FACULDADE DE DIREITO DE VITÓRIA
GRADUAÇÃO EM DIREITO

BRUNA LUCHI FIOROT

A PLAUSIBILIDADE DA UTILIZAÇÃO DO BIG DATA PARA A PREDIÇÃO DE CRIMES NO BRASIL FRENTE AOS SEUS RISCOS E CONSEQUÊNCIAS

VITÓRIA
2021

BRUNA LUCHI FIOROT

A PLAUSIBILIDADE DA UTILIZAÇÃO DO BIG DATA PARA A PREDIÇÃO DE CRIMES NO BRASIL FRENTE AOS SEUS RISCOS E CONSEQUÊNCIAS

Trabalho de Conclusão de Curso (TCC) apresentado ao curso de Direito da Faculdade de Direito de Vitória – FDV, como requisito parcial para a obtenção do título de Bacharel de Direito.

Orientador: Prof. Me. Anderson Burke Gomes.

VITÓRIA
2021

BRUNA LUCHI FIOROT

A PLAUSIBILIDADE DA UTILIZAÇÃO DO BIG DATA PARA A PREDIÇÃO DE CRIMES NO BRASIL FRENTE AOS SEUS RISCOS E CONSEQUÊNCIAS

Trabalho de Conclusão de Curso (TCC) apresentado ao Curso de Direito da Faculdade de Direito de Vitória – FDV, como requisito para obtenção do grau de bacharel em Direito.

Aprovado em: _____

COMISSÃO EXAMINADORA:

_____

Prof. Me. Anderson Burke Gomes
Faculdade de Direito de Vitória – FDV
Orientador

_____

Examinador
Faculdade de Direito de Vitória - FDV

RESUMO

O avanço da tecnologia e a interatividade que dela advém tem proporcionado um grande aumento da disponibilização de dados ao redor do mundo, os quais são coletados e armazenados na internet, incorporando-se ao chamado Big Data. A partir desse enorme conjunto de dados é possível extrair informações e realizar os mais diversos tipos de análises, incluindo análises preventivas de ações criminosas, de forma a indicar quais os locais prováveis de ocorrência de crimes e até mesmo quais indivíduos são mais suscetíveis ao cometimento de delitos, permitindo, assim, que a polícia atue preventivamente. Ao passo que a análise preditiva de crimes em Big Data é uma técnica promissora no combate à criminalidade, capaz de auxiliar a atuação do Estado e a garantia da segurança pública, sua aplicação pode ocasionar riscos aos direitos e liberdades dos cidadãos. Além do possível conflito com princípios constitucionais como o da privacidade e da presunção de inocência, há a preocupação de que, a depender dos critérios utilizados nestas análises, padrões existentes de discriminação sejam reproduzidos e tendências errôneas sejam reforçadas, motivando tomadas de decisões injustas por parte da polícia. Estes riscos agravam-se na medida em que não há qualquer lei que regule o tratamento de dados no âmbito penal, existindo apenas, por ora, um anteprojeto de lei de proteção de dados no que tange a persecução penal e a segurança pública. Dessa forma, o presente trabalho busca verificar a plausibilidade da utilização do Big Data para a predição de crimes no Brasil a partir de uma análise acerca do funcionamento e eficácia desta técnica; dos critérios utilizados nas análises preditivas; dos riscos e limites que a mesma apresenta; e da legislação brasileira que dispõe do tratamento de dados pessoais.

Palavras chaves: Big Data. Dados pessoais. Análise preditiva da criminalidade. Criminologia. Processo Penal. Direitos e garantias fundamentais.

SUMÁRIO

INTRODUÇÃO

Nos dias de hoje, grande parte das atividades realizadas no cotidiano possuem o auxílio da internet. Segundo um relatório produzido pela agência We Are Social, atualmente mais de 4,5 bilhões de usuários utilizam a internet ativamente, ou seja, quase 60% da população mundial (KEMP, 2020). Isso significa que as informações desses bilhões de usuários que navegam na internet são coletadas e armazenadas diariamente, incorporando o chamado Big Data, um enorme conjunto de dados do qual é possível extrair informações e realizar os mais diversos tipos de análises.

Nos Estados Unidos, o Big Data vem sendo utilizado há duas décadas com o intuito de melhorar a ordem e a segurança pública. Com o auxílio desta ferramenta, são realizadas análises preditivas a partir dos dados coletados, revelando padrões de atividades criminosas, locais mais prováveis de ocorrência da criminalidade e quais pessoas são mais suscetíveis ao cometimento de ilícitos penais. Os resultados obtidos a partir dessas análises permitem que a polícia direcione sua atuação e aja preventivamente, de modo a impedir a ocorrência de crimes.

Todavia, ao passo que o Big Data pode trazer benefícios significativos à segurança pública, auxiliando a atuação do Estado e a aplicação da lei, pouco tem se falado sobre os limites e efeitos da utilização dessa serventia. Ainda que esta seja uma ferramenta promissora para a garantia da segurança, também é possível que reproduza e agrave preconceitos sociais e raciais a depender dos critérios utilizados para a realização das análises. Adiante, há a preocupação que a aplicação dessa técnica conflite com alguns dos direitos individuais previstos constitucionalmente, tais como a privacidade e o princípio da presunção de inocência.

Por essa razão, o presente trabalho irá tratar sobre a eficácia e as consequências da aplicação desta técnica, buscando verificar se é plausível a utilização do Big Data para a predição de crimes no Brasil a partir de três problemas centrais: (I) Esta técnica demonstra resultados concretos na diminuição da criminalidade nos locais onde é aplicada? (II) Os critérios utilizados na análise preditiva da criminalidade por meio da utilização do Big Data no Brasil contribuem, de alguma forma, para a

estigmatização social dos cidadãos? (III) A atuação preventiva da polícia a partir da análise de dados pessoais encontra algum limite na legislação brasileira?

Para que tais questionamentos sejam respondidos, esta pesquisa tem como objetivo analisar o funcionamento e a eficácia de alguns dos principais sistemas de análise preditiva da criminalidade; investigar quais critérios estão sendo utilizados nestas análises preditivas e se os mesmos contribuem para a estigmatização social dos cidadãos; analisar se a atuação preventiva da polícia afronta, de alguma forma, os princípios e direitos previstos na Constituição; e verificar se há amparo legal no Brasil para que esta tecnologia seja aplicada de maneira segura.

Frente ao rápido e significativo avanço desta tecnologia, torna-se evidente a relevância do tema aqui tratado. Além de ser essencial trazer luz para a necessidade da devida cautela na execução e utilização das plataformas de predição de crimes, a análise do problema se mostra pertinente visto que ainda foi pouco explorado pela comunidade acadêmica. Assim, o presente estudo busca contribuir de maneira não apenas teórica, mas também prática para a solução da problemática exposta.

Para a realização desta pesquisa será utilizado o método dialético, por meio do qual pretende-se “verificar com mais rigor os objetos de análise, justamente por serem postos frente a frente com o teste de suas contradições possíveis” (MEZZAROBA; MONTEIRO, 2009, p. 72). Assim, a ideia de que a análise preditiva de crimes é uma técnica eficaz e segura no combate à criminalidade será confrontada com suas possíveis contradições para que se chegue a uma conclusão verossímil. Além disso, será utilizado o método auxiliar comparativo, de modo a cotejar a aplicação desta tecnologia no Brasil e em outros países onde já vem sendo aplicada há mais tempo.

Desse modo, para que não restem dúvidas sobre o tema aqui tratado, pretende-se abordar no primeiro capítulo o conceito de dados pessoais e de Big Data, explicando como são utilizados atualmente e qual valor é possível extrair desta tecnologia. Já no segundo capítulo, será esclarecido em maior detalhe como o Big Data é utilizado para a realização de análises da criminalidade, expondo a forma de funcionamento e a efetividade de alguns dos sistemas de policiamento preditivo em uso nos Estados Unidos, assim como a dos poucos sistemas atualmente em uso no Brasil.

Ainda no segundo capítulo, tratar-se-á da cadeia de custódia das provas digitais, tendo em vista que todos os dados pessoais coletados e utilizados nas análises em Big Data são vestígios que podem, futuramente, se tornar provas em um processo penal, sendo, por esse motivo, importante que as particularidades de seu tratamento sejam devidamente elucidadas.

No terceiro capítulo, algumas das controvérsias associadas à predição de crimes serão abordadas. Em primeiro lugar, será discutido o risco da estigmatização social dos indivíduos a partir da análise de dados pessoais sensíveis, relacionando a forma de funcionamento dos algoritmos à perpetuação do pensamento criminológico positivista, o qual consiste na compreensão de que as características fisionômicas e sociais dos indivíduos podem determinar se estes são ou não criminosos. Sucedendo este raciocínio, será tratado sobre a importância prática da criminologia crítica e da teoria do “Labeling Approach” que, por sua vez, defende que as noções sobre o crime e o criminoso não são inatas, mas socialmente construídas.

Adiante, ainda no terceiro capítulo, será explicitado o conflito entre as técnicas de predição e alguns dos princípios e direitos previstos na Constituição Federal de 1988. Pretende-se discorrer sobre o princípio fundamental da não discriminação (art. 3º, IV, CF/88), sobre o direito à privacidade (art. 5º, X, CF/88), sobre o princípio da presunção de inocência (art. 5º, LVII, CF/88) e sobre o princípio da individualização da pena (art. 5º, XLVI, CF/88), demonstrando de que maneira cada um eles pode ser posto em risco com a aplicação das técnologias de predição de crimes.

Finalmente, no quarto e último capítulo, tratar-se-á sobre a Lei Geral de Proteção de Dados (LGPD) e a necessidade de regulamentos específicos voltados para a proteção dos dados pessoais utilizados para fins penais. Existe atualmente no Brasil um anteprojeto de lei que objetiva regular o tratamento de dados no tocante à persecução penal e segurança pública, o qual será analisado em maior detalhe neste capítulo a fim de averiguar se o mesmo possui as condições necessárias para que as técnicas de predição de crimes sejam aplicadas com segurança e concluir, por fim, se é plausível a utilização do Big Data para a predição de crimes no Brasil.

1 OS DADOS PESSOAIS E O BIG DATA: CONCEITOS E FORMAS DE APLICAÇÃO

No mundo contemporâneo, a tecnologia tem sido uma das grandes aliadas para o desenvolvimento humano, uma vez que a interatividade que dela advém tem facilitado e agilizado as relações interpessoais e econômicas. Essa interatividade tem sido efetivada pelo avanço de plataformas como o Google, o Whatsapp, o Facebook, além de dispositivos de inteligência artificial como a Amazon Alexa, que amparam as necessidades humanas e permitem a livre comunicação, a rápida obtenção de informações e o compartilhamento de dados.

Vivemos hoje, portanto, em uma verdadeira sociedade da informação, definida por Victor Sales Pinheiro e Alexandre Pereira Bonna como a “forma de organização social que recorre ao intensivo uso da tecnologia da informação para coleta, produção, processamento, transmissão e armazenamento de informações, como no uso das tecnologias de computação e telecomunicações” (2020, p. 367).

Diariamente, as informações de milhões de usuários são disponibilizadas e armazenadas na internet, o que pode ocorrer de maneira explícita, quando determinado indivíduo realiza uma postagem sobre sua vida pessoal nas redes sociais, ou de maneira implícita, quando realiza o cadastro em um site ou utiliza o GPS do automóvel, por exemplo. O fato é: tudo que fazemos hoje com o auxílio da internet deixa rastros digitais, gerando um enorme banco de dados.

Toda a informação relacionada à pessoa natural identificada ou identificável que compõe esse banco de dados é considerada um dado pessoal, conforme a definição disposta no artigo 5º, inciso I, da Lei 13.709/2018, conhecida como a Lei Geral de Proteção de Dados (LGPD). Nesse sentido, são dados pessoais as informações básicas como nome, gênero, data e local de nascimento, e também informações mais detalhadas como histórico de pagamentos e hábitos de consumo (SERPRO, 2019).

A LGPD conceitua, ainda, as diferentes categorias de dados, distinguindo os dados pessoais sensíveis dos dados pessoais anonimizados. O primeiro refere-se a informações como “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (BRASIL, 2018), conforme disposto em seu art. 5º, inciso II. São chamados de dados sensíveis pois sua circulação e seu tratamento são capazes de pôr em risco a personalidade do indivíduo, pois, em razão de seu conteúdo, podem ser utilizados para fins discriminatórios (MENDES, 2014, e-book).

Já os dados anonimizados, de acordo com o art. 5º, inciso III, são aqueles relativos “a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento” (BRASIL, 2018). Laura Schertel Mendes explica que este tipo de dado se refere a pessoas indeterminadas e pode ser utilizado para fins estatísticos, tendo como finalidade a proteção do indivíduo por meio do anonimato (MENDES, 2014, e-book).

Todos os dados pessoais são ativos extremamente valiosos nesta era de globalização, pois, conforme explica Danilo Doneda,

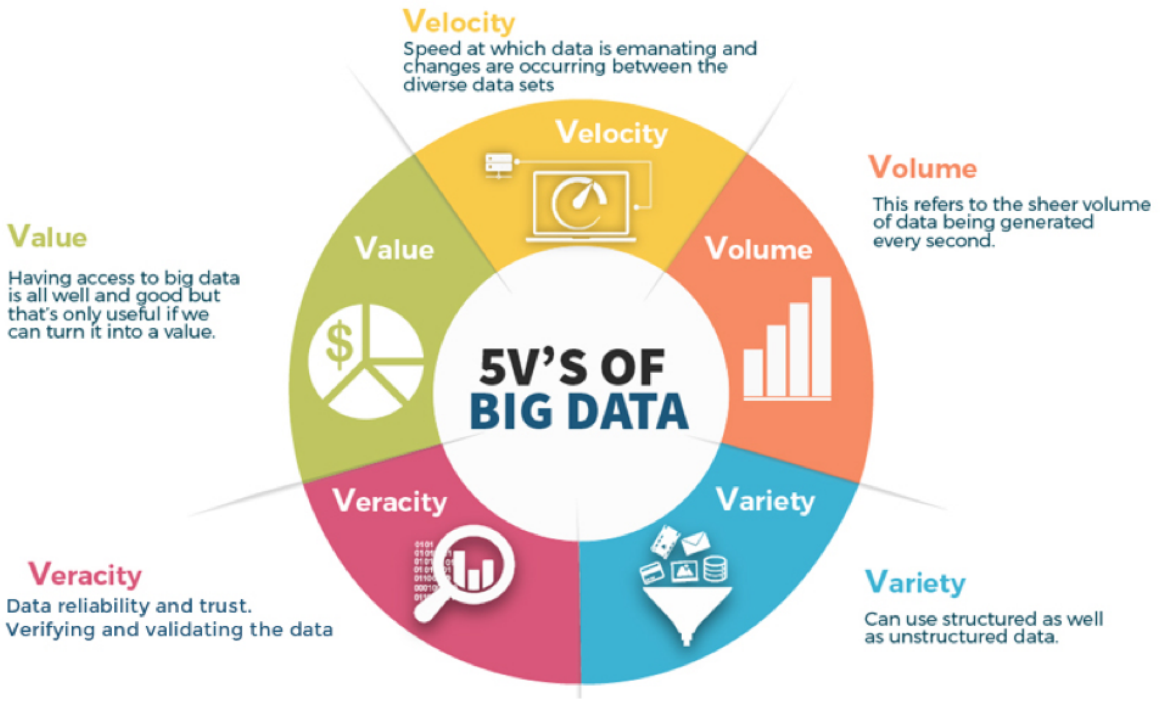
> aumentando-se a capacidade de armazenamento e comunicação de informações, cresce também a variedade de formas pelas quais ela pode ser apropriada ou utilizada. Sendo maior sua maleabilidade e utilidade, mais e mais ela se torna elemento fundamental de um crescente número de negócios e utilidades, aumentando sua possibilidade de influir em nosso cotidiano (DONEDA, 2019, p. 39).

O que Doneda quer dizer é que, na medida em que os dados pessoais de milhões de usuários são coletados e armazenados diariamente, torna-se possível que os mesmos sejam utilizados para a identificação de tendências e comportamentos, auxiliando, assim, as mais diversas áreas, especialmente a dos negócios, a tomarem as decisões corretas para atingir seus objetivos.

Esse enorme volume e vasta variedade de dados coletados incorporam o chamado Big Data, definido pela empresa de pesquisa e consultoria Gartner (2001) como o conjunto de “dados com maior variedade que chegam em volumes crescentes e com velocidade cada vez maior”. Tal definição foi articulada pelo analista Doug Laney,

que determinou os “três V's" do Big Data como variedade, volume e velocidade (2001, p. 01-04). Hoje em dia, no entanto, popularizou-se o conceito que inclui mais duas características a esse conjunto, a veracidade e o valor, resultando nos “cinco V’s do Big Data” (MARR, 2014):

Figura 1 - Os “5 (cinco) V’s do Big Data”



Fonte: https://marketingthings.home.blog/2019/09/04/how-internet-of-things-big-data-are-used/

O volume diz respeito à vasta quantidade de dados gerados diariamente e incorporados ao Big Data. O volume de troca de e-mails, transações bancárias, interações em redes sociais e registros de chamadas são alguns exemplos de atividades do cotidiano que estão constantemente ocorrendo e integrando este enorme banco de dados.

A velocidade se refere ao “imediatismo que um dado é gerado, coletado, tratado, transacionado e cruzado para sua finalidade, devendo o Big Data processá-los na mesma velocidade em que são gerados, para que não se tornem obsoletos” (AGUDO; TEIXEIRA, 2020, p. 237). Uma inteligente analogia trazida em um comercial da empresa IBM (CURTIS, 2011) pode ser utilizada para explicar este aspecto: o narrador questiona se o espectador, ao olhar para uma fotografia tirada do tráfego há cinco minutos atrás, teria confiança em cruzar a rua neste momento.

Por óbvio, a resposta a essa pergunta seria negativa, pois, visto que já não informa as atuais condições do tráfego, aquela informação se tornou irrelevante. Essa é a importância da velocidade na atualização dos dados.

A variedade refere-se ao vasto campo de informações armazenadas, que advém de diferentes fontes. Diferentes tipos de dados podem ser utilizados: os estruturados, que são facilmente organizáveis, armazenáveis e transferíveis num modelo de dados definidos, estando geralmente sequenciados em um padrão fixo e constante; os semi-estruturados, que acompanham padrões heterogêneos e, por seguirem diversos padrões, são mais difíceis de serem identificados; e os não estruturados, que não possuem um modelo de dados definido ou uma estrutura comum identificável, como imagens, áudios e textos (MAGRO, 2020, p. 18-19).

A veracidade diz respeito à necessidade em obter-se dados verídicos para, então, obter-se resultados verídicos. Esta característica anda de mãos dadas com o aspecto velocidade, pois é preciso que os dados estejam atualizados para serem tidos como verossímeis, uma vez que dados passados não podem ser considerados verídicos para o momento em que são analisados (AGUDO; TEIXEIRA, 2020, p. 237).

Por fim, o valor “se mostra como uma junção de todos os anteriores, para que a utilização do Big Data seja abordada de forma proveitosa, vantajosa e eficiente para o receptor dos dados, valorando, na essência, cada uma das informações coletadas” (AGUDO; TEIXEIRA, 2020, p. 237). Destaca-se que o acesso ao Big Data pressupõe a pretensão de extrair algum valor das informações ali contidas, pois, caso contrário, torna-se inútil.

Estando claro o conceito do Big Data, pergunta-se: qual valor é possível extrair dele? Como já mencionado, o Big Data é uma ferramenta de grande utilidade nos mais diversos ramos, visto que é possível identificar padrões a partir dos dados extraídos e, assim, realizar análises precisas. Esta técnica já é empregada ativamente pelo ramo dos negócios, da manufatura, da saúde e qualquer outro que busque melhorar suas estratégias e obter maior lucro e eficiência em suas atividades por meio das conclusões provenientes destas análises.

A forma mais usual da aplicação deste mecanismo pode ser observada no âmbito comercial. Ao navegar em sites da internet ou em redes sociais como o Facebook e o Instagram, é extremamente comum que anúncios de produtos ou serviços relacionados aos interesses do usuário sejam exibidos. Isso ocorre justamente porque, a partir da análise de dados pessoais, as informações coletadas “são organizadas em perfis que classificam as pessoas em rankings de acordo com os seus hábitos e preferências sobre os mais diversos assuntos” (ABREU; NICOLAU, 2017), tornando possível, assim, a realização de publicidades direcionadas por parte dos anunciantes.

Adhemar Della Torre Netto e Alfredo Emanuel Farias de Oliveira exemplificam outras possíveis áreas de aplicação deste mecanismo em nosso cotidiano:

> Através da análise desse imenso volume de informações, é possível ter uma compreensão até então inédita, que transita entre a localização geográfica de uma pessoa específica até os hábitos de consumo de uma determinada sociedade. Pode-se antecipar eventos cataclísmicos, como terremotos e furacões, em como tomar-se medidas para prevenção de epidemias em seu epicentro, prevenindo-se uma patologia, potencialmente capaz de atingir toda a população mundial (NETTO; OLIVEIRA, 2019, p. 03).

Dentre os exemplos citados, os autores incluem até mesmo a previsão de eventos cataclísmicos e epidemias, que, embora pareça inexequível, é possível através da análise de dados, que encontra padrões e correlações indicadores desses eventos. Um estudo realizado pela Escola de Medicina de Harvard demonstrou que o método mais eficiente para monitorar a epidemia de cólera no Haiti em 2010 foi a análise do número de reportagens informais e de postagens no Twitter sobre a doença, pois descobriu-se que conforme o número oficial de casos aumentava e diminuía, o volume de reportagens informais sobre a cólera na mídia também aumentava ou diminua (HIRSCHFELD, 2012).

Em razão da alta eficiência nos resultados obtidos por meio da análise de dados, esta técnica atualmente é utilizada também no combate à criminalidade, tornando possível prever em quais locais há maior probabilidade de ocorrência de crimes, bem como identificar potenciais criminosos. Esta prática já é melhor desenvolvida e

aplicada em países como os Estados Unidos e Inglaterra, porém tende a se difundir na medida em que a tecnologia avança rapidamente ao redor do mundo.

O desenvolvimento dessa tecnologia é capaz de produzir inúmeros benefícios para a coletividade, agilizando a atuação do Estado e proporcionando maior segurança à população. Por outro lado, existe a preocupação sobre a maneira como essa técnica é aplicada e o consequente risco de ocasionar medidas injustas, o que abre portas para relevantes e necessárias discussões. Assim, os próximos capítulos do presente trabalho abordarão em maior detalhe as diferentes ferramentas e sistemas de predição da criminalidade, bem como seus desdobramentos e possíveis consequências.

2 A UTILIZAÇÃO DO BIG DATA PARA A PREDIÇÃO DE CRIMES

A utilização da tecnologia para prever e prevenir crimes certamente parece uma ideia muito distante, plausível apenas em obras de ficção como “The Minority Report”. Nesta obra escrita por Philip K. Dick em 1956, a qual se tornou filme em 2002, um departamento de polícia é capaz de antecipar crimes e deter criminosos com base em previsões realizadas por mutantes denominados “Precogs”, impedindo que tais crimes ocorram. Entretanto, essa premissa é mais real do que muitos podem imaginar, pois a atividade realizada pelos “Precogs” equivale, nos dias de hoje, à análise preditiva em Big Data.

Antes da existência do Big Data, modelos matemáticos e estatísticos já eram utilizados para descrever os locais de maior ocorrência de delitos e, assim, auxiliar o policiamento ostensivo. Contudo, foi apenas nas últimas duas décadas que desenvolveu-se a análise preditiva de crimes com o auxílio dos poderosos softwares de mapeamento, sistemas de processamento de dados e mídias sociais, tornando possível uma atuação antecipada da polícia frente às ameaças identificadas (MUGGAH, 2019, p. 02).

Esta forma de atuação antecipatória é denominada policiamento preditivo, que consiste na “aplicação de técnicas analíticas – particularmente técnicas quantitativas – para identificar alvos prováveis de intervenção policial e prevenir crimes ou resolver crimes passados, fazendo previsões estatísticas” (PERRY, 2013, p. 13). As técnicas analíticas utilizadas para o policiamento preditivo podem ser melhor compreendidas quando comparadas à sismologia, conforme elucida o cientista político Robert Muggah:

> Muito geralmente, o crime é análogo a terremotos: características embutidas no ambiente influenciam fortemente os tremores secundários associados. Por exemplo, crimes associados a uma boate, a um condomínio de casas ou a uma esquina em particular podem influenciar a intensidade e a disseminação de atividades criminosas futuras (MUGGAH, 2016, tradução nossa).

Assim, da mesma maneira que um grande terremoto normalmente é seguido de réplicas na área em que ocorreu, os crimes ocorridos em determinada localidade tendem a influenciar a disseminação de crimes similares no futuro. Sabendo disso, a polícia direciona seu patrulhamento, dando prioridade a esses locais.

No entanto, a partir da utilização do Big Data, tornou-se possível gerar previsões associadas não apenas ao local, mas também a tipos específicos de crime, horários do dia e dias da semana, visto que esta ferramenta permite que sejam processados dados mais detalhados e em um ritmo mais rápido (MUGGAH, 2019, p. 02). Esta técnica, que possibilita identificar quando e onde um crime pode ocorrer, é denominada mapeamento preditivo (VAN BRAKEL, 2016, 04), o tipo de policiamento preditivo mais aplicado atualmente ao redor do mundo.

O outro tipo de policiamento preditivo é o chamado identificação preditiva, “onde a análise é em nível individual ou de grupo; isso pode se concentrar em prever potenciais infratores, identidades de infratores, comportamento criminoso e potenciais vítimas de crime” (VAN BRAKEL, 2016, p. 04). Já é possível, portanto, que a alta quantidade de informações extraídas do Big Data seja utilizada a fim de mensurar e classificar indivíduos a partir do nível de risco/perigo ao ordenamento social, definindo quais deles são mais suscetíveis ao cometimento de delitos.

Assim, o que se observa é a possibilidade de uma mudança de abordagem pós-crime para uma "pré-crime" (termo criado por Philip K. Dick em "The Minority Report), de modo que as evidências reveladas pela análise de dados possam ser utilizadas não como "uma 'prova' *ex post facto*, mas como um vetor que permitiria agir antes do fato, ou antes da ação" (BRUNO, 2016, p. 36).

É claro que, tratando-se da prevenção de delitos, ainda não existem danos a serem refutados, o que faz surgir muitas críticas e preocupações quanto a tais medidas, como a possibilidade de que, no futuro, as prisões fiquem lotadas de pessoas condenadas por crimes sem vítimas (O'NEIL, 2016, p. 87). Contudo, conforme destaca Anderson Burke, o Estado busca a prevenção de delitos "utilizando como fundamento a defesa em potencial de bens jurídicos necessários para a segurança da 'sociedade'" (2019, p. 45), ou seja, a vítima objeto da tutela penal, neste caso, é a sociedade como um todo.

O desenvolvimento de novas ferramentas predição e o constante avanço dos sistemas analíticos em uso atualmente sugerem que essas e outras preocupações somente crescerão daqui para a frente, motivo pelo qual é importante que seus benefícios e a real eficácia desta tecnologia seja devidamente ponderada frente aos seus riscos.

2.1 FUNCIONAMENTO E EFETIVIDADE DOS SISTEMAS DE POLICIAMENTO PREDITIVO

Desde 2011, o Big Data vem sendo largamente aplicado nos Estados Unidos com o intuito de prever crimes e, assim, auxiliar na garantia da segurança pública. Contudo, o primeiro uso documentado de modelos de policiamento preditivo ocorreu em 2008, quando o Departamento de Polícia de Los Angeles, em parceria com UCLA (Universidade da Califórnia em Los Angeles), implantou o sistema PredPol e estimou que a probabilidade de prever com precisão a ocorrência de crimes dobrou (MUGGAH, 2019, p. 06).

Os co-fundadores deste sistema, Jeff Brantingham and George Mohler, acreditavam ser possível prever certos crimes da mesma forma que é possível prever a distribuição de tremores secundários de terremotos. Assim, o PredPol, que é software de policiamento preditivo mais conhecido atualmente, se baseia em três anos de dados (ponderando mais fortemente os dados recentes) para determinar o local, tipo e hora de crime passados e, dessa forma, indicar áreas onde crimes específicos futuros são mais prováveis de ocorrer (BOYD; BRAYNE; ROSENBLAT, 2015, p. 06).

Uma avaliação realizada em 2013 pelos fundadores do PredPol na cidade de Los Angeles demonstrou que, com a utilização deste sistema, houve uma redução média de 7,4% no volume de crimes em função do tempo de patrulha e uma redução de 12% no números de crimes contra a propriedade em comparação ao ano anterior. Em Santa Cruz, na Califórnia, o relatório de resultados de 2011 demonstrou uma redução inicial de 11% em roubos, chegando a uma redução de 19% em um período de 6 meses de utilização do PredPol (MUGGAH, 2019, p. 12-13).

Este sistema é hoje utilizado não apenas em grande parte dos Estados Unidos, mas em diversos outros países, pois, além de ter grande eficácia, o mesmo não utiliza informações pessoais sobre indivíduos ou grupo de indivíduos, o que elimina o risco de análises tendenciosas e possíveis ameaças às liberdades individuais que tal técnica pode acarretar.

Outro sistema popular, porém que utiliza uma estratégia analítica diferente, é o Hunchlab, atualmente aplicado em Chicago, Miami, Nova Iorque e Filadélfia. Este software não apenas mapeia locais mais suscetíveis à criminalidade, mas também examina o porquê de determinadas áreas apresentarem maior risco, estando muitas dessas causas associadas ao ambiente ou à demografia de uma área. Mais especificamente, o Hunchlab se utiliza de um sistema de informações geográficas para explorar a relação entre o crime e as características espaciais que o influenciam, como a localização de parques, casas, bares, pontos de transporte público, etc (CAPLAN; KENNEDY, 2010).

Em Chicago, onde as técnicas de policiamento preditivo são largamente exploradas, a polícia utiliza o Hunchlab integrado à uma tecnologia chamada ShotSpotter, que é capaz de identificar e registrar sons de tiros e sua localização aproximada. Com a implementação desses sistemas integrados, que auxiliam na tomada de decisões da polícia por meio da análise massiva de informações como detenções, chamadas para o 911 (emergência) e atividades de gangues, houve em Chicago uma diminuição no número de tiroteios em 49% e 66% nos meses de fevereiro e março, respectivamente, de 2017 (BRAGA, 2019, p. 36).

A polícia de Chicago utiliza, ainda, uma técnica especialmente controversa, denominada Strategic Subject List (SSL), em que um algoritmo preditivo gera uma lista ordenada de sujeitos de acordo com o risco de estarem envolvidos com crimes violentos, chamada “heat list”. Este algoritmo, por se tratar de segredo industrial, ainda é obscuro e desconhecido, porém, segundo o Departamento de Polícia de Chicago, inclui fatores como “histórico criminal, prisões, status de liberdade condicional e se o alvo foi identificado como parte de uma gangue” (FERGUSON, 2017, tradução nossa).

Estes dados são utilizados para classificar cada sujeito com uma pontuação numérica que varia de 1 a 500, de forma que, quanto mais alta for a pontuação, maior risco o indivíduo apresenta (FERGUSON, 2017). Uma vez identificado como risco, o cidadão está sujeito a receber uma visita da polícia em seu próprio domicílio o advertindo, mesmo que não tenha cometido qualquer infração. Além disso, em investigações de crimes posteriores, é mais provável que a polícia investigue os indivíduos incluídos na lista, em especial aqueles que foram registrados com pontuação acima de 250 (FERGUSON, 2017).

Além da SSL não demonstrar qualquer eficácia concreta na redução da violência, conforme relatório da RAND Corporation de 2016 (STROUD, 2016), técnicas como esta apresentam um risco evidente às liberdades individuais dos cidadãos, uma vez que, ao serem classificados como perigosos, passam a receber um tratamento diferenciado, de forma justificada ou não, podendo ocasionar em medidas injustas por parte do Estado.

Na medida em que a tecnologia avança, as ferramentas de previsão do crime tendem a se disseminar. Segundo Robert Muggah, novas plataformas já estão sendo testadas com o objetivo de “classificar automaticamente o crime relacionado a gangues, combinar mídia social com histórico criminal para prever crimes e usar inteligência artificial para identificar indivíduos com perfis mais suscetíveis a cometer atos terroristas” (2019, p. 09, tradução nossa). A rápida implantação dessas ferramentas levanta, consequentemente, questões éticas complexas em relação à ação policial e aos direitos civis.

Embora esse cenário possa parecer muito distante da realidade brasileira, este tipo de tecnologia já começou a ser implantada no Brasil. Em 2014, o governo do Estado de São Paulo firmou uma parceria com a Microsoft e adquiriu o sistema de monitoramento criminal Detecta, que utiliza o Big Data para análise dos dados da polícia e de radares e câmeras de vigilância. Desde a sua implementação até meados de 2018, a análise das imagens captadas contribuíram para a prisão de 9.424 pessoas em flagrante delito, a interceptação de 5.689 veículos e a apreensão de 517 armas de fogo ilegais, segundo informações da Secretaria de Segurança Pública (SOUSA, 2018).

O Detecta, associado ao sistema Ômega, tem auxiliado nas investigações policiais e no combate à criminalidade no Estado de São Paulo. Ômega é um sistema que integra determinados bancos de dados e torna possível o acesso a diferentes informações em um só lugar. Esta rede integrada contém informações de cadastros: civil, criminal, armas, veículos roubados e furtados, Junta Comercial, Disque Denúncia, Delegacia Eletrônica (boletins de ocorrência e inquéritos policiais) e Detran. Tal ferramenta permite, ainda, o acesso à informações de referência geográfica, ou seja, dados do Infocrim (informações criminais) e mapas, além do sistema de identificação biométrica Phoenix, trazendo dados como impressões digitais, gravação de voz e fotos de suspeitos em várias dimensões (PORTAL DO GOVERNO DE SP, 2009).

A tecnologia até então aplicada no Brasil tem sido de grande ajuda na manutenção da ordem e no cumprimento da lei. As câmeras de reconhecimento facial, por exemplo, foram um grande avanço na identificação de criminosos procurados. Um

destes casos ocorreu em Salvador, em março de 2019, quando um jovem de 19 anos que possuía um mandado de prisão expedido contra si desde 2018 foi flagrado por uma dessas câmeras e, então, abordado por policiais militares (G1 BA, 2019).

Contudo, são pouquíssimos os Estados brasileiros que de fato realizam análises preditivas para auxiliar nas estratégias de policiamento e prevenção de crimes. Um desses Estados é o Rio de Janeiro, que adquiriu o software da empresa Oracle (DIAS; HVISTENDAHL, 2021), o qual utiliza o Big Data para a realização de análises preditivas de crimes e, assim, torna possível o policiamento preditivo naquele local. Este sistema é, no entanto, alvo de muitas críticas, uma vez que utiliza dados de redes sociais e dados pessoais sensíveis em suas análises, o que, como já dito, pode gerar conclusões tendenciosas e levar a ações arbitrárias por parte da polícia.

Com o surgimento de novas ferramentas de predição e a consequente normalização dessa prática dentre os procedimentos de segurança, surgem não apenas preocupações acerca das controversas questões éticas ligadas à essa técnica, mas também acerca da natureza da aplicação da lei, que tende a sofrer alterações. Visto que os dados coletados e armazenados no Big Data podem vir a ser posteriormente utilizados em uma investigação ou em um processo criminal, exige-se uma cautela especial em seu tratamento, sendo fundamental a adoção de procedimentos que garantam a proteção das informações.

2.2 A CADEIA DE CUSTÓDIA DAS PROVAS DIGITAIS

Conforme já explicado anteriormente, tudo o que fazemos hoje com o auxílio da internet deixa “vestígios digitais”, seja por meio de uma mensagem enviada pelo celular, uma publicação realizada nas redes sociais, ou pelo cadastro em algum site ou aplicativo. O vestígio, de acordo com o artigo 158-A, §3º do Código de Processo Penal brasileiro, “é todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal” (BRASIL, 1941).

O Código de Processo Penal dispõe ainda, em seu artigo 158, caput, que “quando a infração deixar vestígios, será indispensável o exame de corpo de delito [...]” (BRASIL, 1941), ou seja, o exame pericial sobre os elementos de materialidade da suposta infração penal. Embora possa parecer inviável, isso se aplica também aos vestígios virtuais, os quais devem ser devidamente analisados por um perito antes que possam ser considerados evidências de uma infração.

Antes de mais nada, é importante esclarecer que evidência é qualquer vestígio que, após avaliações de cunho objetivo, demonstra vinculação direta com o delito investigado (MALLMITH, 2007). Quando essas evidências são documentadas e utilizadas no processo penal, as mesmas são chamadas de provas, constituindo o “meio e modo de que usam os litigantes para convencer o juiz da verdade da afirmação de um fato, bem como o meio e modo de que se serve o juiz para formar sua convicção sobre os fatos que constituem a base empírica da realidade” (MARQUES, 1997, p. 207).

Portanto, uma vez que as provas periciais oferecem campo para que o juiz realize uma apreciação objetiva e segura dos fatos, é essencial que seja assegurada a preservação de qualquer vestígio desde o momento que é identificado até o momento em que poderá ser descartado. A isso dá-se o nome de cadeia de custódia, que, conforme o artigo 158-A do CPP, consiste no “conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte” (BRASIL, 1941).

A observância da cadeia de custódia é de extrema importância na garantia da autenticidade e idoneidade da prova pericial, pois a falha neste procedimento é capaz de gerar imensos prejuízos ao processo. Um exemplo disso é o caso de O.J. Simpson, jogador de futebol americano dos Estados Unidos que foi absolvido do crime de duplo homicídio por conta de falhas nos elementos probatórios. A ausência de cuidado na preservação da cena do crime e a falta de técnica por parte dos peritos, que sequer usaram luvas para a coleta dos vestígios no local dos fatos, facilitou a manipulação das evidências, o que contribuiu com a mitigação da possibilidade de condenação criminal (CUNHA, 2020, p. 177).

Por esse motivo, é indispensável que as etapas previstas na cadeia de custódia da prova, atualmente dispostas no artigo 158-B do CPP, sejam obedecidas. Caso haja a violação deste procedimento, a prova deve ser considerada ilícita, uma vez que torna-se extremamente difícil a comprovação de sua idoneidade e, conforme pontua Carlos Edinger, "nada impede que seja ela objeto de manipulação e seleção unilateral de provas" (2016, p. 256).

Neste sentido, o artigo 157 do CPP define que "são inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais" (BRASIL, 1941), em conformidade com o artigo 5º, inciso LVI, da Constituição Federal de 1988, que prevê a inadmissibilidade das provas obtidas por meios ilícitos no processo.

Tratando-se de provas digitais que, em razão de sua natureza, são indiscutivelmente muito frágeis, o cuidado em seguir os procedimentos da cadeia de custódia deve ser ainda maior. As provas eletrônicas ou digitais, definidas como "qualquer classe de informação (dados) que tenha sido produzida, armazenada ou transmitida por meios eletrônicos" (MARTÍN, 2020, p. 55), apresentam maior fragilidade pois é possível que sejam facilmente modificadas e, diferentemente de uma prova convencional, isso pode ocorrer de forma indetectável (PARODI, 2021).

De acordo com Parodi (2021), "pode ser modificado seu conteúdo, podem ser modificados metadados (blocos de informações estruturadas sobre características e história de um arquivo) e podem ser modificadas suas características (datas, autor, origem, identificação, nome, extensão etc.)". Assim, resta evidente que, nos processos em que espera-se apresentar dados digitais como prova, é essencial que sua integridade seja devidamente comprovada.

Nesse sentido, Jacob Heilik (2019) explica que os elementos-chave para que a idoneidade da prova digital seja assegurada é a capacidade de autenticá-la e de demonstrar de onde veio, isto é, sua proveniência. Segundo o autor, a cadeia de custódia da prova

> [...] pode fornecer procedência e autenticação para qualquer item específico de evidência digital. A proveniência é importante porque fornece uma ligação clara entre as informações introduzidas e a fonte legalmente adquirida de onde provêm. A autenticação é importante para estabelecer que as informações introduzidas não foram alteradas desde o momento em que foram coletadas - ou seja, não são nem mais nem menos do que os dados de origem originais (HEILIK, 2019, e-book, tradução nossa).

Ou seja, a obediência aos procedimentos da cadeia de custódia dos vestígios é capaz de diminuir suas chances de violação, garantindo a certeza de que os dados em análise provém das fontes anunciadas e não foram modificados em nenhum momento.

Contudo, é comum que os peritos encontrem dificuldades ao desempenhar sua função, uma vez que os vestígios virtuais podem ser coletados de diversas fontes. Segundo Joaquín Delgado Martín, a informação digital pode estar disponível nas redes sociais e páginas da Web; em dispositivos eletrônicos, como um celular ou computador; armazenados em provedores de serviços; ou armazenados na nuvem (2020, p. 55-56).

Dessa forma, a mera apreensão de um computador, por exemplo, não garante que a informação contida nele será autenticada com segurança, sendo necessário que os peritos adotem métodos de criptografia de algoritmos, de forma a assegurar e preservar o conteúdo dos vestígios (MARTÍNEZ, 2020, p. 336-337). Assim, os mesmos devem realizar cópias das informações e obter o seu valor *hash*, isto é, um resumo criptográfico dos blocos de dados que objetiva garantir sua integridade (PISA, 2012).

No entanto, estes cuidados nem sempre são respeitados, especialmente por não haver qualquer órgão no Brasil que defina as regras e procedimentos a serem seguidos durante a análise de vestígios especificamente virtuais. Isso já ocorre em outros países, onde a documentação detalhada, precisa e rigorosa de toda a fase de coleta da prova eletrônica é exigida por órgãos internacionais, como a Association of Chief Police Officers (ACPO) da Inglaterra e o National Institute of Standards and Technology (NIST) dos Estados Unidos (PRADO, 2021).

Resta evidente, portanto, que a plausibilidade da utilização de provas digitais no processo penal decorre necessariamente da obediência à cadeia de custódia, sendo imprescindível o desenvolvimento de um regulamento mais específico no Brasil quanto ao tratamento de vestígios digitais, de forma a garantir maior segurança às partes envolvidas no processo.

Toda a tutela é necessária frente à digitalização da vida que atualmente experienciamos. Uma vez que os dados pessoais de milhões de brasileiros são coletados pelas mais diversas fontes e podem ser utilizados até mesmo para prever possíveis crimes, é essencial que os cidadãos estejam legalmente protegidos de qualquer risco à sua liberdade.

3 CONTROVÉRSIAS E OBSTÁCULOS ASSOCIADOS À PREDIÇÃO DE CRIMES

Por todo o exposto até este ponto, ficou evidente que as ferramentas de análise preditiva são capazes de reduzir a criminalidade e agilizar a atuação da polícia, proporcionando maior segurança à população. Por outro lado, conforme já mencionado, há a preocupação sobre a maneira como essa técnica é aplicada e os riscos que dela advém, uma vez que é capaz de conflitar com relevantes questões éticas e normativas.

Existe o temor de que as ferramentas de predição possam influenciar uma atuação desproporcional por parte da polícia, fazendo com que o foco seja sempre os bairros e comunidades marginalizadas; de que as informações como raça e idade sejam utilizadas para a construção de perfis criminosos; de que a forma de funcionamento destas ferramentas entrem em conflito com princípios constitucionais; além da preocupação quanto os direitos de privacidade e as liberdades civis, questões que devem ser devidamente ponderadas frente aos benefícios que o Big Data é capaz de trazer.

3.1 A ANÁLISE DE DADOS PESSOAIS SENSÍVEIS O RISCO DA ESTIGMATIZAÇÃO SOCIAL DOS INDIVÍDUOS

Embora o objetivo do policiamento preditivo seja reduzir os índices de criminalidade, os critérios utilizados na análise preditiva e os limites da atuação policial são questionados no âmbito internacional. Isto pois, conforme explica Robert Muggah (2019), a depender da forma de programação dos algoritmos, estes podem reproduzir padrões existentes de discriminação e reforçar tendências errôneas a partir das informações embutidas nos bancos de dados.

Cathy O'Neil, em seu livro “Weapons of Math Destruction”, aponta que os algoritmos que comparam indivíduos à tendências acabam por julgá-los pelo comportamento de outras pessoas. Sobre isso, a autora faz a seguinte analogia:

> Podemos ser cobrados a mais pelo seguro de automóveis não porque éramos maus motoristas, mas porque outras pessoas com nossas compras ou históricos de crédito eram maus motoristas no passado. Essa é a essência do preconceito: presumir que uma pessoa se comportará como as outras de sua categoria (O’NEIL, 2016, tradução nossa).

Ou seja, é comum que os algoritmos presumam que indivíduos com características similares se comportem da mesma maneira. Dessa forma, as tendências e comportamentos de usuários, identificados a partir da coleta e análise de seus dados pessoais, acabam sendo utilizados para classificá-los e enquadrá-los em determinados grupos e categorias, como o do exemplo citado acima.

O que torna essa questão ainda mais preocupante é que, se outrora a análise de dados revelava muito pouco sobre cada indivíduo em si, hoje em dia, com o avanço das análises em Big Data, o conjunto de dados coletados permite que o perfil de cada usuário seja traçado a partir de seus dados, sendo muitos deles sensíveis, os quais, como já mencionado, são aqueles definidos pelo artigo 5º, inciso II, da LGPD como dados referentes à origem racial ou étnica, convicção religiosa, opinião política, saúde, etc (BRASIL, 2018).

Tanto Cathy O’Neil, como Robert Muggah, advertem que se os algoritmos forem projetados de maneira precária e falha, de modo que os dados utilizados para

alimentar o sistema apresentem alguma predisposição ou tendência, é possível que preconceitos sociais sejam perpetuados sob um verniz de credibilidade científica. Dessa forma, um indivíduo corre o risco de ser rotulado injustamente como um potencial criminoso baseado em dados como raça, idade, sexo e etnia, o que acaba por prejudicar excessivamente os grupos considerados como marginalizados ou vulneráveis.

Contudo, a grande dificuldade em projetar algoritmos neutros deve-se ao fato de que os sistemas de inteligência artificial são projetados por seres humanos e aprendem a partir de uma base de dados fornecida também por seres humanos, os quais são incapazes de ser totalmente neutros e destituídos de valores. Isto porque, conforme explica Carolina Braga, as perspectivas e crenças de cada indivíduo são moldadas desde tenra idade por fatores como cultura, educação, religião, mídia e política, de modo que a associação dessas informações pode levar à formação de estereótipos que nem sempre refletem a realidade (2019, p. 10).

Por essa razão, é possível que os programadores transfiram preconceitos naturais aos sistemas de inteligência artificial de forma a estigmatizar (mesmo que involuntariamente) determinados indivíduos, uma vez que “a própria seleção dos dados que alimentarão a máquina é uma atividade subjetiva” (BRAGA, 2019, p. 53). Esse processo pode ser melhor compreendido quando examinado à luz da criminologia, que, conforme define José Frederico Marques, “é a ciência que cuida das leis e fatores da criminalidade, consagrando-se ao estudo do crime e do delinquente, do ponto de vista causal - explicativo" (1954, p. 52).

3.1.1 A influência dos algoritmos preditivos na perpetuação do pensamento criminológico positivista

O fato de critérios pessoais como gênero, raça, idade e etnia poderem ser utilizados para classificar alguém como potencial criminoso nos dias de hoje certamente remete às teorias criminológicas positivistas, criadas nos séculos XIX e XX. A Escola Positiva considera que o criminoso é o sujeito determinado à prática de uma infração

penal, de modo que “apresenta uma patologia hereditária própria (determinismo biológico) ou se sujeita a processos causais alheios (determinismo social)” (VALENTE, 2018, p. 61).

O movimento criminológico positivista iniciou-se a partir das idéias de Cesare Lombroso, conhecido como o pai da antropologia criminal. Lombroso examinava com profundidade as características fisionômicas de indivíduos e as comparava com os dados estatísticos da criminalidade, buscando definir qual é o perfil do homem criminoso. Em sua obra "L'Uomo Delinquente”, o autor traçou a figura do delinquente nato, defendendo que “o homem não é livre na sua vontade, pois, com base em seu determinismo biológico, carrega certa hereditariedade da demência moral e, portanto, é predeterminado à prática de infrações penais” (VALENTE, 2018, p. 61).

Por meio de estudos experimentais, Lombroso chegou a conclusão de que os criminosos possuíam uma série de características em comum, apresentando um perfil físico e social padronizado. Conforme o pensamento deste autor,

> O delinquente padece uma série de estigmas degenerativos comportamentais, psicológicos e sociais (fronte esquiva e baixa, grande desenvolvimento dos arcos supraciliares, assimetrias cranianas, fusão dos ossos atlas e occipital, grande desenvolvimento das maçãs do rosto, orelhas em forma de asa, tubérculo de Darwin, uso frequente de tatuagens, notável insensibilidade à dor, instabilidade afetiva, uso frequente de um determinado jargão, altos índices de reincidência etc.) (MOLINA; GOMES, 2006, p. 149)

Observa-se, assim, que as conclusões alcançadas por Lombroso baseiam-se em claras discriminações, uma vez que o autor acreditava que a fisionomia de um indivíduo poderia determinar se o mesmo é ou não um criminoso. Nesse sentido, sua teoria negava a existência do livre arbítrio, uma vez que entendia que a motivação humana advém de forças inatas e inerentes ao indivíduo, pensamento que obteve colaboração de Enrico Ferri, criminologista que acreditava no determinismo sociológico, ou seja, que o delinquente estaria propenso às práticas criminosas em razão do meio em que vive, inexistindo o livre arbítrio (VALENTE, 2018, p. 60-61).

Tais teorias foram posteriormente refutadas, pois demonstrou-se que as características biológicas ou sociais não tornam alguém criminoso, mas apenas

tornam possível o etiquetamento desse indivíduo pelo sistema de controle social. Sobre isso, Alessandro Baratta explica que

> As maiores chances de ser selecionado para fazer parte da "população criminosa" aparecem, de fato, concentradas nos níveis mais baixos da escala social (subproletariado e grupos marginais). A posição precária no mercado de trabalho (desocupação, subocupação, falta de qualificação profissional) e defeitos de socialização familiar e escolar, que são características dos indivíduos pertencentes aos níveis mais baixos, e que na criminologia positivista e em boa parte da criminologia liberal contemporânea são indicados como as causas da criminalidade, revelam ser, antes, conotações sobre a base das quais o status de criminoso é atribuído (BARATTA, 2011, p. 165).

Assim, como bem explicou Baratta, o que os pensadores da Escola Positiva entendiam como causas da criminalidade são, em realidade, apenas causas para inserir indivíduos na categoria de potenciais criminosos, havendo uma maior probabilidade de que as pessoas mais pobres e marginalizadas sejam as selecionadas, devido a baixa escolarização, falta de qualificação profissional e déficits de socialização, como aponta o autor.

Neste sentido, a análise de dados em Big Data tem o potencial de perpetuar, mesmo que de forma involuntária, o pensamento criminológico positivista ao classificar determinados indivíduos em categorias específicas com base em seus dados pessoais, o que acaba por prejudicar excessivamente os grupos considerados como vulneráveis, fazendo com que sejam colocados sistematicamente em posição de desvantagem em relação às outras camadas da sociedade.

Estudos financiados pela US National Science Foundation nos últimos anos demonstraram que os modelos de policiamento preditivo são suscetíveis a "ciclos de feedback descontrolados", em que "a polícia é enviada repetidamente para os mesmos pontos críticos identificados, independentemente das verdadeiras taxas de criminalidade" (MUGGAH, 2019, p. 09, tradução nossa). Essa situação demonstra o perigo nas decisões automatizadas, que acabam por evidenciar a estigmatização dos grupos marginalizados.

À vista disso, Cathy O'Neil alerta que a forma de funcionamento dos sistemas de policiamento adotados pela polícia americana

> [...] cria um feedback loop destrutivo. O próprio policiamento cria novos dados, que justificam mais policiamento. E nossas prisões ficam lotadas com centenas de milhares de pessoas condenadas por crimes sem vítimas, ou seja, sem grande lesividade. A maioria delas vem de bairros empobrecidos e são, em sua maioria, negros ou latinos. Então, mesmo que o modelo seja indiferente à cor, o resultado é tudo menos isso. Nas nossas cidades segregadas a geografia é um dado aproximado muito eficiente para raça (O'NEIL, 2016, p. 87).

Dessa forma, o processamento incorreto de dados faz com que a polícia se direcione sempre às mesmas comunidades, muitas vezes se valendo de critérios raciais e sociais. Observa-se, portanto, que é errônea a concepção de que os resultados obtidos através dos sistemas de predição são justos por utilizarem algoritmos matemáticos, pois, na realidade, tais algoritmos não estão livres de preconceitos humanos.

Um exemplo prático é a utilização das "heat lists" pelo departamento de polícia da cidade de Chicago. Embora haja pouca divulgação de dados por parte da polícia, "ativistas pelos direitos de rede descobriram que mais de 50% das pessoas negras, com idade de 20 a 29 anos, estão na lista, enquanto apenas 2% das pessoas brancas estão na mesma" (LUCENA, 2019, p. 10). Resta claro, portanto, que o critério racial é levado em conta, sendo a população negra a mais prejudicada pelos algoritmos.

Importante destacar que, mais do que o mero risco de serem abordados injustamente pela polícia, esses indivíduos também correm o risco de serem condenados de maneira injusta. Como exemplo disso temos o sistema COMPAS, uma ferramenta de análise de risco utilizada pelos tribunais dos Estados Unidos que calcula o grau de periculosidade de indivíduos e as chances destes se tornarem reincidentes, prevendo qual é a probabilidade de criminosos condenados cometerem crimes futuros (MUGGAH, 2019, p. 09).

O sistema COMPAS permite que juízes justifiquem as penas impostas em suas sentenças com base nos relatórios que emitem os cálculos de risco para cada réu. O grande problema é que esta ferramenta já foi acusada de ser tendenciosa contra minorias, tendo um repórter da ProPublica exposto, em 2016, que os réus negros

eram identificados como possíveis reincidêntes em escala muito mais alta do que os réus brancos. Segundo a reportagem, 45% dos réus negors haviam sido sinalizados como de alto risco, enquanto apenas 23% dos réus brancos que não eram reincidentes haviam sido considerados da mesma forma (BRAGA, 2019, p. 50).

Novamente, observa-se uma perpetuação do pensamento criminológico positivista, uma vez que a Escola Positiva entendia que os estudos que demonstravam as causas biopsíquicas do crime e as características do criminoso facilitavam o trabalho do juiz na imposição da pena, “principalmente pelo fato de a ele corresponderem os estudos da personalidade no momento da individualização judicial” (CARVALHO, 2008, p. 131). Ocorre que, como já mencionado, esses estudos eram baseados em discriminações e preconceitos humanos, os quais acabam sendo refletidos nos sistemas preditivos.

3.1.2 A importância prática da teoria do “Labeling Approach” e da criminologia crítica

Com o reconhecimento das falhas e perigos nas teorias criminológicas positivistas, a Escola Positivista tem fim e surge a teoria do “Labeling Approach”, ou teoria do etiquetamento social, que defende que as noções sobre o crime e o criminoso são socialmente construídas por meio de definições legais e ações de controle social. De acordo com essa abordagem, a criminalidade não é inerente ao sujeito, mas um rótulo atribuído a tais indivíduos considerados desviantes pela sociedade (BARATTA, 2011, p. 159-161).

Esse entendimento abriu espaço para um novo movimento nos estudos criminológicos: a criminologia crítica. Segundo Alessandro Baratta, os estudiosos da criminologia crítica compreendem que “a criminalidade não é mais uma qualidade ontológica de determinados comportamentos e de determinados indivíduos, mas se revela, principalmente, como um status atribuído a determinados indivíduos” (2011, p. 161). A partir desta ideia, entende-se que o status de criminoso é distribuído de modo desigual e, por esse motivo, critica-se a ideia do direito penal como o direito

igual por excelência (BARATTA, 2011, p. 162), uma vez que é evidente que tal igualdade não existe, havendo um alvo claramente delimitado.

Nas análises preditivas em Big Data, esse rotulamento dos indivíduos se dá por uma técnica denominada “profiling”, que, conforme ensina Danilo Doneda, consiste em uma síntese dos hábitos, preferências pessoais e outros registros da vida de cada indivíduo por meio da coleta e análise de dados, a qual pode ser utilizada “para traçar um quadro das tendências de futuras decisões, comportamentos e destinos de uma pessoa ou grupo” (DONEDA, 2006, p. 173). Dessa forma, tendências e vieses são perpetuados com base em algoritmos, reproduzindo discriminações construídas socialmente.

A compreensão desses preceitos criminológicos é fundamental no momento de elaboração dos softwares de análise preditiva da criminalidade. Os criadores do sistema PredPol, por exemplo, levaram em consideração teorias sociológicas do crime como o do Etiquetamento Social no momento de sua criação, de modo a diminuir os índices de má aplicação dos dados na atividade de patrulhamento e uso racional de recursos públicos (LUCENA, 2019, p. 06). Por essa razão, esse sistema apenas utiliza critérios como local, hora e data de crimes passados em suas análises, conforme já mencionado no capítulo anterior.

No entanto, conforme enfatiza Cathy O’Neil, embora os desenvolvedores do PredPol busquem anular qualquer critério discriminatório em seu sistema, os “ciclos de feedback destrutivos” ainda ocorrem. Em entrevista ao El País em 2018, a autora explicou que

> O mapa da delinquência gerado desse modo traça na realidade um rastro de pobreza. [...] Continuamos prendendo negros por coisas pelas quais não prendemos brancos, mas agora já não o dizemos abertamente e disfarçamos de ciência porque o fazemos com o PredPol. Continuamos com o ciclo, porque continuamos prendendo gente de um bairro e os dados nos dizem que precisamos voltar a esse bairro, dessa forma a injustiça policial continua (PEIRÓ, 2018).

Com isso, o que O’Neil quer dizer é que mesmo que decidamos usar conjuntos de dados neutros, algoritmos aplicados dentro de um ambiente injusto criam, consequentemente, um ciclo nocivo, que ajuda a criar o ambiente que justifica suas

suposições. Dessa forma, o algoritmo de previsão de crime não apenas realiza previsões, mas acaba modelando matematicamente a sociedade.

Isso deixa os cientistas de dados, especialistas em ética e desenvolvedores em uma posição desafiadora. Conforme explica Jacob Metcalf (2016), além de ainda não existirem normas específicas sobre como essas tecnologias devem ser revisadas e como seus danos podem ser mitigados, os cientistas de dados tampouco possuem uma solução para acabar com os ciclos de feedback destrutivos, uma vez que os desafios éticos peculiares da análise de dados em Big Data estão apenas começando a ser articulados e discutidos em âmbito internacional.

O que pode ser afirmado com certeza é que é de extrema importância o reconhecimento da teoria do “Labeling Approach” no momento de elaboração dos softwares de predição, de forma a aduzir a compreensão de que a criminalidade não é inerente a determinados indivíduos em razão de suas características e informações sensíveis, sendo essencial que os mesmos não sejam rotulados por esse motivo.

3.2 O CONFLITO ENTRE AS TÉCNICAS DE PREDIÇÃO E OS PRINCÍPIOS E DIREITOS CONSTITUCIONAIS BRASILEIROS

Para que seja plausível a aplicação das técnicas de predição de crimes no Brasil, é essencial que as mesmas não infrinjam os princípios, direitos e garantias fundamentais previstos na Constituição Federal de 1988. Isto é essencial pois os princípios, previstos no Título I da Constituição, guardam os valores fundamentais da ordem jurídica, ao passo que os direitos e garantias fundamentais, previstos no Título II, “são direitos protetivos que garantem o mínimo necessário para que um indivíduo exista de forma digna dentro da sociedade” (FACHINI, 2020).

Proteger a dignidade de cada cidadão significa resguardar o valor intrínseco que estes possuem, definido por Alexandre de Moraes como “um valor espiritual e moral inerente à pessoa, que se manifesta singularmente na autodeterminação consciente

e responsável da própria vida e que traz consigo a pretensão ao respeito por parte das demais pessoas" (1999, p. 66). Dessa forma, como bem pontua Carolina Braga, a dignidade humana "garante às pessoas o direito de serem respeitadas como indivíduos e não como fonte de dados" (2019, p. 74), não podendo tal valor ser diminuído por outras pessoas e muito menos por sistemas de inteligência artificial.

Nesse sentido, é essencial que as normas constitucionais sejam respeitadas para que os direitos individuais inerentes a cada cidadão sejam de fato garantidos, de forma que a tecnologia não seja um empecilho para o alcance destas garantias, mas sim uma ferramenta que auxilie na proteção do ser humano. Todavia, a partir dos exemplos já citados nos tópicos anteriores, resta evidente que os softwares de predição de crimes são capazes de conflitar e pôr em risco alguns dos direitos protegidos pela Constituição, os quais serão abordados neste tópico.

3.2.1 Princípio fundamental da não discriminação

O princípio fundamental da não discriminação, disposto no artigo 3º, inciso IV, da CF/88, determina a promoção do "bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação" (BRASIL, 1988) como um dos objetivos fundamentais da República Federativa do Brasil. Assim, este princípio preza pela igualdade no tratamento de todos os indivíduos independentemente de qualquer característica que os diferencie.

Conforme ressalta Caitlin Sampaio Mulholland, este princípio "deve ser refletido em todas as circunstâncias em que o uso de dados, sejam sensíveis ou não, gere algum tipo de desvalor ou indução a resultados que seriam inequitativos" (2018, p. 174), isto é, o princípio da não discriminação deve servir como fundamento para a tutela dos dados pessoais, de modo a evitar que a utilização do Big Data leve a análises probalisticas tendenciosas e discriminatórias.

Todavia, o que se observa em alguns dos sistemas preditivos é a utilização da técnica de "profiling", onde fatores pessoais como idade, raça e sexo são utilizados

para a criações de perfis que, posteriormente, auxiliarão na tomada de decisões automatizadas. O grande problema reside no fato de que a aplicação desta técnica perpetua vieses e tendências extremamente prejudiciais à parcelas específicas da população, uma vez que faz uso das características pessoais sensíveis de indivíduos para prever o nível de risco que os mesmos podem apresentar à sociedade.

Dessa forma, o status de “potencial criminoso” acaba sendo atribuído à indivíduos específicos de maneira desigual e discriminatória, visto que toma como base justamente as características citadas no inciso IV do artigo 3º da CF/88. Segundo David Lyon, a classificação dos indivíduos com base em informações pessoais obtidas em bancos de dados implica, consequentemente, em uma vigilância por parte de organismos privados ou estatais, capaz de afetar diretamente e de maneira expressiva as oportunidades de vida destes cidadãos na sociedade (2003, p. 01).

Isso ocorre porque, conforme observado por David Lyon, Sarah Brayne e Linnet Taylor, alguns cidadãos, grupos e áreas são fiscalizados com maior regularidade do que outros em razão da desigual distribuição dos mecanismos de vigilância (que se dá com base nos dados e informações coletados sobre os mesmos), de modo a reforçar as desigualdades sociais (NEIVA, 2019, p. 40). Verifica-se uma vigilância em maior intensidade direcionada a grupos marginalizados e socialmente excluídos, tais como “pessoas a cumprir liberdade condicional, indivíduos com medidas sociais, emigrantes, grupos étnicos minoritários” (NEIVA, 2019, p. 40), entre outros.

Destaca-se que, ainda que as informações sensíveis não forem utilizadas para a análise preditiva de crimes, “os dados utilizados como *proxies*, como endereço, podem também, junto com outros dados, gerar perfis relacionados com gênero, raça, preferência sexual e outros considerados como vulneráveis" (BARROCAS, 2016 *apud* BRAGA, 2019, p. 51), o que, de qualquer forma, contribuiria para a discriminação de determinados indivíduos. Assim, a análise preditiva em Big Data sempre correrá o risco de infringir o princípio fundamental da não discriminação.

3.2.2 Direito à privacidade

Em seu artigo 5º, inciso X, a Constituição Federal garante o direito à privacidade, determinando que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988). O disposto neste inciso consiste, portanto, em uma proibição de interferência estatal na vida privada, excepcionados os casos em que tal interferência é permitida por razões importantes e legítimas de interesse público (ARANHA; FERREIRA, 2020).

Para melhor compreensão e valoração deste direito, é importante que a definição de vida privada esteja bem delimitada, sendo possível tomar como base a teoria dos círculos concêntricos de Heinrich Henkel, a qual divide a vida privada em três esferas: a privacidade (esfera maior), em que repousam as relações interpessoais mais rasas, podendo ser facilmente violada por razões de interesse público; a intimidade (esfera intermediária), que congloba informações mais restritas sobre o ser humano, estando protegidos nesta esfera o sigilo domiciliar, profissional e das comunicações telefônicas, que sofrem restrições mais agudas para sua abertura; e o segredo (esfera menor), no qual são guardadas as informações pessoais mais íntimas e sobre as quais o interesse público não poderá interferir, a exemplo da opção sexual, filosófica e religiosa (DI FIORE, 2012, p. 02).

A partir deste conceito, é perceptível o risco que as análises preditivas em Big Data são capazes de ocasionar para a privacidade dos indivíduos, uma vez que é possível que dados que se enquadram na esfera da “intimidade” e do “segredo”, sejam utilizados para criar um perfil de cada indivíduo e determinar seu risco para a sociedade. Segundo Robert Muggah, novas plataformas de previsão de crimes já estão sendo testadas, algumas com o objetivo de combinar redes sociais com histórico criminal para prever crimes, utilizar a inteligência artificial para identificar indivíduos com perfis de maior risco de cometer atos terroristas, entre outros métodos (2019, p. 09), o que muito provavelmente implicará na coleta e uso de dados pessoais sensíveis para tal.

Com os novos riscos que emergem desta coleta e utilização de dados e informações pessoais, tornou-se insuficiente a definição de privacidade como o “direito a ser deixado só”, tendo evoluído para a possibilidade de cada cidadão controlar o uso das informações que lhe dizem respeito (MACHADO, 2014, p. 345). Assim, o direito à privacidade deixa de consistir apenas em uma proibição de interferência estatal e passa a abarcar também a proteção de dados pessoais, não mais se apresentando apenas como “a liberdade negativa de recusar ou proibir a utilização das informações sobre a própria pessoa”, mas como a “liberdade positiva de poder controlar os dados concernentes à própria pessoa” (MACHADO, 2014, p. 346).

Conforme explica Joana Machado, a “possibilidade de os indivíduos e grupos controlarem o exercício dos poderes baseados na disponibilização de informações, é o chamado direito à autodeterminação informativa” (2014, p. 345), o qual se caracteriza como um dos aspectos do direito à privacidade, referente à proteção dos dados pessoais. A autodeterminação informativa permite, portanto, que cada indivíduo exerça controle sobre seus dados e possa decidir, em determinadas situações, se os mesmos podem ou não ser objetos de tratamento e análise por terceiros (BESSA, 2020).

A observância desse direito é de extrema necessidade frente aos novos sistemas que estão sendo implantados no país. Segundo uma reportagem do site The Intercept Brasil, a polícia do Rio de Janeiro comprou softwares de análise de dados da empresa Oracle, também utilizados em países autoritários como a China, os quais apresentam a “possibilidade de combinar dados de recursos humanos, saúde, localização, registros de DNA e dados de doenças mentais” (DIAS; HVISTENDAHL, 2021) nas análises preditivas em Big Data.

Importante ressaltar que este tipo de dados, especificamente referente à saúde, registros de DNA e dados de doenças mentais, “são considerados dados *sensíveis* ou *supersensíveis* porque concernem à saúde e requerem uma tutela jurídica reforçada por afetar o núcleo mais profundo da intimidade das pessoas” (SOUZA, 2010, p. 332). Assim, por integrarem a menor esfera da vida pessoal (nos termos da teoria dos círculos concêntricos), a coleta e tratamento de dados genéticos oferece um risco ainda maior à privacidade do que os dados pessoais comuns (SOUZA,

2010, p. 332), sendo inadmissível a utilização dos mesmos sem a devida autorização por parte do paciente.

Nesse sentido, tem-se que a falta de autodeterminação informativa por parte dos cidadãos põe em risco não apenas o direito garantido no artigo 5º, inciso X, da CF/88, mas também aquele garantido no artigo 21 do Código Civil, que prevê que “a vida privada da pessoa natural é inviolável” (BRASIL, 2002); no artigo 7º, inciso I, do Marco Civil da Internet, que assegura a inviolabilidade da intimidade e da vida privada dos usuários no acesso à internet, e no artigo 8º desta mesma lei, que determina a garantia do direito à privacidade e à liberdade de expressão nas comunicações como condição para o pleno exercício do direito de acesso à internet (BRASIL, 2014).

No entanto, o direito à autodeterminação informativa somente tem relevância no contexto deste estudo quando tratamos dos softwares que utilizam dados pessoais controláveis pelo usuário, como por exemplo informações das redes sociais, dados cadastrais e dados genéticos. Ocorre que a maioria dos softwares de prevenção da criminalidade em uso atualmente consiste em sistemas de monitoramento por meio de câmeras de vigilância e de reconhecimento facial, o que não é algo que os cidadãos podem controlar. É patente que o objetivo do Estado com a implementação deste tipo de mecanismo é a manutenção e melhoria da segurança, porém, na medida em que se observa um aumento exacerbado da vigilância tecnológica em alguns locais ao redor do mundo, cria-se um embate entre a segurança e a privacidade.

Na cidade chinesa de Chongqing, por exemplo, o governo, com o intuito de rastrear suspeitos e prever crimes, tem se utilizado de reconhecimento facial e inteligência artificial para analisar imagens de câmeras de vigilância instaladas em áreas públicas, rastreando movimentos rotineiros da população em busca de comportamentos suspeitos (MUGGAH, 2019, p, 09). O problema reside no fato de que mais de 20 milhões de câmeras controladas pelo Estado foram instaladas na China desde 2017, havendo até mesmo câmeras implantadas nas portas das casas das pessoas (GAN, 2020), o que faz com que a vigilância ocorra em praticamente todos os ambientes que o cidadão frequenta, mitigando o conceito de vida privada.

Adalberto Simão Filho e Germano André Doederlein Schwartz explicam que com o advento do Big Data e da Internet das Coisas, os meios de controle e de vigilância multiplicam-se, de modo que

> Locais públicos e privados de qualquer natureza, possuem câmeras que registram movimentos e, em muitos casos, o som do ambiente. Redes sociais usam de meios tecnológicos para processar e transmitir na velocidade do pensamento, o conjunto de dados sequenciais, decorrentes da transformação tecnológica de sons, diálogos, fotografias, vídeos, possibilitando, através de seus geolocalizadores tecnológicos, determinar com margem de segurança e precisão, os locais de onde são provenientes as transmissões e, por via de consequência, detectar onde se encontra a pessoa, numa aparente ou clara invasão de privacidade (SIMÃO FILHO; SCHWARTZ, 2016, p. 323).

Observa-se, portanto, que o estado de vigilância constante através das máquinas gera um grande dilema, fazendo com que nos questionemos até que ponto é válido que a vida privada de cada indivíduo seja violada em nome da segurança. Destaca-se que, segundo Muggah, no ano de 2019, “membros do recém-eleito governo brasileiro visitaram a China para aprender sobre a tecnologia e estão estudando a possibilidade de usar sistemas chineses de biometria facial na rede brasileira de Circuito Fechado de Televisão” (2019, p. 09, tradução nossa), fato que certamente levantará preocupações acerca do direito à privacidade no país.

A respeito disso, a doutrina propõe o reconhecimento de uma dimensão social da privacidade, a qual Américo Bedê Júnior explica apresentar um duplo aspecto: “primeiro, como uma necessidade de qualquer sociedade, e, segundo, como o reconhecimento da possibilidade de o interesse social justificar o afastamento da privacidade individual” (2015, p. 198). Entende-se, portanto, que a privacidade não pode ser considerada um direito absoluto, pois as medidas preventivas no combate à criminalidade são necessárias para a garantia da segurança, que também é um direito fundamental, previsto no artigo 5º, caput, da CF/88 (BEDÊ JÚNIOR, 2015, p. 106).

Nesse mesmo sentido entendeu o então juiz da 1ª Vara da Fazenda Pública do Rio Grande do Sul, Fernando Carlos Tomasi Diniz, ao julgar improcedente ação movida pela ONG Somos Comunicação Saúde e Sexualidade contra o município de Porto

Alegre e o Estado, em que a instituição se opunha à instalação de câmeras de vídeo em espaços públicos da capital. O magistrado entendeu que “câmeras de vídeo auxiliam na segurança pública e não ofendem a dignidade da pessoa humana e o direito à intimidade e privacidade”, complementando ao dizer que “a restrição da intimidade já ocorre pelo simples fato das pessoas estarem em local público, e não pelas imagens que a câmera possa captar nestes locais” (CONJUR, 2009).

Portanto, é razoável afirmar que, neste caso, o interesse social é relevante o suficiente para flexibilizar a privacidade individual, pois “há um consectário lógico entre a validade das filmagens e a necessidade de proteção” (BEDÊ JÚNIOR, 2015, p. 197). Tendo em vista que nos encontramos hoje na era da tecnologia, é ilusória a ideia de acabar com as filmagens em âmbito público, sendo mais coerente prezar pela sua devida regulamentação e utilização, de modo a impedir que as mesmas sejam divulgadas ou utilizadas para outros fins.

3.2.3 Princípio da presunção de inocência

O artigo 5º, inciso LVII, da Constituição Federal dispõe que “ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória” (BRASIL, 1988), instituindo o princípio da presunção de inocência. Este princípio assegura, portanto, que o acusado só poderá ser condenado por um crime depois de ter “se utilizado de todos os meios de prova pertinentes para sua defesa (ampla defesa) e para a destruição da credibilidade das provas apresentadas pela acusação (contraditório)” (LIMA, 2014, p. 49), isto é, ao término do devido processo legal.

Nesse sentido, como elucida Gustavo Badaró, o princípio da presunção de inocência “é reconhecido, atualmente, como componente basilar de um modelo processual penal que queira ser respeitador da dignidade e dos direitos essenciais da pessoa humana” (2015, p. 57), pois, como explica o autor, este princípio tem ligação direta com a própria finalidade do processo penal, que busca a verificação jurisdicional da ocorrência do delito e de sua autoria, sendo inadmissível que se presuma a culpabilidade de alguém antes que isso ocorra.

Felizmente, as ferramentas de prevenção do crime atualmente em uso no Brasil não são uma ameaça direta à este princípio, pois consistem em medidas não punitivas, as quais buscam reduzir as oportunidades de cometimento de crimes por meio de análise de dados baseados em fatores sociais e territoriais (CHERNEY; SUTTON; WHITE, 2008). Contudo, com o avanço da tecnologia e o desenvolvimento de novas ferramentas preditivas, em breve poderá se falar em uma abordagem “pré-crime”, de modo que os resultados obtidos por meio de análises de dados poderão legitimar a atuação antes da ocorrência do crime.

Conforme explica Jude McCulloch e Sharon Pickering, essa já é uma possibilidade dentre as medidas contra o terrorismo. Diferentemente das técnicas de prevenção de crimes, em que busca-se a causa raiz do crime de modo a preveni-lo, as medidas antiterrorismo pré-crime “prevêem danos graves específicos e criminalizam aqueles que se acredita que cometerão esses possíveis danos futuros, ignorando fatores sociais e territoriais mais amplos” (McCULLOCH; PICKERING, 2009, p. 629, tradução nossa). Assim, a abordagem pré-crime se concentra em erradicar futuros terroristas, “vinculando a polícia coercitiva substancial ou a ação do Estado à suspeita sem a necessidade de acusação, processo ou condenação” (McCULLOCH; PICKERING, 2009, p. 629-630, tradução nossa).

Na medida em que atuação policial e estatal dispensa a necessidade do devido processo legal para que alguém seja considerado culpado de um crime, tem-se a completa obliteração do princípio da presunção de inocência e, consequentemente, uma grave violação da dignidade da pessoa humana. Em razão dos direitos e garantias fundamentaos assegurados na CF/88, este é um cenário improvável no Brasil, porém a discussão acerca desta possibilidade não deixa de ser relevante, uma vez que, conforme já mencionado anteriormente, sistemas de predição que utilizam inteligência artificial para identificar indivíduos com perfis mais suscetíveis ao terrorismo já estão sendo desenvolvidos e testados (MUGGAH, 2019, p. 09).

Frente a este possível cenário, é importante destacar que o princípio da presunção de inocência não se aplica somente à fase judicial da persecução penal, mas também à fase de investigação criminal, com suas devidas adaptações. Conforme

explica Jordi Nieva Fenoll, a forma de atuação da polícia viola inevitavelmente a presunção de inocência, pois, caso contrário, jamais enxergaria os suspeitos como possíveis perpetradores, apenas como inocentes (2016, p. 08). Por essa razão, as suas hipóteses “só podem ser tidas em conta para recolher vestígios de um possível ato criminoso, mas nunca devem ser consideradas no julgamento como se fossem a prova de um ato criminoso” (FENOLL, 2016, p. 08, tradução nossa).

Assim, é inadmissível que os resultados das análises de dados em Big Data sirvam como uma licença para tomar medidas “pré-crime”, isto é, que possam ser utilizados para culpabilizar e punir alguém com a presunção de que este cometerá um delito. As conclusões obtidas por meio de análises preditivas devem servir apenas como evidências, que, conforme já explicado no tópico 2.2 do presente estudo, poderão eventualmente ser utilizadas como prova no processo penal após a devida observância à cadeia de custódia. Somente assim, ao fim do devido processo legal, será possível definir determinado indivíduo como culpado, respeitando o artigo 5º, inciso LVII, da CF/88.

3.2.4 Princípio da individualização da pena

Outro princípio constitucional que merece atenção é o da individualização da pena, disposto no artigo 5º, inciso XLVI, da CF/88. Este princípio preza para que, no momento de uma condenação, "o tratamento penal seja totalmente voltado para características pessoais do agente a fim de que possa corresponder aos fins que se pretende alcançar com a pena ou com as medidas de segurança" (BETTIOL, 2000, p. 336). Ou seja, o indivíduo só pode ser condenado com base em suas próprias ações, de modo a garantir que a pena seja individualizada de acordo com as peculiaridades de cada caso em concreto.

No entanto, se a prova utilizada para condenar alguém é resultado de uma análise preditiva em Big Data, é possível que a aplicação deste princípio seja dificultada. Isto porque, como vimos, os algoritmos preditivos costumam comparar indivíduos à tendências, presumindo, com base em suas características, que determinado grupo

ou categoria de pessoas se comportarão da mesma forma. Como exemplo disso, Cathy O'Neil (2016) cita a diferença na cobrança dos seguros de automóveis, que podem ser mais caros para determinadas pessoas não porque elas dirigem mal, mas porque pessoas com características parecidas tendem a dirigir mal.

Assim, quando um potencial criminoso é detectado pelos softwares de predição, o mesmo não está sendo julgado somente com base em suas próprias ações e características, mas sim com base "em dados relativos a pessoas que compartilham características sociais, demográficas, ou afiliações de grupos geográficos com o indivíduo" (BRAGA, 2019, p. 58). Por essa razão, ferramentas que utilizam algoritmos com a intenção de identificar potenciais criminosos baseando-se em seus perfis conflitam não apenas com o princípio da não discriminação, mas também com o princípio da individualização da pena, caso o mesmo venha a ser condenado com base nessas informações.

Contudo, conforme mencionado anteriormente, os softwares em uso atualmente buscam prevenir que o crime ocorra, e não condenar indivíduos com base na probabilidade de que o cometerão. Desse modo, as análises pautadas em dados geográficos e sociais visam, primariamente, identificar as causas da criminalidade e auxiliar a atividade ostensiva da polícia. Por essa razão, não é possível afirmar que o princípio garantido no artigo 5º, inciso XLVI, da CF/88 está atualmente em risco, uma vez que medidas "pré-crime" não são aplicadas no Brasil.

4 A INAPLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS E A NECESSIDADE DE NOVOS REGULAMENTOS

Conforme foi demonstrado no decorrer deste estudo, a utilização do Big Data e a massiva coleta e análise de dados pessoais é bastante vantajosa e útil na prevenção do crime, uma vez que produz resultados concretos na diminuição da criminalidade nos locais em que esta tecnologia é aplicada. Em contrapartida, surgem "os riscos, os perigos e a tênue linha entre o tratamento de dados pessoais na estrita

legalidade, e a violação de direitos fundamentalmente garantidos pela Constituição Federal a partir deste" (AGUDO; TEIXEIRA, 2020, p. 240).

Frente a esses riscos, a devida regulamentação acerca da coleta e do tratamento de dados pessoais é extremamente necessária, independentemente da finalidade pela qual serão utilizados. No Brasil, a Lei Geral de Proteção de Dados (Lei nº 13.709/18) foi sancionada em agosto de 2018 visando uniformizar as questões envolvendo esse tratamento, "inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018), segundo o seu artigo 1º, caput.

Conforme explica Hugo Crivilim Agudo e Tarcísio Teixeira, a LGPD "traz conceitos e imposições normativas a serem respeitadas, no intuito de limitar tanto a coleta de dados pessoais, quanto a utilização destes, a partir do Big Data, sem o expresso consentimento dos detentores iniciais das informações" (2020, p. 232), ou seja, a Lei preza pelo respeito à autodeterminação informativa, sendo essencial que os titulares dos dados expressem consentimento para sua utilização. Destaca-se que este consentimento vai além do simples aceite por parte do usuário, sendo definido pelo artigo 5º, XII, da LGPD como "a manifestação da vontade livre, informada e inequívoca" (BRASIL, 2018), a qual deve ser expressa por escrito ou por outro meio que a demonstre, nos termos do artigo 8º, caput (BRASIL, 2018).

Ao tratarmos da utilização de dados pessoais no âmbito dos negócios, como é o caso das publicidades direcionadas, as empresas possuem o dever de informar os usuários sobre a coleta, o uso e o compartilhamento dos seus dados (MORELLATO; SANTOS, 2021, p. 192). Conforme explica Ana Carolina Morellato e André Filipe Reid dos Santos, esta etapa preliminar é necessária pois o titular deve ter ciência sobre como seus dados pessoais serão utilizados e "deve ser capaz de controlar seus dados sem coação física ou moral, a fim de que a autodeterminação informacional seja livre e verdadeira" (2021, p. 192).

Contudo, no contexto aqui tratado, expressar o consentimento pode ser uma tarefa difícil, tendo em vista que muitos sistemas de análise preditiva de crimes utilizam

algoritmos obscuros e desconhecidos sob a alegação de segredo industrial ou até mesmo dados biométricos a partir de câmeras de vigilância. Como já exemplificado anteriormente, os algoritmos operam sobre dados e são capazes de ordená-los, classificá-los, descobrir conhecimento, estabelecer perfis (profiling), reconhecer faces, tomar decisões automatizadas (FREITAS, 2020), dentre muitas outras funções, sendo que na maioria das vezes isso ocorre sem que os usuários possam saber quais de seus dados estão sendo coletados e como estão sendo utilizados.

Embora a LGPD estabeleça em seu artigo 20 que os usuários possuem o direito de "solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses" (BRASIL, 2018), esse dispositivo não pode ser aplicado quando tratamos das análises realizadas para a prevenção ou repressão de ilícitos penais. Isso porque o artigo 4º, inciso III, da LGPD define que a lei não se aplica ao tratamento de dados pessoais realizados para fins exclusivos de: "a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais" (BRASIL, 2018).

Dessa forma, os usuários que possuem seus dados pessoais coletados e analisados pelo Estado sob a finalidade de prever, prevenir e reduzir a criminalidade não são protegidos pela lei, uma vez que se enquadram nas hipóteses previstas no inciso III do artigo 4º. Segundo o parágrafo 1º deste mesmo artigo, "o tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público" (BRASIL, 2018), no entanto, até hoje não há qualquer lei específica efetivada que regulamente o tratamento de dados no tocante à persecução penal e segurança pública.

Não há de se ignorar que a legislação brasileira trata sobre o sigilo de informações e sua quebra em diferentes situações, tal como nas comunicações telefônicas (Lei 9.296/96) e nas comunicações eletrônicas (Lei 12965/14 - Marco Civil da Internet), regulando as condições em que dados considerados sigilosos podem ser acessados pelas autoridades (MOURA, 2021). Contudo, no que tange às questões relacionadas

à proteção e tratamento de dados pessoais gerais para fins penais, ainda não há a devida e necessária regulamentação.

4.1 O ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS PARA A SEGURANÇA PÚBLICA E PERSECUÇÃO PENAL

Para preencher a lacuna deixada pela LGPD, uma Comissão de Juristas foi instituída, em novembro de 2019, para a elaboração de uma lei específica que regulamente o tema e proporcione “segurança jurídica para as investigações e os procedimentos criminais, sem deixar de lado a transparência no uso de informações individuais pelos órgãos de segurança” (PORTAL STJ, 2020). O Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal, que ficou conhecido como “LGPD-Penal”, foi recebido pelo presidente da Câmara dos Deputados um ano depois, em novembro de 2020 (MOURA, 2021).

A partir do nome dado ao anteprojeto é perceptível que o mesmo regula apenas as alíneas “a” e “d” do artigo 4º, III, da LGPD, quais sejam, respectivamente, a segurança pública e as atividades de investigação e repressão de infrações penais. Segundo especialistas, esta foi uma boa escolha pois

> “[...] entende-se que o balanceamento entre interesses coletivos e individuais difere bastante quando se trata de defesa nacional e segurança do Estado. Nesse sentido, abarcar todas alíneas do art. 4º, III, em uma mesma lei poderia prejudicar a intenção deste anteprojeto de ser uma lei geral — se obrigando a apresentar diversas exceções — e impedir um debate público de qualidade, devido às variadas finalidades” (FERNANDES et al, 2021, p. 02).

Nesse sentido, restringir a abrangência às alíneas “a” e “d” é uma forma de proteger mais adequadamente e de maneira universal o tratamento dos dados pessoais no âmbito penal, uma vez que a garantia da defesa nacional e da segurança do Estado demandaria diretrizes diferentes. É claro que, deixando de fora as alíneas “b” e “c” do artigo 4º, inciso III, a lacuna existente na LGPD seria apenas parcialmente preenchida, porém este fato não diminui a urgência da efetivação do anteprojeto aqui tratado.

Conforme mencionado na exposição de motivos do próprio anteprojeto, a necessidade de sua elaboração se evidencia a partir de dois problemas centrais que decorrem da lacuna legislativa: (i) a falta de adequação aos padrões internacionais de segurança sobre o tratamento de dados, o que impede a integração do Brasil com órgãos de investigação internacionais e, consequentemente, obsta o acesso à bancos de dados relevantes; e (ii) a falta de proteção dos cidadãos por não haver regulação sobre a "licitude, a transparência ou a segurança do tratamento de dados em matéria penal, tampouco direitos estabelecidos ou requisitos para utilização de novas tecnologias que possibilitam um grau de vigilância e monitoramento impensável há alguns anos" (CÂMARA DOS DEPUTADOS, 2020).

Levando estes pontos em consideração, a Comissão de Juristas tomou como inspiração a LGPD e a Diretiva nº 680/2016 da União Europeia para estruturar o anteprojeto da LGPD-Penal, formando 12 capítulos com 68 artigos que tratam sobre o "âmbito de aplicação da Lei; condições de aplicação; base principiológica; direitos e obrigações; segurança da informação; tecnologias de monitoramento; transferência internacional de dados e; a autoridade de supervisão" (CÂMARA DOS DEPUTADOS, 2020).

Logo em seu artigo primeiro, o anteprojeto dispõe que o objetivo da Lei é "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (CÂMARA DOS DEPUTADOS, 2020), definido, para isso, os fundamentos da disciplina da proteção de dados pessoais nas atividades de segurança pública e de persecução penal, quais sejam:

> Art. 2º [...]
> I - a dignidade, os direitos humanos, o livre desenvolvimento da personalidade, e o exercício da cidadania pelas pessoas naturais;
> II - a autodeterminação informativa;
> III - o respeito à vida privada e à intimidade;
> IV - a liberdade de manifestação do pensamento, de expressão, de informação, de comunicação e de opinião;
> V - a presunção de inocência;
> VI - confidencialidade e integridade dos sistemas informáticos pessoais; e
> VII - garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal (CÂMARA DOS DEPUTADOS, 2020).

Observa-se, a partir dos fundamentos listados, que os legisladores reconheceram a possibilidade de conflito entre o uso desenfreado das tecnologias de vigilância e os

direitos e liberdades individuais dos cidadãos, e estabeleceram, assim, quais direitos devem ser necessariamente observados durante todo o processo de coleta e tratamento de dados. Dessa forma, a LGPD-Penal busca alcançar uma harmonia, visando assegurar o interesse da coletividade ao regular a atividade do Estado, ao passo que se preocupa em minimizar os possíveis efeitos da aplicação dessas tecnologias na vida privada de cada cidadão (MIGLIORINI; TRIVIÑO, 2020).

Destaca-se que o anteprojeto determina ainda, em seu artigo 40, que as autoridades competentes forneçam “informações claras e atualizadas sobre a base legal, a finalidade, os objetivos específicos, os procedimentos e as práticas utilizadas para a execução dessas atividades” (CÂMARA DOS DEPUTADOS, 2020). Além disso, define como um direito dos titulares que as decisões tomadas com base no tratamento automatizado de seus dados pessoais sejam precedidas de autorização do Conselho Nacional de Justiça (CNJ) e de publicação de um relatório de impacto, de modo a comprovar “a adoção das garantias adequadas para os direitos e liberdades do titular, incluído o direito de solicitar a revisão da decisão por uma pessoa natural” (CÂMARA DOS DEPUTADOS, 2020).

Como forma de concretizar essa proteção, buscando maior controle sobre a vigilância estatal e a preservação ao direito à privacidade dos dados, o anteprojeto prevê, em seu artigo 42, que a aplicação de tecnologias de monitoramento ou tratamento de dados pessoais que representem alto risco para os direitos e garantias dos titulares de dados dependerá de previsão legal específica (CÂMARA DOS DEPUTADOS, 2020). Para isso, é necessária a elaboração de um documento denominado “análise de impacto regulatório”, o qual irá instruir o processo legislativo acerca da autorização para a utilização de tais tecnologias, nos termos do artigo 5º, inciso XIX, do Anteprojeto de Lei (CÂMARA DOS DEPUTADOS, 2020).

Ademais, deverá ser elaborado um relatório de impacto à proteção de dados pessoais, que, segundo o artigo 5º, XVIII, da LGPD-Penal, consiste em uma documentação do controlador contendo “a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco” (CÂMARA DOS DEPUTADOS, 2020). Este relatório é exigido não apenas nos

casos de aplicação de uma nova tecnologia, mas toda vez que ocorrer o tratamento de dados pessoais sensíveis, conforme dispõe o parágrafo único do artigo 13 da LGPD-Penal (CÂMARA DOS DEPUTADOS, 2020).

Adiante, o artigo 43 determina que

> No âmbito de atividades de segurança pública, é vedada a utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial (CÂMARA DOS DEPUTADOS, 2020).

O artigo citado veda, portanto, a livre utilização de tecnologias de vigilância que identifiquem pessoas indeterminadas em tempo real, como por exemplo as câmeras de segurança que utilizam biometria e reconhecimento facial. Assim, observa-se que, neste ponto, o anteprojeto "mitiga os riscos de violação de diversos direitos como a privacidade, a liberdade de expressão e a liberdade de associação" (FERNANDES et al, 2021, p. 05), porém acaba por mitigar também o direito à segurança, uma vez que impõe significativas restrições às atividades voltadas para a segurança pública.

Outra vedação ocorre no artigo 45 do anteprojeto de lei, o qual determina que o uso compartilhado de dados pessoais entre autoridades competentes somente poderá ocorrer mediante autorização legal ou judicial, além de proibir, em seu §1º, "o compartilhamento direto e contínuo de bancos de dados que contenham dados pessoais estabelecidos no âmbito de atividades de segurança pública com órgãos responsáveis pela persecução penal" (CÂMARA DOS DEPUTADOS, 2020), ressalvadas as hipóteses legais. O problema em determinar tal restrição reside no fato de que o compartilhamento de bancos de dados entre estes órgãos "consiste em emanação concreta do princípio da eficiência, contribuindo sobremaneira para a proteção suficiente de bens jurídicos de relevância constitucional, notadamente o direito fundamental à segurança" (BARRETO; MARQUES; NETO, 2020).

Portanto, a partir de uma leitura do anteprojeto, nota-se que sua redação apresenta uma base sólida para a proteção dos direitos fundamentais e garantias processuais dos cidadãos brasileiros frente à implementação de sistemas de análise preditiva da

criminalidade e o tratamento de dados pessoais, mas, para isso, estabelece diversas restrições à atividade estatal. Outrossim, faz um bom trabalho ao estabelecer os deveres do Estado na prevenção de ilícitos criminais, auxiliando na tutela da segurança e da ordem pública. É claro que, ainda que haja a devida regulamentação, é plenamente possível que conflitos de interesse ocorram e, uma vez que os direitos fundamentais não são absolutos, far-se-á necessário que cada caso concreto seja devidamente analisado considerando suas particularidades.

De toda forma, a concretização de uma LGPD Penal se mostra cada vez mais necessária, pois, como pontua Naiara Moura, observa-se atualmente no Brasil "uma grande tendência de investimento nas tecnologias de vigilância, compreendidos no avanço da inteligência artificial e o interesse das empresas de tecnologia na venda de seus produtos e serviços para o Estado" (2021). Como mencionado anteriormente, membros do governo brasileiro já até mesmo prestaram uma visita à China buscando aprender sobre tecnologias de vigilância, além de que, no Rio de Janeiro, softwares de análise preditiva da criminalidade já estão sendo implementados.

Com as novas tecnologias em ascensão, conclui-se que enquanto a lacuna na legislação existir, os cidadãos brasileiros estarão à mercê da livre atuação do Estado quando esta for baseada na proteção da ordem e da segurança pública ou na investigação e repressão de infrações penais. Além disso, preencher essa lacuna é essencial para garantir que os próprios órgãos responsáveis pela segurança pública "detenham maior segurança jurídica para exercer suas funções com maior eficiência e eficácia" (CÂMARA DOS DEPUTADOS, 2020).

Visto que no Brasil esta discussão está apenas no início e que o anteprojeto é uma proposta embrionária, a expectativa é que os juristas enfrentem muitos obstáculos. Contudo, apenas com o devido regulamento será possível nortear a atividade das autoridades e tornar segura a aplicação das novas tecnologias e tratamento de dados, de modo a garantir o respeito ao princípio da não discriminação, à privacidade, a autodeterminação informativa e aos princípios processuais penais como o devido processo legal, a presunção de inocência, a ampla defesa e o contraditório.

CONCLUSÃO

O avanço e a disseminação das tecnologias preditivas têm proporcionado melhorias significativas na segurança e na ordem pública nos locais em que são utilizadas, uma vez que tornam possível, por meio de análises estatísticas, a identificação de lugares de risco, de horários prováveis de ocorrência de crimes e até mesmo de potenciais infratores, viabilizando uma atuação preventiva da polícia.

Assim como muitos outros países, o Brasil está buscando implementar novos sistemas que objetivam prever e impedir a ocorrência de crimes a partir da análise de dados pessoais em Big Data, visto que esta técnica tem demonstrado resultados concretos na diminuição de atividades criminosas nas cidades em que é aplicada. Contudo, embora seja uma técnica promissora, ainda há muitos desafios a serem enfrentados antes que a mesma possa ser aplicada no Brasil de forma segura.

Em primeiro lugar, os riscos que advém da utilização das tecnologias preditivas devem ser previamente reconhecidos para que possam ser mitigados. Conforme foi explicado, há um risco inerente aos sistemas que utilizam dados pessoais sensíveis (tais como origem racial ou étnica, convicção religiosa, opinião política, etc.) para a realização das análises preditivas da criminalidade, uma vez que a forma de programação dos algoritmos pode fazer com que padrões existentes de discriminação sejam reproduzidos e que tendências errôneas sejam reforçadas a partir das informações embutidas nos bancos de dados.

Assim como foi demonstrado no terceiro capítulo, esta técnica tem o potencial de perpetuar o pensamento criminológico positivista, o qual consiste na crença de que é possível determinar o perfil do homem criminoso com base em suas características físicas e sociais. Da mesma forma, muitos sistemas preditivos utilizam as análises em Big Data para traçar os perfis de cada usuário baseando-se em informações de sua personalidade, sendo possível que sejam classificados como maior ou menor risco para a sociedade, o que posteriormente influenciará a atuação da polícia.

Classificar alguém como um potencial criminoso com base em sua cor da pele, idade, religião ou até mesmo no local onde mora é, no entanto, um ato explícito de discriminação, sendo incontestável que, em nosso país, a população negra e os mais pobres seriam excessivamente prejudicados por tais medidas. Assim como foi provado que a criminologia positivista é completamente falha, esta técnica, embora funcione por meio de algoritmos, tampouco possui embasamento científico, sendo apenas uma forma de atribuir o status de criminoso a determinados indivíduos com base em preconceitos humanos.

Neste ponto, evidencia-se a importância do pensamento criminológico crítico, que, ao contrário do anteriormente explicado, entende que as noções sobre o crime e o criminoso não são inatas, mas socialmente construídas, ou seja, ocorre um rotulamento dos indivíduos, o que se denomina “Labeling Approach” ou teoria do etiquetamento social. Este rotulamento é feito quando os sistemas preditivos utilizam-se das técnicas de “profiling”, ou seja, quando são traçados perfis criminosos com base nas informações sensíveis de cada usuário.

A compreensão destes preceitos é fundamental no momento de elaboração dos sistemas preditivos, uma vez que o viés discriminatório dos algoritmos é ocasionado por falhas presentes desde o desenvolvimento dos sistemas de predição. Assim, é essencial que os desenvolvedores analisem, de forma consciente, técnica e isenta, o perfil de aplicação dos softwares e a quem se destina (LUCENA, 2019), a fim de evitar que discriminações socialmente construídas sejam reproduzidas.

De todo modo, para que os riscos de estigmatização social dos cidadãos sejam efetivamente mitigados, a melhor alternativa é excluir dos sistemas as análises baseadas em dados sensíveis e criação de perfis, pois, além de ser inevitável que certo nível de discriminação ocorra, este tipo de análise demonstra pouca (ou quase nenhuma) efetividade na diminuição do crime e da violência, de forma que sua aplicação não compensa os riscos. Assim, a utilização de critérios como local, hora e data de crimes passados para a realização de previsões certamente proporcionará maior segurança aos usuários ao passo que continuará a auxiliar na garantia da segurança e da ordem pública.

Adiante, para que seja viável a aplicação dos sistemas de predição da criminalidade, é essencial que os mesmos não infrinjam os direitos e garantias constitucionais. No entanto, como vimos no terceiro capítulo, é possível que haja um conflito entre ambos. Pelo exposto nos parágrafos acima, já é possível notar que o princípio fundamental da não discriminação é posto em risco em razão das técnicas de perfilamento, uma vez que o status de criminoso é atribuído à indivíduos específicos de maneira desigual e discriminatória, prejudicando sempre as mesmas camadas da população. Logo, a exclusão destas técnicas minimizaria esta ameaça.

A exclusão das técnicas de “profiling” reduziria também o conflito com o direito à privacidade, tendo em vista que os dados pessoais sensíveis utilizados nas análises fazem parte da esfera da intimidade de cada cidadão. Ainda assim, as análises em Big Data não deixariam de conflitar com este direito, pois muitos softwares de prevenção da criminalidade em uso atualmente consistem em monitoramento por câmeras de vigilância e de reconhecimento facial, implicando em um aumento exacerbado da vigilância tecnológica. No entanto, é importante levar em conta o entendimento doutrinário e jurisprudencial de que os direitos fundamentais não são absolutos, sendo razoável que a privacidade individual seja flexibilizada em prol do interesse social, desde que as tecnologias sejam utilizadas de maneira consciente.

Além disso, há a preocupação acerca de alguns dos princípios constitucionais do processo penal, tendo sido destacados especificamente o princípio da presunção de inocência e o da individualização da pena no terceiro capítulo. Tais princípios passam a ser ameaçados a partir do momento em que as análises em Big Data são utilizadas como um vetor que permite agir antes do fato, isto é, quando as previsões realizadas pelos softwares são utilizadas como uma licença para culpabilizar e punir alguém com a presunção de que este cometerá um delito, antes que possa se utilizar de todos os meios de prova viáveis para sua defesa.

Todavia, com base nas investigações realizadas ao longo deste estudo, não há qualquer indicação de que o Brasil planeja realizar abordagens “pré-crime”, uma vez que é um procedimento extremamente duvidoso e arriscado. Conforme mencionado, esta é uma medida utilizada atualmente em alguns países especificamente para prevenir atos terroristas, de modo a criminalizar aqueles que se acredita que

cometerão danos futuros. Caso o Brasil eventualmente considere a adoção de tais medidas, é preciso que haja uma forte regulamentação acerca deste tema, assim como há o Terrorism Act no Reino Unido e USA PATRIOT Act nos Estados Unidos.

No entanto, como visto no último capítulo deste trabalho, sequer há no Brasil uma lei que proteja os dados pessoais quando utilizados para fins penais, elemento essencial para que as tecnologias de predição de crimes sejam aplicadas de maneira segura. Por ora, aguarda-se a aprovação do Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal, o qual busca estabelecer limites ao uso dos dados pessoais por parte das autoridades e garantir maior transparência e segurança na aplicação da tecnologia aqui tratada.

A necessidade deste regulamento manifesta-se frente às ameaças que a má aplicação destas técnicas e a falta de limites no uso e tratamento de dados pessoais pode ocasionar aos direitos e liberdades dos cidadãos. Conforme disposto no próprio anteprojeto da LGPD-Penal, a ausência de uma lei que regule sua utilização e implicações no âmbito penal gera uma grande assimetria de poder entre o Estado e os cidadãos, uma vez que os os titulares de dados são deixados sem garantias normativas mínimas e mecanismos institucionais aplicáveis para resguardar seus direitos de personalidade, suas liberdades individuais e a observância do devido processo legal (CÂMARA DOS DEPUTADOS, 2020).

Destaca-se, ainda, que além de ser necessária a regulação da atividade dos controladores de dados para este fim, é importante também que sejam definidas regras e procedimentos a serem seguidos durante a análise de vestígios especificamente virtuais, pois, conforme explicado neste trabalho, os dados pessoais coletados e utilizados nas análises em Big Data podem, futuramente, se tornar provas em um processo penal. Assim, tendo em vista que a plausibilidade da utilização de provas no processo penal decorre necessariamente da obediência à cadeia de custódia, é imprescindível o desenvolvimento de um regulamento mais específico no Brasil quanto ao tratamento de vestígios digitais, de forma a garantir maior segurança às partes envolvidas no processo.

Portanto, tendo em vista todas as questões investigadas e analisadas no decorrer deste trabalho, conclui-se que a utilização do Big Data para a predição de crimes ainda não é plausível no Brasil, uma vez que, até o presente momento, não há qualquer legislação que regule a aplicação desta técnica e defina os limites da atuação Estatal, o que acaba por deixar os cidadãos em estado excessivo de vulnerabilidade. Felizmente, o novo anteprojeto de lei deverá abrir portas para este debate tão relevante frente ao crescente e incontível desenvolvimento da tecnologia.

REFERÊNCIAS

ABREU, Giovanna; NICOLAU, Marcos. Big Data, publicidade e o consumidor dataficado: o caso da série House of Cards. **Revista Culturas Midiáticas**, Ano X, n. 18, p. 135-151, jan/jun. 2017. Disponível em: <https://periodicos.ufpb.br/index.php/cm/article/download/35074/17935/> Acesso em: 09 abr. 2021.

AGUDO, Hugo Crivilim; TEIXEIRA, Tarcisio. As limitações da utilização de mecanismos de Big Data à luz da lei geral de proteção de dados. In: TEIXEIRA, Tarciso; MAGRO, Américo Ribeiro (Coord.). **Proteção de Dados:** Fundamentos Jurídicos. Salvador: Editora JusPodivm, 2020. p. 229-265.

ARANHA, Estela; FERREIRA, Lucia Maria Teixeira. **O direito fundamental à proteção de dados e a importância da proposta de alteração constitucional nº 17/2019.** OAB RJ, 2020. Disponível em: <http://www.oabrj.org.br/noticias/artigo-direito-fundamental-protecao-dados-importancia-proposta-alteracao-constitucional> Acesso em: 20 abr. 2021.

BADARÓ, Gustavo Henrique. **Processo Penal**. 3ª ed., ver. atual e ampl. São Paulo: Thomson Reuters Brasil, 2015.

BARATTA, Alessandro. **Criminologia crítica e crítica do direito penal:** introdução à sociologia do direito penal. 6ª ed. Rio de Janeiro: Editora Revan, 2011.

BARRETO, Pablo Coutinho; MARQUES, Paulo Rubens Carvalho; PAULO NETO, Octávio Celso Gondim. **O anteprojeto da 'LGPD penal' e a (in) segurança pública e (não) persecução penal.** JOTA, 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-anteprojeto-da-lgpd-penal-e-a-in-seguranca-publica-e-nao-persecucao-penal-09122020#_ftn3> Acesso em: 20 maio 2021.

BEDÊ JÚNIOR, Américo. **A retórica do direito fundamental à privacidade:** a validade da prova obtida mediante filmagens nos ambientes públicos e privados. Salvador: Editora JusPodivm, 2015.

BESSA, Leonardo Roscoe. **A LGPD e o direito à autodeterminação informativa.** 2020. Disponível em: <http://genjuridico.com.br/2020/10/26/lgpd-direito-autodeterminacao-informativa/> Acesso em: 20 abr. 2021.

BETTIOL, Giuseppe. **Direito penal**. Campinas: Red Livros, 2000.

BONNA, Alexandre Pereira; PINHEIRO, Victor Sales. Sociedade da informação e direito à privacidade no Marco Civil da Internet: fundamentação filosófica do Estado de Direito em John Finnis. **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 21, n. 3, p. 365-394, set./dez. 2020. Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1555/574> Acesso em: 18. maio 2021.

BOYD, Danah; BRAYNE, Sarah; ROSENBLAT, Alex. Predictive policing. In: **Data & Civil Rights:** A New Era Of Policing And Justice. 2015. Disponível em: <https://datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf> Acesso em: 13 mar. 2021.

BRAGA, Carolina Henrique da Costa. **Decisões automatizadas e discriminação:** pesquisa de proposras éticas e regulatórias no policiamento preditivo. Dissertação (Pós graduação em Princípios Fundamentais e Novos Direitos) - Universidade Estácio de Sá, Rio de Janeiro - RJ, 2019. Disponível em: <https://portal.estacio.br/media/4679621/carolina-henrique-da-costa-braga.pdf> Acesso em: 12 mar. 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Diário Oficial da União, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 20 maio 2021.

_____. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Brasília: Diário Oficial da União, 1941. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm> Acesso em: 20 maio 2021.

_____. **Lei nº 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Brasília: Diário Oficial da União, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm> Acesso em: 20 maio 2021.

_____. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Diário Oficial da União, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 20 maio 2021.

_____. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Diário Oficial da União, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 20 maio 2021.

BRUNO, Fernanda. **Rastrear, classificar, performar**. Ciência e Cultura, São Paulo, v. 68, n. 1, p. 34-38, jan./mar. 2016. Disponível em: <http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252016000100012> Acesso em: 29 mar. 2021.

BURKE, Anderson. **Vitimologia**: Manual da Vítima Penal. Salvador: JusPodivm, 2019.

CÂMARA DOS DEPUTADOS. **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal**. 2020. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf> Acesso em: 20 maio 2021.

CÂMERAS de segurança não invadem a privacidade. **CONJUR**, 2009. Disponível em: <https://www.conjur.com.br/2009-set-24/cameras-seguranca-ruas-nao-invadem-privacidade-decide-juiz> Acesso em: 02 maio 2021.

CAPLAN, Joel M.; KENNEDY, Leslie K. **Risk Terrain Modeling Manual:** Theoretical Framework and Technical Steps of Spatial Risk Assessment for Crime Analysis. Newark, 2010.

CARVALHO, Salo de. **Pena e Garantias**. 3ª ed. Rio de Janeiro: Lumen Juris, 2008.

CHERNEY, Adrian; SUTTON, Adam; WHITE, Rob. **Crime Prevention:** Principles, perspectives and practices. Cambridge: Cambridge University Press, 2008.

COMISSÃO entrega à Câmara anteprojeto sobre tratamento de dados pessoais na área criminal. **PORTAL STJ**, 2020. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx> Acesso em: 17 maio 2021.

CUNHA, Rogério Sanches. **Pacote Anticrime - Lei 13.964/2019**: Comentários às alterações no CP, CPP e LEP. Salvador: Editora Juspodivm, 2020.

CURTIS, Hillman. Vídeo (30 seg). COMMERCIAL: IBM: The Road. **Vimeo**, 06 mar. 2011. Disponível em: <https://vimeo.com/20718357> Acesso em: 02 mar. 2021.

DIAS, Tatiana; HVISTENDAHL, Mara. **Polícia do Rio comprou tecnologia da Oracle usada por países autoritários.** The Intercept Brasil, 10 mar. 2021. Disponível em: <https://theintercept.com/2021/03/10/policia-rio-tecnologia-oracle-policias-paises-autoritarios/ > Acesso em: 16 mar. 2021.

DI FIORE, Bruno Henrique. **Teoria dos círculos concêntricos da vida privada e suas repercussões na praxe jurídica**. 2012. Disponível em: <http://www.flaviotartuce.adv.br/assets/uploads/artigosc/201109281258590.Artigo_brunofiore.doc> Acesso em: 29 abr. 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães. LONGUI, João Victor Rozatti (Coord.) **Direito Digital**: direito privado e internet. SP: Foco, 2019. p. 36-53.

EDINGER, Carlos. Cadeia de custódia, rastreabilidade probatória. **Revista Brasileira de Ciências Criminais**, v. 24, n. 120, p. 237-257, mai./jun. 2016. Disponível em : <https://www.ibccrim.org.br/publicacoes/edicoes/685/7687> Acesso em: 14 abr. 2021.

FACHINI, Tiago. **Direitos e garantias fundamentais**: conceito e características. ProJuris, 2020. Disponível em: <https://www.projuris.com.br/o-que-sao-direitos-fundamentais#conclusao> Acesso em: 19 abr. 2021.

FENOLL, Jordi Nieva. La razón de ser de la presunción de inocencia. **InDret - Revista para el Análisis del Derecho**, Barcelona, n. 1, p. 1-23, jan. 2016. Disponível em: <https://indret.com/wp-content/uploads/2018/05/1203_es.pdf> Acesso em: 18 abr. 2021.

FERGUSON, Andrew Guthrie. **Beyond Data-Driven Policing**. American Scientist, 2017. Disponível em: <https://www.americanscientist.org/article/beyond-data-driven-policing> Acesso em: 19 mar. 2021.

FERNANDES, Elora et al. **Comentários ao Anteprojeto de Lei de Proteção de Dados para a Segurança Pública**: Tecnologia de Reconhecimento Facial. Instituto de Tecnologia & Sociedade do Rio, 2021. Disponível em: <https://itsrio.org/wp-content/uploads/2021/04/UK-Comentarios_LGPDPenal.pdf> Acesso em: 19 maio 2021.

FREITAS, Cinthia Obladen de Almendra. **A obscuridade dos algoritmos e a LGPD**. 2020. Disponível em: <https://www.inpd.com.br/post/a-obscuridade-dos-algoritmos-e-a-lgpd> Acesso em: 12 maio 2021.

GAN, Nectar. **Na China, há câmeras na porta da casa das pessoas - às vezes, do lado de dentro.** CNN, 29 abr. 2020. Disponível em: <https://www.cnnbrasil.com.br/internacional/2020/04/29/na-china-ha-cameras-na-porta-da-casa-das-pessoas-as-vezes-do-lado-de-dentro> Acesso em: 22 abr. 2021.

HEILIK, Jacob. **Chain of Custody for Digital Data:** A Practitioner's Guide. Canadá: Independently published, 2019.

HIRSCHFELD, Daniela. **Twitter data accurately tracked Haiti cholera outbreak**. 2012. Disponível em: <https://www.nature.com/news/twitter-data-accurately-tracked-haiti-cholera-outbreak-1.9770> Acesso em: 23 fev. 2021.
KEMP, Simon. **Digital 2020**: 3.8 billion people use social media. We Are Social, 2020. Disponível em: <https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media> Acesso em: 21 maio 2021.

LANEY, Doug. **3-D Data Management:** Controlling Data Volume, Velocity, and Variety. META Group, 2001. Disponível em: <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf> Acesso em: 11 abr. 2021.

LIMA, Renato Brasileiro de. **Manual de processo penal**. vol. único, 2ª ed. Salvador: JusPodivm, 2014.

LUCENA, Pedro Arthur Capelari de. **Policiamento preditivo, discriminação algorítmica e racismo:** potencialidades e reflexos no brasil. VI Simpósio Internacional LAVITS - Assimetrias e (In)visibilidades: Vigilância, Gênero e Raça. Salvador, 2019. Disponível em: <https://lavits.org/wp-content/uploads/2019/12/Lucena-2019-LAVITSS.pdf > Acesso em: 09 abr. 2021.

MACHADO, Joana de Moraes Souza. A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados. **Revista da AJURIS**, Porto Alegre, v. 41, n. 134, p. 337-363, jun. 2014. Disponível em: <http://ajuris.kinghost.net/OJS2/index.php/REVAJURIS/article/viewFile/206/142> Acesso em: 20 abr. 2021.

MAGRO, Américo Ribeiro. A (in)eficácia do direito à anonimização de dados pessoais em face da análise de Big Data dos metadados produzidos no âmbito da internet das coisas. In: TEIXEIRA, Tarciso. MAGRO, Américo Ribeiro (Coord.). **Proteção de Dados:** Fundamentos Jurídicos. Salvador: Editora JusPodivm, 2020. p. 13-51.

MALLMITH, Décio de Moura. **Vestígio material, corpo de delito, evidência e indício**. 2007. Disponível em: <https://acrigs.com.br/wp-content/uploads/2020/11/Vestigio.pdf > Acesso em: 08 mar. 2021.

MARQUES, José Frederico. **Curso de Direito Penal**. Vol. I. São Paulo: Saraiva, 1954.

MARQUES, José Frederico. **Manual de Direito Processual Civil**. Vol. II. 1ª edição. Campinas: Bookseller, 1997.

MARR, Bernard. **Big Data:** The 5 Vs Everyone Must Know. 2014. Disponível em: <https://www.linkedin.com/pulse/20140306073407-64875646-big-data-the-5-vs-everyone-must-know> Acesso em: 22 fev. 2021.

MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación tecnológica de la justicia:** Obtención, tratamiento y protección de datos en la justicia. 1ª ed. Madrid: Wolters Kluwer, 2020.

MARTÍNEZ, Juan Carlos Férnandez. Especialidades de la prueba cuando, esta, es tecnológica. In: BURGOS, Enrique Ortega (Dir.). **Actualidad:** Nuevas Tecnologías. Valencia: Tirant lo Blanch, 2020.

MCCULLOCH, Jude; PICKERING, Sharon. Pre-Crime and Counter-Terrorism: Imagining Future Crime in the “War on Terror”. **The British Journal of Criminology**, Oxford, v. 49, n. 5, p. 628-645, set. 2009. Disponível em: <https://doi.org/10.1093/bjc/azp023> Acesso em: 12 mar. 2021.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014.

METCALF, Jacob. **Ethics review for pernicious feedback loops:** reading Weapons of Math Destruction. 2016. Disponível em: <https://points.datasociety.net/ethics-review-for-pernicious-feedback-loops-9a7ede4b610e> Acesso em: 10 abr. 2021.

MIGLIORINI, Ana Carolina; TRIVIÑO, Aline Melsone Marcondes. **Por que o Brasil precisa de lei para proteger dados pessoais na esfera penal.** 2020. Disponível em: <https://www.conjur.com.br/2020-dez-07/opiniao-brasil-lgpd-penal> Acesso em: 17 maio 2021.

MOLINA, Antonio García-Pablos; GOMES, Luiz Flávio. **Criminologia:** introdução a seus fundamentos teóricos; introdução às bases criminológicas da Lei nº 9.099/95, Lei dos juizados especiais criminais. 5. ed. São Paulo: Revista dos Tribunais, 2006.

MORAES, Alexandre de. **Direito Constitucional**. 5ª ed. São Paulo: Atlas, 1999.

MORELLATO, Ana Carolina B.; SANTOS, André Filipe P. Reid dos. Capitalismo de vigilância e a Lei Geral de Proteção de Dados**:** perspectivas sobre consentimento, legítimo interesse e anonimização. **Revista Brasileira de Sociologia do Direito**, v. 8, n. 2, p. 184-211, maio/ago. 2021. Disponível em: <http://revista.abrasd.com.br/index.php/rbsd/article/view/455/261> Acesso em: 20 maio 2021.

MOURA, Naiara. **LGPD no âmbito da persecução penal e segurança pública.** JOTA, 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lgpd-no-ambito-da-persecucao-penal-e-seguranca-publica-12042021#_ftn1> Acesso em: 14 maio 2021.

MUGGAH, Robert. **Does Predictive Policing Work?** Instituto Igarapé, 2016. Disponível em: <https://igarape.org.br/does-predictive-policing-work/> Acesso em: 05 mar. 2021.

MUGGAH, Robert. **Future Crime:** Assessing twenty first century crime prediction. Instituto Igarapé, 2019. Disponível em: <https://igarape.org.br/wp-content/uploads/2019/07/2019-07-12-NE_33_Future_Crime.pdf> Acesso em: 6 mar. 2021.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018. Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603/pdf> Acesso em: 19 maio 2021.

NEIVA, Laura Carvalho de Oliveira. **Big Data na investigação criminal:** previsão do risco, vigilância e expectativas sociais na União Europeia. Tese de Mestrado (Mestrado em Crime, Diferença e Desigualdade) - Universidade do Minho, Braga, 2019. Disponível em: <http://repositorium.sdum.uminho.pt/handle/1822/61235> Acesso em: 01 maio 2021.

NETTO, Adhemar Della Torre; OLIVEIRA, Alfredo Emanuel Farias de. Big Data e a proteção de direitos fundamentais: perigos da má utilização da técnica e uma proposta para o resgate do ideal sofista de Paideia no campo da educação. **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 2, n. 3, abr./jun. 2019. Disponível

em: <https://www.thomsonreuters.com.br/pt/juridico/webrevistas/rdtec-revista-de-direito-e-as-novas-tecnologias.html> Acesso em: 04 maio 2021.

O'NEIL, Cathy. **Weapons of Math Destruction**: How Big Data Increases Inequality and Threatens Democracy. Nova York: Crown Publishers, 2016.

O QUE são dados pessoais, segundo a LGPD. **SERPRO**, 2019. Disponível em: <https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-pessoais-lgpd> Acesso em: 14 fev. 2021.

PARODI, Lorenzo. **O prejuízo para a defesa derivante da quebra da cadeia de custódia de provas digitais**. Migalhas de Peso, 2021. Disponível em: <https://www.migalhas.com.br/depeso/341170/o-prejuizo-para-a-defesa-derivante-da-quebra-da-cadeia-de-custodia> Acesso em: 03 abr. 2021.

PEIRÓ, Patricia. **Assim os algoritmos perpetuam a desigualdade social**. El País, 17 abr. 2018. Disponível em: <https://brasil.elpais.com/brasil/2018/04/12/tecnologia 1523546166_758362.html> Acesso em: 10 abr. 2021.

PERRY, Walter L. **Predictive Policing:** The Role of Crime Forecasting in Law Enforcement Operations. Rand Corporations, 2013.

PISA, Pedro. **O que é Hash?**. 2012. Disponível em: <https://www.techtudo.com.br/artigos/noticia/2012/07/o-que-e-hash.html> Acesso em: 16 mar. 2021.

PRADO, Geraldo. **Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital**. 2021. Disponível em: <https://www.conjur.com.br/dl/artigo-geraldo-prado.pdf> Acesso em: 29 mar. 2021.

PROCURADO por homicídio vai para o carnaval de Salvador vestido de mulher e é preso após ser flagrado por câmera. **G1 BA**, 05 mar. 2019. Disponível em: <https://g1.globo.com/ba/bahia/carnaval/2019/noticia/2019/03/05/procurado-por-homicidio-vai-para-o-carnaval-de-salvador-vestido-de-mulher-e-e-preso-apos-ser-flagrado-por-camera.ghtml> Acesso em: 19 mar. 2021.

SAISSE, Renan. **Big Data contra o crime:** efeito Minority Report. 2017. Disponível em: <http://direitoeti.com.br/artigos/big-data-contra-o-crime-efeito-minority-report/> Acesso em: 15 mar. 2021.

SIMÃO FILHO, Adalberto; SCHWARTZ, Germano André Doederlein. “Big Data”, big problema! Paradoxo entre o direito à privacidade e o crescimento sustentável. **Conpedi Law Review**, Onãti, v. 2, n. 3, p. 311-331, jan./jun. 2016. Disponível em: <https://www.indexlaw.org/index.php/conpedireview/article/view/3644/pdf#> Acesso em: 10 maio 2021.

SISTEMA secreto da polícia pode rastrear qualquer um. **PORTAL DO GOVERNO DE SP**, 23 nov. 2009. Disponível em: <https://www.saopaulo.sp.gov.br/spnoticias/na-imprensa/sistema-secreto-da-policia-pode-rastrear-qualquer-um/> Acesso em: 11 mar. 2021.

SOUSA, Larissa. **Segurança:** cidade deve aderir ao Sistema Detecta. GAZETA DE PIRACICABA, 2018. Disponível em: <http://www.gazetadepiracicaba.com.br/_conteudo/2018/05/canais/piracicaba_e_regiao/550252-seguranca-cidade-deve-aderir-ao-sistema-detecta.htm> Acesso em: 28 fev. 2020.

SOUZA, Paulo Vinicius Sporleder de. Proteção jurídico-penal de dados genéticos para fins médicos. In: GAUER, Ruth Maria Chittó (Coord.). **Criminologia e sistemas jurídico-penais contemporâneos II**. Porto Alegre: EDIPUCRS, 2010. p. 322-336.

STROUD, Matt. **Chicago’s predictive policing tool just failed a major test**. The Verge, 19 ago. 2016. Disponível em: <https://www.theverge.com/2016/8/19/12552384/chicago-heat-list-tool-failed-rand-test> Acesso em: 13 mar. 2021.

VALENTE, Victor. **Direito Penal:** fundamentos preliminares e parte geral. Salvador: Editora JusPodivm, 2018.

VAN BRAKEL, Rosamunde. Pre-emptive Big Data surveillance and its (dis)empowering consequences: the case of predictive policing. In: VAN DER SLOT, Bart; BROEDERS, Dennis; SCHRIJVERS, Erik (Coord.), **Exploring the Boundaries of Big Data**. Amsterdam, 2016.