Investigação criminal e tecnologias digitais: algumas reflexões sobre o policiamento preditivo e a admissibilidade de provas digitais

Criminal investigation and digital technologies: some considerations on predictive policing and the admissibility of digital evidence

Andrey Bruno Cavalcante Vieira[1]
Universidade Federal de Alagoas - Maceió/AL, Brasil
andrey.vieira10@gmail.com
http://lattes.cnpq.br/9767688309371000
https://orcid.org/0000-0001-5146-3708

Hugo Leonardo Rodrigues Santos[2]
Universidade Federal de Alagoas - Maceió/AL, Brasil
hugo.santos@fda.ufal.br
http://lattes.cnpq.br/6520668011243642
https://orcid.org/0000-0003-0139-0525

Resumo: Este trabalho reflete sobre o uso de tecnologias preditivas como ferramenta de orientação para políticas públicas. Objetiva-se examinar como as forças de segurança estão realizando o tratamento de dados e alertar sobre os riscos da aplicação indiscriminada dessas abordagens. Além disso, intenta visualizar a cadeia de custódia como crucial para garantir a autenticidade e integridade das evidências, especialmente no contexto das provas digitais. A pesquisa tem natureza

[1] Mestre em direito público pela Universidade Federal de Alagoas (UFAL). Pós-graduado em direito penal e processo penal aplicados pela Escola Brasileira de Direito (EBRADI). Graduado em direito pela Universidade Federal de Alagoas (UFAL). Advogado.

[2] Professor da graduação e pós-graduação (mestrado) em direito da Universidade Federal de Alagoas (UFAL). Doutor e Mestre em direito pela Universidade Federal de Pernambuco (UFPE). Cocoordenador do grupo de pesquisas Biopolítica e Processo Penal.

qualitativa e caráter exploratório. Foi utilizada a técnica de análise de documentos da literatura jurídica e criminológica, pelo método hipotético-dedutivo, a fim de avaliar como novas tecnologias, especificamente a inteligência artificial, impactam a investigação criminal e o processo penal brasileiro. Verificou-se a necessidade de adaptar procedimentos jurídicos à era digital, especialmente no tocante à admissibilidade de provas digitais, através do exame de sua integridade e autenticidade. Conclui-se pela urgência da adaptação dos procedimentos de investigação criminal, dada a influência da virtualização na persecução penal, uma vez que a argumentação jurídica agora depende de ferramentas e provas digitais.

Palavras-chave: Investigação criminal; Policiamento preditivo; Provas digitais; Cadeia de custódia.

Abstract: *This article addresses the use of predictive technologies as a guidance tool for public policies. It aims to examine how security forces use data processing and warn of the risks of indiscriminate application of these approaches. Furthermore, it attempts to view the chain of custody as crucial to guaranteeing the authenticity and integrity of evidence, especially in the context of digital evidence. The research is qualitative and exploratory. The technique of analyzing documents from legal and criminological literature was used, through hypothetical-deductive method, to assess how new technologies, specifically artificial intelligence, impact on criminal investigation and the Brazilian criminal process. It is necessary to adapt legal procedures to the digital era, especially regarding the admissibility of digital evidence, by examining its integrity and authenticity. It is concluded that there is an urgency to adapt criminal investigation procedures, given the influence of virtualization on criminal prosecution, since legal arguments now depend on digital tools and evidence.*

Key-words: *Criminal investigation; Predictive policing; Digital evidence; Chain of custody.*

Introdução

Na era digital contemporânea, a vida em sociedade transcende o meio físico e adentra o ambiente eletrônico, por meio da *internet*, dos perfis em redes sociais, dos *e-mails* e dos documentos eletrônicos. A *internet* e as novas tecnologias provenientes da digitalização ampliaram as potencialidades das relações humanas vivenciadas nos últimos anos, promovendo uma nova valoração de bens jurídicos, além de proporcionar uma nova gama de direitos e objetos virtuais cuja proteção merece a consideração do direito.

A velocidade da disseminação de informações e ideias é um dos principais aspectos da sociedade atual, pautada pela digitalização. Ao mesmo tempo, o acesso ao ambiente digital passou a ser considerado um direito essencial à personalidade humana na contemporaneidade. A informação se tornou o principal ingrediente do que produzimos, fazemos, compramos e vendemos, tornando a administração do capital intelectual a tarefa econômica mais importante dos indivíduos, empresas e países.

O presente artigo analisa questões relacionadas ao uso e tratamento de dados através de inteligência artificial pela área da segurança pública, como forma – por vezes equivocada – de desenvolver parâmetros preditivos e aplicar políticas públicas balizadas por ela. Com esse objetivo, em um primeiro momento, o trabalho refletirá sobre os riscos advindos da aplicação indiscriminada de tais fontes, diante da possibilidade de discriminação algorítmica, mascarada pela irreal percepção de neutralidade da tecnologia, com a consideração dos efeitos desse fenômeno para o processo penal contemporâneo.

Em seguida, será realizada uma abordagem linguística do meio digital e de suas especificidades, trazendo caracterizações necessárias ao bom entendimento do contexto digital e do tratamento de provas dessa natureza. Por fim, será discutido o fenômeno da externalização da investigação criminal e a necessidade de redefinição dos sujeitos processuais penais, com atenção para a observância da ampla defesa e da paridade de armas digital.

A investigação é qualitativa e possui caráter experimental. A metodologia da pesquisa é hipotético-dedutiva, com a utilização da técnica de análise da literatura jurídica e criminológica a respeito da utilização,

na segurança pública, de novas tecnologias, mais especificamente da inteligência artificial, bem como sobre as dificuldades para a consideração de provas digitais no processo penal brasileiro.

1. A relevância da informação na sociedade atual

A "era da informação" denomina o período atual pós-industrial e/ou neoliberal, no qual a informação passou a exercer um papel central como novo padrão de acumulação de riquezas. Como opinou Thomas Stewart, o conhecimento agora é essencial em tudo o que produzimos e comercializamos, e gerenciar esse conhecimento se tornou crucial, uma vez que o capital intelectual, composto por conhecimento, informações, propriedade intelectual e experiência, é a matéria-prima para criar riqueza (1998, p. 11-23).

No mesmo sentido, afirmou Byung-Chul Han:

> Chamamos regime de informação a forma de dominação na qual informações e seu processamento por algoritmos e inteligência artificial determinam decisivamente processos sociais, econômicos e políticos. Em oposição ao regime disciplinar, não são corpos e energias que são explorados, mas informações e dados. Não é, então, a posse de meios de produção que é decisiva para o ganho de poder, mas o acesso a dados utilizados para vigilância, controle e prognóstico de comportamento psicopolíticos. O regime de informação está acoplado ao capitalismo da informação, que se desenvolve em capitalismo da vigilância e que degrada os seres humanos em gado, em animais de consumo e dados (2022, p. 7).

O deslocamento virtual de negócios e informações cria vínculos e responsabilidades corriqueiras disponíveis de forma instantânea e atemporal. Esse movimento quebra conceitos e estruturas estáveis, as quais foram estabelecidas historicamente, dando luz à novos arranjos sociais[3]. Para

[3] Sobre os dados digitais e sua transformação em produto, Geraldo Prado registrou: "Os dados digitais temporariamente convertem-se de mercadorias em artefatos empregados em uma disputa política que no rastro da globalização limita significativamente o poder de interferência do próprio Estado sem com isso impedir que em reação à restrição 'territorial' seja concentrada e

se ter uma ideia da popularização da informação digital e de seu acesso pela sociedade em geral, uma recente pesquisa realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE) (2020) concluiu que 93,2% das pessoas com mais de 10 anos de idade possuem telefone celular no Brasil e 79,1% dos domicílios brasileiros dispõem de acesso à internet.

A tecnologia ganhou um papel destacado, pois a forma como é utilizada e controlada se relaciona à própria qualidade da democracia participativa, em Estados democráticos de direito (como pretende o Brasil), sendo inerente ao exercício da cidadania. Tanto assim que há fundadas preocupações quanto ao uso inadequado e mesmo malicioso de algoritmos e redes sociais para a difusão de discursos autoritários e visando ao beneficiamento em pleitos eleitorais (Empoli, 2020) (Alvim; Rubio Núñez; Monteiro, 2024). Os poderes sem controle não devem ser tolerados num ambiente democrático. Assim, "as maneiras de exercer controle no tocante ao poder digital variam conforme também variam os consórcios que se estabelecem no contexto do exercício desses poderes" (Prado, 2020).

Deve-se dar atenção à economia da informação, própria da sociedade capitalista contemporânea – que atribuiu ao conhecimento um componente essencial para a estruturação de relações de poder[4].

> A informação se tornou uma moeda de troca nas interações sociais e comerciais na sociedade da informação (...). Conjugadas, a evolução da internet e da sociedade provocaram uma profunda e inquestionável transformação na dimensão política de nossas vidas. O poder é exercido para produzir e difundir conteúdos de informação, sob o controle de interesses específicos, mostrando que a internet não é um instrumento de liberdade (Menezes; Colaço, 2019).

---

incrementada a violência física e simbólica por agentes estatais. (...) A busca pelo equilíbrio é, necessariamente, a busca por domesticar o 'poder digital'. Sem controle, transparência, equilíbrio e prestação pública de contas, quaisquer que sejam os sujeitos que o exerçam estarão sempre em condições de concentrar este poder e o empregar não no interesse da comunidade, hoje, inevitavelmente, um corpo social que transcende as fronteiras dos Estados nacionais, mas em proveito próprio" (Prado, 2020).

[4] "O capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais" (Zuboff, 2019, p. 18).

Tecnologias avançadas como as utilizadas atualmente permitem que ferramentas digitais funcionem como meios de controle social altamente precisos, embora manipuláveis e de difícil compreensão[5], as quais escondem decisões políticas que controlam os parâmetros de conteúdo e funcionamento de programas eletrônicos. Por isso, é necessário se debruçar sobre os procedimentos de investigação e persecução penal fundamentados em instrumentos tecnológicos que se utilizam de inteligência artificial (IA), os quais visam a otimizar o desempenho das forças policiais com o tratamento de dados[6].

Essas técnicas objetivam identificar possíveis suspeitos criminosos ou áreas com maior probabilidade de ocorrência de delitos, porém, sem considerar a possibilidade de reprodução de modos de policiamento seletivo historicamente estabelecidos e de propagar discriminações tipicamente humanas, decorrentes do uso indiscriminado dessas ferramentas e da presunção de sua imparcialidade. Isso faz com que seja necessário proteger o juízo de admissibilidade da prova, como uma questão prévia, e não de valoração.

Com o fenômeno da *big data*[7], o campo da segurança pública passou a utilizar ferramentas tecnológicas visando a "aperfeiçoar" a atividade policial, em termos de demanda, regionalidade e diálogo informacional. Todavia, evidenciam-se riscos decorrentes dos vieses de gênero, raça, classe e sexualidade, aptos a gerar prejuízos resultantes da vigilância excessiva[8] por parte do Estado.

---

5 Shoshan Zuboff ensinou que "O capitalismo de vigilância reivindica unilateralmente a experiência humana como matéria-prima gratuita para tradução em dados comportamentais" (2019, p. 8).

6 "Art. 5º, da Lei nº 13.709/2018: "Para os fins desta Lei, considera-se: (...) X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

7 Conjunto de dados digitais que vem crescendo de forma exponencial, a ponto de ultrapassar a capacidade das ferramentas convencionais de capturar, gerenciar e analisar essas informações (Taurion, 2013).

8 Zygmunt Bauman e David Lyon fizeram a seguinte ressalva: "os principais meios de obter segurança, ao que parece, são as novas técnicas e tecnologias de vigilância, que supostamente nos protegem, não de perigos distintos, mas

Nesse sentido, no ano de 2020, o Supremo Tribunal Federal (STF) ofereceu um importante pronunciamento, em decisão proferida na Ação Direta de Inconstitucionalidade (ADI) 6387 MC-Ref/DF (julgada em conjunto com as ADIs 6388, 6389, 6390 e 6393). Ao se debruçar sobre a Medida Provisória 954/2020 (que determinava o compartilhamento de dados pessoais de todos os brasileiros com o Instituto Brasileiro de Geografia e Estatística – de telefonia fixa e móvel), a Corte citada reconheceu a autonomia do direito fundamental à proteção de dados pessoais, com *status* constitucional guiado pelas cláusulas que garantem a liberdade individual (art. 5º, *caput*), a privacidade e o livre desenvolvimento da personalidade (art. 5º, X e XII), e pela garantia do devido processo legal informacional (art. 5º, LIV), balizando limites do tratamento de dados pessoais (Estellita, 2023). Na sequência, serão explorados os riscos advindos da utilização da inteligência artificial

2. Tecnopolíticas[9] de vigilância na segurança pública: inteligência artificial, policiamento preditivo e o tratamento de dados

O fascínio humano com a ideia de prever o futuro tem sido bastante retratado em obras de ficção científica, tal como no filme *Minority Report*, de Steven Spielberg, baseado em um conto de Philip K. Dick (Hudson, 2009). No entanto, para além da fantasia, a realidade já dispõe de recursos tecnológicos que visam a antecipar a informação de ocorrência de delitos.

É o que se dispõe a oferecer a análise preditiva via IA, com técnicas de *machine learning* (ML) – "área da inteligência artificial (IA) e da ciência da computação que se concentra no uso de dados e algoritmos para imitar a maneira como os humanos aprendem, melhorando gradualmente

de riscos nebulosos e informes (...) as inseguranças são um corolário prático das sociedades securitizadas de hoje" (2013, p. 95-101).

[9] O termo corresponde à emergência de estratégias de vigilância fundamentadas no uso de tecnologias e suas repercussões sociais. Nesse sentido, as tecnopolíticas dizem respeito "tanto ao desenvolvimento de novas formas de vigilância e controle quanto à experimentação de resistências e subversões que dialogam com elas" (Bruno *et al*, 2018, p. 9).

sua precisão" (IBM, 2023) – com a finalidade de minerar dados colhidos anteriormente (como relatórios policiais e registros de ocorrência).

Através do processamento dos dados, com métodos estatísticos aplicados a algoritmos treinados para fazer classificações ou previsões, traçam-se tendências futuras, influenciando diretamente nas práticas de policiamento, seja no desenvolvimento de estratégias de segurança pública seja por meio da escolha de alocação de recursos. Nesse contexto, surgiu o policiamento preditivo, que diz respeito a "sistemas computadorizados cujo processamento de informações por algoritmos se utilizam tanto de bancos de dados robustos quanto de análises estatísticas para fins de predição de um acontecimento criminoso futuro" (Moraes, 2022, p. 35).

É bem verdade que, mesmo antes do surgimento da IA, já vinha sendo sedimentada a utilização de uma lógica de gerenciamento de riscos na política criminal de segurança pública (Dieter, 2013, p. 148), através da utilização de estatísticas e técnicas atuariais para o desenvolvimento de investigações criminais e da antecipação de informações relacionadas à detecção de suspeitos. A facilitação do acesso às novas tecnologias e a aceleração social dela decorrente aprofundou essa tendência.

Nesse contexto, Silva Sanchez observou que a sociedade do risco resulta em um Estado vigilante, policial-preventivo, no qual "a barreira de intervenção do Estado nas esferas jurídicas dos cidadãos se adianta de modo substancial" (Silva Sanchez, 2011, p. 165). A própria sociedade tende a aceitar e normalizar a cultura de vigilância (Garland, 2008).

Ao passo em que mais e mais interações sociais são mediadas digitalmente, as pessoas passaram a ser participantes ativos da vigilância, deixando a posição passiva anterior em que se colocavam apenas submetidos à observação. Isso fica evidente especialmente nas mídias sociais e na internet, onde as mentalidades e práticas de vigilância se tornaram cotidianas, principalmente diante de sua aceitação generalizada por parte das pessoas, que as adotam como algo corriqueiro e natural – embora ainda exista resistência correspondente à maior valorização da privacidade eletrônica, em certos contextos (Lyon, 2018, p. 159).

Entretanto, é importante chamar a atenção para a falsa percepção de neutralidade dessas tecnopolíticas (Dias, 2022, p. 157). O uso de modelos estatísticos para a predição de comportamentos humanos

tende a reproduzir problemas e enviesamentos[10] disseminados na sociedade. Isso, porque

> os dados são frequentemente imperfeitos, o que permite que esses algoritmos acabem herdando preconceitos de tomadores de decisão anteriores. (...) o data mining pode revelar regularidades surpreendentemente úteis, mas que, em verdade, são apenas padrões preexistentes de exclusão e desigualdade (Barocas; Selbst, 2016, p. 671).

As inovações tecnológicas estão remodelando o direito criminal, especialmente no contexto das transformações nas investigações criminais, através da identificação de vestígios. Isso afeta diretamente a lógica dos procedimentos e evidências, gerando debates sobre os impactos no sistema legal e nos direitos individuais dos investigados (Gloeckner; Eilberg, 2019). Desse modo, a investigação criminal foi incrementada com ferramentas de controle por geolocalização (GPS) – seja para monitorar ou encontrar pessoas –, de processamento de dados informáticos (redes sociais, fotos, IP's, nuvens, e-mails e informações pessoais), de coleta por servidores de internet, de mensagens instantâneas, entre outros.

Com o aumento da sensação de insegurança e do medo social (Bauman, 2008, p. 7-11) (Young, 2002, p. 33-35), agravados pelo movimento de guerra ao terror instaurado a partir dos eventos de 11 de setembro de 2001 nos EUA, houve um recrudescimento das formas de controle, com adoção de práticas de vigilância (Arruda; Resende; Fernandes, 2022, p. 668-669). Aqui, as novas tecnologias inspiraram estratégias para detectar e impedir criminosos antes que tenham a oportunidade de perpetrar suas transgressões (Stalder; Lyon, 2003, p. 90). Como esclareceu Ulrich Beck:

> "Sociedade de risco" significa que vivemos em um mundo fora de controle. Não há nada certo além da incerteza. Mas vamos

[10] Explica Tobias Baer: "vieses algoritmos podem ser inseridos pelo desenvolvedor, sendo classificados em: i) viés de confirmação: que configura o algoritmo para replicar um viés presente na própria mente do programador; ii) esgotamento do ego: onde o programador tem um cansaço mental que introduz ou aumenta vieses para minimizar o esforço cognitivo; iii) excesso de confiança: onde o programador rejeita os sinais de que o algoritmo pode ser tendencioso" (2019, versão do kindle, em livre tradução).

> aos detalhes. O termo 'risco' tem dois sentidos radicalmente diferentes. Aplica-se, em primeiro lugar, a um mundo governado inteiramente pelas leis da probabilidade, onde tudo é mensurável e calculável. Esta palavra também é comumente usada para referir-se a incertezas não quantificáveis, a 'riscos que não podem ser mensurados'. Quando falo de 'sociedade de risco', é nesse último sentido de incertezas fabricadas. Essas 'verdadeiras' incertezas, reforçadas por rápidas inovações tecnológicas e respostas sociais aceleradas, estão criando uma nova paisagem de risco global. Em todas essas novas tecnologias incertas de risco, estamos separados da possibilidade e dos resultados por um oceano de ignorância (not knowing) (Beck, 2006).

A disseminação dos riscos e a informatização da sociedade atual ofereceram a justificativa para que os sistemas criminais adotassem amplamente as tecnologias de vigilância em massa (Dempsey, 2020, p. 200), com o argumento de combate mais eficaz ao terrorismo e à criminalidade em geral, e de incremento na proteção de direitos fundamentais. A popularização das tecnopolíticas e o seu impacto no policiamento e no processo penal trouxeram o tema para debate na justiça brasileira, inclusive no âmbito da jurisdição constitucional.

Assim, no julgamento da ADI 5527, relatado pela Ministra Rosa Weber, que discutiu os arts. 10, § 2º, e 12, III e IV, do marco civil da internet (lei 12.965/2014), o Supremo Tribunal Federal reconheceu a "proliferação de sistemas de vigilância", destacando que a "emergência das mídias sociais, juntamente com a manipulação de dados pessoais em redes computacionais por inúmeros, e frequentemente desconhecidos, agentes públicos e privados" constata riscos aos direitos fundamentais com o tratamento de dados, e assim ao próprio regime democrático (p. 13). No voto de relatoria, registrou-se que 'conhecimento de que a comunicação é monitorada por terceiros interfere em todos esses elementos componentes da liberdade de informação: os cidadãos podem mudar o modo de se expressar ou até mesmo absterem-se de falar sobre certos assuntos, no que a doutrina designa por efeito inibitório (chilling effect) sobre a liberdade de expressão" (p. 10), de forma que "não podem a hermenêutica constitucional e o desenvolvimento legislativo ficar alheios a essas mudanças no tempo, tendo em vista a

manutenção do equilíbrio entre proteção da privacidade e os limites da atuação do Estado" (p. 14)[11].

Dentre as técnicas de vigilância eletrônica que passaram a ser amplamente utilizadas, encontra-se o policiamento preditivo. Três das principais ferramentas no campo da segurança pública se destacam (Goodfellow, 2016, p. 5-25): a) Redes *Multilayer Perceptron* (MLP), que é usado em casos de aprendizado supervisionado, como reconhecimento e classificação de padrões em imagens e arquivos de áudio; b) Redes Neurais Convolucionais (RNC), que permitem a classificação de imagens e agrupamento por similaridades, sendo bastante usada para leitura de placas de veículos e motocicletas com câmeras de videomonitoramento; c) Redes Neurais Recorrentes (RNR), que são usadas para aprendizado com dados sequenciais, temporais e processamento de linguagem natural, principalmente para modelagem de linguagem e reconhecimento de fala (Bottino; Vargas; Prates, 2023, p. 35).

O tratamento dos dados via IA visa a inferir áreas de maior criminalidade em determinado período, bem como as pessoas envolvidas (vítima ou ofensor), para "otimizar o exercício do controle social e mitigar as taxas de criminalidade" (Braga, 2020, p. 693), a fim de prever futuros infratores e infrações. Essas ferramentas são muito utilizadas nos Estados Unidos com a finalidade de prever reiterações delitivas, subsidiando informações para a fundamentação da tomada de decisões sobre liberdade, prisão provisória, aplicação e execução da pena (Silva, 2020, p. 11).

Os sistemas *PredPol*, *Palantir* e *HunchLab* são exemplos de *softwares* de policiamento preditivo baseados no lugar (aqui, objetiva-se direcionar um maior quantitativo de policiais para determinada localidade). De outro lado, o sistema *Beware* é um exemplo de aplicações digitais baseado na pessoa, como ferramentas de reconhecimento facial e listas de calor.

Os sistemas preditivos são criados a partir de modelos estatísticos de regressão múltipla ou multivariada, funcionando através de associações significativas entre variáveis explicativas e uma variável dependente. Elencam-se como argumentos favoráveis à sua utilização (Rios; Silva, 2021, p. 67-68): a) que promoveriam uma nova racionalidade de decidir, sustentando *evidence-based decisions* (decidir com base

[11] BRASIL. ADI 5527/DF. Rel. Min. Rosa Weber.

em dados empíricos mediante procedimentos metodológicos); b) que permitiriam a padronização de critérios decisórios, diminuindo espaços para o subjetivismo; c) que incrementariam os objetivos de segurança pública e diminuiriam os níveis de encarceramento, via prisão de pessoas "de alta periculosidade"; d) que permitiriam a identificação, administração e gestão do risco de reiteração delitiva, com a definição das medidas aplicáveis ao caso concreto; e) que seriam de aplicação simples, precisa, transparente e rápida, indo além da objetividade humana.

Todavia, essas ferramentas preditivas compreendem o homem a partir de uma perspectiva meramente estatística, por meio de uma relação entre a base de dados e os padrões de regularidades comportamentais de uma população (Garland, 1997, p. 182), sem qualquer análise ideográfica e interpretativa do caso concreto. Por sua própria natureza, a IA não abarca a singularidade de cada comportamento e seu contexto único[12], o que é vital no âmbito da segurança pública e do processo penal.

Exatamente por essa razão, é possível apontar exemplos de erros cometidos por softwares de IA que utilizam a tecnologia de predição, decorrentes de vieses existentes nas práticas do sistema criminal, as quais servem como base de dados para esses *softwares*. Por exemplo, em 2024, uma mulher foi presa erroneamente em Copacabana, após ser identificada por sistema de reconhecimento facial (Extra, 2024). Antes disso, no ano de 2019, uma mulher foi detida por engano no Rio de Janeiro, após ter sido confundida pelo sistema de reconhecimento facial da Polícia Militar (G1, 2019). Também em 2024, um jovem torcedor de um time de futebol sergipano foi conduzido por policiais militares durante a final do campeonato estadual, na cidade de Aracajú, devido a uma falha na tecnologia de reconhecimento facial (FAN F1, 2024). Também na capital do Sergipe, no evento festivo "Pré-caju" do ano de 2023, uma mulher negra foi abordada de forma truculenta e levada por policiais, após ter sido confundida com outra suspeita pelo reconhecimento facial em um (FAN F1, 2023). Em 2021, a cidade do Rio de Janeiro/RJ adquiriu um pacote de serviços de infraestrutura da *Oracle*, com *softwares* para cruzamentos e análises de

[12] Mehozay e Fischer afirmaram que: "algoritmos são epistemologicamente performativos (...) eles não fazem reivindicações quanto à verdade, apenas buscam funcionar" (2019, p. 12).

grandes volumes de dados (The Intercept Brasil, 2021), sendo possível reunir diferentes bases de dados, organizar e hierarquizar informações como ocorrências policiais, armas de fogo, celulares, veículos, pessoas e dados biométricos.

Uma pesquisa do *National Institute of Standards and Technology* (NIST) constatou (Scientific american, 2019) que os 189 algoritmos de reconhecimento facial existentes à época, criados por 99 programadores diferentes, tinham de 10 a 100 vezes mais chances de identificar o rosto de uma pessoa negra ou asiática, em comparação com o de uma pessoa branca. Em outra pesquisa, o *Institute of Electrical and Electronics Engineers* (IEEE) (Klare, 2012) pontuou que o reconhecimento facial possui menor precisão entre mulheres, negros e jovens de 18 a 30 anos, em diferentes grupos demográficos. Sobre o assunto, explicou Tainá Aguiar Junquilho:

> Na realidade nenhuma tecnologia é neutra, nem a tecnologia que era aplicada na revolução industrial era uma tecnologia neutra. Então, um sistema de inteligência artificial é tão neutro quanto for a pessoa que vai desenvolver e aplicar o sistema, ou seja, é impossível ter neutralidade quando a gente está diante de tecnologia. (...) Então o mundo desse sujeito é o mundo que é refletido na programação. (...) o fato de que as pessoas são reconhecidamente preconceituosas no sentido de que elas têm preconcepções, de ter determinadas realidades de vida. Então necessariamente esse viés vai aparecer, porque se essa inteligência artificial trabalha com dados, esses dados reproduzem a realidade (2022, p. 160).

Em Alagoas, no ano de 2024, instalou-se um novo sistema de videomonitoramento, contando com mais de 150 câmeras distribuídas por diversos bairros de Maceió. Além disso, há totens de segurança habilitados com reconhecimento de veículos e de placas, além de botão de pânico. Segundo informado pelo governo estadual, as câmeras estão habilitadas para fazer reconhecimento facial (Governo de Alagoas, 2024). No mesmo estado foi editada uma lei que estabelece os princípios e diretrizes para o uso de inteligência artificial no âmbito da administração pública estadual (lei ordinária estadual nº 9.095/2023)[13].

[13] Estado de Alagoas. *Lei nº 9.095, de 11 de dezembro de 2023*. Estabelece os princípios e diretrizes para o uso da inteligência artificial, no âmbito da

Destacam-se do referido instrumento normativo dois dispositivos: o artigo 3º, que indica que o desenvolvimento, a implementação e o uso de sistemas de inteligência artificial observarão parâmetros éticos e princípios como a autodeterminação e liberdade de decisão e de escolha, a participação e supervisão humana, a não discriminação, e devido processo legal, contestabilidade e contraditório; e o artigo 4º, que indica os direitos à informação prévia, explicação sobre a decisão, recomendação ou previsão, contestação a decisões ou previsões, determinação e participação humana, não-discriminação e correção de vieses discriminatórios como direitos a serem exercidos por pessoas afetadas por sistemas de Inteligência Artificial.

Acontece que tais mecanismos tendem a se sobrepor em relação aos procedimentos tradicionais de apuração da infração penal e sua autoria. Os casos anteriormente citados atestam o perigo em somar o "fetiche da prova técnica" com o "controle social" – majoritariamente aplicado aos dissidentes e/ou mais vulneráveis – incrementando assim as possibilidades de se iniciarem processos de criminalização indevidos.

Essas tecnopolíticas caminham para uma "presentificação do passado e do futuro" (Prado, 2020b), prevendo hipoteticamente cenários prováveis por meio da consideração de acontecimentos passados, a partir do tratamento dos dados. Incorre dessa maneira em um alto risco de produção de resultados tendenciosos e discriminatórios.

Ao processar dados, os algoritmos terminam considerando preconceitos e falsas percepções contidas nessas informações, de modo a reproduzir "práticas ostensivamente racistas, sexistas ou mergulhadas em distorcidos ideais de meritocracia neoliberal" (Dias, 2002, p. 155). Surge assim o fenômeno da discriminação algorítmica, decorrente de falhas humanas de seus criadores bem como do fato de que as bases de dados utilizados nos sistemas podem ser enviesadas e não representar adequadamente todos os segmentos da sociedade. Isso evidencia a sutil incorporação de formas de discriminação em processos técnicos, perpetuando-se por meio de algoritmos que muitos ainda consideram como

administração pública estadual. Disponível em: <https://sapl.al.al.leg.br/media/sapl/public/normajuridica/2023/2799/lei_no_9.095_de_11_de_dezembro_de_2023_.pdf>. Acesso em: 22 dez. 2023.

imparciais e precisos (Duarte; Negócio, 2021, p. 228-230). Nesse sentido, a discriminação algorítmica é um efeito colateral do funcionamento dessas soluções tecnológicas.

O viés discriminatório dos algoritmos pode surgir (Mendes; Mattiuzzo; Fujimoto, 2021, p. 446): a) por erro estatístico, seja na coleta ou no tratamento dos dados, ou algum erro no algoritmo que ocasiona segregação de grupos; b) pelo uso de dados sensíveis, que podem gerar discriminações e danos aos titulares; c) por generalização injusta, por classificar alguém em grupo que não pertence; e d) limitadora do exercício de direitos, quando o titular é discriminado ao exercer seu direito de acesso à informação de seus dados (vedada pelo art. 21 da Lei Geral de Proteção de Dados).

A vigilância (ou criminalização) automatizada, que decorre da atuação tecnopolítica de antecipar delitos e criar estratégias de segurança pública balizadas pelo tratamento de dados colhidos previamente, reproduz o *modus operandi* dos agentes de controle social, marcado pela seletividade das práticas de policiamento.

Justamente devido aos vieses e à discriminação algorítmica, é importante indagar quais informações são empregadas para efetuar essas previsões, como elas são avaliadas pelas ferramentas tecnológicas e como isso repercute na maximização de chances de erros. Isso significa que o tema deve ser refletido a partir de um "ceticismo epistêmico", considerando que

> (...) é preciso estar alerta para as debilidades probatórias que representam injustificado incremento do risco de detenção de inocentes e desconfiar dos parâmetros a partir dos quais os mecanismos de identificação por reconhecimento facial têm sido elaborados (Vieira *et al*, 2021, p. 32).

As ferramentas preditivas são produzidas pela iniciativa privada e vendidas com a (falsa) promessa de impedir a repercussão dos preconceitos dos tomadores de decisão humana. O processamento dos sistemas é protegido por segredo industrial, não havendo acesso às informações sobre os dados efetivamente utilizados. No mais, não são fornecidos critérios para a responsabilização, em casos de danos gerados por vieses ou evidências de má conduta (Braga, 2020, p. 693) (Dias, 2022, p. 161).

A criminologia crítica pontua que a intervenção punitiva tende a perpetuar as desigualdades sociais, ao mesmo tempo em que serve aos interesses de acumulação de capital. Os sistemas de policiamento preditivo reforçam essa argumentação, posto que podem ser utilizados para justificar a intensificação da vigilância sobre comunidades marginalizadas e grupos estigmatizados (Dias, 2022, p. 170). Dessa maneira, atuariam como mais uma estratégia inclinada à seletividade penal, reforçando a decisão tradicional de enfrentamento da criminalidade preferencialmente (ou exclusivamente) por meio de ações repressivas e seletivas.

> Essa forma de entender a segurança pública, como garantia da ordem em detrimento da garantia de direitos, é sustentada pela estrutura social, conformada em torno de uma engenharia de punição e vigilância. Note-se que a introdução de novas tecnologias no âmbito jurídico-penal, portanto, reproduz a lógica segregacionista que reserva a resposta penal aos indivíduos que não interessam à sociedade neoliberal. Ou melhor, interessam na medida em que fornecem dados que podem auxiliar na conformação de práticas de vigilância, e não na promoção da dignidade humana (Arruda; Resende; Fernandes, 2022, p. 683).

A implementação de dispositivos encarregados de automatizar os serviços públicos configura o alargamento das políticas gerenciais punitivas voltadas para lidar com a pobreza, e os algoritmos usados prestam-se à condução de vigilância estatal (Eubanks, 2022, p. 683-684). A vigilância, por sua vez, reforça a repressão penal, impulsiona o sistema de justiça criminal e os estereótipos que lhes são decorrentes, além de promover a segregação social e a compartimentalização do espaço público em domínios privados (Firmino, 2018), estampando o uso do poder punitivo para hierarquização social, através de indicadores sociais (raça, gênero, condição econômica e outros) inseridos nos *softwares* do sistema de segurança pública (Mendes; Vechi, 2020).

3. A LINGUAGEM CIBERNÉTICA E O DOMÍNIO DA PROVA DIGITAL

Com o aprofundamento da digitalização das relações sociais, a persecução penal depende cada vez mais do controle de ferramentas e

plataformas eletrônicas. Além disso, necessita utilizar uma linguagem digital, própria desse contexto virtual, exigindo assim uma metalinguagem que entrelaça as narrativas cibernética e jurídica.

Quanto à paridade de armas, pode-se afirmar que essa característica produz resultados que ultrapassam a tendência tradicional de desvantagem inicial da defesa técnica em comparação com a acusação, decorrente da vantagem cognitiva do acusador durante a investigação. Hoje, também é importante levar em consideração a disparidade tecnológica, que possui dois aspectos distintos: a) obtenção e produção de provas; e b) verificação e controle das evidências apresentadas pela parte adversária.

Para compreender esse fenômeno, é bastante útil lançar mão do conceito de tecnodiscursos, os quais são "enunciados nativos digitais que possuem suas formas profundamente afetadas e definidas pela tecnologia, sendo que esta atua não apenas como suporte, mas também como atribuidora de significado" (Paveau, 2021, p. 31). Não é possível conceber o discurso digital ignorando-se a própria máquina e sua complexidade. Isso porque o próprio ambiente virtual determina os caminhos e as possibilidades de interação possíveis para o escritor-leitor. Nesse sentido, "os discursos digitais nativos não são de ordem puramente linguageira (...) as determinações técnicas coconstroem as formas tecnolinguageiras" (Paveau, 2021, p. 31).

Marie-Anne Paveau concebeu definições para analisar os aspectos linguístico e tecnológico de forma conjunta, sem esquecer tópicos sensíveis da análise do discurso enquanto memória discursiva e historicidade. Defendeu a necessidade de se considerar o conceito de "tecnologia discursiva" –pautada por ferramentas materiais (base de dados, agendas, sites, ferramentas de busca) ou não materiais (a linguagem), para pensar e categorizar, cognitivamente e de forma colaborativa – e de "discurso nativo digital" - que é próprio da *web*, produzido e expandido internamente - com certas características:

> 1) efeito compósito – discursos digitais são constituídos por matéria mista que reúne indistintamente o linguageiro e o tecnológico em suas diversas modalidades e assim devem ser analisados; 2) deslinearização – discursos não seguem eixos específicos, podem ser quebrados por links; 3) ampliação – discursos têm enunciação ampliada por conta da conversacionalidade da Web Social e podem

> produzir um enunciador ampliado (que origina uma discussão, mas não mais a detém), e um enunciador coletivo (co-produzindo textos colaborativos em conjunto com as funcionalidades dos sistemas); 4) investigabilidade – os discursos se inscrevem em universos que nada esquecem (são localizáveis e coletáveis) – mesmo aqueles usuários que "apenas" leem as páginas da Web Social deixam inscritos seus rastros, pois a audiência é captada pelos algoritmos; 5) imprevisibilidade – os discursos são parcialmente projetados pelos algoritmos e pelos humanos (o leitor inesperado é aquele que pode fazer diferentes rotas de leitura, escolhendo a ordem de links que desejar e o lurker – o leitor que não se pronuncia, mas acessa tudo – muito menos tem influência total de alguma forma como foi moldado o discurso na interface. Além disso, existe a idiodigitalidade: a idiossincrasia da forma como está configurado o ambiente de cada um, o que torna ainda mais imprevisível saber como as informações são disponibilizadas para o leitor da Web; 6) relacionalidade – os discursos são inscritos em uma relação integrada devido à reticularidade da Web e permitem enunciados coproduzidos com os sistemas. (Melo, 2021, p. 2).

Assim, o convencimento da ocorrência de fatos através das provas deve considerar as necessidades provenientes da ambientação virtual na qual ela se extrai. Ou seja, deve-se ter em mente as especificidades linguísticas do ecossistema digital, além do fato de que elas são aptas a cadenciar contextos diversos e maleáveis. A produção nativa digital se destaca fundamentalmente pelo seu potencial de relacionalidade. Isso porque as relações baseadas em algoritmos, ao mesmo tempo em que integram as produções, também garantem seu funcionamento e sua circulação, pela característica linguisticamente inéditas da clicabilidade.

Nos tecnodiscursos, a máquina atua de forma dominante, em conjunto com os recursos que oferta para a criação e circulação de falas, com o fulcro de alimentar a relação entre sujeito, linguagem e sociedade[14].

[14] Letícia Cesarino parece aderir a essa constatação, ao aprofundar a hipótese de que "a coprodução cada vez mais intensiva e extensiva entre cognição maquínica e humana possa estar levando a um alinhamento no sentido de uma 'redução' da última, mais complexa, à primeira, menos complexa" (2022, p. 40).

Por isso, "os sentidos são constituídos em um *continuum* entre linguagem e ambiente de produção" (Silva; Lopes, 2023, 144).

> Assim, pode-se afirmar que os recursos morfolexicais corroboram a manutenção de uma verdade, fazendo com que semelhantes opiniões se engatilhem. Dessa maneira, o conceito de tecnodiscurso colabora com a compreensão do complexo funcionamento do digital ao incorporar as relações subjacentes entre sujeito, linguagem, máquina e sociedade, ou mesmo para que as análises de textos nativos do ambiente digital sejam tratadas tão somente de uma perspectiva saussuriana e dualista, ou seja, observável e analisável apenas do material linguageiro. Há que se considerar que, nos tecnodiscursos, os agentes não humanos assumem papel preponderante: a máquina e os recursos que oferta para a formulação e circulação de dizeres nutre a relação sujeito, linguagem e sociedade. Na máquina e em rede, os sentidos são constituídos em um continuum entre linguagem e ambiente de produção (Silva; Lopes, 2023, 143-144).

Essa conjuntura deixa mais evidente o problema que se quer destacar. A influência da virtualização global na persecução penal faz com que a investigação criminal e a argumentação jurídica dependam cada vez mais de ferramentas e plataformas digitais. Por sua vez, isso torna necessária uma metalinguagem que conecte as narrativas cibernética e jurídica, já que o discurso digital não pode ser compreendido sem que se leve em conta a máquina e sua complexidade. Portanto, a persuasão por meio de provas depende da consideração das características específicas do ecossistema digital em que elas são obtidas.

Hoje, empresas privadas de mídia social[15] são personagens-chave da gestão das condições concretas de autodeterminação informativa, proteção da segurança e cooperação nas investigações e processos criminais. Isso faz com que as estratégias processuais e mesmo as condições para o seu desenvolvimento dependam de atores privados, o que interfere no

[15] Algumas dessas empresas, situadas no Norte global e "associadas a plataformas de uso intensivo de dados" têm sido denominadas de *big techs* (Morozov, 2018, p. 144).

papel tradicional dos atores processuais (polícias, ministério público, defensores e judiciário).

As especificidades do contexto hodierno demandam a formulação de uma nova teoria dos sujeitos processuais penais, que abarque em sua estrutura titulares de poderes privados. Desse modo, é importante compreender que, no cenário atual, a acusação dispõe de poderes que poderiam ser exercidos antes mesmo da formalização do processo. Nesse sentido, Renato Vieira constatou a existência, antes mesmo do processo, de um "antagonismo dos interesses em jogo", para além do embate entre acusação e defesa. Assim, a ressignificação da atuação de tais empresa tem o fulcro de equilibrar direitos e garantias individuais, sob a ótica da paridade de armas, uma vez que tal antagonismo não considera interesses particulares (Vieira, 2013, p. 96).

A prática de diligências de investigação digital que estão sob domínio ou controle de empresas privadas é chamada de "externalização da investigação criminal" (Gascón Inchausti, 2019, p. 192-194), seja quando da aquisição e preservação de dados e informações, ou ainda, quando de seu tratamento. Sobre o tema, Rodrigo de Oliveira Camargo registrou:

> A consecução de diligências de investigação eletrônica para a aquisição, preservação de informações, tratamento e análise de dados no âmbito de empresas privadas pode ser definida como externalização da investigação, colaboração muitas vezes essencial para o acesso a informações penalmente relevantes. (Camargo, 2022, p. 146)

Assim, considerando que as empresas são guardiãs dos dados eletrônicos de interesse probatório, conclui-se que elas podem dificultar enormemente o acesso às informações penalmente relevantes ou mesmo obstá-lo, caso desejem não cooperar. Ou seja, esses atores privados podem afetar diretamente o arbitramento da responsabilidade penal pelo magistrado competente. São necessárias garantias processuais concretas, direcionadas ao melhor interesse do indivíduo.

Do mesmo modo, também ocorre a externalização quando apenas as empresas privadas podem tratar e analisar adequadamente os dados, por razões de conhecimento técnico e *expertise*.

> A nova geometria de poder que entrega a iniciativa da investigação a entes privados, aliada ao desenvolvimento tecnológico que entrega ao indivíduo capacidade de coleta de dados acessíveis a um clique, enseja novas problematizações no fator tradição defensiva e sua estruturação, sobretudo em razão da ampliação dos campos de atuação (Camargo, 2022, p. 162).

Ao receberem uma determinação de diligência, são mais comuns três reações de parte das empresas. Na primeira delas, os atores privados alegam a proteção da liberdade de expressão do usuário em face de "ações abusivas do Estado" (*Meta* e *Google*, majoritariamente), e que, por essa razão, atuariam apenas no gerenciamento do conteúdo disseminado em suas redes sociais, via algoritmos. A segunda postura, também frequente, é a de que as empresas cooperem com as investigações criminais, oferecendo equipes de pesquisas privadas. Por último, há também as situações em que o Estado determina que o uso dos dados administrados pelas companhias seja vinculado a um programa de integridade que proteja a privacidade dos usuários (Jørgensen, 2019, p. 167-180).

É importante lembrar que os defensores normalmente não têm capacidade – fática ou mesmo técnica – de dialogar efetivamente com esses atores privados e tampouco possuem um protocolo de compartilhamento de dados e informações relevantes. De outro lado e diversamente, ao menos em tese, a polícia e o ministério público atuam com acesso e compartilhamento ilimitado a esses dados.

Apesar disso, seria possível robustecer a paridade de armas por meio da quebra do monopólio probatório do Estado. Como apontou Rodrigo de Oliveira Camargo, isso possibilita minimizar o peso de investigações enviesadas e proporciona a utilização de estratégias probatórias favoráveis à ampla defesa (2022, p. 149). Ao descentralizar o poder de investigar, deve-se ter em conta que (i) informação é coisa pública; (ii) a ideia de "investigação" supõe o acesso ao poder de saber; e (iii) os avanços tecnológicos ampliaram os meios de acesso à informação e, por isso, balizam o direito à participação e ampliação do direito à informação, em todo e qualquer ato que leva a decisões de poder.

A influência da virtualização global na persecução penal é evidente, na medida em que a investigação e a argumentação jurídica dependem

cada vez mais de ferramentas digitais e plataformas. E, se entende-se o discurso digital incompreensível sem a consideração da máquina e de sua complexidade, conclui-se que a persuasão processual por meio de provas necessita considerar as características específicas do ecossistema digital em que elas são obtidas.

Com o crescente domínio da prova digital, empresas privadas de mídia social tornaram-se atores essenciais na governança das condições concretas de autodeterminação informativa, proteção da segurança e cooperação nas investigações e processos criminais. As empresas, de fato, detêm poder para controlar o acesso a informações penalmente relevantes e, por essa razão, podem afetar diretamente o desfecho dos casos criminais. Além disso, a capacidade técnica e expertise das *big techs* as coloca em posição privilegiada para tratar e analisar os dados – possivelmente em detrimento da defesa.

A autodeterminação informativa foi reconhecida pelo Supremo Tribunal Federal no julgamento das ações diretas de inconstitucionalidade nº 6387, 6388, 6389, 6393 e 6390, com o entendimento de que a privacidade somente poderia ser mitigada diante de justificativa legítima. Isso porque "a proteção de dados pessoais e autodeterminação informativa são direitos fundamentais autônomos extraídos da garantia da inviolabilidade da intimidade e da vida privada"[16]. Assim, não há qualquer espaço discricionário - no âmbito probatório – que permita sequer cogitar considerar quaisquer dados eventualmente coletados como insignificantes ao caso, para deixá-los desapercebidos, num cenário de automatização de processos, uma vez que eles podem servir como garantia de controle de suas próprias informações aos usuários.

Descentralizar o poder de investigar implica reconhecer que a informação é um bem público e que o acesso ao conhecimento é inerente à investigação criminal. No ponto, deve-se ter em mente a preservação da cadeia de custódia das provas[17] (art. 158-A, do Código de Processo Penal),

---

[16] Brasil. ADI 6387/DF. Julgamento em 07 mai. 2020. p. 55.

[17] Que pode ser definida como "a história cronológica escrita, ininterrupta e testemunhada, de quem teve a evidência desde o momento da coleta até que ela seja apresentada como prova no tribunal" (Badaró, 2017, 561).

como forma de manter e documentar a história cronológica da evidência, com o fulcro de promover uma documentação formal do processo.

A cadeia de custódia tem como uma de suas finalidades indicar todas as pessoas que tiveram contato com a fonte de prova, de forma consecutiva. Por isso, há quem a considere "a prova da prova" (Lima; Romanelli, 2021, p. 99) ou uma "atividade probatória secundária" (Pastore; da Fonseca, 2022, p. 99). Assim, a preservação da cadeia de custódia da prova digital é fulcral no processo penal hodierno, ante a necessidade de demonstração da autenticidade (no que diz respeito à origem) e integridade (no que diz respeito à conservação) de cada elemento de prova, advindo dos princípios da ampla defesa e do contraditório. Tanto assim, que a quinta turma do Superior Tribunal de Justiça reconheceu a aplicabilidade da cadeia de custódia para as provas digitais, em decisão proferida no Agravo Regimental no Habeas Corpus nº 143.169/RJ[18].

A lei n. 13.964/2019 (pacote anticrime), que introduziu o art. 158-A no Código de Processo Penal, não previu expressamente qual seria a consequência da quebra da cadeia de custódia. Alguns doutrinadores defendem que essa violação ensejaria a ilicitude da prova, com sua consequente inadmissibilidade ou exclusão do processo (Prado, 2021, p. 216) (Lopes Júnior, 2020, p. 459). De outro lado, também há quem entenda que a quebra da cadeia de custódia afeta apenas a valoração da prova, e não sua admissibilidade ou validade (Badaró, 2020, p. 514-515).

Com a tecnologia atual, a plena preservação da cadeia de custódia das provas demanda a identificação dos agentes que tiveram contato com a prova digital, a fim de garantir sua autenticidade e integridade.

> Com isso, por exemplo, a apreensão de computadores por si só não garante integridade da informação e autenticidade da fonte de prova, estas sujeitas a adoção de métodos que consideram algoritmos criptografados destinados a reter e preservar os dados (cópias espelho e lógica e cálculo da função HASH). (...) Acrescentem-se ao arsenal investigativo as tecnologias de acesso remoto e o domínio ou não, pelas autoridades de investigação, das chaves de acesso aos repositórios de dados e se compreenderá a imperatividade atribuída

[18] BRASIL. *AgRg em HC nº 143.169/RJ*. Rel. p/ acórdão: Min. Ribeiro Dantas. Julgamento em 07/02/2023.

> à adoção de métodos de preservação da cadeia de custódia da prova digital em guias e roteiros de investigação digital (Prado, 2021).

Desse modo, pretende-se certificar se a prova (i) se encontra da mesma forma que foi originalmente produzida (integralidade); (ii) se houve alterações durante o manuseio e/ou análise (espoliação - degradação magnética, elétrica, por temperatura, pela umidade, por choques ou vibrações); e (iii) se ela é passível de alteração, devido a fatores mecânicos, ambientais ou cronológicos (volatilidade). É que "um elemento probatório não custodiado como deveria tem o potencial lesivo de dar suporte a uma hipótese fática possivelmente falsa, conferindo-lhe injustificados contornos persuasivos" (Matida, 2021, p. 22). Assim, a admissão de um elemento de prova cuja integridade não foi devidamente preservada eleva as chances de condenação via elementos inidôneos de prova[19].

Prado afirma a existência do princípio processual da "desconfiança" (2021, p. 151), que se fundamenta na lógica de que "ninguém necessita crer que algo é aquilo que a parte que o apresenta diz que é, simplesmente porque ela assim o diz" (Baytelman; Duce, 2005, p. 284, em tradução livre). Em outras palavras, não devem ser reconhecidas credibilidades preconcebidas a nenhuma das partes. No mesmo sentido, entendeu a quinta turma do Superior Tribunal de Justiça, na supramencionada decisão proferida no Agravo Regimental no Recurso em Habeas Corpus nº 143.169/RJ:

> Da forma como redigidos os laudos, polícia e Ministério Público nos pedem, na prática, que apenas confiemos na eficiência e honestidade do perito e da atuação estatal como um todo – mesmo diante desses evidentes e graves lapsos de profissionalismo – para acreditar que nenhum dado foi perdido ou alterado enquanto os computadores estiveram sob a custódia do Estado. Algo como: se o Estado diz que a prova é confiável, e ainda que tenha perdido todas as oportunidades de comprovar essa confiabilidade, então ela o é.

[19] A norma da ABNT/ISO 27037/2014 menciona técnicas de manuseio da evidência digital quanto a auditabilidade, justificabilidade, repetibilidade e reprodutibilidade. O procedimento é dividido em identificação, coleta, aquisição e preservação. Essa regulamentação pode ser seguida de forma complementar às etapas do art. 158-B do Código de Processo Penal.

> Essa lógica ignora que, no processo penal, a atividade do Estado é objeto do controle de legalidade, e não o parâmetro do controle[20].

As evidências eletrônicas aumentam os perigos relacionados à manipulação e ao uso indevido do sistema legal para perseguir certos indivíduos e grupos. Destaca-se a necessidade de incremento da desconfiança, sob pena de se incorrer mais facilmente em condenações errôneas, prejudicar inocentes e balizar comportamentos estatais ilícitos.

Na investigação criminal, a defesa costuma ter seu acesso às informações restringido, sob a alegação de que haveria o potencial prejuízo à privacidade de terceiros. Contudo, os agentes da persecução penal não são impedidos de obterem essas informações, em desfavor do réu. Rebeca Wexler denomina esse fenômeno de assimetria de privacidade (2021, p. 20-23), a qual poderia ser minimizada, assegurando-se a cadeia de custódia na obtenção de provas digitais.

O tratamento de dados pessoais para a segurança pública e a persecução criminal não foram regulados pela lei geral de proteção de dados (Lei n. 13.709/2018). Com efeito, esse diploma normativo se limitou a registrar que lei específica disciplinará a matéria (art. 4º, III, "a" e "d", e § 1º). Tampouco houve regramento a respeito da cadeia de custódia específica das provas digitais. Sobre o tema, Scalcon e Quito afirmaram:

> (...) pouco ou nada se sabe a respeito do que é feito dos dados obtidos de quebras de sigilo a partir do momento em que são compartilhados com as agências investigativas. Não apenas não se tem previsibilidade ou controle sobre o percurso feito pelos dados que serão introduzidos na persecução criminal enquanto elementos de prova, como não se sabe o que acontece com as informações obtidas em excesso. Considerando que nuvens podem guardar arquivos de todos os tipos (fotos, vídeos, arquivos de áudio, texto, etc.) e que a capacidade de armazenamento nesses sistemas alcança a casa dos terabytes, as respectivas quebras de sigilo possibilitam ao Estado obter quantidades exorbitantes de informações, sem qualquer filtro de adequação ou necessidade, sobretudo quando as quebras desconhecem limites temporais (2023, p. 63).

---

[20] BRASIL. *AgRg em HC nº 143.169/RJ*. Rel. p/ acórdão: Min. Ribeiro Dantas. Julgamento em 07/02/2023. p. 9.

Assim, a produção probatória decorrente, por exemplo, de quebras de sigilos de dados, diante da ausência de previsibilidade ou controle sobre o seu percurso, pode compor acervo probante sem que se saiba o destino das informações obtidas "em excesso". Isso poderia configurar uma pescaria probatória (*fishing expedition*), possibilitando o Estado de alcançar um enorme leque de dados disponíveis das pessoas investigadas, com a finalidade de obter algo "útil" à persecução criminal. Logo, "a atual inexistência de qualquer lei que diga claramente o que o Estado pode ou não fazer a partir do momento em que obtém dados para fins de persecução criminal acaba por permitir tratamentos desproporcionais e incompatíveis com as finalidades antevistas" (Scalcon; Quito, 2023, p. 64).

Considerações finais

A vida em sociedade atualmente se estende para o mundo digital, por meio da internet, redes sociais, e-mails e documentos eletrônicos. A internet e a digitalização transformaram as relações humanas, redefinindo valores de bens, direitos e propriedades. A disseminação instantânea de informações é uma característica central dessa sociedade de informações. O acesso ao ambiente digital é considerado um direito fundamental na contemporaneidade, sendo a informação o eixo central das atividades econômicas individuais, empresariais e nacionais.

Entretanto, o uso e tratamento de dados por meio de inteligência artificial preditiva na área da segurança pública pode implicar riscos à sociedade, diante da possibilidade de discriminação algorítmica. A análise preditiva via IA e *machine learning* é usada para minerar dados, traçar tendências futuras e influenciar políticas públicas na área de segurança pública, por meio do policiamento preditivo. No entanto, essa abordagem levanta questões sobre a neutralidade da tecnologia, uma vez que os modelos estatísticos de previsão podem resultar em práticas enviesadas e discriminatórias.

Foram discutidos casos de comprovado erro em sistemas de reconhecimento facial, especialmente em relação a indivíduos pertencentes a minorias, e demonstrou-se que a aplicação dessas tecnologias

poderia ensejar a exclusão de grupos sociais e limitar o exercício de direitos. O policiamento preditivo, baseado em dados e IA, pode reproduzir estereótipos e discriminação. Assim, a implementação de dispositivos automatizados pode servir para a ampliação de políticas punitivas para controle da pobreza, resultando em vigilância e repressão que perpetuam hierarquias sociais, violam direitos fundamentais e enfraquecem o devido processo penal.

O uso da tecnologia na segurança pública faz emergir a importância de considerar seus riscos e impactos sociais. Torna-se necessário adaptar os procedimentos de investigação criminal e produção de provas ao contexto digital, sendo crucial estabelecer regras para a admissibilidade dessas provas em processos judiciais, com o fulcro de permitir o contraditório na autenticidade das fontes e na integridade dos conteúdos das provas digitais.

Ficou clara a necessidade de se desenvolver uma nova teoria dos sujeitos processuais penais que leve em consideração os poderes privados, já que empresas de mídia social desempenham papel essencial na autodeterminação informativa e na segurança. A atuação de empresas privadas na obtenção e tratamento de provas digitais pode afetar a dinâmica do processo penal, alterando o equilíbrio entre acusação e defesa. As empresas possuem efetivamente o poder de controlar o acesso às informações, podendo impactar a apuração da responsabilidade penal.

Por fim, destacou-se que o estabelecimento da cadeia de custódia das provas busca registrar todos os elos que formam a trajetória de um elemento probatório, garantindo sua autenticidade e integridade. Sua relevância advém de uma abordagem cautelosa no processo probatório, que se torna ainda mais crucial no caso das evidências digitais, devido às suas características particulares. Ao documentar a história de um vestígio, a cadeia de custódia não apenas pode assegurar a confiabilidade da prova digital, mas também tem a capacidade de prevenir a manipulação de informações pelos agentes estatais e fornecer dados contextuais significativos da investigação.

Referências

ALVIM, Frederico Franco; Rubio Núñez, Rafael; MONTEIRO, Vitor de Andrade. *Inteligência artificial e eleições de alto risco*: ciberpatologias e ameaças sistêmicas da nova comunicação política. Rio de Janeiro: Lumen Juris, 2024.

ARRUDA, A. J. P.; RESENDE, A. P. B. A.; FERNANDES, A. F. Sistemas de policiamento preditivo e afetação de direitos humanos à luz da criminologia crítica. *Direito Público*, Brasília, v. 18, n. 100, p. 664-689, 2022. https://doi.org/10.11117/rdp.v18i100.5978.

BADARÓ, G. H. A cadeia de custódia e sua relevância para a prova penal. In: SIDI, R.; LOPES, A. B. (orgs.). *Temas atuais da investigação preliminar no processo penal*. Belo Horizonte: D'Plácido, 2017.

BADARÓ, G. H. *Processo penal*. São Paulo: Thomson Reuters Brasil, 2020.

BAER, T. *Understand, manage, and prevent algorithmic bias*: a guide for business users and data scientists. Nova Iorque: Apress, 2019. https://doi.org/10.1007/978-1-4842-4885-0.

BAROCAS, S.; SELBST, A. D. Big data's disparate impact. *California Law Review*, Berkeley v. 104, p. 671-732, 2016. http://dx.doi.org/10.2139/ssrn.2477899

BAUMAN, Z. *Medo líquido*. Rio de Janeiro: Jorge Zahar, 2008.

BAUMAN, Z.; LYON, D. *Vigilância líquida*. Rio de Janeiro: Zahar, 2013.

BAYTELMAN A., Andrés; DUCE J., M. *Litigación penal*: juicio oral y prueba. México: FCE, 2005.

BECK, U. Sociedade de risco. O medo, hoje. Entrevista especial com Ulrich Beck. *Revista IHU On-Line*, São Leopoldo, n. 181, 2006. Disponível em: <https://www.ihu.unisinos.br/categorias/159-entrevistas/616847-sociedade-de-risco-o-medo-hoje-entrevista-especial-com-ulrich-beck>. Acesso em: 20 nov. 2023.

BOTTINO, T.; VARGAS, D.; PRATES, F. *Segurança pública na era do big data*: mapeamento e diagnóstico da implementação de novas tecnologias no combate à criminalidade. Rio de Janeiro: FGV Direito Rio, 2023.

BRAGA, C. Discriminação nas decisões por algoritmos: polícia preditiva. In: FRAZÃO, A.; MULHOLLAND, C. (coord.). *Inteligência artificial e Direito*: ética, regulação e responsabilidade. São Paulo: Revista dos Tribunais, 2020.

BRUNO, F. *et al.* Apresentação. In: BRUNO, Fernanda *et al* (orgs.). *Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018.

BUSHWICK, S. SABARIEGO, J.; AMARAL, A. J. do.; SALLES, E. B. C. *Algoritarismos*. São Paulo: Tirant lo blanch, 2020.

CAMARGO, R. O. de. *Tratamento de dados, persecução penal e garantia do direito de defesa*. Tese (Doutorado em Direito) - Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2022.

CESARINO, L. *O mundo do avesso*: verdade e política na era digital. São Paulo: Ubu, 2022.

DEMPSEY, J. X. Privacy and mass surveillance: balancing human rights and government security in the era of big data. In: GONTIJO, B. M.; LIMA, H. C. S. (orgs.). *Direito, tecnologia e inovação*. Belo Horizonte/São Paulo: D'Plácido, 2020.

DIAS, F. V. *Criminologia midiática e tecnopolítica*. São Paulo: Tirant lo blanch, 2022.

DIAS, T.; HVISTENDAHL, M. *Polícia do Rio comprou tecnologia da Oracle usada por países autoritários*. Disponível em: https://www.intercept.com.br/2021/03/10/policia-rio-tecnologia-oracle-policias-paises-autoritarios/>https://theintercept.com/2021/03/10/ policia-rio-tecnologia-oracle-policias-paises-autoritarios/. Acesso em 01/08/ ago. 2023.

DIETER, M. *Política criminal atuarial*: a criminologia do fim da história. Rio de Janeiro: Revan, 2013.

DUARTE, A.; NEGÓCIO, R. de V. Todos são iguais perante o algoritmo? uma resposta cultural do direito à discriminação algorítmica. *Direito Público*, Brasília, v. 18, n. 100, p. 218-244, 2021. https://doi.org/10.11117/rdp.v18i100.5869.

EMPOLI, Giuliano da. *Os engenheiros do caos*. São Paulo: Vestígio, 2020.

ESTELLITA, H. "Sou fruto do meu tempo e tenho que ter os olhos voltados para o futuro": um panorama do legado da Ministra Rosa Weber no âmbito da proteção da privacidade e do tratamento de dados pessoais (com repercussões na esfera penal). In: ROCHA, M. E. G. T.; SILVA, C. O. P. da.; SILVA, C. M. G. N. da (orgs.). *Ela pede vista*: estudos em homenagem à Ministra Rosa Weber. Londrina: Thoth, 2023.

EUBANKS, V. *Automating inequality*: how high-tech tools profile, police, and punish the poor. Nova Iorque: St. Martin's Press, 2018.

FAN F1. *"Fiquei tão nervosa que eu urinei nas calças", diz mulher confundida com suspeita de crime por reconhecimento facial no Pré-Caju*. Disponível em: <https://fanf1.com.br/2023/11/06/fiquei-tao-nervosa-que-eu-urinei-nas-calcas-diz-mulher-confundida-com-suspeita-de-crime-por-reconhecimento-facial-no-pre-caju/>. Acesso em: 23 mai. 2024.

FAN F1. *Jovem relata constrangimento após falha de reconhecimento facial no Batistão*. Disponível em: <https://fanf1.com.br/2024/04/15/jovem-relata-constrangimento-pela-policia-militar-apos-falha-em-tecnologia-de-reconhecimento-facial/>. Acesso em: 23 mai. 2024.

FIRMINO, R. J. Securitização, vigilância e territorialização em espaços públicos. In: BRUNO, F. *et al* (orgs.). *Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018.

G1 Rio. *Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano*. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml>. Acesso em: 01 ago. 2023.

GARLAND, D. "Governmentality" and the problem of crime: Foucault, criminology, sociology. *Theoretical criminology*, Londres, v. 1, n. 2, p. 173-214, 1997. https://doi.org/10.1177/1362480697001002002.

GARLAND, D. *Cultura do controle do crime*: crime e orden social na sociedade contemporânea. Rio de Janeiro: Revan, 2008.

GASCÓN INCHAUSTI, F. Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial. In: CONDE FUENTES, J.; SERRANO HOYO, G. (orgs.). *La justicia digital en España y la Unión Europea:* situación actual y perspectivas de futuro. Barcelona: Atelier Libros Jurídicos, 2019.

GLOECKNER, R. J.; EILBERG, D. D. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. *Revista brasileira de ciências criminais*, São Paulo, v. 156, n. 27, p. 353-393, 2019.

GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. *Deep learning*, Cambridge, v. 1, 2016. Disponível em: <http://imlab.postech.ac.kr/dkim/class/csed514_2019s/DeepLearningBook.pdf>. Acesso em: 01 ago. 2023.

GOVERNO DE ALAGOAS. *Novo sistema de videomonitoramento da segurança pública começa a funcionar em Alagoas*. Disponível em: < https://alagoas.al.gov.br/noticia/novo-sistema-de-videomonitoramento-da-seguranca-publica-comeca-a-funcionar-em-alagoas>. Acesso em 09 jan. 2024.

GRINBERG, F.; ARAÚJO, V. *Mulher identificada por reconhecimento facial em Copacabana é solta após constatado erro em sistema*. Disponível em: <https://extra.globo.com/rio/casos-de-policia/noticia/2024/01/mulher-identificada-pelo-sistema-de-reconhecimento-facial-em-copacabana-e-liberada-apos-ser-

constatado-que-mandado-de-prisao-estava-no-sistema-por-erro.ghtml>. Acesso em: 05 abr. 2024.

HAN, Byung-Chul, *Infocracia*: digitalização e a crise da democracia. Petrópolis: Vozes, 2022.

HUDSON, B. Minority report: prevendo o futuro na vida real e na ficção. *Direitos fundamentais & democracia*, Curitiba, v. 5, 2009. Disponível em https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/222. Acesso em 15 jul. 2024.

IBGE. *Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal 2018*. Rio de Janeiro: Instituto Brasileiro de Geografia e Estatística, 2020. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101705_informativo.pdf>. Acesso em 04 out. 2023.

IBM. "*O que é aprendizado de máquina (ML)?*". Disponível em: <https://www.ibm.com/br-pt/topics/machine-learning>. Acesso em: 05 ago. 2023.

JØRGENSEN, R. F. Rights talk: in the kingdom of online giants. In*: Human rights in the age of platforms*. JØRGENSEN, R. F. Cambridge: The MIT Press, 2019.

JUNQUILHO, T. A. *Inteligência artificial no Direito*: limites éticos. São Paulo: JusPodium, 2022.

KLARE, B.; BURGE, M. J.; KLONTZ, J. C.; VORDER BRUEGGE, R. W.; JAIN, A. K. Face recognition performance: role of demographic information. In: *IEEE Transactions on Information Forensics and Security*, v. 7, n. 6, p. 1789-1801, 2012. https://doi.org/10.1109/TIFS.2012.2214212.

LIMA, P. G. C.; ROMANELLI, L. L. A cadeia de custódia a partir da reforma do CPP: atividade probatória de segundo grau. *Revista do Ministério Público Militar*, Brasília, v. 48, n. 34, p. 1-38, 2021. https://revista.mpm.mp.br/rmpm/article/view/81.

LOPES JR., Aury. *Direito processual penal*. São Paulo: Saraiva Educação, 2020.

LYON, D. Cultura da vigilância: envolvimento, exposição e ética na modernidade digital. In*:* BRUNO, F. *et al* (orgs.). *Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018.

MATIDA, J. A cadeia de custódia é condição necessária para a redução dos riscos de condenações de inocentes. *Revista da Defensoria Pública do Estado do Rio Grande do Sul*, Porto Alegre, n. 27, p. 17-26, 2021. Disponível em https://revista.defensoria.rs.def.br/defensoria/article/view/269. Acesso em 20/07/2024.

MEHOZAY, Y.; FISHER, E. The epistemology of algorithmic risk assessment and the path towards a non-penology penology. *Punishment & Society*, Londres, v. 21, n. 5, 2019. https://doi.org/10.1177/1462474518802336.

MELO, L. B. Fake news sobre a covid-19: como o discurso digital em agências de fact-checking combate a infodemia. In: *Anais do XII workshop sobre aspectos da interação humano-computador na web social (WAIHCWS)*, Porto Alegre, v. 12, p. 41-48, 2021. https://doi.org/10.5753/waihcws.2021.17543.

MENDES, C. H. F.; VECHI, F. Tecnovigilância e controle e(m) tempos securitários: quem são os alvos?. In*:* SABARIEGO, J.; AMARAL, A. J do.; SALLES, E. B. C. *Algoritarismos*. São Paulo: Tirant lo blanch, 2020.

MENDES, L. S.; MATTIUZZO, M.; FUJIMOTO, M. T. Discriminação algorítmica à luz da lei geral de proteção de dados. In: DONEDA, D. *et al* (coord.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

MENEZES, J. B. de.; COLAÇO, H. S. Quando a lei geral de proteção de dados não se aplica? In: TEPEDINO, G.; FRAZÃO, A.; OLIVA, M. D. (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019.

MORAES, F. de. *Policiamento preditivo e aspectos constitucionais*. Belo Horizonte: Dialética, 2022.

MOROZOV, E. *Big tech*: a ascensão dos dados e a morte da política. São Paulo: Ubu, 2018.

PASTORE, A. M.; FONSECA, M. A. C. da. Cadeia de custódia de provas digitais nos processos do direito administrativo sancionador com a adoção da tecnologia blockchain. *Cadernos técnicos da CGU*, Brasília, v. 3, p. 97-109, 2022. Disponível em: <https://revista.cgu.gov.br/Cadernos_CGU/article/view/597>. Acesso em 20 jul. 2024.

PAVEAU, M. A. *A análise do discurso digital*: dicionário das formas e das práticas. Campinas: Pontes, 2021.

PRADO, G. *A cadeia de custódia da prova no processo penal*. Rio de Janeiro: Marcial Pons, 2021.

PRADO, G. *Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital*. Disponível em: <https://geraldoprado.com.br/artigos/breves-notas-sobre-o-fundamento-constitucional-da-cadeia-de-custodia-da-prova-digital/>. Acesso em: 20 jul. 2024.

PRADO, G. *Notas sobre proteção de dados, prova digital e o devido processo penal - parte I*. Disponível em: <https://www.conjur.com.br/2020-ago-18/geraldo-prado-protecao-dados-prova-digital-devido-processo-penal>. Acesso em 05 out. 2023.

PRADO, G. *Notas sobre proteção de dados, prova digital e o devido processo penal — parte II*. Disponível em: <https://www.conjur.com.br/2020-ago-25/geraldo-prado-dados-prova-digital-devido-processo-penal-parte-ii>. Acesso em 05 out. 2023.

PRADO, G. *Notas sobre proteção de dados, prova digital e o devido processo penal — parte III*. Disponível em: <https://www.conjur.com.br/2020-ago-26/geraldo-prado-dados-prova-digital-devido-processo-penal-parte-iii>. Acesso em 05 out. 2023.

RIOS, R. R.; SILVA, M. C. Justiça criminal e algoritmos computacionais na predição de comportamentos: exigências constitucionais e impactos discriminatórios a partir da experiência estadunidense. *Revista judicial brasileira*, Brasília, v. 1, n. 1, p. 61-90, 2021. https://doi.org/10.54795/rejub.n.1.77.

SCALCON, R.; QUITO, C. Intervenções estatais sobre a autodeterminação informacional para fins de persecução penal: limites e desafios. In: *Revista do Advogado*, São Paulo, n. 160, p. 59-65, 2023.

SCIENTIFIC AMERICAN. *How NIST tested facial recognition algorithms for racial bias*. Disponível em: < https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias/>. Acesso em 01 ago. 2023.

SILVA SANCHEZ, J. M. *A expansão do direito penal*: aspectos da política criminal nas sociedades pós-industriais. São Paulo: Revista dos Tribunais, 2011.

SILVA, A. C. F.; LOPES, M. A. P. Nos caminhos do digital, formações discursivas e(m) tecnodiscursos: uma análise de postagens no twitter sobre a legalização do aborto. *Porto das Letras*, Palmas, v. 9, n. 1, p. 199-159, 2023. Disponível em: <https://sistemas.uft.edu.br/periodicos/index.php/portodasletras/article/view/15611>. Acesso em 27 jun. 2023.

SILVA, M. C. *Encarcerando o futuro*: prisão preventiva, reiteração delitiva e avaliação atuarial de risco. Porto Alegre: Yoyô ateliê gráfico, 2020.

STALDER, F.; LYON, D. Electronic identity cards and social classification. In: LYON, D. *Surveillance as social sorting*: privacy, risk, and digital discrimination. Londres: Routledge, 2003.

STEWART, T. A. *Capital intelectual*: a nova vantagem competitiva das empresas. Rio de Janeiro: Campus, 1998.

TAURION, C. *Big data*. Rio de Janeiro: Brasport livros e multimídia Ltda., 2013.

VIEIRA, R. S. *Paridade de armas no processo penal*: do conceito à aplicação no direito processual penal brasileiro. Dissertação (Mestrado em Direito) – Universidade de São Paulo, São Paulo, 2013.

VIEIRA, A. *et al*. Dados biométricos e tecnologia: o panóptico dos dias atuais: as novas tecnologias de identificação facial. In: *Trincheira democrática, ano 4, n. 16*. Salvador: Instituto Baiano de Direito Processual Penal, 2021.

WEXLER, R. Assimetrias de privacidade. In: CRUZ, F. B.; SIMÃO, B. (orgs.). *Direitos fundamentais e processo penal na era digital*. São Paulo: Internetlab, 2021.

YOUNG, J. *A sociedade excludente*: exclusão social, criminalidade e diferença na modernidade recente. Rio de Janeiro: Revan, 2002.

ZUBOFF, S. *The age of surveillance capitalism*: the fight for a human future at the new frontier of power. Nova Iorque: Public affairs, 2019.

Authorship information

Andrey Bruno Cavalcante Vieira. Mestre em Direito Público pela Universidade Federal de Alagoas, pós-graduado em Direito Penal e Processo Penal Aplicados pela EBRADI, bacharel em Direito pela Universidade Federal de Alagoas, advogado. andrey.vieira10@gmail.com

Hugo Leonardo Rodrigues Santos. Professor da graduação e pós-graduação (mestrado) em direito da Universidade Federal de Alagoas (UFAL), doutor e mestre em direito pela Universidade Federal de Pernambuco (UFPE), cocoordenador do grupo de pesquisas biopolítica e processo penal. hugo.santos@fda.ufal.br

Additional information and author's declarations (*scientific integrity*)

Conflict of interest declaration: the authors confirm that there are no conflicts of interest in conducting this research and writing this article.

Declaration of authorship: all and only researchers who comply with the authorship requirements of this article are listed as authors; all coauthors are fully responsible for this work in its entirety.

- *Andrey Bruno Cavalcante Vieira*: conceptualization, methodology, data curation, investigation, writing – original draft, writing – review and editing, final version approval.
- *Hugo Leonardo Rodrigues Santos*: conceptualization, methodology, writing – final draft, validation, writing – review and editing, final version approval.

Declaration of originality: the authors assure that the text here published has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; they also attest that there is no third-party plagiarism or self-plagiarism.

Editorial process dates (https://revista.ibraspp.com.br/RBDPP/about)

- Submission: 21/07/2024
- Desk review and plagiarism check: 10/08/2024
- Review 1: 19/08/2024
- Review 2: 21/08/2024
- Review 3: 26/08/2024
- Transfer to V11N1: 25/10/2024
- Preliminary editorial decision: 30/12/2024
- Correction round return: 10/01/2025
- Final editorial decision: 10/02/2025

Editorial team

- Editor-in-chief: 1 (VGV)
- Reviewers: 3

How to cite (ABNT Brazil):

VIEIRA, Andrey B. C.; SANTOS, Hugo L. R. Investigação criminal e tecnologias digitais: algumas reflexões sobre o policiamento preditivo e a admissibilidade de provas digitais. *Revista Brasileira de Direito Processual Penal*, v. 11, n. 1, e1072, jan./abr. 2025. https://doi.org/10.22197/rbdpp.v11i1.1072