III ENCONTRO VIRTUAL DO CONPEDI

CRIMINOLOGIAS E POLÍTICA CRIMINAL II

GRASIELLE BORGES VIEIRA DE CARVALHO

GUSTAVO NORONHA DE AVILA

MATHEUS FELIPE DE CASTRO

C928

Criminologias e política criminal II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Grasielle Borges Vieira De Carvalho; Gustavo Noronha de Avila; Matheus Felipe de Castro – Florianópolis: CONPEDI, 2021.

Inclui bibliografia
ISBN: 978-65-5648-347-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: segurança humana para a democracia

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Criminologias. 3. Política criminal. III Encontro Virtual do CONPEDI (1: 2021 : Florianópolis, Brasil).

CDU: 34

CONPEDI

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

III ENCONTRO VIRTUAL DO CONPEDI

CRIMINOLOGIAS E POLÍTICA CRIMINAL II

Apresentação

APRESENTAÇÃO

Na segunda tarde de Inverno do ano pandêmico de 2021, durante os trabalhos do III Encontro Virtual do Conpedi, nos reunimos para discutir sobre temas persistentes e emergentes das Criminologias e da Política Criminal. Foram representados Programas de Pós-graduação do Brasil inteiro em trabalhos que demonstraram uma perspectiva bastante heterogênea e plural das ciências criminais.

Em nosso primeiro trabalho apresentado, Carolina Carraro Gouvea pretendeu analisar a atuação do Sistema Interamericano de Direitos Humanos e sua efetividade. A partir de um referencial internacionalista, sugere novas estratégias como mecanismo específico de proibição da tortura neste âmbito.

A seguir, Mariana Engers Arguello discutiu os diferentes problemas do sistema carcerário brasileiro em meio à pandemia. Além dos argumentos criminológicos, também foram analisadas decisões de decretação de prisões preventivas que abordaram a questão da Covid-19.

Angélica da Silva Corrêa trabalhou o tema do racismo estrutural e a violência policial no Brasil. Desde os dados do último Mapa da Violência, foram analisados os índices de homicídio em relação aos negros, pobres e periféricos.

Ainda no campo das interseccionalidades, Thais Janaina Wenczenovicz, Émelyn Linhares e Marlei Angela Ribeiro dos Santos, analisam os efeitos do cárcere em relação aos povos indígenas n Brasil. Para tanto, partem de uma metodologia quali-quantitativa para demonstrar o quanto o cárcere costuma ser especialmente violento em relação a nossa população originária.

Adentrando a linha dogmático-penal com referencial da política criminal, Alessandra Pangoni Balbino Santos enfrenta a persistente questão da intervenção mínima no Direito Penal brasileiro. Também na perspectiva político-criminal, Marco Adriano Tamos Fonsêca e Roberto Carvalho Veloso discutem o enfrentamento da corrupção.

Luana Rodrigues Meneses de Sá e Andréa Flores analisam as relações entre a Criminologia Crítica e os Direitos Humanos. Concluem pela necessária renovação das estruturas de poderes relacionadas ao processo de criminalização, com o reforço de uma perspectiva mínima de direito penal.

Em sequência, a (im)possibilidade de recepção do acordo de não persecução penal no processo brasileiro é tratado por Júlia Faipher e Bartira Macedo Miranda. A expansão dos espaços de consenso é critica pela dificuldade em compatibilizá-los com as garantias fundamentais individuais.

Discutindo a influência transversal da dignidade humana ao sistema pena, Hamilton da Cunha Iribure Júnior, Rodrigo Pedroso Barbosa e Douglas de Morais Silva, trabalham o persistente tema da expansão do Direito Penal. Concluem que este movimento traz sérios riscos de violação aos direitos fundamentais, representando uma violência estatal em regra desproporcional em relação à própria violação.

Melina de Albuquerque Wilasco e Salo de Carvalho trabalham a partir da seguinte pergunta: a Justiça Restaurativa pode funcionar como uma alternativa à prisão? Desde que uma perspectiva crítica seja adotada, é possível abolir o sistema penal a partir de uma nova cultura forjada pela Justiça Restaurativa Crítica.

A apresentação seguinte contou com as aproximações entre Inteligência Artificial e a conduta em direito penal. Bruna Azevedo de Castro, a partir da teoria de Juarez Tavares, estabelece critérios de imputação de forma a evitar a responsabilidade objetiva.

Lorena Melo Coutinho e Priscilla Macêdo Santos discutem o problema do policiamento atuarial feito por algoritmos que poderiam analisar os prognósticos de riscos na segurança pública. Desde uma técnica bibliográfica-documental, apresentam as possíveis dificuldades e riscos para a sua utilização na prática.

Também sobre a Inteligência Artificial e seus efeitos é o texto apresentado por Ana Lúcia Tavares Ferreira. O artigo analisa essas repercussões aos direitos e garantias fundamentais do acusado.

Por fim, o tema da Justiça Restaurativa Crítica volta a ser tratado por Camila Diógenes de Mendonça e Juliana Trindade Ribeiro Pessoa Pordeus. As autoras tratam de uma experiência concreta, em Novo Hamburgo-RS, avaliando a possibilidade de estarmos diante de uma verdadeira Justiça Restaurativa.

Foi uma tarde rica em discussões e de muitos reencontros, ainda que virtuais. Esperamos que os textos aqui contidos possam reverberar, provocando novas pesquisas e diálogos!

Boa leitura!

Espaço Virtual, Junho de 2021.

Grasielle Borges Vieira De Carvalho (Universidade Tiradentes/SE)

Gustavo Noronha de Ávila (UNICESUMAR)

Matheus Felipe de Castro (UFSC/UNOESC)

INTELIGÊNCIA ARTIFICIAL E SISTEMA PENAL: PROTEÇÃO DE DIREITOS FUNDAMENTAIS E MECANISMOS DE CONTROLE

ARTIFICIAL INTELLIGENCE AND CRIMINAL JUSTICE SYSTEM: PROTECTION OF FUNDAMENTAL RIGHTS AND CONTROL MECHANISMS

Ana Lúcia Tavares Ferreira

Resumo

As tecnologias de inteligência artificial têm sido crescentemente utilizadas nos sistemas penais, contribuindo para o melhor desempenho de atividades policiais e judiciais. A Lei 13.675/2018 introduziu as tecnologias de inteligência artificial no sistema penal brasileiro. Entretanto, a utilização das novas tecnologias pressupõe o acesso dados pessoais de indivíduos, implicando risco de lesão aos direitos fundamentais. O artigo descreve as experiências de inteligência artificial no sistema penal e seu impacto sobre os direitos fundamentais, demonstrando a necessidade de investigação dos modelos adotados no Brasil e desenvolvimento de uma moldura teórica e normativa para regulamentação dos modelos adotados no sistema penal brasileiro.

Palavras-chave: Algoritimos, Direitos humanos, Policiamento preditivo, Reconhecimento facial, Identificação biométrica

Abstract/Resumen/Résumé

Artificial intelligence technologies have been increasingly used in criminal systems, contributing to the better performance of police and judicial activities. Law 13.675/2018 introduced artificial intelligence technologies in the Brazilian penal system. However, the use of new technologies presupposes access to personal data of individuals, implying a risk of violation to fundamental rights. The article describes the experiences of artificial intelligence in the penal system and its impact on fundamental rights, showing the need to investigate the models adopted in Brazil and the development of a theoretical and normative framework for the regulation the models adopted in the Brazilian penal system.

Keywords/Palabras-claves/Mots-clés: Algorithms, Human rights, Predictive policing, Facial recognition, Biometric identification

1. Introdução

A evolução da ciência de dados e as tecnologias de inteligência artificial (IA) vem transformando diversas atividades humanas, desde o desempenho de tarefas cotidianas até o desenvolvimento de pesquisas científicas e políticas governamentais e militares, desde a década de 1990.

As tecnologias de IA tem repercutido também no âmbito da segurança pública e do sistema penal, podendo-se observar, desde o final do Século XX, uma tendência de crescente substituição de decisões humanas por cálculos produzidos por computadores e robôs, em tarefas típicas do controle de criminalidade, persecução e jurisdição penal.

Os diferentes modelos tem sido objeto de intensos questionamentos e criticas, além de investigações, pesquisas empíricas, avaliações externas e auditorias profissionais, apontando-se a necessidade de uma regulação legal específica, destinada a garantir a proteção dos direitos fundamentais contra possíveis excessos praticados pelo Estado no uso das novas tecnologias.

A utilização das ferramentas de AIP no Sistema Penal brasileiro tem como marco a introdução, pela Lei 13.675 de 11 de junho e 2018, do Sistema Único de Segurança Pública (SUSP), da Política Nacional e Segurança Publica e Defesa Social (PNSDPS) e do Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, e Material Genético, de Digitais e de Drogas (SINESP).

O artigo trata da utilização das tecnologias de IA no sistema penal, buscando demonstrar a necessidade de elaboração de moldura teórica e arcabouço normativo para proteção dos direitos fundamentais dos indivíduos envolvidos.

No primeiro tópico, será fornecida uma sucinta descrição das tecnologias de IA utilizadas nos sistemas penais, para o desenvolvimento de atividades policiais e judiciais.

No segundo tópico, serão apresentadas as experiências de policiamento preditivo desenvolvidos a partir de modelos algorítmicos e seu impacto sobre os direitos fundamentais dos indivíduos.

A utilização da inteligência artificial nos sistemas de identificação biométrica será abordada na terceira seção, apontando-se, também nesse caso, a possibilidade de lesão aos direitos fundamentais dos indivíduos implicados.

Na quarta seção será apresentada a experiência brasileira no que diz respeito à utilização de inteligência artificial, demonstrando-se a deficiência da atual normativa brasileira para a efetiva proteção dos direitos fundamentais.

Nas considerações finais, serão extraídas algumas conclusões a partir dos temos abordados ao longo do artigo, apontando-se direcionamentos para o futuro encaminhamento do tema.

2. Inteligência artificial e Sistema Penal

O impacto da ciência de dados sobre o sistema penal intensificou-se nas duas últimas décadas, devido ao recente desenvolvimento das tecnologias de inteligência artificial (IA),[1] com capacidade para o gerenciamento e processamento de grande volume de dados, possibilitando uma rápida e precisa tomada de decisões em situações complexas.

As tecnologias de IA tem sido incorporadas aos sistemas penais em diversos países, nas atividades policiais (*policing*), para a prevenção e investigação da criminalidade (Inteligência Artificial Policial ou IAP), e judiciais (Inteligência Artificial Judicial ou IAJ) para a atribuição de responsabilidade criminal, determinação da medida da pena, fixação de regime (*sentencing*) e análise e previsão de risco (*risk assessment*).

No que se refere à IAJ, pode-se identificar a utilização de ferramentas que auxiliam o juiz na valoração das provas ou organização das razões decisórias na fase de fundamentação das decisões judiciais.

Além disso, utiliza-se a IAJ como instrumento de medição de risco e previsão de comportamentos futuros para fins de embasamento de decisões judiciais de determinação de quantidade de pena, regime de execução, liberdade provisória ou livramento condicional, por meio da busca de padrões e relações entre variáveis em um conjunto de dados (MIRÓ LLINHARES, 2018).

[1] Sistemas de Inteligência Artificial sào aqueles que agem para a abordagem de objetivos complexos, nos planos físico e digital, por meio de coleta e interpretação de dados estruturados ou desestruturados. (CORNELIUS, 2020).

3. Inteligência artificial e policiamento preditivo.

A IAP vem contribuindo para o desenvolvimento de novas ferramentas de policiamento preditivo (Predpol), que consistem na aplicação de técnicas analíticas quantitativas para identificar prováveis alvos de intervenção policial e prevenir crimes por meio de previsões estatísticas (WILSON, 2018, p.109).

Assim, antigos modelos geoespeciais de previsão de concentração de futuros crimes (*hotspots*) por meio de estatísticas computadorizadas (COMStat) vem sendo substituídos por instrumentos de IA preditivos, que utilizam as técnicas de megadados para investigar condutas passadas e acessar a fase preparatória do crime, identificando não só os *hotspots*, mas uma lista de prováveis autores de crimes, gerada por algoritmos (as chamadas *heatlists*) (ZAVRŠNIK , 2020).

A maioria das novas tecnologias de policiamento preditivo foram inicialmente desenvolvidas nos EUA (WALTER;MACINNIS;PRICE, 2013) e sua adoção ampliou-se consideravelmente nas duas últimas décadas com a implementação de diversos modelos em países da Europa (HARDYNS; RUMMENS, 2018) (Alemanha, Áustria, Bélgica, Dinamarca, Espanha, França, Itália, Reino Unido e Suécia) e América Latina (Uruguai, Brasil) (ALTENHAIN, 2018).

Os sistemas europeus são formulados na sua maioria com ênfase no espaço-tempo (hotspots), embora também sejam adotadas tecnologias baseadas em dados reativos à identificação de futuros autores de crimes (listas de calor).

Dentre as experiências europeias, as mais avançadas são as seguintes:

Table 1. Experiências de policiamento preditivo na Europa

País	Sistema	Ano	Empresa/Órgão
França	I2 Analyst's Notebook	2005	IBM
Itália	KeyCrime	2007	Milan Police HQ
Reino Unido	Predpol	2013	Predpol
Países Baixos	Crime Antecipation System (CAS	2013	Amsterdam Police Department
Alemanha	Precobs	2014	IfmPt

Alemanha	Skala	2015	State Investigation Office of North Westphalia and IBM

A utilização da IAP no policiamento preditivo apresenta ainda mais utilidade no que diz respeito à criminalidade cibernética, na medida em que contribui para a identificação de vulnerabilidades em infraestruturas digitais que possibilitam invasões e outras ameaças, além de fornecer ferramentas para analisar os fatores humanos dos crimes cibernéticos e investigar o papel desempenhado pelas redes sociais *online* nos processos de radicalização que resultam em outras formas de criminalidade, como o terrorismo.

As tecnologias de IA tem sido celebradas como uma estratégia perfeita de prevenção ao crime por órgãos estatais de segurança, desenvolvedores de software privado e parte da mídia, especialmente nos EUA, onde o modelo foi adotado pela primeira vez.

Embora seja indiscutível o potencial da IA para a melhoria de desempenho dos órgãos do Sistema Penal e, mais especificamente, da Segurança Pública, a utilização dessas ferramentas tecnológicas pode implicar restrições significativas aos direitos fundamentais dos indivíduos envolvidos (WILSON, 2020).

Além disso, a maioria das experiências de utilização da IA por órgãos de segurança não foram avaliados ou testados por profissionais externos. A falta de validação confiável leva a questionamentos sobre sua eficiência e promove desconfiança e hesitação (BENNETT MOSES, 2018).

Uma das principais preocupações é o risco de violação ou erosão dos direitos fundamentais pelo uso de sistemas de IA pelas agências estatais para fins de investigação, identificação criminal e análise preditiva.

A revisão da literatura mostra que diversos estudos abordaram questões relacionadas à potencial ameaça do policiamento preditivo aos direitos fundamentais e à necessidade do desenvolvimento de um quadro normativo para orientar a futura regulação pelos legisladores.

O uso de dados pessoais no policiamento preditivo para fins de segurança e identificação ou investigações criminais implica consequências graves, podendo resultar na submissão do indivíduo à vigilância por longo prazo, persecução criminal ou mesmo a imposição de prisão preventiva.

Além disso, a necessidade de uso dados para informar modelos computacionais preditivos desencadeou o rápido desenvolvimento de sistemas de vigilância em massa (que dependem de tecnologias de IA para detectar correlação e padrões) para coleta e retenção de dados (conteúdos de comunicações eletrônicas e metadados, dados de redes sociais, dados de

hábitos do consumidor, etc.) em parceria com empresas privadas, sem o consentimento ou conscientização do indivíduo alvo.

Modelos de previsão computacional são frequentemente construídos para trabalhar com base em suposições para designar um risco maior para áreas geográficas, grupos ou indivíduos únicos, que serão colocados sob vigilância, mesmo que nunca tenham cometido um crime (GLESS, 2018).

Nesse contexto, os algoritmos preditivos implicam violação ao princípio da presunção de inocência e legalidade ou a proibição da sanção penal sem lei *(nulla poena sine lege*).

Além disso, a previsão de risco pode afetar diretamente o sistema de justiça criminal, resultando na inversão do ônus da prova no processo penal, já que as determinações preditivas produzidas por modelos computacionais opacos são praticamente impossíveis de contestação pelo indivíduo afetado.

O uso inadequado do software de predição também pode criar o risco de discriminação social ou racial, uma vez que um indivíduo pode ser indicado como suspeito por causa de alguns fatores pessoais ou comportamentais circunstanciais, como desemprego, dívidas financeiras, residir em um bairro considerado um local de crimes, etc (SCHLEHAHN, 2015).

Mesmo que os modelos preditivos sejam projetados para excluir certas informações pessoais da análise, as tecnologias de aprendizado de máquina podem desenvolver e tomar decisões autônomas, incluindo mais variáveis, independentemente do treinamento inicial do *designer*.

Além disso, os dados inseridos em modelos computacionais não refletem necessariamente a realidade da atividade criminosa, devido à natureza seletiva do sistema de justiça criminal.

O policiamento preditivo pode levar, portanto, ao uso excessivo de policiamento direcionado a certos crimes ou indivíduos (super policiamento), negligenciando outras atividades criminosas relevantes (sub-policiamento).

O uso do policiamento preditivo em si também pode levar a resultados discriminatórios, mesmo que os algoritmos não sejam tendenciosos. As previsões do algoritmo levam ao direcionamento das patrulhas e ao aprimoramento da vigilância em áreas de crimes, elevando os níveis de registros criminais nessa mesma área, que produzirá mais dados coletados e analisados pelo software, perpetuando a decisão de discriminação (BENNETT MOSES, 2018).

A opacidade da tomada de decisão automatizada também o direito fundamental de acesso à justiça. Como o Estudo do Comitê de Especialistas em Intermediários da Internet (MS-

NET (2016)06) sobre as Dimensões de Direitos Humanos das Técnicas Automatizadas de Processamento de Dados (em particular algoritmos) e possíveis implicações regulatórias (CONSELHO DA EUROPA, 2016) afirma:

> Processos automatizados de tomada de decisão geram a desafios particulares para a capacidade dos indivíduos de obter um remédio eficaz. Estes incluem a opacidade da decisão em si, sua base, e se os indivíduos consentiram com o uso de seus dados na tomada dessa decisão ou mesmo estão cientes da decisão que os afeta. A dificuldade em atribuir a responsabilidade pela decisão também complica a identificação da autoridade competente para revertê-la.

Os pressupostos sobre os quais se baseia a penologia algorítmica representam uma mudança de paradigma no que diz respeito às categorias básicas e princípios sobre os quais foram construídas teorias criminais.

Modelos de policiamento preditivo são projetados com base na suposição de que o comportamento humano pode ser previsto por algoritmos com maior eficiência do que por cálculos estatísticos derivados de modelos teóricos.

Esse pressuposto evoluiu da lógica penal da penologia gerencial, modelo teórico que mesclou conceitos da criminologia clássica e positivista, para desenvolver um sistema baseado na avaliação de riscos e na incapacitação seletiva.

Os modelos estatísticos de avaliação de risco sempre foram baseados em pesquisas empíricas desenvolvidas a partir de determinada moldura teórica, levando em consideração fatores de risco associados a informações pessoais circunstanciais, como status de emprego, abuso de substâncias, entre outros.

A previsão algorítmica de crimes e as avaliações de risco, no entanto, baseiam-se no pressuposto de que o comportamento pode ser previsto com base na constatação de correlação e padrões, conceito que representa uma ruptura com a antiga avaliação atuarial, no sentido de que se afasta dos modelos teóricos criminológicos.

Os modelos de previsão orientados por dados são teóricos e determinísticos, pois negam qualquer possibilidade de racionalidade, melhoria, tratamento ou correção. Em outros termos, o uso do policiamento preditivo para identificação de possíveis reincidentes tem potencial para justificar o encarceramento ou vigilância prolongados baseados exclusivamente em correlações e padrões e no pressuposto de que os indivíduos não têm capacidade de mudança, conflitando assim com o direito à reintegração na sociedade de autores de crimes pretéritos (SCHLEHAHN, 2015).

4. Inteligência artificial e identificação biométrica remota

Os sistemas de IAP também tem sido utilizados no âmbito da segurança pública, por meio de algoritmos de análise de dados biométricos (impressões digitais, leitura da íris, fotografias, perfil genético, padrão de voz, etc.) para fins de identificação e investigação criminal.

Destacam-se, nesse contexto, as tecnologias de reconhecimento facial automatizado, que possibilitam a análise de imagens (estáticas ou de câmeras de vigilância, em tempo real) para fins de comparação com fotografias armazenadas em volumosos bancos de imagens, possibilitando a identificação de pessoas em caso de dúvida sobre a identidade, ou a captura de procurados pela polícia, por exemplo.

Trata-se de um sistema de algoritmos complexos que traduzem as características faciais (o tamanho do nariz ou da boca, o ângulo e distância entre os traços da face etc.) em dados numéricos e comparam as informações de cada imagem, apontando uma maior ou menor probabilidade de coincidência entre os elementos comparados.

A coleta e armazenamento de dados biométricos para fins de identificação e investigação criminal é uma das atividades tradicionalmente desenvolvidas no âmbito da segurança pública, nos limites da proteção dos direitos fundamentais do indivíduo, estabelecidos pela Constituição e respectiva regulamentação legal.

Assim, por exemplo, no Brasil, o art. 5º, inciso LVIII da Constituição da República assegura ao civilmente identificado o direito de não ser criminalmente identificado, salvo nas hipóteses legais, as quais foram estabelecidas na Lei 12.037/09.

As formas de identificação autorizadas pela Lei 12.037/09 ─ coleta de impressões digitais e de material biológico para a obtenção do perfil genético ─ constituem métodos de identificação biométrica imediata (IBI), ou seja, meio utilizado para fins de verificação da identidade de pessoa determinada, em caso de dúvida fundada sobre os dados informados, geralmente no contexto de detenção, mediante proximidade física com o indivíduo submetido à verificação e com a sua ciência.

O reconhecimento facial, por outro lado, constitui um dado biométrico de nova geração (assim como a geometria da mão, leitura de íris, padrões vasculares, hormônios, marcha etc.), que possibilita a identificação biométrica remota (IBR), isto é, voltada para um número indeterminado de indivíduos, no espaço público, sem aviso prévio ou consentimento, de forma contínua e ininterrupta.

A normativa atual sobre a coleta de dados biométricos orienta-se de acordo os modelos tradicionais de IBI, salvaguardando os direitos fundamentais de pessoas individualizadas (com ciência do indivíduo e em episódios isolados) contra coleta e armazenamento de dados pessoais sensíveis.

Entretanto, as novas tecnologias possibilitaram ao Estado a prática IBR de um número indeterminado de pessoas que transitam nas vias públicas, sem seu consentimento ou mesmo ciência, independentemente de qualquer suspeita ou mandado judicial.

Além disso, os algoritmos de reconhecimento facial são alimentados por imagens extraídas de bases de dados da polícia e outros órgãos governamentais, implicando o acesso aos dados pessoais de um universo ilimitado de pessoas.

Isso significa que um *software* que tenha acesso ao banco de dados do Departamento de Trânsito, por exemplo, pode submeter todos os cidadãos com licença para dirigir a um ato de reconhecimento, sem que eles tenham ciência de que estão sendo identificados para fins de investigação criminal.

Assim, a IBR por meio de reconhecimento facial pode importar lesão aos direitos fundamentais dos indivíduos por ela afetados, destacando-se, principalmente, o potencial violador quanto ao direito à privacidade, à não discriminação, à presunção de inocência, a não obrigatoriedade de autoincriminação e ao devido processo legal.

A regulamentação legal atual não está apta a salvaguardar os direitos fundamentais protegidos pela Constituição contra os excessos praticados por meio das novas tecnologias e métodos de IBR, sendo necessário o desenvolvimento de uma moldura teórica capaz de estabelecer parâmetros e limites para a utilização das tecnologias de reconhecimento facial automatizado.

Não se trata de excluir inteiramente a possibilidade de utilização das tecnologias de inteligência artificial no reconhecimento facial. Tem-se apontado que o nível de violação de direitos fundamentais varia conforme o modelo adotado, em função de variáveis como a quantidade de pessoas cuja imagem é captada, o tamanho e a origem dos bancos de dados utilizados, a ciência prévia aos envolvidos, o grau de exatidão dos resultados produzidos pelo software, entre outras.

É preciso, em vez disso, avaliar os diversos modelos adotados nas experiências e projetos em andamento ou em vias de implementação, no que se refere aos níveis de lesão aos direitos fundamentais, apontando mecanismos de controle e proteção dos indivíduos.

Para isso, é necessário desenvolver uma moldura teórica que forneça princípios, normas e diretrizes que sirvam como parâmetro para a avaliação das novas tecnologias, além da introdução de normas legais adequadas à proteção dos direitos fundamentais.

5. Inteligência Artificial Policial e Identificação Biométrica Remota no Brasil

A utilização das ferramentas de AIP no Sistema Penal brasileiro tem como marco a introdução, pela Lei 13.675 de 11 de junho e 2018, do Sistema Único de Segurança Pública (SUSP), da Política Nacional e Segurança Publica e Defesa Social (PNSDPS) e do Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, e Material Genético, de Digitais e de Drogas (SINESP) (BRASIL, 2018).

A partir desse marco regulatório inicial, desenvolveu-se o projeto SINESP BIG DATA e Inteligência Artificial para Segurança Pública, no âmbito do Ministério da Justiça e Segurança Pública (MJSP), em convênio dom o Departamento de Computação da Universidade Federal do Ceará (UFC), inspirado nas experiências da Secretaria de Segurança Pública e Defesa Social do Ceará (MJSP, 2020).

O produto será utilizado nos estados que formarão o projeto-piloto Em Frente, Brasil: Espírito Santo, Goiás, Pará, Paraná e Pernambuco. A intenção é que o projeto chegue a mais oito estados até o fim do ano: Acre, Alagoas, Amapá, Piauí, Rio Grande do Norte, Roraima, Sergipe e Tocantins.

O desenvolvimento do SINESP BIG DATA objetiva disponibilizar soluções de segurança pública, dentre as quais destacam-se as seguintes: i) a criação de uma plataforma Big Data e painel analítico; utilizando os dados do SINESP; ii) georreferenciamento das ocorrências criminais; iii) rastreamento de objetos móveis, monitoramento inteligente para rápida intervenção, acompanhamento de ocorrências criminais, detecção por sensores, câmeras de segurança, viaturas e agentes de pessoas com restrição de liberdade que fazem uso de tornozeleiras eletrônicas; iv) fornecer um painel analítico de relacionamentos que compõem o comportamento delitivo (LEMES, 2019).

No que se refere às tecnologias de reconhecimento facial, foram implementadas várias experiências no Brasil em 2019, nos estados do Rio de Janeiro, Bahia e São Paulo, com recursos do Fundo Nacional de Segurança Pública, de acordo com a Portaria 792/2019 do MJSP. Além

disso, Espírito Santo, Minas Gerais, Pará e Distrito federal apresentaram projeto de implementação futura.

Segundo o relatório elaborado pela Rede de Observatórios de Segurança, foram realizadas 151 prisões em decorrência da utilização dos sistemas de reconhecimento facial nos estados, sendo essas prisões distribuídas da seguinte forma (NUNES, 2020):

Tabela 1 – Prisões efetuadas em decorrência do uso de tecnologias de reconhecimento facial automatizado.

Estado	**Proporção de prisões**
Bahia	51,7%
Rio de Janeiro	37,1%
Santa Catarina	7,3%
Paraíba	3,3%

Apesar do reconhecido potencial de lesão aos direitos fundamentais, a utilização da IA sistema penal brasileiro tem sido objeto de escassa regulamentação.

Além disso, a atual moldura normativa sobre a identificação e investigação criminal é insuficiente no que se refere à proteção dos direitos fundamentais de eventuais violações e riscos produzidos pelas novas tecnologias, não se dispondo, assim, de parâmetros e diretrizes para a sua implantação.

Note-se que nem mesmo a Lei 13.709 de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD) contemplou a matéria, tendo em vista a exclusão expressa, no art. 4º, do tratamento de dados pessoais para fins exclusivos de segurança pública, segurança do Estado e atividades de investigação e repressão de infrações penais, estabelecendo, no § 1º do citado dispositivo, que o tratamento de dados pessoais, nesses casos, será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular.

Também a produção bibliográfica nacional sobre o tema é escassa, podendo-se apontar alguns relatórios que tratam de temas específicos, com grande ênfase nos sistemas de reconhecimento facial, além de artigos doutrinários (FRANCISCO, HUREL, RIELLI, 2020).

Assim, mostra-se necessários investigar as experiências brasileiras de utilização de tecnologias de inteligência artificial no sistema penal no que se refere às tecnologias utilizadas

e ao nível de violação dos direitos fundamentais, apontando possíveis mecanismos de controle e proteção dos indivíduos afetados.

Faz-se necessária, assim, uma análise abrangente das novas tecnologias na perspectiva jurídica, para o desenvolvimento de parâmetros normativos que possam orientar a implementação de sistemas de IA no âmbito do sistema penal brasileiro, proporcionando a melhoria dos serviços de segurança pública, persecução e justiça penal, sem, contudo, importar desprezo à dignidade humana, postulado fundamental do Estado Democrático de Direito.

Para tanto, é preciso desenvolver um arcabouço teórico destinado ao estabelecimento de parâmetros para avaliação e controle da das novas tecnologias no ordenamento jurídico brasileiro, contribuindo com um aporte teórico para a evolução normativa do tema, por meio da elaboração princípios e diretrizes que poderão orientar a futura regulação da matéria bem como as políticas públicas futuras, de forma a evitar, ou reduzir ao mínimo possível, eventual lesão ou risco de lesão aos direitos fundamentais dos indivíduos afetados.

É necessário também, desenvolver mecanismos de controle da utilização das citadas tecnologias, optando-se por uma abordagem de prevenção de possíveis lesões aos direitos fundamentais.

6. Considerações Finais

As tecnologias de IA tem sido celebradas como uma estratégia perfeita de prevenção ao crime por órgãos estatais de segurança, desenvolvedores de software privado e parte da mídia, porém a utilização dessas ferramentas tecnológicas pode implicar restrições significativas aos direitos fundamentais dos indivíduos envolvidos.

Apesar do reconhecido potencial de lesão aos direitos fundamentais, a utilização da IA sistema penal brasileiro tem sido objeto de escassa regulamentação.

Além disso, a atual moldura normativa sobre a identificação e investigação criminal é insuficiente no que se refere à proteção dos direitos fundamentais de eventuais violações e riscos produzidos pelas novas tecnologias, não se dispondo, assim, de parâmetros e diretrizes para a sua implantação.

Faz-se necessária, assim, o desenvolvimento de parâmetros normativos que possam orientar a implementação de sistemas de IA no âmbito do sistema penal brasileiro, proporcionando a melhoria dos serviços de segurança pública, persecução e justiça penal, sem,

contudo, importar desprezo à dignidade humana, postulado fundamental do Estado Democrático de Direito.

REFERÊNCIAS

ALTENHAIN, C. (n.d.). Tropicalizing Surveillance: How big data policing “migrated” from New York to São Paulo. 14.

AMARAL, Fernando. Introdução à Ciência de Dados. Rio de Janeiro: Altabooks, Edição Kindle. 2006.

ANTONIALLI, Dennys Marcelo. FRAGOSO, Nathalie. MASSARO, Heloisa Maria Machado. Da investigação ao encarceramento: as propostas de incremento do uso da

BATISTA, M. de M., DALLABONA FARINIUK, T. M., & Mello, S. C. B. de. (2016). Smart surveillance em aplicações recentes no Brasil: Um estudo de caso nas cidades de Recife e Curitiba. Revista de Gestão e Secretariado, 7(2), 104–137. https://doi.org/10.7769/gesec.v7i2.549.

BENNETT MOSES, L., & Chan, J. (2018). Algorithmic prediction in policing: Assumptions, evaluation, and accountability. Policing and Society, 28(7), 806–822. https://doi.org/10.1080/10439463.2016.1253695.

BLÜHDORN, I., Butzlaff, F., Deflorian, M., Hausknost, D., & Mock, M. (2020). Nachhaltige Nicht-Nachhaltigkeit: Warum die ökologische Transformation der Gesellschaft nicht stattfindet. transcript-Verlag. https://doi.org/10.14361/9783839454428.

BRASIL. LEI Nº 13.675, DE 11 DE JUNHO DE 2018. Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública, nos termos do § 7º do art. 144 da Constituição Federal; cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS); institui o Sistema Único de Segurança Pública (Susp); altera a Lei Complementar nº 79, de 7 de janeiro de 1994, a Lei nº 10.201, de 14 de fevereiro de 2001, e a Lei nº 11.530, de 24 de outubro de 2007; e revoga dispositivos da Lei nº 12.681, de 4 de julho de 2012. DOU de 12.6.2018.

_____. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados (LGPD). DOU de 15.8.2018.

BURLINGAME, Noreen. NIELSEN, Lars. A Simple Introduction to Data Science. Wickford: New Street Communications, 2012.

CARDOSO, B. de V. (2019). A lógica gerencial-militarizada e a segurança pública no Rio de Janeiro: O CICC-RJ e as tecnologias de (re)construção do Estado. 3, 23.
CÉRÉ, Jean-Paul. RASCAGNÈRES, Joan Miquel. VERGÉS, Etiennes (dir.). Droit pénal et nouvelles technologies. Paris : L'Harmattan, 2015.

CINELLI, V., & Manrique, A. (2019). El uso de programas de análisis predictivo en la inteligencia policial: Una comparativa europea. Revista de Estudios en Seguridad Internacional, 5(2), 1–20. https://doi.org/10.18847/1.10.1.

COMISSÃO EUROPEIA. Livro Branco sobre a inteligência artificial – Uma bordagem europeia virada para a excelência e confiança. Bruxelas, 19 de fevereiro de 2020.

CORNELIUS, Kai. Künstliche Intelligenz", Compliance und sanktionsrechtliche Verantwortlichkeit. Zeitschrift für Internacionale Straferechtsdogmatik. ZIS 2/2020.

de LAAT. Paul B. The disciplinary power of predictive algorithms: a Foucauldian perspective. Ethics and Information Technology (2019) 21:319–329.

FERGUSON, A. G. (2014a). Big Data and Predictive Reasonable Suspicion. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2394683.

FRANCISCO. Pedro Augusto. HUREL, Louise Marie. RIELLI, Mariana Marques. Regulação do Reconhecimento Facial no Setor Público: avaliação de experiências internacionais. Instituto Igarapé. Data Privacy Brasil Research. Junho 2020.

FUSSEY, Pete. MURRAY, Daragh. Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. Human Rights Center. University of Essex, July 2019.

GAFFNEY, C., & ROBERTSON, C. (2018). Smarter than Smart: Rio de Janeiro's Flawed Emergence as a Smart City. Journal of Urban Technology, 25(3), 47–64. https://doi.org/10.1080/10630732.2015.1102423.

GLESS, Sabine. Policiamento preditivo: em defesa dos verdadeiros positivos. Revista Direito GV. V. 16 N. 1, 2020.

HANNAH-MOFFAT, K. (2019). Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates. Theoretical Criminology, 23(4), 453–470. https://doi.org/10.1177/1362480618763582.

HARDYNS, W., & Rummens, A. (2018). Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges. European Journal on Criminal Policy and Research, 24(3), 201–218. https://doi.org/10.1007/s10610-017-9361-2
Knobloch, D. T. (n.d.). Vor di¬e Lage Kommen¬: Predictive Policing in Deutschland. 46.

KOSS, K. K. (n.d.-b). Leveraging Predictive Policing Algorithms to Restore Fourth Amendment Protections in High-Crime Areas in a Post-Wardlow World. 90, 35.

LECLERC, B., & Savona, E. U. (Eds.). (2017). Crime Prevention in the 21st Century. Springer International Publishing. https://doi.org/10.1007/978-3-319-27793-6.

LEMES, Marcelle Martins. Inteligência Artificial, Algoritmo e Policiamento Preditivo no Poder Público Federal Brasileiro. Monografia apresentada no Programa de Graduação da Faculdade de Direito da Universidade de Brasília como requisito à obtenção do título de Bacharel em Direito., Brasília, 2019.

MADENSEN, T., Eck, J. E., United States, Department of Justice, & Office of Community Oriented Policing Services. (2008). Spectator violence in stadiums. U.S. Dept. of Justice, Office of Community Oriented Policing Services. https://purl.fdlp.gov/GPO/LPS114905.

MAGUIRE, M., & John, T. (2006). Intelligence Led Policing, Managerialism and Community Engagement: Competing Priorities and the Role of the National Intelligence Model in the UK. Policing and Society, 16(1), 67–85. https://doi.org/10.1080/10439460500399791.

MEHOZAY, Y., & Fisher, E. (2019). The epistemology of algorithmic risk assessment and the path towards a non-penology penology. Punishment & Society, 21(5), 523–541. https://doi.org/10.1177/1462474518802336.

MIRÓ LLINHARES, Fernando. Inteligencia Artificial y Justicia Penal: más allá de los resultados lesivos causados por robots. Revista de Derecho Penal y Criminología. Núm. 20 (2018).

MJSP. Ministério entrega aos estados primeiras ferramentas de Big Data e Inteligência Artificial para combater a criminalidade. Disponível em https://www.justica.gov.br/news/collective-nitf-content-1566331890.72. Acesso em 07 e setembro de 2020.

MOURAO KANASHIRO, M. (2002). Surveillance Cameras in Brazil: Exclusion, mobility regulation, and the new meanings of security. Surveillance & Society, 5(3). https://doi.org/10.24908/ss.v5i3.3424.

NEW YORK CITY BAR ASSOCIATION. Power, Pervasiveness and Potential: the Brave new World of Facial Recognition through a Criminal Law Lens (and Beyond). August, 2020.

NUNES, Pablo. Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. Disponível em https://www.ucamcesec.com.br/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf. Acesso em 06 de setembro de 2020.

OSWALD, M., Grace, J., Urwin, S., & Barnes, G. C. (2018). Algorithmic risk assessment policing models: Lessons from the Durham HART model and 'Experimental' proportionality. Information & Communications Technology Law, 27(2), 223–250. https://doi.org/10.1080/13600834.2018.1458455.

PAULLI, Tom. Introdução à Inteligência Artificial: Uma Abordagem não Técnica. São Paulo: Novatec, 2020. Edição Kindle.

RICHARDSON, R., Schultz, J., & Crawford, K. (n.d.). Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, And Justice. 30.

SANTOS, R., Nunes, F., Oliveira, M., & Júnior, M. (2017). Um Survey sobre a utilização de técnicas de Data Mining e Data Analytics por agências de investigação criminal do Brasil. Anais do Simpósio Brasileiro de Sistemas de Informação (SBSI), 593–600. https://doi.org/10.5753/sbsi.2017.6092.

SAUNDERS, J., Hunt, P., & Hollywood, J. S. (2016). Predictions put into practice: A quasi-experimental evaluation of Chicago's predictive policing pilot. Journal of Experimental Criminology, 12(3), 347–371. https://doi.org/10.1007/s11292-016-9272-0.

SCHLEHAHN, E., Aichroth, P., Mann, S., Schreiner, R., Lang, U., Shepherd, I. D. H., & Wong, B. L. W. (2015). Benefits and Pitfalls of Predictive Policing. 2015 European Intelligence and Security Informatics Conference, 145–148. https://doi.org/10.1109/EISIC.2015.29.

SHAPIRO, A. (2017). Reform predictive policing. Nature, 541(7638), 458–460. https://doi.org/10.1038/541458a/

Shapiro, A. (2019). Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing. Surveillance & Society, 17(3/4), 456–472. https://doi.org/10.24908/ss.v17i3/4.10410

SILVA, Rosane Leal. SILVA, Fernanda dos Santos Rodrigues da Silva. Reconhecimento Facial e Segurança Pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro. Anais do 5º Congresso Internacional de Direito e Contemporaneidade:mídias e direitos da sociedade em rede (2019).

WILSON, Dean. Algorithmic patrol: The futures of predictive policing. In ZAVRSNIK, Ales. Big Data, Crime and Social Control. New York: Routledge, 2018. Edição Kindle. p. 109.

ZAVRŠNIK. Ales. Criminal justice, artificial intelligence systems, and human rights. ERA Forum 20, 567–583 (2020). Disponível em https://doi.org/10.1007/s12027-020-00602-0. Acesso em 07 de setembro de 2020.