelo americano, com base nos princípios da não-regulação comercial e da anti-censura, focando na concepção de dados como mercadoria a ser monetizada pelas empresas de tecnologia com poucas restrições, apostando no mercado livre e na baixa intervenção estatal, em uma abordagem orientada pelo mercado (destacam-se neste sentido: o “Communications Decency Act”, de 1996 e sua famosa Seção 230 excluindo de responsabilidade as empresas de tecnologia em relação ao conteúdo das redes sociais, o "Global Internet Freedom Act" de 1997, em prol da livre circulação de informações, a proteção de jornalistas e dissidentes políticos online e o "Global Internet Freedom Task Force” de 2006, do Departamento de Estado dos EUA a favor de tais princípios em países com regimes repressivos).

Outra divergência significativa é um maior equilíbrio entre de um lado a proteção da privacidade e de outro restrições à vigilância estatal no entender da EU, ao passo que para os EUA o peso maior cai a favor da vigilância digital para fins de aplicação da lei ou segurança nacional, mesmo que de forma contraditória condene no cenário internacional a conduta chinesa quanto a vigilância estatal digital. Diversos julgados do Tribunal de Justiça da EU destacam o abuso da retenção indiscriminada, desnecessária e desproporcional de metadados pessoais contidos em comunicações eletrônicas (caso Digital Rights Ireland de 2014), mesmo em caso de controle de crimes.

Assim como se fala no fim da era da autorregulação e no “efeito Bruxelas” da EU no caso do GPPR, com as empresas tendo optado por cumprir as suas exigências regulatórias, também ocorreria a mesma dinâmica em outras áreas interligadas, como regras antitruste, discurso de ódio e desinformação, e a tendência é que o mesmo ocorra no âmbito da IA. Neste sentido destaca-se a EU como um padrão global de conformidade regulatória, já que as empresas preferem não seguir a linha da customização, e adotar um “compliance” para cada sistema regulatório de cada país,

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

o que é corroborado pelo fato de haver 150 países adotando leis de proteção de dados semelhantes ao nível da regulação da UE. Aponta-se, pois que o AI ACT terá este mesmo efeito de moldar as demais regulações e compliances quanto a aplicações da IA globalmente já que estas seriam na maior das vezes dependentes de dados europeus, e uma vez tendo sido adotadas medidas de governança de dados para fazer frente as exigências europeias, não faria muito sentido desenvolver de forma customizada outros sistemas de IA ou outras medidas de compliance.

Vigora um mito ou dogma de que a inovação, responsável pela liderança tecnológica, competitividade e crescimento econômico depende de um mercado não regulamentado, como um trade-off necessário e absoluto entre inovação e regulação. O modelo americano, contudo, fundamentou a premissa da não regulação por entender esta como essencial à democracia, contudo, vivemos um momento de crise mundial da democracia, já que há cada vez mais uma concentração de riqueza, potencializada pelo monopólio de big techs quanto ao desenvolvimento da IA, além de mutilação do princípio do voto livre e da livre manifestação de vontade ou consciência já que as ferramentas de IA são utilizadas para manipular comportamentos e emoções, ou seja, cada vez mais vemos um hiato entre as premissas democracia forte e regulação fraca. Por outro lado também é questionável que a única razão para a EU não ser líder tecnológico seria a regulação da tecnologia, já que a legislação da IA via AI ACT é extremamente recente, e já não havia uma premissa tecnológica dos países europeus, sendo apontados outros fatores para a não competitividade tecnológica da Europa, como a existência de um mercado digital único (DSM) fragmentado, leis e culturas diversas, além do aspecto punitivo das leis de falência, desestimulando a tomada de riscos e da ausência de uma política de imigração que possibilite atrair talentos estrangeiros.

Alguns exemplos paradigmáticos são citados por Anu Bradford no livro “Digital empires”, como o caso da Apple, pois apesar de afirmar o respeito à privacidade e aos demais direitos humanos fundamentais, há uma distância entre a teoria e prática, e certa maquiagem comercial, a exemplo do que também se dá no âmbito do compliance e da ética, falando-se em lavagem ética e de compliance, quando não são realizadas mudanças substanciais, atuando-se na superfície como um efeito de fachada. Isso porque a Apple de um lado apoia-se em princípios que são caros aos EUA, mas de outro, no âmbito de suas relações e práticas comerciais com a China, derroga estes princípios, para se adequar aos valores e condições impostas pelo país,

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

permitindo o armazenamento dos dados dos seus usuários em servidores chineses, e seu gerenciamento por funcionários estatais chineses, bem como ao permitir o armazenamento das chaves necessárias para desbloquear criptografias localmente na China. Com tais ressalvas possibilita-se o acesso pelo governo chinês de dados pessoais dos usuários da Apple, ao redor do mundo, ampliando-se o sistema de vigilância. A fim de que tal exigência fosse possível de ser cumprida a Apple traçou uma estratégia que lhe permitiu não violar as leis dos EUA que proíbe tal ação, ao conceder a propriedade dos dados de seus clientes chineses a uma empresa estatal chinesa, a Guizhou-Cloud Big Data, em afronta aos princípios da transparência, boa-fé e confiança.

Outra conduta contrária aos princípios de um Estado Democrático de Direito e contrária aos valores americanos foi o bloqueio de aplicativos pela Apple em sua App Store chinesa que não têm a aprovação da liderança política chinesa, a exemplo de serviços de notícias estrangeiros ou serviços de encontros para homossexuais, aplicativos envolvendo temas sensíveis, como o Dalai Lama e a independência de Taiwan ou Tibete, ou aplicativos usados para organizar protestos pró-democracia. Da mesma forma ao remover em 2021 o aplicativo do Alcorão na China, cedendo à exigência chinesa que entende se tratar de textos religiosos ilegais.

Há também uma certa assimetria, pois as empresas chinesas não encontrariam os mesmos obstáculos para operarem nos EUA, com base em valores de abertura econômica e de internet livre,, contudo, desde o fortalecimento da guerra tecnológica EUA-China, há uma mudança de postura por parte do governo dos EUA, tentando trazer certos limites às práticas que poderiam caracterizar como vigilância estatal chinesa e ameaça à segurança nacional, com comprometimento da soberania estatal e digital americana, fortalecendo a supervisão das empresas de tecnologia chinesas, a exemplo dos aplicativos TikTok e do WeChat já que provavelmente o governo chinês teria acesso aos dados pessoais de todos os usuários, além de poder direcionar a propaganda para ser amigável aos ditames do Partido Comunista, e censurar o que entender que lhe seja ameaçador. No caso do Tiktok, mesmo com sua gestão baseada nos EUA, e dados de usuários americanos armazenados nos EUA e em Singapura, não se tem certeza de que os mesmos não são fiscalizados e acessados pelo governo chinês, sendo ambas as empresas objeto de ordem executivas pelo Presidente Trump visando seu banimento do país em razão da ameaça à segurança nacional.

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

Trata-se, pois, de uma nova ordem tecnológica, com retaliações de ambos os lados, com destaque para as iniciativas do governo Trump em limitar a atuação da Huawei nos EUA e proibição dos aplicativos chineses, e por parte da China, por meio do Ministério do Comércio da China (MOFCOM) com a criação da Lista de Entidades Não Confiáveis (UEL) de 2020, com foco em empresas estrangeiras consideradas como perigosas à soberania nacional, segurança ou interesses de desenvolvimento da China, ou que violassem os princípios normais de transação no mercado, causando danos graves aos direitos e interesses legítimos do país.

Contraditoriamente, apesar da China ser conhecida por desenvolver aplicações de IA para fins de vigilância e controle da sociedade, visando minimizar as ameaças ao regime, ela traz iniciativas legislativas que visam impedir a espionagem cibernética, com vistas a soberania digital, com destaque para a Lei de Segurança de Dados (DSL) de 2021, associando as temáticas de segurança dos dados e segurança nacional, aumentando o controle governamental sobre dados das empresas privadas e limitando o acesso de dados para o exterior, reforçando as diretrizes da Lei de Cibersegurança de 2016 que exige que as empresas armazenem informações pessoais e dados comerciais importantes na China. No mesmo sentido de contra-medidas chinesas destacam-se as Regras sobre a Contraposição à Aplicação Extraterritorial Injustificada de Legislação Estrangeira e Outras Medidas, conhecidas como “Regras de Bloqueio” de 2021 visando impedir que empresas fora dos EUA sigam quaisquer sanções com fulcro na lei americana, forçando as empresas a ter que optar entre observar tais regras ou as regras chinesas, e a Lei Anti-Sanções Estrangeiras (AFSL) de 2021 autorizando o uso de contra-medidas contra indivíduos e entidades que auxiliam na criação ou implementação de sanções contra a China.

2 VIGILÂNCIA EM MASSA

Verifica-se, pois, um aumento global de atividades de vigilância com a utilização de IA, ao mesmo tempo que há uma redução de países democráticos, como apontam as pesquisas da Freedom House, em especial o relatório “Freedom on the Net”de 2021, com a redução da liberdade na internet e ao mesmo tempo o crescimento da utilização de spyware, permitindo a vigilância sem quaisquer limites ou regulações.

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

O aumento da vigilância se dá geralmente sob argumentos de um lado em prol da segurança nacional e soberania digital e de outro como medida em prol de redução das taxas de criminalidade, em especial com a utilização do reconhecimento facial e policiamento preditivo, mas geralmente sem se considerar o necessário balanceamento entre direitos fundamentais em rota de colisão e sem considerar que ante a falta de transparência não se tem acesso as reais taxas de eficácia da medida, além da possibilidade de sua utilização para controle populacional e perseguição de minorias dissidentes politicas ou religiosas, a exemplo do que ocorre com a China, e de pesquisas que apontam a perseguição de jornalistas e de defensores de direitos humanos.

Deve haver, pois, uma responsabilização da empresa que vende a tecnologia e não apenas para quem a utiliza, assim como ocorre com a responsabilidade solidária em termos do Código de Defesa do Consumidor, não sendo suficiente, diante do potencial de dano da tecnologia considerada como de alto risco pelo AI Act e em diversos documentos internacionais, que apenas a responsabilidade pelo mau uso recaia no usuário, como relata a empresa chinesa de reconhecimento facial CloudWalk, apontando que não é responsável e sim o governo zimbabuense, que decide como a tecnologia é implantada, além de ir contra os princípios do “privacy by design”, em especial a proatividade.

A China é o país que mais exporta tal tecnologia, segundo aponta a Carnegie Endowment for International Peace, em relatório de 2019, destacando-se, outrossim, a tecnologia de vigilância de spyware denominada “Pegasus” produzido pela empresa israelense NSO Group, havendo ações de responsabilidade nos EUA já que há indícios de que a empresa forneceu tal sistema para governos estrangeiros com o fim de perseguição de ativistas políticos, líderes empresariais e jornalistas. O malware Pegasus permitiria o amplo acesso a smartphones sem depender de qualquer ato prévio pelo usuário, tal como demonstrou estudo da organização Citizen Lab, falando da utilização de tal tecnologia em 45 países, inclusive no Brasil. O estudo aponta para a utilização de outras ferramentas similares, como o dispositivo Universal Forensic Extraction Device (UFED), permitindo o monitoramento comunicacional e informacional no Brasil, Honduras, El Salvador e na Argentina.

Revista Jurídica unicuritiba
Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

Um caso relevante mapeado pela pesquisa do instituto Igarape[2] é o sistema de monitoramento inteligente denominado “Detecta”, desenvolvido pela Microsoft e implementado pelo governo do estado de São Paulo. O Detecta realiza o monitoramento utilizando-se de câmeras, sendo responsável pelo maior banco de dados de informações policiais da América Latina. A pesquisa aponta para o aumento do uso de ferramentas de vigilância pelos governos, para fins de monitoramento de opositores, ativistas, jornalistas, e dissidentes políticos, como no caso da utilização de spyware, por meio do envio de um malware para a vítima, sendo um exemplo de práticas denominadas de hacking governamental, sendo citado ainda o caso de exploração de vulnerabilidades por governos e flexibilização da criptografia, a denominada estocagem ou compra de vulnerabilidades críticas, também chamadas de “zero-days” ou “0-days”.

A vigilância é uma dimensão-chave do mundo moderno, e está atualmente intimamente relacionada com o big data (Projeto “The Big Data Surveillance” Centro de Estudos de Vigilância do Canadá[3], a exemplo de aplicações de IA como reconhecimento facial, policiamento preditivo, em termos de uma vigilância que agora se caracteriza em massa, sob o slogan “coletar tudo”, a partir da análise e acesso a um enorme volume de dados pessoais.

A principal característica da atual inteligência de segurança é a extensa colaboração com empresas de tecnologia, as quais armazenam, tratam e utilizam nossas pegadas digitais, recorrendo ao big data, ampliando-se o leque anterior que focava mais na colaboração com empresas de telecomunicações, a exemplo da AT&T ajudando os EUA na vigilância, objeto de processo judicial movido pela Electronic Frontier Foundation (EFF), um grupo de defesa da privacidade e da liberdade de expressão. O caso judicial, contudo, foi arquivado com base na aprovação pelo Congresso da controvertida Lei de Vigilância da Inteligência Estrangeira (FISA) de 1978, concedendo imunidade retroativa à AT&T e permitindo a partir de 2008, com base em posteriores alterações, que o Procurador-Geral pleiteie o arquivamento do caso, se o governo certificar secretamente ao tribunal que a vigilância não ocorreu, foi legal ou foi autorizada pelo presidente, quer seja legal ou ilegal. Com base em uma imunidade retroativa, para casos envolvendo responsabilidade penal, anulou-se a possibilidade de criminalização com base na lei que proibia as escutas sem mandado,

[2] Implementacao-de-tecnologias-de-vigilancia-no-brasil-e-na-america-latina.pdf.
[3] https://www.surveillance-studies.ca

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

sendo a lei substituída pela ordem presidencial, seja ela legal ou ilegal, ferindo-se os alicerces da separação de poderes, e do Estado de Direito.

Tal imunidade torna-se a regra, sendo utilizada cada vez com maior frequência pelos governos para viabilizar suas atividades de vigilância em massa. A imunidade retroativa revela a origem ilegal da vigilância em massa, atuando em uma zona de anti-direito, borrando os limites entre a vigilância legal e ilegal, já que tais práticas situam-se em uma espécie de "zona cinzenta".

Um dos exemplos do crescimento das tecnologias de vigilância e da hegemonização de tal modelo de negócio com base no big data é o crescimento na oferta de serviços e softwares informacionais às instituições públicas de ensino de forma "gratuita" pelas maiores empresas de tecnologia de dados do mundo – conhecidas pelo acrônimo GAFAM (Google, Apple, Facebook, Amazon, Microsoft), tendo como contrapartida, todo o acesso aos dados pessoais de milhares de usuários, afetando o que se pode entender por soberania do Estado, já que as Big Techs estão quase todas nos EUA e em maioria crescente na China, em um relação obscura, sem fornecimento de dados para se verificar os detalhes de tal operação, já que não há dados oficialmente divulgados pelas empresas nem pelas instituições.

Os acordos entre empresas e universidades brasileiras, em especial quanto ao Google Suite for Education e Microsoft Office 365 for Schools & Students, são reveladores de como tais relações são opacas, verdadeiras caixas pretas, faltando com o requisito fundamental para se falar em uma IA de confiança, qual seja, a transparência, em especial para aqueles que estão tendo seus dados pessoais utilizados.[4]

Neste sentido, David Lyon, no curso realizado como iniciativa do CEADIN – Centro Avançado de Estudos, em Inovação e Direito da Universidade de São Paulo, Faculdade de Direito, campus Ribeirão Preto, aponta que na origem, na década de 90 a vigilância era definida como a atenção sistemática e rotineira a pormenores pessoais com a intenção de influenciar, gerir, proteger ou orientar indivíduos, envolvendo, pois, uma observação direcionada, sistemática e rotineira, com diversos fins, entre eles, influência nos meios de comunicação social, as relações laborais e o comportamento

[4] "Spying on Students: School-Issued Devices and Student Privacy", https://www.eff.org/de/node/95598.

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

organizacional. Embora geralmente associada a entidades como a polícia, agências de segurança, controles fronteiriços e similares, a vigilância também pode exercer influência nas escolhas de vida, nas decisões de compra ou no trabalho, tendo seu conceito sido, posteriormente, alargado para incluir tanto a operação como a experiência da vigilância, envolvendo recolha, análise e utilização de dados pessoais para moldar escolhas ou gerir grupos e populações.

Na época moderna, ou pós-moderna, a vigilância do século XXI, caracteriza-se, por sua vez, pela sua natureza omnipresente, envolvendo uma "cultura da vigilância", uma nova dimensão da vigilância, que agora conta com nossa participação voluntária, como exercendo um fator fundamental, e tendo por principal ingrediente os dados pessoais. Os smartphones, por exemplo, tornaram-se os dispositivos de vigilância predominantes devido à sua adoção generalizada, sendo sua capacidade de análise de dados usada pelas grandes empresas, entidades públicas e privadas e organismos governamentais para monitorizar indivíduos, muitas vezes mesmo sem quaisquer indícios de serem suspeitos.

Entre as diversas obras de David Lyon destaca-se "Vigilância Líquida" escrita em co-autoria com Zygmunt Bauman (LYON, BAUMAN, 2014), sendo fruto de sucessivas trocas de mensagens, diálogos e atividades realizadas de forma conjunta, como as participações na conferência bianual de 2008 da Rede de Estudos sobre Vigilância. Os A. apontam para a nova fase da vigilância líquida, móvel e flexível, infiltrando-se e espalhando-se por diversas áreas das nossas vidas, sendo um aspecto cada vez mais presente, assumindo características sempre em mutação, diferenciando-se da antiga forma de panóptico estudada por Foucault e por Deleuze.

Segundo Foucault, ao estudar as sociedades disciplinares, da regulamentação e normalização o panóptico é um dos principais instrumentos do poder disciplinar, um mecanismo de vigilância, que possibilita ver e nunca ser visto, produzindo o efeito de um estado de visibilidade constante. A arquitetura é pensada para que a luz passe. Tudo deve ser iluminado, tudo deve poder ser visto! Na sociedade da transparência, nada deve ficar de fora.

Por sua vez, para Deleuze, as sociedades de controle, tal como dispõe em seu "Post-Scriptum sobre as Sociedades de Controle" caracterizam-se por máquinas de informática e computadores, como uma mutação do capitalismo. Nas sociedades de controle o essencial não é mais uma assinatura e nem um número, mas uma cifra:

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

a cifra é uma senha. Os indivíduos tornaram-se “dividuais”, divisíveis, e as massas tornaram-se amostras, dados, mercados ou “bancos”.

A característica do panóptico digital, no entender de Byung-Chul Han ao falar da “sociedade da transparência” é permitir o alcance globalizado dos ventos digitais transforma o mundo em um único panóptico: “não existe um fora do panóptico; ele se torna total, não existindo muralha que possa separar o interior do exterior”. Gigantes da rede como Google e Facebook, apresentam-se como espaços de liberdade, porém, também podem ser instrumentos da adoção de formas panópticas, a exemplo das revelações feitas por Edward Snowden, em 2013, sobre o projeto PRISM, cujo programa permitia à Agência Nacional de Segurança dos Estados Unidos (NSA) obter praticamente o que quisesse das empresas de internet. Ocorre como traço fundamental do panóptico digital o protocolamento total da vida, substituindo-se a confiança pelo controle, seguindo-se uma lógica da eficiência. A possibilidade de um protocolamento total da vida substitui a confiança inteiramente pelo controle. No lugar do Big Brother, entra o big data. Vive-se a ilusão da liberdade (autoexposição e autoexploração). Aqui todos observam e vigiam a todos. O mercado de vigilância no Estado democrático tem uma proximidade perigosa do Estado de vigilância digital. No lugar do biopoder surge o psicopoder, pois há condições de intervir nos processos psicológicos. É mais eficiente do que o biopoder pois vigia, controla e influencia o ser humano não de fora, mas a partir de dentro. Era da psicopolítica digital.

Os grandes volumes de dados são, pois, um fator de mudança decisivo. Do onipresente código de barras permitindo a identificação de produtos segundo o tipo ou a fábrica, evoluímos para os chips de identificação por radiofrequência (RFID - Radio Frequency Identification), compreendendo em identificadores individuais para cada produto, e para os códigos de resposta rápida (QR, de Quick Response Code), conjuntos de símbolos colocados em produtos e que são escaneados por smartphones, e braceletes de silício com um QR permitindo a leitura de dados de contato e links de mídia social como um verdadeiro hyperlink humano.

Acerca do novo sistema de vigilância em massa Snowden no seu livro “Eterna vigilância”, afirma que passamos de uma vigilância direcionada a indivíduos à vigilância em massa de populações inteiras, com destaque para os bilhetes de identidade nacionais como um dos fatores centrais, conjugando-se tecnologia de alta precisão com biometria incorporada e chips RFID, com argumentos em torno de melhor exatidão, eficiência e rapidez, controle de imigração, medidas anti-terrorismo,

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

governo eletrônico, contudo, apesar de tais pretensos benefícios há diversos perigos em potencial, com destaque para fracasso dos sistemas, custos financeiros imprevistos, ameaças acrescidas à segurança e uma imposição inaceitável aos cidadãos, sendo essencial uma avaliação independente e contínua dos riscos e uma revisão regular das práticas de gestão (LYON, David, BENNETT, Colin J. 2008). Fala-se na existência de um verdadeiro 'Cartel de Cartões' envolvendo o Estado, empresas e normas técnicas, gerando grandes controvérsias em alguns países tais como Austrália, Reino Unido, Japão e França.

3 SOU VISTO, LOGO EXISTO

Sou visto, logo existo. A frase reflete o desejo de ser visto em redes sociais, o que leva ao compartilhamento de dados pessoais de forma voluntária e até entusiástica, empregados pelo mercado para a personalização de anúncios com alto potencial de manipulação da escolha (pela sedução, não pela coerção) e, pois, à comoditização de nossas vidas e personas. Ao mesmo tempo haveria uma vigilância do consumidor, em um sentido positivo, voltada ao mercado de consumo, e em sentido negativo, acerca dos que não se conformam às expectativas, como aponta Oscar Gandy ao mencionar como a “discriminação racional” realizada por grandes empresas tem efeitos negativos, criando uma espiral negativa, onde os pobres se tornam mais pobres e aumenta-se a concentração de riquezas (LYON, David, 2005).

Relacionando-se à vigilância na área do big data destacam-se a questão das inferências e o perfilamento, por meio de enorme quantidade de dados pessoais, o que é potencializado pelo papel questionável dos data brokers que vendem os dados pessoais, em atividades antiéticas e ilegais, já que não há um necessário consentimento real (informado, fragmentado, e mediante um novo consentimento a cada nova finalidade e mudança de empresa que está se beneficiando de tais dados), sendo tais dados utilizados em análise via aprendizado profundo, por meio de otimização quantitativa a fim de potencializar a manipulação comportamental e emocional, ou seja, são feitos anúncios personalizados a fim de maximizar a probabilidade de uma compra ou do tempo em uma rede social, sendo um fato fundamental na criação de desejos até então inexistentes.

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

Como aponta Morozov (MOROZOV, Evgeny Morozov, 2018, p. 33 e ss.) em 2012 o Facebook celebrou acordo com a empresa Datalogix permitindo associar o que compramos no mercado aos anúncios que são disponibilizados no Facebook, da mesma forma, o Google possui o aplicativo Google Fiel permitindo a análise de lojas e restaurantes vizinhos ao usuário para indicação de ofertas.

Por sua vez diversos casos interessantes são citados por Kai-Fu Lee no seu livro "2041: Como a inteligência artificial vai mudar sua vida nas próximas décadas" (LEE, Kai-Fu, 2022), e embora seja um livro com histórias ficcionais, o mesmo traz informações, exemplos e cenários que já ocorrem na realidade, a exemplo da existência de fintechs (empresas de tecnologia financeira) com base em IA, como a Lemonade, nos Estados Unidos e a Waterdrop, na China, com o fim de venda de seguros por aplicativo ou a contratação de empréstimos por aplicativo, com aprovação instantânea.

No capítulo genocídio quântico Kai-Fu Lee afirma que a tecnologia é inerentemente neutra, na linha do que Jose van Dijck chama de "dataísmo", correspondendo à crença na "objetividade da quantificação", e na linha do que se denomina de "solucionismo", imaginando que a solução de todos os problemas sociais estão nas mãos dos dados, e na análise dos resultados, e não das causas, e que as "tecnologias disruptivas podem se tornar nosso fogo de Prometeu, ou caixa de Pandora, dependendo de como são usadas," considerando como o maior perigo advindo da IA as armas autônomas comandadas por IA. Na parte fictícia do livro é citado por sua vez o exemplo do seguro Ganhesha com a função objetiva do algoritmo de reduzir ao máximo o valor do seguro, e a cada comportamento dos segurados, por conseguinte, o valor do seguro aumenta ou reduz, além de estar vinculado a uma série de aplicativos, compartilhando dados dos usuários, englobando e-commerce, recomendações e cupons, investimentos, ShareChat (uma rede social popular indiana) e o fictício FateLeaf, um aplicativo de vidência. Uma das possíveis alternativas mencionadas pelo A. para balancear tal função objetiva voltada à maximização do lucro empresarial, seria a de ensinar a IA a ter funções objetivas complexas, como baixar o preço do seguro e manter a justiça, embora entenda ser possível tal exigência apenas via regulação, pois esbarraria no interesse comercial para atuar de forma voluntária, além de mencionar o importante papel da responsabilidade corporativa, a exemplo da ESG - governança ambiental, social e corporativa.

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

No livro “Big Data Surveillance and Security Intelligence - the Canadian case”, de David Lyon e David Murakami Wood (LYON, David, MURUKAMI, D. 2020) é enfatizada a mudança da prática da vigilância com a utilização do “big data” e de novos métodos de análise de dados para se verificar possíveis riscos à segurança nacional, destacando-se a parceria “Cinco Olhos” envolvendo Austrália, Canadá, Nova Zelândia, Reino Unido e Estados Unidos, com a interligação entre “inteligência de segurança” e “vigilância”, incluindo atualmente o monitoramento da internet e, especialmente, das redes sociais, vinculados, pois, a análise de dados pessoais. Expande-se a noção de segurança para abranger uma série de novos domínios, permitindo-se a utilização de tortura e interrogatório como meios extraordinários, a exemplo do que aconteceu com o canadense Maher Arar após o evento de 11 de setembro de 2001, considerado como suspeito.

A ligação de atividades em prol da segurança nacional com o big data e a vigilância agora em termos de “vigilância em massa” são corroboradas pelas denúncias de agentes de segurança americanos como William Binney, Thomas Drake, Mark Klein e Edward Snowden, inclusive com a utilização de metadados a partir do estudo de mais de 500 documentos divulgados por Snowden que mostram como os metadados podem ser utilizados para construir perfis detalhados da vida das pessoas vigiadas (LYON, David, MURUKAMI, D. 2020).

4 HACKING GOVERNAMENTAL

Duas aplicações específicas de IA relacionam-se intimamente com a temática da vigilância, o reconhecimento facial e o policiamento preditivo, havendo diversas críticas por parte da doutrina e relatórios de institutos especializados, em razão do grande número de vieses, ou seja, falsos positivos, envolvendo mulheres, negros, asiáticos, nativos americanos, índios americanos, índios do Alasca e ilhéus do Pacífico, como aponta o Relatório “Interagency Report 8280” do National Institute of Standards and Technology (NIST, 2019). Segundo o Relatório a tecnologia de reconhecimento facial no caso de 189 algoritmos apresentou viés racial em relação

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

às mulheres de cor, além de não conseguirem, de modo geral, identificar corretamente uma pessoa que usava máscara quase 50% do tempo[5].

Entre as principais críticas ao reconhecimento facial podem ser apontadas, de forma geral, a ausência ou escassez de acesso à informação sobre os resultados e eficiência decorrente do uso da tecnologia, falta de transparência sobre a aquisição e implementação dos sistemas, bem como sobre seus protocolos de uso e métodos de coleta dos dados.

Um dos pontos centrais envolvendo tal tecnologia é a questão do risco de vazamento de dados biométricos, altamente sensíveis, e que não são possíveis de serem alterados após um acesso não autorizado, ao contrário de senhas, PINs ou endereços de e-mail, agravando as consequências de um potencial vazamento.

Já há alguns exemplos noticiados de vulnerabilidade e acesso não autorizado de dados biométricos, como no caso de pesquisa de 2019 apontando para a vulnerabilidade em um sistema de segurança biométrico denominado Biostar 2, gerido pela Suprema, empresa sul-coreana, permitindo o acesso não autorizado de informações e dados de 1 milhão de pessoas[6]. No mesmo sentido pesquisadores holandeses de segurança cibernética em relatório de 2019 apontaram falhas em sistema permitindo o acesso a base de dados de reconhecimento facial da empresa chinesa SenseNets, responsável pela criação de sistemas de software de segurança baseados em IA para reconhecimento facial, análise de multidões e verificações, afetando 2,5 milhões de pessoas.[7]

Em 18 de janeiro de 2020, o jornal The New York Times publicou matéria da jornalista Kashmir Hill, sobre um aplicativo de reconhecimento facial criado pela empresa *Clearview AI*, utilizando-se de um banco de dados de cerca de 3 bilhões de fotos públicas capturadas ao redor da internet e das redes sociais, sendo utilizada por diversos policias em 2019, apesar da afronta à diversos direitos fundamentais. O aplicativo retornava ao policial informações e dados obtidos sobre determinada pessoa. Além das falhas de tal tecnologia, outra questão problemática é permitir o acesso pela *Clearview AI* a todo o conteúdo das buscas e achados da polícia (e de empresas de segurança que contratem seus serviços). Agrava-se tal situação o fato

[5] fonte: https://learn.g2.com/ethics-of-facial-recognition.
[6] https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms
[7] https://www.forbes.com/sites/kateoflahertyuk/2019/02/18/china-facial-recognition-database-leak-sparks-fears-over-mass-data-collection/#788f83aafb40.

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

de a empresa Clearview perder toda a lista de clientes e fotos, devido a um ataque de hackers como anunciado em 26.02.2020 (URIA, Daniel, 2020).

Diversos casos judiciais pelo uso abusivo do reconhecimento facial foram ajuizados nos EUA com destaque para o caso Parks x. McCormac, de 29.01.2024, envolvendo a prisão injusta de Parks, homem negro, a partir da utilização de tal tecnologia pela polícia de Woodbridge; a polícia enviou uma imagem desfocada e sombreada da fotografia da carta de condução do suspeito de crime de furto a um investigador, que utilizando-se de sistema de reconhecimento facial informou aos agentes da polícia de que Nijeer Parks era um "possível alvo", sem fundamentação em quaisquer outros documentos ou provas, dando ensejo à prisão do mesmo. De acordo com a pesquisa a maioria dos casos de falsos positivos envolveram a detenção de uma pessoa negra[8].

Outro caso semelhante é o de Williams v. City of Detroit, também envolvendo a prisão de um homem negro inocente, objeto de acordo judicial alcançando diversos departamentos de polícia, restringindo o uso da tecnologia de reconhecimento facial, determinando que a polícia estaria obrigada a comprovar os resultados obtidos com a tecnologia com provas independentes e fiáveis antes de efetuar qualquer detenção. Os polícias também terão de receber formação sobre a tecnologia em especial acerca do potencial de "bias", além de ser determinada a realização de auditoria de todos os casos desde 2017 em que houve tal utilização.

No mesmo sentido o caso ACLU v. Clearview AI, alegando-se violação dos direitos de privacidade dos residentes de Illinois e, pois, afronta à Lei de Privacidade de Informações Biométricas de Illinois (BIPA), com acordo celebrado entre as partes, restringindo as práticas da Clearview em todos os Estados Unidos, proibindo a mesma de disponibilizar a sua base de dados de impressões faciais à maioria das empresas e outras entidades privadas, e de vender o acesso à sua base de dados a qualquer entidade no Illinois, incluindo a polícia estatal e local, durante cinco anos.

Destaca-se, outrossim, ação judicial coletiva envolvendo o uso de reconhecimento facial pelo Facebook como parte da sua funcionalidade "Tag Suggestions", ajuizada em prol dos usuários em Illinois. A ferramenta utilizada na

[8] https://www.aclu.org/cases/parks-v-mccormac; In re Facebook Biometric Information Privacy Litigation (15-cv-03747-JD) (N.D. Cal.)

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

marcação de fotografias teria violado a Lei da Privacidade da Informação Biométrica de Illinois[9] , já que não houve ciência nem consentimento dos usuários.

Várias cidades, incluindo São Francisco, Berkeley e Oakland, na Califórnia, e Springfield e Cambridge, em Massachusetts adotaram legislação que proíbe o uso do reconhecimento facial pelo governo, e o estado da Califórnia bloqueou a utilização da tecnologia nas câmeras corporais utilizadas pela polícia.[10]

Tais ferramentas de IA utilizadas no sentido de vigilância a partir do big data possuem, pois, um potencial de "bias", no sentido de uma retroalimentação, um "feedback loop" de preconceitos e dados tendenciosos, a exemplo do que ocorreria também na vigilância contra o terrorismo, por conter preconceitos estruturais, repassados para banco de dados e reproduzidos via algoritmos, que reproduzem o viés dos bancos de dados (LYON, David, MURAKAMI, David, 2020).

Outras problemáticas relacionam-se a ausência de mecanismos de prestação de contas aos cidadãos sobre os seus direitos e de medidas preventivas e mitigadoras de danos e de segurança da informação, além da ausência de avaliações sobre a proporcionalidade dos impactos negativos em face das externalidades positivas, geralmente associadas à maior efetividade, a qual, contudo, é questionável como aponta relatório da LAPIN de 2021, afirmando que há falta de transparência diante da ausência de dados estatísticos sistematizados, consolidados ou publicizados sobre o tratamento de dados realizado por meio de tecnologias de reconhecimento facial pela Administração Pública, não havendo provas, pois de que tais tecnologias ensejariam maior eficiência das atividades do setor público, ou seja, de acordo com os dados divulgados, "a narrativa da eficiência da tecnologia parece não se confirmar estatisticamente".[11]

A título de exemplo, no carnaval de Salvador de 2020, das 11,7 milhões de pessoas entre adultos e crianças que estiveram presentes, o uso das mais de 80 câmeras com tal tecnologia deram ensejo à detecção de 42 foragidos. No Rio de Janeiro, houve com tal utilização o cumprimento de 63 mandados de prisão durante a Copa América de 2019, computando-se dois casos de falsos positivos. Verifica-se,

[9] https://edelson.com/Facebook-Settlement
[10] https://www.aclu.org/press-releases/aclu-sues-clearview-ai

[11] "Relatório sobre o uso de tecnologias de reconhecimento facial e câmaras de vigilância pela Administração Pública no Brasil" - https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/.

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

pois que há uma possível desproporcionalidade, se observarmos o número de captura de 42 foragidos, e o acesso a dados pessoais biométricos de 11,7 milhões de pessoas, ou seja, parece que o benefício não seria proporcional ao potencial de danos a direitos fundamentais de milhões de pessoas que sem serem suspeitas foram submetidas à vigilância massiva do Estado.

O instituto Igarapé em recente relatório denominado "Implementação de Tecnologias de Vigilância no Brasil e na América Latina"[12] aponta que o uso de tal tecnologia deve ser precedido de autorização legislativa específica, e que em diversos casos de sua utilização não há previsão de suporte técnico por parte das empresas fornecedoras após o período de testes, além do desconhecimento pelos agentes públicos acerca dos modos de uso do equipamento, bem como seus riscos e formas de mitigação, ocorrendo a má gestão de tecnologia, impossibilidade de se verificar sua acurácia e efetividade, dificultando o escrutínio público. Tampouco há informações de exclusão dos dados após o fim do contrato, forma de descarte e sobre a elaboração prévia do Relatório de Impacto à Proteção de Dados e da avaliação de impacto algorítmico.

No mesmo sentido a pesquisa da Lapin afirma que em nenhum dos casos analisados foi identificada a elaboração de qualquer avaliação de impacto pela Administração Pública de modo a avaliar os riscos à proteção de dados e a outros direitos fundamentais, com exceção apenas do Serviço Federal de Processamento de Dados (SERPRO), no contexto do serviço DataValid.

Há ainda atos normativos do Poder Executivo que dificultam a coleta de informações acerca da tecnologia de reconhecimento facial, a exemplo da Portaria CGAI n. 1 de 2016, da Controladoria e Ouvidoria-Geral do Estado do Ceará, classificando como sigilosos os documentos e informações sobre o uso de equipamentos de vigilância pela Administração Pública estadual[13].

A fim de se reduzir a mitologia acerca da neutralidade e objetividade dos algoritmos e de suas predições, cumpre salientar que os dados são apenas uma amostra, e que nunca falam por si próprios, sendo certo que as correlações podem ser aleatórias, podendo gerar informações equivocadas à medida que há uma

[12] https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regulação-do-reconhecimento-facial-no-setor-público.pdf

[13] https://www.cgd.ce.gov.br/wp-content/ uploads/sites/33/migracao/2899.pdf.

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

carência de conhecimentos contextuais e específicos do domínio, sendo fundamental que as equipe técnicas, geralmente da área das exatas (computação, matemática e engenharia) sejam ampliadas para conter pessoal qualificado e com expertise nas áreas do direito, da filosofia (ética), e da sociologia, em uma análise interdisciplinar e holística.

Em São Paulo há uma série de iniciativas no tocante à implantação de até 40.000 câmeras equipadas com reconhecimento facial na linha do projeto Smart Sampa[14], visando a implementação de uma plataforma única de videovigilância abrangendo serviços de emergência e de trânsito e as forças policiais, não obstante sua suspensão por ações judiciais, apontando-se para o risco de afronta a LGPD e riscos concretos de reprodução do racismo estrutural, já que segundo pesquisa da Rede de Observatórios da Segurança 90% das prisões feitas no Brasil por meio dessa tecnologia foram de pessoas negras, e entre elas houve erros de identificação que levaram inocentes à prisão.[15] Posteriormente a suspensão foi cassada em sede de recurso sob argumentos totalmente equivocados, tais como de que não é possível o Judiciário interferir em decisões da administração pública, sendo possível somente em caso de "flagrante ilegalidade", entendendo que a LGPD não se aplicaria ao caso, e que não haveria comprovação de falsos positivos, ignorando que os princípios da LGPD são aplicáveis e que inúmeros relatórios nacionais e internacionais apontam para falhas graves do sistema e para o viés racial (Processo: 1027876-45.2023.8.26.0053), a exemplo dos estudos do Big Brother Watch, afirmando que 98% das correspondências obtidas por câmeras que alertam a polícia do Reino Unido identificaram incorretamente inocentes como se fossem foragidos. [16]

5 CONSIDERAÇÕES FINAIS

O presente artigo buscou, pois, trazer reflexões críticas, acerca da questão da vigilância relacionada ao big data, com base em autores como Foucault e seus estudos de sociedade da normalização, disciplina e regulamentação, sua evolução

[14]https://www.prefeitura.sp.gov.br/cidade/secretarias/seguranca_urbana/noticias/index.php?p=365363
[15] https://cesecseguranca.com.br/artigo/levantamento-revela-que-905-dos-presos-por-monitoramento-facial-no-brasil-sao-negros/.
[16] https://bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Biometric-Britain.pdf).

nas obras de Deleuze e de Byung-Chun Han, com a perspectiva da sociedade de controle e do panóptico digital, e David Lyon, conjugando-se tal temática à questão do fim da era da autorregulação quanto à IA, a batalha pela supremacia tecnológica e os desafios envolvendo os três principais modelos de países, quais sejam, EUA, China e EU, o fim da internet globalizada, o surgimento de uma verdadeira balkanização da internet e da economia digital e o fim da era da autorregulação.

Buscou-se, sobretudo, desafiar certos mitos e dogmas com relação à temática da IA, como o da existência de um necessário trade-off entre regulação da tecnologia e a inovação, enfatizando a importância de se evitar abordagens utópicas e também distópicas, apontando para o necessário equilíbrio entre de um lado a busca da inovação, não como um direito absoluto, mas de forma a ser compatibilizada com uma proteção adequada e sistêmica de direitos potencialmente afetados pela tecnologia.

REFERÊNCIAS

BRADFORD, Anu. "***Digital Empires:*** The Global Battle to Regulate Technology", Oxford University Press, 2023.

BAUMAN, Zygmunt, LYON, David. "**Vigilância líquida**", Zahar; 1ª edição, 2014.

CHRISAFIS, Angelique. "***France Considers Extend- ing National State of Emergency***," *Guardian,* 22 January 2016, https://www.theguardian. com/world/2016/jan/22/france-considers-extending-national-state-of-emergency.

CRARY, Jonathan. "24/7 – **Capitalismo tardio e os fins do sono**". São Paulo: Contraponto, 2014.

DEARDEN, Lizzie. "**Paris Attacks:** France's State of Emergency Is Imposing 'Excessive' Restrictions on Human Rights, UN Says," *Independent,* 20 January 2016, http://www. independent.co.uk/news/world/europe/paris-attacks-frances-state-of-emergency-is-imposing-excessive-restrictions-on-human-rights-un-says-a6822286.html.

DERECHOS DIGITALES. https://ia.derechosdigitales.org.

ENGELMANN, Lukas. #**COVID19:** The Spectacle of Real-Time Surveillance. Somatosphere, 2020, http://somatosphere.net/forumpost/covid19-spectacle-surveillance/.

ESCOBAR, Arturo. "***Más allá del Tercer Mundo. Globalización y diferencia***". Bogotá: Instituto Colombiano de Antropología e Historia — Universidad del Cauca, 2005.

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

EVANGELISTA, Rafael. "Review of Zuboff's **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power".** Surveillance & Society 17(1/2): 246- 251, 2018, http://library.queensu.ca/ojs/index.php/surveillance-and-society/index|
FOUCAULT, Michel. Aula de 15 de janeiro, 1975. **Os Anormais**. Curso no Collège de France, 1974-1975. Martins Fontes, 2002.

HILL, Kashmir. "***The Secret Company that Might End Privacy as We Know it"***. The New York Times, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

IGARAPE. https://igarape.org.br/wp-content/uploads/2022/12/Implementacao-de-tecnologias-de-vigilancia-no-brasil-e-na-america-latina.pdf

INTERNETLAB. https://internetlab.org.br/pt/projetos/relatorio-anual-de-vigilancia-sobre-as-comunicacoes-no-brasil/

INTERNETLAB.https://internetlab.org.br/wp-content/uploads/2023/06/Educacao-na-mira-PT_06.pdf

LAPIN.https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/

LAVITS.https://lavits.org/lavits_covid19_14-vigilancia-digital-hiperconexao-e-pandemia/

LAVITS. https://educacaovigiada.org.br/pt/sobre.html

LAVITS. https://lavits.org/pesquisa/territorialidades-da-vigilancia/

LEE, Kai-Fu. "2041: **Como a inteligência artificial vai mudar sua vida nas próximas décadas**", Globo Livros; 1ª edição, 2022.

LYON, David , BENNETT, Colin. J. ***"Playing the Identity Card:*** Surveillance, security and identification in global perspective", Edited By Colin Bennett, 2008.

LAVITS. MURUKAMI, David. "***Big Data Surveillance and Security Intelligence*** - the Canadian case", Wood, UBC Press, 2020.

LAVITS. "**The border is everywhere:** ID cards, surveillance and the other", in E. Zureik e M.B. Salter (orgs.), Global Surveillance and Policing, Cullompton, Willan, 2005.

MACASKILL, Ewen. ***"How French Intelligence Agencies Failed before the Paris Attacks,"*** *Guardian,* 15 November 2015, https://www.theguardian. com/world/2015/nov/19/how-french-intelligence-agencies-failed-before-the-paris - attacks.

MOROZOV, Evgeny. **"Big Tech_ a ascensão dos dados e a morte da política**", Ubu, 2018.

Submetido em: 18/02/2023
Aprovado em: 10/06/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-753X

NOBLE, Safiya Umoja. "***Algorithms of Oppression:*** How Search Engines Reinforce Racism", NYU Press, 2018.
SEGADA, Jean. **Covid-19:** scales of pandemics and scales of anthropology. Somatosphere, 2020. http://somatosphere.net/2020/covid-19-scales-of-pandemics-and-scales-of-anthropology.html/.

TSING, A.. **Friction:** An Ethnography of Global Connection. Princeton University Press, 2011. Friction | Princeton University Press.

URIA, Daniel. "**Facial recognition firm's entire client list exposed in data breach".** U.S. News, 2020; https://www.upi.com/Top_News/US/2020/02/26/Facial-recognition-firms-entire-client-list-exposed-in-data-breach/3231582765378/

WEIZMAN, Eyal. **Surveilling the Virus.** Março, 2020. https://lareviewofbooks.org/article/quarantine-files-thinkers-self-isolation/#_ftn24

WILLSHER, Kim. "***France Approves 'Big Brother' Surveillance Powers despite UN Concern,"*** *Guardian,* 24 July 2015, https://www.theguardian.com/world/2015/jul/24/france-big-brother-surveillance-powers.