POLÍCIA PREDITIVA E "NEGRITUDE": MODELOS PARA A REPRODUÇÃO DE UM ESTADO SEM DIREITOS

PREDICTIVE POLICE AND "NEGRITUDE": MODELS FOR THE REPRODUCTION OF A STATE WITHOUT RIGHTS

Recebido: 07/02/2021
Aceite: 16/11/2022

Leticia Fontestad Portalés
Professora Titular de Direito Processual da Universidade de Málaga (Espanha). Pos-Doutora em Direito . Investigadora convidada em distintos centro de Educação Superior. Doutora em Direito Processual pela Universidade de Málaga
E-mail: lfp@uma.es
https://orcid.org/0000-0001-5382-7990

Paulo Ramón Suárez Xavier
Investigador convidado pósdoutoral na Universidade de Salamanca (Espanha). Doutor em Direito Processual pela Universidade de Málaga (Espanha). Realiza estudos de Pós-doutorado em Direito Público pela Universidade de Las Palmas de Gran Canaria. Professor Colaborador na Universidade de Málaga
E-mail: ramonsuarez@uma.es
https://orcid.org/0000-0002-6937-4209

Thiago Reis Oliveira Guimarães
Doutorando em Ciências Sociais pela Universidade Federal da Bahia (UFBA). Mestre em Ciências Sociais (UFBA) e bacharel em Direito (UFBA)
E-mail: thiago.reis.guimaraes@gmail.com
https://orcid.org/0000-0001-9959-8839

Karina da Hora Farias
Mestranda em Direito pelo Universidade Federal da Bahia (UFBA) Salvador - Bahia; bacharela em Direito pela Universidade Estadual de Santa Cruz (UESC) Ilhéus/Ba; especialista em Gestão da Segurança Pública pela UFBA. D esenvolve pesquisas sobre o eixo de conhecimento nos Direitos Humanos, Direito Penal, Segurança Pública, Crimes Cibernéticos
E-mail: karina.hora@ufba.br
http://lattes.cnpq.br/0355585640813755

RESUMO

O presente trabalho aborda como a expansão tecnológica manifestada pelo advento dos fenômenos da smartificação da Administração ou Algoritmização da vida se refletem em vías de inovação nas atividades de segurança pública, notadamente no que respeita às atividades de policiamento, com o surgimento e implantação dos chamados sistema de polícia preditiva. Neste sentido, examinaremos em que consiste e como funcionam os sistemas de polícia preditiva, assim como seu eventual potencial para aprofundar as desigualdades sociais e o sistema penal excludente existente no Brasil, que identifica a pobreza e a negritude com a criminalidade, destacando a eventual necessidade ou desnecessidade de uma regulação específica do sistema de proteção de dados em matéria penal, com vistas à proteção dos cidadãos em geral, mas especialmente das minorias sociais e raciais, usuárias maioritárias que são dos serviços públicos no Brasil.

Palavras-Chave: Inteligência Artificial. Polícia Preditiva. Direito Penal. Proteção De Dados. Sesgo Discriminatório. Negritude.

ABSTRACT

The present work addresses how the technological expansion manifested by the advent of the smartification phenomena of Administration or Algorithmization of life is reflected in innovation paths in public security activities, notably with regard to policing activities, with the emergence and implantation of the so-called system of predictive police. In this sense, we will examine what the predictive police systems are and how they work, as well as their potential to deepen social inequalities and the exclusionary criminal system in Brazil, which identifies poverty and blackness with criminality, highlighting the possible need or unnecessary specific regulation of the data protection system in criminal matters, with a view to protecting citizens in general, but especially social and racial minorities, who are the majority users of public services in Brazil.

***Keywords*:** Artificial Intelligence. Predictive Police. Criminal Law. Data Protection. Slight Discrimination. Blackness.

1. INTRODUÇÃO

Neste breve ensaio, examinaremos os reflexos que o desenvolvimento e aplicação de sistemas de polícia preditiva podem acarretar na reprodução de processos de exclusão pela via penal e policial e trataremos sobre a eventual necessidade de ampliar os mecanismos legais destinados à construção de um modelo de proteção de dados mais intuitivo, especialmente em matéria penal.

Assim, na primeira epígrafe deste breve artigo, trataremos do processo de transformação digital da segurança pública de forma genérica, destacando a influência

de fenômenos como a smartificação da Administração Pública e os reflexos que este processo origina, apontando algumas importantes discussões e consequências, que desempenham um papel fundamental para compreender desde uma ótica global o processo ante o qual nos encontramos.

Destarte, no seguinte apartado, trataremos de como este processo de smartificação da Administração Pública se está refletindo nos mecanismos de prevenção de delitos e proteção dos cidadãos, com o desenvolvimento de técnicas e aplicações de polícia preditiva, conceito sobre o qual trataremos de forma mais aprofundada.

Por outro lado, examinaremos como estes sistemas podem constituir formas de controle capazes de reproduzir e amplificar os mecanismos clássicos de exclusão social, representada em condutas contrárias a direito realizadas pela Administração Pública no âmbito da segurança pública, especialmente centrando-nos no conceito de sesgo ou viés discriminatório e seus efeitos na implementação destes sistemas.

Posteriormente, trataremos sobre a aplicabilidade e a suficiência do atual marco legislativo em matéria de proteção de dados para regular a implantação destes sistemas no seio da Administração Pública, questionando a necessidade de uma regulação específica em matéria penal para o marco de proteção de dados, além de examinar de forma muito breve alguns dispositivos da Lei Geral de Proteção de Dados, a Lei n.º 13.709/2018.

Toda esta análise busca verificar se na atual conformação do sistema jurídico brasileiro, encontramos espaço para a defesa das minorias nesse processo de smartificação da Administração e implantação da inteligência artificial em sendas como a atividade policial, com a implementação de técnicas de polícia preditiva ou se, ao contrário, a insuficiência de regulação sobre a matéria pode consistir no combustível para a reprodução e aprofundamento do sistema penal como forma de exclusão social, denominado pela doutrina, em uma conhecida obra da qual trataremos, como as “prisões da miséria”.

Neste sentido, o objetivo último deste artigo é abrir as portas para o diálogo sobre a necessidade de empregar a técnica regulatória como recurso contra hegemônico para a emancipação social, oferecendo um marco jurídico de igualdade e liberdade ante o Direito Penal.

2. DIGITALIZAÇÃO E SEGURANÇA PÚBLICA

A digitalização e a smartificação da Administração Pública implicam na adoção de modelos rompedores nas distintas atividades desenvolvidas pelo Poder Público em distintos aspectos e manifestações das potestades do Estado.

Neste cenário, que encontra diversos exemplos de incorporação de novas

tecnologias nos mais diversos ordenamentos jurídicos[1], se encontram estas tecnologias, de que empregam técnicas preditivas no âmbito da segurança pública, que servem como instrumentos de planejamento, execução e controle das atividades policiais, mas que podem carrear em questionamentos no que diz respeito à proteção de dados sensíveis[2] dos cidadãos.

Ainda que possa parecer, a discussão sobre a criação ou utilização de bancos de dados ou o uso de dados que figuram em poder da Administração Pública não constitui novidade, valendo citar, por exemplo, as discussões sobre a utilização e criação dos chamados biobancos e as consequências de sua utilização para os direitos fundamentais que se relacionam com a intimidade, por exemplo[3].

Neste sentido, da mesma forma como a constituição de biobancos para a realização de investigações criminais poderia acarretar em lesões aos direitos fundamentais relacionados à intimidade e à identidade, a utilização e cruzamento de dados por meio de sistemas inteligentes, baseados em inteligência artificial para as distintas técnicas de polícia preditiva poderia violar não somente o direito à proteção de dados pessoais, mas também outros direitos fundamentais, como o direito à presunção de inocência e o direito a um processo com todas as garantias, especialmente considerando as dificuldades aplicativas e conceituais que essas operações prospectivas produzem.

Neste sentido, Gustavo Rodrigues sustenta que os órgãos de segurança pública dos Estados brasileiros estão utilizando, de modo sistemático, sistemas de reconhecimento por imagens, entre os quais se incluem o facial e de placas de veículos, que trabalham com recursos de mineração de dados, assim como sistemas de reconhecimento instantâneo através de aplicativos que identificam suspeitos sem identificação, mesmo sem haver legislação específica para tal fim[4].

Nesta seara, cabe destacar a aprovação, pelo Distrito Federal, da Lei nº 6.712, de 10/11/2020, que estabelece a possibilidade de utilização da tecnologia de reconhecimento facial (TRF) em atividades de segurança pública, consignando em seu artigo 6º que as informações obtidas pelo uso destes sistemas constituem dados pessoais, cujo acesso deve ser restrito ao uso autorizado, de acordo com a Lei Geral de Proteção de Dados (LGPD) - Lei federal nº 13.709, de 14 de agosto de 2018.

---

1 Veja-se, a teor de exemplo, RAMIÓ, Carles. Inteligencia artificial y administración pública: robots y humanos compartiendo el servicio público. Los Libros de la Catarata, 2019.

2 Uma definição de dado pessoal sensível é oferecida pela legislação nacional: "dado pessoal sobre 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;". artigo 5º, Inciso II da Lei 13.709, de 14 de agosto de 2018 (LGPD).

3 DE SOUZA, Paulo Vinicius Sporleder. Biobancos, dados genéticos e proteção jurídico-penal da intimidade. Revista AMRIGS, n. 56 (3), jul-set 2012, pág. 268-273.

4 RODRIGUES, G. LGPD penal: um remédio contra o solucionismo tecnológico na segurança pública? 11 nov 2020. Disponível em: https://irisbh.com.br/lgpd-penal-um-remedio-contra-o-solucionismo-tecnologico-na-seguranca-publica/ acesso em 10/01/2021.

No que tange ao compartilhamento destes dados, o artigo 7 da Lei o autoriza sua realização entre outros entes da Federação, especialmente no âmbito do Sistema Nacional de Segurança Pública, estabelecendo um prazo de guarda e custódia de cinco anos sobre ditos dados.

Sem embargo, cabe destacar que não existe um marco legal único para a realização dessas atividades, como ocorre com as medidas de investigação tecnológica como a interceptação de chamadas telefônicas e à interceptação do fluxo de comunicações em sistemas de informática e telemática, que conduzem à aplicação da Lei nº 9.296, de 24 de julho de 1996.

Se trata de uma questão complexa, já que implica, primeiro, em compreender o que é e em que fase do processo penal se encontra a utilização de técnicas de polícia preditiva, e que demanda maior aprofundamento para sua melhor compreensão.

Neste sentido, passaremos a examinar o conceito de polícia preditiva e suas imbricações no processo penal, com vistas a compreender seu funcionamento, como técnica, e definir sua natureza desde uma ótica processual, sem aprofundarmos no que se refere aos distintos empregos que podem conferidos à polícia preditiva.

3. INTELIGÊNCIA ARTIFICIAL, CONTROLE E POLÍCIA PREDITIVA

3.1 Inteligência Artificial, Controle e Polícia Preditiva

As sociedades modernas experimentaram profundas mudanças, que resultam de um processo mais ou menos avançado de digitalização das interações que se produzem no seio das distintas atividades levadas a efeito no âmbito privado e também no âmbito público, fenômeno que Klaus Schwab denomina de Quarta Revolução Industrial[5].

Ainda que pareça extremamente rápido e avassalador, o certo é que o avanço do uso da inteligência artificial, tanto na esfera pública como na esfera privada, resulta de um processo de desenvolvimento que se estende a antecedentes muito anteriores a Alan Turing e os processos realizados na década de 50 do Século XX, remontando aos estudos de Ada Lovelace sobre a máquina de Babbage no Século XIX e os posteriores estudos que definiram as duas principais linhas de aplicação da IA, a engenharia do conhecimento e o conexionismo[6].

O desenvolvimento e a aplicação de modelos baseados nessas duas distintas correntes, somada a inovações, como a amplificação da capacidade de processamento

5 SCHWAB, Klaus. A quarta revolução industrial. Edipro, 2019.

6 Sobre o tema, veja-se SUÁREZ XAVIER, Paulo Ramón. Gobernanza, Inteligencia Artificial y Justicia Predictiva: los retos de la Administración de Justicia ante la Sociedad en Red. Tese de doutoral. Universidade de Málaga, 2020.

do hardware disponível e o advento do *cloud computing* (processamento na nuvem), favoreceram não somente o desenvolvimento, mas a expansão das tecnologias baseadas em inteligência artificial na esfera pública e privada.

Sem embargo, além dos avanços especialmente produzidos no âmbito da engenharia do conhecimento, não estaríamos equivocados ao sinalizar que este processo depende em grande medida do processo de digitalização da sociedade, impulsado pela democratização do acesso às novas tecnologias, resultando na produção massiva de dados que até muito pouco tempo atrás não tinham uma utilidade prática.

Essa produção massiva de dados, manifestada pelo fenômeno do big data, que se origina da digitalização, somada à maior capacidade processamento e armazenagem de dados, resulta no processo de smartificação que se revela atualíssimo nos mais distintos âmbitos da atividade humana, daí porque alguns autores como Silvia Barona Vilar, entendam que os dados são o petróleo do Século XXI[7].

Dito de outra maneira, se poderia afirmar que a smartificação se constitui em um processo de renovação das técnicas clássicas de funcionamento das instituições, que se baseia no fenômeno do *big data* para empregar a inteligência artificial, mediante o uso de algoritmos nas atividades levadas a cabo por ditas instituições, tornando-as inteligentes, já que passam a aproveitar melhor os dados que resultam de sua própria atividade, assim como dados externos.

Neste sentido, parece patente o fato de que a inteligência artificial pouco a pouco vai se espraiando da esfera privada para a esfera pública, transformando não somente às instituições, como também o perfil dos profissionais que atuam nas mais distintas áreas, como sinala Richard Susskind[8].

De todo este processo de transformação, como vimos, emerge também uma série de questionamentos, especialmente em âmbitos tradicionalmente caracterizados pelo imobilismo e manutenção de técnicas tradicionais, como a Administração Pública, cuja reticência e vinculação pelo princípio da legalidade reclamam a adoção de cautelas distintas daquelas adotadas pelo setor privado.

Isso porque, como defende Carles Ramió[9], a Administração Pública não é uma empresa privada, se encontrando vinculada pelo princípio da legalidade, pelo dever de eficiência, consagrados pelo artigo 37 de nossa Lei Maior, e, por isso, a implantação de sistemas baseados em inteligência artificial em qualquer âmbito da atividade

7 VILAR, Silvia Barona. La sociedad postcoronavirus con big data, algoritmos y vigilancia digital,¿ excusa por motivos sanitarios?,¿ y los derechos dónde quedan?. Revista Boliviana de Derecho, 2020, no 30, p. 14-39.

8 SUSSKIND, Richard; SUSSKIND, Daniel. El futuro de las profesiones: cómo la tecnología transformará el trabajo de los expertos humanos. Oxford University Press, Estados Unidos, 2015.

9 RAMIÓ, Carles. Inteligencia artificial y administración pública: robots y humanos compartiendo el servicio público. Los Libros de la Catarata, 2019, p. 83-110.

administrativa reclama uma regulação específica, especialmente quando tratamos de esferas como a penal, onde regem princípios de especial transcendência, como a presunção de inocência e o direito ao contraditório e ampla defesa.

Neste sentido, predicar a aplicação de técnicas com tanta transcendência nos âmbitos penal e administrativo, como as de polícia preditiva reclama uma série de debates que não podem nem devem ser ignorados, especialmente considerando a fragilidade e a sistemática vulneração de direitos fundamentais no Estado Brasileiro, especialmente considerando recentes informes sobre a violação de direitos humanos de minorias no Brasil[10].

Assim, considerando o atual quadro penal do Brasil, onde a população carcerária está formada principalmente por negros e onde a prisão se constitui como forma de reprodução e disseminação das desigualdades sociais entre ricos e pobres, brancos e negros, se questiona se a adoção dessas novas tecnologias, como as técnicas de polícia preditiva pode ter um impacto negativo ou, sem embargo, pode contribuir à ampliação do abismo racial existente no nosso país.

A modo de ilustração, Reis Friede destaca que, "no que se refere ao perfil dos presos, especificamente a cor de pele, cerca de 64% da população prisional é composta por negros" e ademais, que "a maior população carcerária negra se encontra entre os estados do Acre, totalizando aproximadamente em 95%, do Amapá, com média de 91% e da Bahia, em torno de 89%"[11].

Em conclusão, a implantação das novas tecnologias na Administração Pública não pode servir para perpetuar este sistema de exclusão que consolida a prisão como gueto e o Estado como mecanismo de controle e extermínio da população jovem, negra e pobre, senão ao contrário, garantindo a segurança pública, a prevenção de delitos e a emancipação, permitindo que o objetivo de construir uma sociedade livre, justa e solidária não reduza a papel molhado.

Por tudo isso, entendemos que é imprescindível realizar alguns apontamentos sobre o que é, como funciona e sobre a eventual necessidade de regulação das técnicas de polícia preditiva, tarefa à qual nos dedicaremos desde agora.

3.2 Polícia Preditiva: conceito e funcionamento

Até este ponto de este breve ensaio, analisamos de forma muito breve o fenômeno da smartificação da Administração Pública e nos deparamos com o papel fundamental

10 O informe elaborado pela Associação o Terra de Direitos à Assembleia Geral das Nações Unidas pode ser consultado em: https://terradedireitos.org.br/uploads/arquivos/Written-Statement.pdf. Acesso em 17 de janeiro de 2021.

11 FRIEDE, Reis. As prisões brasileiras e a condição humana do encarcerado. Revista Interdisciplinar de Direito, 2019, vol. 17, no 1, p. 215-230.

que o fenômeno do *big data*, somado à ampliação da capacidade de processamento dos novos dispositivos e o cloud computing tiveram para a consolidação deste movimento, que se espraia às distintas facetas da atividade humana, incluída a atividade de polícia, da qual nos ocuparemos desde agora.

Cabe, neste sentido, definir um conceito de polícia preditiva, tarefa complexa, já que no referido conceito podem ser englobadas distintas atividades, o que gera, ao mesmo tempo, desconcerto e confusão na doutrina.

Para Provost y Fawcet[12], o uso de uma quantidade massiva de dados históricos, que se analisam mediante uma técnica quantitativa para estimar um valor desconhecido por meio de algoritmos, serve de base para o funcionamento destas tecnologias, operando, como aponta Santos Hermoso, por meio de semelhanças e analogias[13].

Outros autores, como Cinelli, destacam que a polícia preditiva não goza de autonomia conceitual, estando incluída entre os distintos recursos que conformam a inteligência policial, restringindo-se ao conceito de análise preditiva[14].

Sem embargo, reduzindo esta concepção técnica a simples função de predição de delitos com fins de prevenção, outra parte de doutrina impõe um caráter utópico à polícia preditiva, como Miró-Llinares, que defende:

> "Embora não possa (e nunca possa) prever a perpetração de crimes, ajuda a identificar a probabilidade de eventos futuros com base em um melhor conhecimento de eventos anteriores e seus fatores condicionantes. Assim, permite a adoção de estratégias preventivas para fins de prevenção, redução ou mitigação delitiva.
> Na realidade, a utopia da antecipação é apenas uma amplificação do otimismo perfeitamente compreensível sobre a "cientificização" dessas atividades. Os benefícios da tecnologia também vão além da prevenção do crime, por exemplo, na gestão mais eficiente dos recursos policiais e menos subjetividade na tomada de decisão policial. A capacidade dos algoritmos de processar grandes quantidades de dados permite que eles avaliem mais informações mais rapidamente do que qualquer policial, analista criminal ou departamento individual jamais poderia. Em um momento de crescentes demandas públicas por justiça e responsabilidade, isso se torna um valor em si. Além disso, essas ferramentas poderiam corrigir o preconceito humano ao superar o tratamento discriminatório historicamente sofrido por vários grupos sub-representados." discriminatório historicamente sofrido por vários grupos sub-representados." [15]

12 PROVOST, F. Data Science for Business: What you need to know about data mining and data - analytic thinking. O'Reilly Media, 2013, p. 22 y ss.

13 SANTOS-HERMOSO, Jorge. Policía Predictiva en España. Aplicación y retos futuros. Behavior & Law Journal, 6(1), 26-41.

14 CINELLI, Virginia. El uso de programas de análisis predictivo en la inteligencia policial: una comparativa europea. Revista de Estudios en Seguridad Internacional, V. 05, nº. 02, (2019), p. 1-19.

15 LLINARES, Fernando Miró. Policia predictiva: utopia o distopia? Sobre les actituds cap a l'ús d'algorismes de big data per a l'aplicació de la llei. IDP: revista d'Internet, dret i política, 2020, no 30, p. 6-7.

a ideia clássica de programas informáticos, como salienta Pino Diez.

Neste sentido, seria correto afirmar que polícia preditiva constitui, não um conjunto de aplicativos, senão uma técnica, que emprega conhecimentos e base científica criminológica e estatística, utilizando quantidades massivas de dados processados por algoritmos e sistemas expertos de distinta índole, para a realização e apoio de atividades de polícia.

É preditiva, porque funciona mediante a extrapolação de dados e informações que se obtém de uma ou mais bases de dados (data set), mediante critérios previamente definidos pela experiência, ou bem por critérios cronológicos, estatísticos ou de qualquer outra índole, cuja definição é de responsabilidade de um experto humano.

Assim, o primeiro ponto que devemos ter em mente quando queremos conceituar polícia preditiva é que sua margem de acerto se baseia em dois fatores fundamentais, o primeiro é que sua margem de falibilidade é diretamente proporcional à do experto ou grupo de expertos humanos que realiza a definição dos critérios que devem ser empregados pelo algoritmo no processo de treinamento ou no processo de definição de indicadores e informações relevantes a serem observados no processo de desenvolvimento do algoritmo[1].

Em segundo lugar, também é imprescindível compreender que o nível de acurácia, de exatidão das conclusões esposadas nestes processos dependem fundamentalmente da quantidade de informações das quais dispõe o algoritmo, assim como o modelo de algoritmo empregado, especialmente no que se refere às questões relativas à chamada "caixa-preta" desenvolvida por alguns modelos de algoritmo, como o de bosques aleatórios ou redes bayesianas, além de outros modelos como o de tensor flow[2].

O que está claro é que, como mantém Miró-Llinares, nenhuma tecnologia, por mais futurística e atual, pode predizer com exatidão comportamentos e atitudes humanas e, mais ainda, não se pode considerar a mera probabilidade de ocorrência de uma conduta delitiva como correspondente ao delito, mesmo já que neste caso nem sequer estaríamos ante atos preparatórios, com referência à dogmática penal e ao crescente expansionismo

1 Sobre veja-se SUÁREZ XAVIER, Paulo Ramón. Gobernanza, Inteligencia Artificial y Justicia Predictiva: los retos de la Administración de Justicia ante la Sociedad en Red. Tese de doutoral. Universidade de Málaga, 2020.

2 Uma perspectiva interesante sobre o tema pode ser encontrada em STEYVERS, Mark. Active Bayesian Assessment for Black-Box Classifiers. Cornel University. Disponível em: https://arxiv.org/pdf/2002.06532.pdf. Acesso em 15/01/2021.

penal na sociedade brasileira[3].

Neste sentido, a ideia de funcionamento das técnicas de polícia preditiva tem como pressuposto a necessidade de criação, manutenção e expansão de bases de dados, relacionadas não somente à política e estatística criminal, mas também dados pessoais, capazes de indicar preferências políticas, idade, posição social e econômica, entre outros, que configuram o conjunto de dados que alimentam estes algoritmos, cuja dinâmica de funcionamento interno não será abordada, mas sobre a qual sinalamos que subverte a ideia clássica de programas informáticos, como salienta Pino Diez[4].

Assim, podemos concluir que as técnicas de polícia preditiva e sua aplicação comportam dois problemas fundamentais: o primeiro, se refere às normas para a coleta, manutenção e tratamento dos dados que conformam as bases de dados que operacionalizam os sistemas que emprega, e o segundo diz respeito à identificação das normas jurídicas aplicáveis a seu funcionamento, já que nesta dinâmica não nos encontramos nem no âmbito de um processo penal, nem de uma investigação criminal, senão de atuações prospectivas e atividades administrativas, cujos contornos não terminam de estar definidos em direito positivo.

A complexidade do tema, assim como as limitações que se manifestam no reduzido espaço do que dispomos neste breve estudo, nos impede de aprofundar nas questões processuais que envolvem o tema, que são da maior relevância e atualidade, obrigando a que nos centremos nas questões atinentes ao funcionamento destas bases de dados como mecanismo de controle e reprodução das desigualdades em sociedades marcadas pela exclusão de grupos minoritários, como a população negra no Brasil, pelo que passaremos a examinar as questões que se referem à construção dessa sociedade de controle.

3.3 Vigilância e sociedade de controle

Estes modelos e técnicas que vão se estruturando tendo por base o fenômeno do *big data* e o tratamento de dados pessoais e públicos, configuram o baldrame de uma nova estrutura de controle social e jurídico, que emprega distintos meios para permear a chamada sociedade rede[5].

3 Veja-se SELVA, Leonardo Vinicius Galvão. A transcendental ameaça do direito penal do inimigo ao estado de direito: a lei antiterrorismo brasileira. Profanações, 2020, vol. 7, p. 431-451.

4 PINO DIEZ, Raúl. Introducción a la Inteligencia Artificial. Universidad de Oviedo. Oviedo: 2001, p. 03.

5 CASTELLS, Manuel. La sociedad red. Alianza Ediorial. Madrid: 1997, p. 88-90.

Surgem, neste cenário, estudos sobre controle e vigilância (*surveillance*). Isto porque, ao mobilizarmos reflexões acerca de como a IA se desenvolveu desde sua aplicação industrial [6]e a forma como se espraia a novos setores da atividade humana em atividades e aplicações como o processamento da linguagem natural ou a aprendizagem automática, acabamos por ser conduzidos à discussão sobre a legitimidade e legalidade desse processo de acúmulo de informações (por meio de bases de dados), monitoramento e tratamento de dados por entes públicos ou privados, em determinadas regiões ou a nível global, compreendidos no contexto dessa sociedade em rede, à qual nos referimos antes.

Cabe destacar que estas dinâmicas de vigilância se constroem a partir de paradigmas e ferramentas operacionalizadas ao longo do tempo. Como destaca Bogard[7], Michel Foucault foi um autor muito significativo para pensar lógicas de vigilância, na medida em que traçou análises histórico-filosóficas sobre a construção de sociedades, partindo de suas dinâmicas de saber-poder. Um dos elementos que está nas análises de saber-poder que Foucault desenvolve ao longo dos anos é a capacidade de produzir informações sobre sujeitos, a partir de uma coleta minuciosa de dados sobre a sua existência individual e coletiva: isto está nas lógicas panópticas de constrição e restrição, com fins de uma normalização de sentimentos, pensamentos e agências, ou nas dinâmicas pós-panópticas de gestão de espaços e pessoas em fluxos.

O ponto de partida do autor para tratar do tema é de máximo interesse para a compreensão do tema ao qual nos ocupamos. Partindo de conceitos consolidados pelo trabalho de Boudrillard, sobre dinâmicas de simulação em estratégias de controle pós panópticas, e Delleuze, acerca das chamadas *sociedade de controle*, referido autor aponta como, de um lado, o panoptismo enquanto lógica de controle e segurança esteve limitado pela sua rigidez material e arquitetura, enquanto as simulações se apresentam em uma lógica pautada por códigos digitais e controles flexíveis e multifuncionais. A simulação estaria pautada a partir da construção do real de acordo com seus próprios modelos, ou seja, sem efetivamente "representar" o real, mas manufaturando realidades hipotéticas para servir a formas específicas de controle.[8]

Enquanto as dinâmicas de controle do panoptismo, observadas entre o final do

6 MAISUECHE CUADRADO, Alberto. Utilización del Machine Learning en la Industriav4.0. Publicação em acesso aberto. Universidad de Valladolid. Valladolid. Recuperado de: https://cutt.ly/qgjnJ0x. Acesso em 10/01/2021.

7 BOGARD, William. Simulation and pos-panopticism. In BALL, Kirstie; LYON, David; HAGGERTY, Kevin D. (Ed.). Routledge handbook of surveillance studies. Routledge, 2012, p. 30.

8 Ibidem, p. 30-31.

século XVIII e o século XIX, estavam principalmente pautadas por uma estratégia de representação de papéis de normalidade e verdade, contidas no entorno de dinâmicas de visibilidade e invisibilidade em espaços constritos, a lógica de simulação trazida por Baudrillard apresenta um processo no qual modelos ideais ou "imaginários" pautam a construção da própria verdade, que passa a ser uma sucesso de manobras de antecipação e pré-condicionamento desta[9].

É a partir destas dinâmicas de simulação que Bogard (2012, p. 36–37) traz o conceito, de Deleuze e Guattari, de *sociedade de controle*: a partir de uma cadeia interconectada de máquina materiais e virtuais, constroem-se sistemas de vigilância que operam modelos de antecipação e previsão de sentimentos, pensamentos e agências, reconstituindo as lógicas do real a partir de estruturas modeladas de repaginação constante das realidades, por meio da acumulação, processamento e ressignificação de uma quantidade massiva de dados. Tais redes de simulação, dentro de *sociedade de controle*, tendem cada vez mais a processos de convergência, nos quais aplicações desenvolvidas para uma dada finalidade são compartilhadas, aumentando as possibilidades de troca de informações e expansão das redes de controle e vigilância.

Um elemento que adquire função central, nestes processos de vigilância, é precisamente o tratamento das incertezas, ou do aleatório definidos por Ceyhan, que trabalhando os conceitos de *governamentalidade* e *biopoder* em Foucault, aponta como, nas análises que desenvolve sobre os *dispositivos de segurança*, o tratamento do aleatório é pareado ao espaço conferido ao exercício da segurança, das normas regulatórias e da população, como quatro dos elementos centrais que atravessam os *dispositivos de segurança*: isto porque, na medida em que o biopoder representa uma gestão da vida a partir do controle dos corpos, e a *governamentalidade* como uma gestão destes corpos em fluxos espaço-temporais, o aleatório está diretamente relacionado aos elementos contingentes e com uma variedade de fatores centrais às lógicas de vigilâncias destes corpos e espaços, instrumentalizados a partir de análises estatísticas e cálculos de probabilidade e custos[10].

Dita percepção se relaciona com a análise elaborada por Habermas ao tratar da desvinculação entre indivíduo e sociedade construída pelo discurso da modernidade, ao romper a dicotomia eu-nós e vincular a racionalidade moral prática a discursos sobre a felicidade pessoal e a individualidade, dissociando a função integrativa que albergava

9 Idem, p. 31.

10 CEYHAN, Ayse. "Surveillance as biopower". In: BALL, Kirstie; LYON, David; HAGGERTY, Kevin D. (Ed.). Routledge handbook of surveillance studies. Routledge, 2012, p. 41-42.

dentro do modelo clássico imposto pelo modo de vida importado do medievo[11].

Neste sentido, Ceyhan destaca que nos modelos atuais de dispositivos de vigilância e segurança, são os algoritmos que desempenham um papel central, e cada vez mais sofisticado, nestes processos, considerando que se realiza por meio de algoritmos uma panóplia de atividades, tais como análises de riscos através de bases de dados computadorizadas, operacionalizadas por meio de *softwares* e mecanismos de processamentos de dados[12].

Estes processos de tratamento de dados são realizados por modelos matemáticos desenvolvidos para executar tarefas complexas e correlacionadas, como cálculos, apreensão de informações e depuração, com a finalidade de construir projeções ou engatilhar eventos programados por meio de extrapolação de informações.

Assim, se constitui um processo de *vigilância silenciosa*[13] em que são empregados instrumentos de análise comportamental e bases de julgamento e ordenação sociais que ultrapassam os meios físicos e avançam para meios não tradicionais, como a Internet, objetos dotados de internet (IoT), interoperabilidade entre sistemas e outras ferramentas, entre as quais nos interessa a técnica de *polícia preditiva*.

Tais mecanismos de *polícia preditiva*, cujo conceito e metodologia de funcionamento foi previamente analisado com anterioridade, em que pese apresentarem uma série de possibilidades inovadoras para o desenvolvimento das atividades policiais em matéria de segurança pública, entre os quais poderíamos citar a inteligência aplicada ao patrulhamento físico, ou o reconhecimento de imagens para a previsão de condutas delitivas ou de meros ilícitos administrativos, levantam ao mesmo tempo uma série de questionamentos sobre a sua validade, eficácia e limites, seja quanto ao seu funcionamento, seja sobre os possíveis efeitos quanto aos direitos fundamentais da cidadania.

Como aponta Ferguson uma série de questionamentos podem advir de sua aplicação, tais como: a) os dados utilizados para alimentar tais sistemas de análise preditiva de riscos podem ser de má qualidade, seja a.1) por erros humanos no preenchimento destes dados, levando a uma série de erros em cadeia no processo de

11 HABERMAS, Jürgen; MCCARTHY, Thomas; MCCARTHY, Thomas. The theory of communicative action. Boston: Beacon press, 1984.

12 CEYHAN, Ayse. “Surveillance as biopower”. In: BALL, Kirstie; LYON, David; HAGGERTY, Kevin D. (Ed.). Routledge handbook of surveillance studies. Routledge, 2012, p. 41-42.

13 Ibidem, p. 44.

coleta, interpretação e replicação destes dados pelos modelos preditivos; a.2) dados fragmentados ou sesgados, seja porque, no primeiro caso, há informações insuficientes para construir uma base de dados sólida sobre uma série de categorias criminais, seja porque, no segundo caso, a construção destes modelos carregam por influência não visíveis de quem as constrói e alimenta, gerando potenciais discriminatórios, ainda que eventualmente não intencionais, no tipo de predição de risco e sob quais grupos tais análises de risco inevitavelmente recairiam[14].

Sobre o conceito de sesgo no funcionamento de sistemas baseados em inteligência artificial, cabe destacar que os sesgos revelam que os sistemas pautados em IA, assim como qualquer outro modelo informático não são perfeitos, primeiro, porque dependem da quantidade de dados que constituem o *data set* sobre o qual operam, o que implica que, quando maior a quantidade de dados empregada, maior eficácia terá o sistema, qualidade que contrasta com a maior amplitude de efeito de inexatidões e sesgos interpretativos possíveis na ampliação destas bases[15].

Além disso, uma ingente quantidade de dados promove problemas relacionados ao sub ajuste das informações e parâmetros oferecidos ao algoritmo, assim como de sobre ajuste e os chamados sesgos de interpretação, conduzindo à conclusão de Pino-Diez de que uma maior margem de sesgos implica em qualquer caso uma aprendizagem mais rápido por parte do algoritmo, mas também menor desempenho e confiabilidade, uma vez que implica na existência de uma diferença entre os valores reais e de previsão do modelo, que também estão relacionados com o modelo de algoritmo usado, como destacamos com anterioridade[16].

Estes sesgos podem ser consolidados em forma de sesgos de compreensão ou cognitivos, que são aqueles que são consequência da ocorrência de erros estatísticos, processamento de informações ou memória que tornam o comportamento se desvia do "racional", constituindo um desvio no processo interpretação[17].

Estes sesgos podem surgir pela própria dinâmica de funcionamento dos algoritmos,

14 FERGUSON, Andrew G. Policing Predictive Policing. Wasington University Law Review, n. º 94. Whashington, 2017. p.1109. Recuperado de: https://openscholarship.wustl.edu/law_lawreview/vol94/iss5/5. Acesso em 10/01/2021.

15 NORVIG, Peter. Artificial Intelligence: A Modern Approach. Ed. Prentice Hall. Nova Jersey, 2003, p. 712.

16 PINO DIEZ, Raúl. Introducción a la Inteligencia Artificial. Universidad de Oviedo. Oviedo: 2001, p. 10 e seguintes.

17 BENÍTEZ, Lucía. Ética y transparencia para la detección de sesgos algorítmicos de género. Estudios sobre el Mensaje Periodístico. N. 25, Año 3 (2019), pp. 1307-1020.

já que neste ponto é quando cobra importância a ideia de "caixa-preta" (*Black box*) dos sistemas baseados em inteligência artificial, já que na maioria das vezes, estes sesgos ou, como parte da recente doutrina brasileira denomina "enviesamento" dos algoritmos se situam em camadas inferiores, em subcapas que por vezes podem estar ocultas e cuja identificação resulta de atividades de inspeção, revisão e auditoria[18].

Nesse sentido, devemos ter claridade na distinção entre os sesgos de compreensão e os sesgos emocionais e discriminatórios, porque esta distinção é importante para entender que os sesgos são uma parte importante do processo de compreensão humana e também do desenvolvimento de sistemas inteligentes baseados em autoaprendizagem, que podem ser formados de forma espontânea, interpretando o algoritmo um banco de dados tendencioso - no caso de aprendizado automático não supervisionado - ou por uma concepção tendenciosa e discriminatória do especialista humano[19].

Sobre este extremo, o autor mantém que:

> "En el primer caso estamos ante un error de interpretación de la máquina que debe ser ajustado y evitado, en el segundo estamos ante un comportamiento absolutamente reprochable y pasible de las responsabilidades pertinentes.
> Por ello, la implantación de estos sistemas y el potencial de escalabilidad que impone a los procesos humanos también debe ser objeto de responsabilidad, para evitar la ocurrencia de interpretaciones sesgadas masivos y para fomentar el buen uso de las nuevas tecnologías.
>
> En cualquier caso, en una sociedad donde se reproduzca un modelo discriminatorio por razones de raza, género, clase social u orientación sexual, el sesgo de la máquina no es más que una reproducción de los valores adoptados en esta sociedad y que lamentablemente se reflejan en el análisis estadístico realizado por los sistemas de autoaprendizaje.
>
> Tal sintomática no es del todo negativa, ya que alumbra lo que antes estaba oculto en las entrañas del sistema social. La discriminación velada se hace aparente cuando se expone la magnitud de sus repeticiones revelada en los datos estadísticos obtenidos de los *data set* de las inteligencias artificiales y revelan el modelo de reproducción de la desigualdad en nuestras sociedades, lo que es un dato importante.[20]

Neste sentido, cabe compreender as importâncias destas discussões não somente

18 Uma visão interesando do tema é conferida por FERNÁNDEZ DE LA MORENA, Berta. Discriminación Algorítmica Estudio del sesgo en arquitecturas de aprendizaje profundo. Universidad Autónoma de Madrid. Monografia de fim de curso. Madrid, 2019.

19 SUÁREZ XAVIER, Paulo Ramón. Gobernanza, Inteligencia Artificial y Justicia Predictiva: los retos de la Administración de Justicia ante la Sociedad en Red. Tese de doutoral. Universidade de Málaga, 2020, p. 345.

20 Idem, p. 345.

na forma como vem sendo abordada pela maior parte da doutrina, com referência à dogmática processual e às garantias fundamentais, sem abordar um tema da máxima importância, que envolvem: primeiro, a possibilidade da existência de bancos de dados desta natureza, não autorizados pela legislação processual penal ou mesmo pela administrativa e, em segundo lugar, as limitações impostas para o uso das distintas bases de dados tratadas.

O ponto principal a considerar, se refere à possibilidade de tratamento de dados pessoais de forma automatizada por autoridades policiais fora do âmbito de uma investigação criminal, já que nestes casos estaríamos fora do âmbito de aplicação da Lei n.º 9.296/1996, que regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal, definindo em seu artigo primeiro que "a interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça", e estendendo sua aplicação, em seu parágrafo único, também à "à interceptação do fluxo de comunicações em sistemas de informática e telemática".

É bem verdade que o tratamento dos dados antes mencionados não dependem diretamente de interceptação de dados dos usuários da rede *W.W.W.*, mas eventualmente podem estar baseados no processamento destas informações, como nos casos, estes mais distantes da realidade brasileira, de doutrinamento para a realização de atividades terroristas, que atualmente se amplifica silenciosamente em Europa e Estados Unidos, mas podem ter interferências diretas como incidente em um processo penal ou de cooperação jurídica internacional.

Por outro lado, estes sistemas algoritmos também podem empregar dados das bases da própria polícia, assim como aqueles que obram nas bases do Poder Judicial e que efetivamente já são empregados de forma corriqueira, como o Banco Nacional de Mandados de Prisão, o Banco Nacional de Monitoramento de Prisões, cujos reflexos processuais se encontram na Lei 12.403/11, que adicionou o artigo 289-A ao Código de Processo Penal, determinando ao Conselho Nacional de Justiça a criação e manutenção de um banco de dados de mandados de prisão, tendo por finalidade registrar todos os mandados de prisão de forma imediata neste banco de dados.

O grande problema do funcionamento de sistemas que se baseiam para predizer onde, quando, ou quem vai cometer um delito empregando estes dados, por exemplo, é que todas estas bases de dados se encontram previamente sesgadas, ou seja, apresentam dados que apontam à negritude do sistema penal brasileiro e à pobreza como forma de

condenação no processo penal nacional.

Se revela, neste sentido, o social-panoptismo anunciado por Loïc Wacquant, que afeta não somente a nível físico, como também a nível digital a população pobre e marginada, senão vejamos:

> "Na verdade, a louvável preocupação com uma maior eficácia na ação social leva a colocar as populações indigentes sob supervisão muito mais estreita e meticulosa, pois as diferentes burocracias encarregadas de lidar diariamente insegurança social - agências de emprego, serviços sociais, bancos de poupança seguradoras de saúde, hospitais, serviços públicos de habitação etc. sistematizam sua coleta de informações, conectam seus bancos em rede dados e coordenar suas intervenções. Sem esquecer de "modernizar" seus procedimentos e modalidades de intervenção de forma a minimizar os "riscos" produzidos pelas populações a seu cargo e torná-los compatível com os dispositivos de segurança que se multiplicam em seus limites territoriais (nossa tradução)"[21]

Neste sentido, se revela uma questão, que se refere ao funcionamento de modelos de polícia preditiva, a partir de um erro denominado *runaway feedback loops.* Como aclara Ensigns, se trata de um processo pelo qual se reproduzem problemas na forma como os *feedbacks* são recebidos e processados pelos modelos de análise preditiva, fazendo com que, em procedimentos de inteligência policial, patrulhas sejam sucessivamente enviadas aos mesmos bairros, independente da taxa real de incidência criminal daquela região, problema especialmente associado à maneira pela qual situações potencialmente criminosas são descobertas *in loco* e reportadas por agentes policiais para alimentar o sistema[22].

Isso porque, na medida em que os locais são selecionados pelo modelo preditivo, aqueles que, por sofrerem patrulhas recorrentes, geram um acúmulo de dados de caráter repetitivo e cíclico, ainda que estes locais não guardem uma efetiva maior incidência de ocorrência de crimes que em outras localidades.

Por outro lado, Shapiro aponta uma série de críticas acerca da incompletude, má qualidade ou sesgos dos dados utilizados para alimentar estes modelos de análise preditiva, de um lado, enquanto agências policiais, cientistas de computadores e empresas produtoras destes serviços, não só alegam que o uso de tais sistemas melhora

21 WACQUANT, Loïc. Las cárceles de la miseria. Buenos Aires, 2000, págs. 124-125.

22 ENSIGN, Danielle et al. Runaway feedback loops in predictive policing. In: Conference on Fairness, Accountability and Transparency. PMLR, 2018. p. 160-171.

a eficiência policial como que, no futuro, será a ferramenta responsável por tornar mais justo o sistema de Justiça. Para compreender tais emaranhados, o autor propõe, inicialmente, que compreendamos que tais mecanismos de predição de comportamentos e atuação policial sempre fizeram parte da própria constituição da polícia enquanto agência pública de controle: o seu trabalho esteve sempre atravessado por espaços de antecipação e predição como instrumentos para prever crimes e gerenciar grupos raciais específicos.[23]

A patrulha policial seria, portanto, uma das principais tecnologias desenvolvidas para prevenção de crimes: na medida em que serviria como instrumento central na função preventiva da polícia, a patrulha serviria como uma tecnologia inata de antecipação espacial , sendo capaz de reconfigurar os espaços urbanos de modo a deter comportamentos inadequados, diminuindo possibilidades de fuga de suspeitos e estabelecendo a logística de operacionalização tática das forças policiais, já que agentes policiais funcionam como instrumento de percepção, mas também são percebidos, levando a um processo de observação-observada, uma via de mão-dupla manifesta em um processo de *mediação social*, na qual seria possível, enquanto manifestação concreta do poder abstrato de polícia do Estado, distribuir, de um lado, segurança e, de outro, dor; de um lado legitimando e autorizando participação social, enquanto de outro lado produzindo espacialidades de risco e perigo[24].

No contexto internacional, o uso de mecanismos de *polícia preditiva* está diretamente associado, em muito espaços, a casos de violência policial letal contra grupos socialmente vulnerabilizados, como populações negras nos EUA: em resposta a estes eventos trágicos, porém rotineiros, levantou-se a necessidade da utilização de mecanismos que fossem capazes de ultrapassar os sesgos e preconceitos existentes na atuação de agentes e agências do sistema de Justiça. Construindo, assim, segundo o autor, um discurso por ele nomeado de *reforma por meio da polícia preditiva (predictive police for reform)*, por meio do qual se pautaria uma reforma da atuação de agências policiais, tornando-as mais objetivas e menos preconceituosas, através de análises algorítmicas preditivas[25].

Neste sentido, Shapiro aponta elementos indispensáveis para apontar a falibilidade desta suposta capacidade de objetividade e precisão de tais mecanismos, sendo um dos elementos apontados as *indeterminações*, na medida em que, em mecanismos de *polícia*

23 SHAPIRO, Aaron. Predictive policing for reform? Indeterminacy and intervention in big data policing. Surveillance & Society, v. 17, n. 3/4, 2019. págs. 456-548.

24 Ibidem, págs. 458-459.

25 Ibidem, págs. 462-464.

preditiva focalizados especialmente em abordagens físicas, só se seria capaz de produzir predições acuradas anteriormente à alimentação das bases de dados, posto que, a partir do momento em que ocorreriam as patrulhas nos locais previstos, a performance do algoritmo perderia sua capacidade de medição, seja pelo fato de, por serem vistos, gerar efeitos reativos em potenciais criminosos – levando, por exemplo, a mudanças de local para execução de crimes –, seja pela produção de novos dados especializados que serviriam para provocar um reforço daquele local e uma repetição de patrulhas (*runaway feedback loops*). Estas, somadas a outras questões apontadas pelo autor, levam a uma possibilidade de intervenções policiais muito mais pelas indeterminações, incertezas e efusividades do funcionamento de tais modelos preditivos[26].

Estes problemas não parecem representar todas as controvérsias que os sistemas de polícia preditiva apresentam, especialmente os relacionados aos sesgos discriminatórios, cabendo citar o conhecidíssimo caso do algoritmo COMPAS, aplicado na elaboração de pareceres sobre progressão de regime nos Estados Unidos, cujo algoritmo apresentava uma série de sesgos sociais e raciais, tomando em consideração dados econômicos e de antecedentes policiais dos indivíduos para opinar de forma negativa ao pedido do paciente[27].

Se revela, neste sentido, a necessidade de regular o uso e a extensão das aplicações das técnicas de polícia preditiva[28], assim como a forma e as limitações do tratamento de dados pessoais e dados que obram em bases de dados da Administração Pública, cujo uso não foi previamente informado, nem conste e uma autorização policial, o que implica em definir os limites de utilização destas tecnologias.

Neste sentido, passamos a examinar o marco legal de proteção de dados no Brasil e sua suficiência, tanto a nível regulatório, como de garantias, especialmente considerando a vulnerabilidade antes apontada da população socialmente excluída, negra e pobre.

4. (IN)SUFICIÊNCIA DO MARCO LEGAL: POR UMA LGPD PENAL(?)

Conforme trabalhamos até este ponto, a utilização de técnicas de polícia preditiva

26 Ibidem, págs. 462-468.

27 Veja-se, neste sentido: WADSWORTH, Christina; VERA, Francesca; PIECH, Chris. Achieving fairness through adversarial learning: an application to recidivism prediction. arXiv preprint arXiv:1807.00199, 2018.

28 Tanto é assim que muito recentemente saiu à luz o projeto de informe dirigido ao Parlamento Europeo sobre a necessidade de regular a utilização da IA no âmbito do Direito Penal pelas autoridades policiais, cujo conteúdo, em versão de rascunho elaborado pela Comissão de Liberdades Civis, Justiça e Assuntos de Interior, pode ser consultado em: https://www.europarl.europa.eu/doceo/document/LIBE-PR-652625_ES.pdf. Acesso em 10/01/2021.

gera questionamentos relacionados à própria aplicação da legislação processual e administrativa, já que não termina de estar devidamente enquadrada nem como atuação administrativa independente nem como uma etapa de um rito processual, estando à míngua de qualquer procedimento específico de investigação e se enquadrando como atuação genérica e, por outro lado, desperta inquietações derredor à utilização de dados pessoais de forma não autorizada pelo Poder Público.

O primeiro aspecto, ainda que resulte de máxima atualidade e relevância, escapa do objeto desta investigação e, neste sentido, nos dedicaremos à segunda faceta das polêmicas surgidas ao sabor da aplicação destas tecnologias, referida à suficiência ou insuficiência do marco legal existente em matéria de proteção de dados.

4.1 Sobre o marco jurídico atual de proteção de dados: a LGPD

A inovação trazida pela Lei Geral de Proteção de Dados (LGPD) - Lei Fedearl nº 13.709, de 14 de agosto de 2018, instrumento normativo modificado pela Lei nº 13.853, de 08 de julho de 2019 e, que dispõe sobre a proteção de dados pessoais, criando a Autoridade Nacional de Proteção de Dados (ANPD), entrou em vigor em 18 de setembro de 2020, com algumas peculiaridades, em razão de Pandemia ocasionada pela difusão do vírus SARS Covid-19.

Estas peculiaridades ocorreram em razão da publicação da Lei Federal nº 14.010, de 10 de junho de 2020, que dispôs sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19) e da Medida Provisória (MP) nº 959 de 29 de abril de 2020 (regras para o auxílio emergencial e adiamento da vigência da LGPD), com fundamento no art. 62 da Constituição da República Federativa do Brasil, que prevê a possibilidade de sua edição em situação de relevância e urgência. Quiçá, fruto do cenário excepcional e das dificuldades com a eclosão da pandemia, na adesão e cobrança adequada sobre o disposto na normativa.

Neste sentido, não obstante a Lei Geral de Proteção de Dados Pessoais tenha entrado em vigor no mês de setembro de 2020, alguns dispositivos tiveram sua vigência prorrogada para 03 de maio de 2021, como, por exemplo, as perspectivas sancionadoras da norma, constantes em seu artigo 65.

Com caráter eminentemente cível, a LGPD trouxe nova proteção e foco no direito à privacidade dos cidadãos, enquanto corolário do direito à intimidade e à imagem (consagrados no artigo 5º, X da CF88), regulando e pondo freio ao acesso irrestrito às

informações e dados pessoais sensíveis pelos entes de direito privado e também entes de direito público, com foco na proteção da privacidade, consoante se verifica do teor de seu artigo 1º, ao dispor que "*esta lei dispõe sobre o tratamento de dados pessoais, 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.*

Neste sentido, cobra relevância o conceito de privacidade, cujo teor, segundo Sérgio Cavalieri Filho, obriga a compreender que (2012, p.146), "*privacidade, segundo doutrina da Suprema Corte dos Estados Unidos, universalmente aceita, é o direito de estar só; é o direito de ser deixado em paz para, sozinho, tomar as decisões na esfera da intimidade*" [29].

Corrobora no mesmo sentido, Márcio Vinicius M. Ribeiro, ao defender que a lei tem como objetivo garantir e proteger a confidencialidade dos dados dos indivíduos contra potencial risco de dano pela exposição, logo, a atividade de tratamento de dados pessoais está posta para garantir privacidade, controle e segurança no uso das informações pessoais pelos diversos meios de comunicação; a lei desse modo, impõe uma filosofia perante os seus cidadãos, visando privacidade e segurança, além de uma cultura de respeito a uma ética da alteridade[30].

Segundo Sampaio Mulholland, a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709/18), reconhece a importância da tutela dos dados para a garantia dos Direitos Fundamentais dos cidadãos, justificando a aplicação da lei para tutela especial da "*proteção da liberdade de expressão e de comunicação, privacidade, honra, imagem, autodeterminação informativa e livre desenvolvimento da personalidade (art. 2º)*"; contudo, de sua análise se observa que algumas questões ainda estão em aberto, demandando discussão e aprofundamento.[31]

Neste esteio, cabe considerar que a LGPD brasileira foi inspirada no Regulamento UE n.º 679/2016, relativo à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e a livre circulação desses dados.

---

29 CAVALIERI, Sérgio Filho. Programa de responsabilização civil. 10.ed.- São Paulo: 2012, p. 146.

30 Veja-se RIBEIRO, Márcio Vinicius M. Nossos dados na era digital: Lei Geral de Proteção de Dados. Conhecimento Interativo, São José dos Pinhais/PR, V. 14, N. 2, p. 362-382, jul/dez. 2020.

31 MULHOLLAND, C. S. 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, v.19, nº 3(2018), p.162. Disponível em: https://doi.org/10.18759/rdgf.v19i3.1603 acesso em 12/01/2021.

Desse modo, a RGDP da Europa, bem como, a LGPD do Brasil nasceu com a mesma finalidade de possibilitar uma maior proteção aos dados pessoais dos cidadãos, demonstrando a crescente preocupação com a privacidade, além de limitar o uso desses dados tanto por empresas, quanto pela Administração Pública.

No que se refere ao tratamento de dados pessoais, a LGPD estabeleceu em seu artigo 11 as possibilidades para a realização do tratamento, definindo no inciso II os casos em que caberia sua utilização sem o consentimento do titular, a saber:

> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> **b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;**
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> e) proteção da vida ou da incolumidade física do titular ou de terceiros;
> f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
> g) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> h) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º

Neste sentido, caberia questionar se a alínea b) do referido artigo autorizaria uma utilização de dados pessoais por sistemas de polícia preditiva, especialmente considerando que as atividades policiais se encontram contidas nas políticas públicas de segurança pública, com previsão legal e regulamentar.

Para melhor compreender este extremo, cabe ressaltar que Patrícia Peck destaca que a LGPD tem por objetivo adotar uma política preventiva, que demanda adaptabilidade aos processos de governança corporativa, logo, demanda das organizações a implementação de programas de conformidade digital (*compliance*); sendo também dependente de investimento, atualização de instrumentos para a segurança de dados e melhoria de processos e fluxos no trato de dados das pessoas, inclusive, agregando mecanismos de controle e auditoria, que possam estabelecer mudança de cultura[32].

32 Veja-se PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018 - LGPD. São Paulo: Saraiva Educação, 2018

Sem embargo, cabe destacar que toda esta ideia está voltada às corporações privadas, não ao Poder Público, que além das disposições da LGPD, também se encontra submetido ao princípio de legalidade, o que implica que os dados utilizados com esteio no artigo 11, II, b), não podem estar conformados por atuações não autorizadas pela Lei.

Assim, causa assombro a amplitude do mandado adoptado no mencionado artigo, já que, copiando as disposições do artigo 23 do Regulamento UE 679/2016, já que a correlata norma europeia exige autorização específica da legislação para a limitação dos direitos relativos à proteção de dados, reclamando, ademais:

> a) a finalidade do tratamento ou as categorias de tratamento;
> b) as categorias de dados pessoais em questão;
> c) o alcance das limitações estabelecidas;
> d) as garantias para evitar acessos ou transferências ilícitas ou abusivas;
> e) a determinação do responsável ou categorias de dirigentes;
> f) os prazos de retenção e as garantias aplicáveis, atendendo à natureza, âmbito e objetivos do tratamento ou categorias de tratamento;
> g) os riscos aos direitos e liberdades das partes interessadas, e
> h) direito dos interessados de serem informados sobre a limitação, salvo se a mesma prejudicar os fins desta.

Não cabe, neste sentido, predicar um mandato tão amplo ao Poder Público para evadir-se à sua vinculação pela LGPD, o que indica, em nossa opinião, que pronto se questionará a constitucionalidade da exceção contida no artigo 11, II, b) da LGPD, já que vai de encontro aos próprios objetivos do legislador ao estabelecer seu âmbito de aplicação e, nesse sentido, deve ser interpretado de forma restrita e à luz dos direitos fundamentais que permeiam a matéria.

Não por outro motivo o legislador definiu, ademais dos mecanismos referentes à transparência às limitações de transferência e conservação de dados, a possibilidade de acudir à esfera jurisdicional, com fundamento no artigo 22, cujo conteúdo transcrevemos: "*a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva"*, o que nos obriga a uma remissão ao CPC e à Lei n.º 9507/1997, que regula o *habeas data*, que segue mantendo sua regulação clássica e que, em nossa opinião, pode ser empregado para exigir as atuações previstas na LGPD sobre transparência, exclusão e retificação de dados[33].

33 Sobre o tema, veja-se FOLLONE, Renata Aparecida; SIMÃO FILHO, Adalberto. A conexão da LGPD e CDC: a proteção de dados pessoais nas relações consumeristas e a sua concretização como direito

Neste sentido, apesar dos destacados pontos positivos da LGPD, esta nasce com lacunas que demandam maiores discussões pela sociedade, pelo sistema jurisdicional e pelos bálcãs acadêmicos, especialmente no tocante à aplicabilidade da LGPD na esfera penal, em especial nos casos em que as informações pessoais podem ser utilizadas de forma indiscriminada.

Por outro lado, ainda que fizéssemos menção ao artigo 11. Inciso II, alínea b para destacar uma eventual possibilidade de aplicação das disposições da LGPD em matéria de segurança pública, devemos destacar que o artigo 4º da citada norma, em seu inciso III, determina que suas disposições não se aplicam à matéria penal, consoante se verifica de sua leitura: "Art. 4º- Esta Lei ***NÃO*** se aplica ao tratamento de dados pessoais: [...] III - realizado para fins exclusivos de: a) ***segurança pública;*** b) ***defesa nacional***; c) ***segurança do Estado***; ou d) *atividades de investigação e repressão de infrações penais*;" ***grifo nosso***.

Para Fabrício Polido, esta exclusão de aplicação da normativa das discussões do âmbito da segurança pública, da defesa da nação, segurança de Estado, investigação e repressão dos delitos penais, fazem permanecer violações no que se refere ao tratamento de dados sensíveis das pessoas, em especial, no tocante as "quebras de sigilo"; diferentemente do regulamento europeu que apesar de possuir exceções semelhantes, legislou para retirar esta lacuna, de modo conjunto com a filosofia da normativa construída sobre proteção de dados[34].

Sobre este extremo, cabe destacar que a posta à disposição dos dados pessoais que obram em poder da Administração Pública é substancialmente maior no caso da população negra e pobre, especialmente considerando que nos segmentos sociais mais desfavorecido a utilização dos serviços públicos é expoencialmente mais elevada que entre a população de classe média.

Neste sentido, se consideramos estes dados, observaremos que não somente a política criminal sesgada, ou seja, carregada de preconceito e com cor no Brasil representariam uma ameaça para os direitos e liberdades da população negra com a implementação de mecanismos de polícia preditiva, senão que a própria base de dados

fundamental. En Anais do Congresso Brasileiro de Processo Coletivo e Cidadania. 2020. p. 937-959.

34 POLIDO, Fabrício Bertini Pasquot et. al. Sigilo online, investigações criminais e cooperação internacional: contribuições para a ADC 51/2017. Instituto de Referência em Internet e Sociedade (IRISBH): Belo Horizonte, 2018. Disponível em: https://irisbh.com.br/wp-content/uploads/2018/08/Sigilo-online-investiga%C3%A7%C3%B5es-criminais-e-coopera%C3%A7%C3%A3o-internacional.pdf acesso em: 05/01/2021.

pessoais a ser explorada nas aplicações empregadas nas técnicas de polícia preditiva estaria alimentada e predisposta a analisar mais perfis pobres e negros, estabelecendo, como sinaliza Wacquant na obra antes citada, um sistema policial de inteligência seletiva, à espreita dos pobres e negros.

Por isso, nos parece indispensável que o Brasil adote políticas de vanguarda sobre a matéria, discutindo e legislando sobre as aplicações de mecanismos de polícia preditiva no seu Sistema Nacional de Segurança Pública, estabelecendo normas muito claras e o respeito à igualdade entre todos seus cidadãos, impedindo a subersão absoluta dos objetivos da República Federativa do Brasil, de construir uma sociedade livre, justa e solidária.

5. CONCLUSÕES

Neste breve ensaio, examinamos como os avanços da inteligência artificial podem produzir vulnerações se não se observa a necessidade de regular esta implementação, garantindo e protegendo a tutela dos direitos fundamentais dos cidadãos.

Vimos que esta discussão ganha especiais contornos, quando tratamos desse processo expansivo na seara punitiva, ou seja, no Direito Penal, especialmente nas atividades que antecedem ao processo penal, como na segurança pública, com o crescente desenvolvimento e expansão de aplicações que empregam técnicas de polícia preditiva e cujo funcionamento se baseia em inteligência artificial.

Não adotamos, propositadamente, o crescente clamor por uma regulação ética, por entender que a Administração Pública, vinculada que está pelo princípio de legalidade, tanto em suas atuações materiais, como na seara regulamentar, não pode nem deve estar sujeita a normas éticas, senão a uma eficaz regulação jurídica.

Tratando sobre este tema e, centrando nossa atenção especialmente na dinâmica de funcionamento das aplicações de polícia preditiva, verificamos que a população negra e pobre, usuária dos serviços públicos, que produzem uma massiva quantidade de dado sensíveis da população usuária, seria a potenciamente mais afetada pelos riscos da implementação desse modelo, especialmente pela possível incidência dos chamados sesgos discriminatórios, o que demanda cautelas técnicas, mas também jurídicas neste processo.

Neste sentido, examinando de forma muito breve as disposições da Lei Geral de Proteção de dados, verificamos duas coisas. Primeiro, a existência de uma cláusula geral absolutamente genérica e com capacidade para profundas vulnerações dos direitos fundamentais dos cidadãos e, segundo, que a inaplicabilidade deste diploma em matéria de segurança pública gera uma lacuna legal que deve ser colmada, e cuja discussão é atual, urgente e necessária.

Assim, noticiamos as recentes discussões que estão sendo levadas a efeito no âmbito da União Europeia, pela Comissão de Liberdades Civis, Justiça e Assuntos de Interior, cujo recente projeto de informe sobre a inteligência artificial no Direito Penal e sua utilização pelas autoridades policiais e judiciais em assuntos penais se encontra em plena discussão, o que evidencia a importância da temática.

Por outro lado, também sinalizamos a vulnerabilidade que decorre dessa lacuna legal para a população negra e pobre, usuária de serviços públicos em um Estado em que as garantias constitucionais se encontram mermadas a cada dia, reclamando-se uma atitude positiva e proativa do Poder Legislativo, assumindo a vanguarda na garantia dos Direitos e Liberdades e a igualdade real de todos e todas as brasileiras, dentro e fora das repartições públicas, orgãos policiais e no âmbito do Poder Judicial.

Neste sentido e à quisa de conclusão, dado que este é um cenário em construção, entendemos que todas estas questões, inclusive aquelas que sinalizamos a importância, ainda que não fizessem parte de nosso objeto de pesquisa, devem ser tratadas não somente pela doutrina, mas pela sociedade civil organizada, já que como defendia o ilustre processualista Calmón de Passos, pelo Direito não se faz justiça social.

REFERÊNCIAS

BENÍTEZ, Lucía. Ética y transparencia para la detección de sesgos algorítmicos de género. **Estudios sobre el Mensaje Periodístico.** N. 25, Año 3 (2019), pp. 1307-1020.

BOGARD, William. *Simulation and pos-panopticism.* In BALL, Kirstie; LYON, David; HAGGERTY, Kevin D. (Ed.). Routledge handbook of surveillance studies. Routledge, 2012, p. 30.

CASTELLS, Manuel**. La sociedad red.** Alianza Ediorial. Madrid: 1997, p. 88-90.

CAVALIERI, Sérgio Filho. **Programa de responsabilização civil.** 10.ed.- São Paulo: 2012, p. 146.

CEYHAN, Ayse. "Surveillance as biopower". In: BALL, Kirstie; LYON, David; HAGGERTY, Kevin D. (Ed.). Routledge handbook of surveillance studies. Routledge, 2012, p. 41-42.

CINELLI, Virginia. "El uso de programas de análisis predictivo en la inteligencia policial: una comparativa europea". Revista de Estudios en Seguridad Internacional, V. 05, nº. 02, (2019), p. 1-19.

DE SOUZA, Paulo Vinicius Sporleder. **"Biobancos, dados genéticos e proteção jurídico-penal da intimidade"**. Revista AMRIGS, n. 56 (3), jul-set 2012, pág. 268-273.

ENSIGN, Danielle et al. Runaway feedback loops in predictive policing. In: Conference on Fairness, Accountability and Transparency. PMLR, 2018. p. 160-171.

ERGUSON, Andrew G. "Policing Predictive Policing". Wasington University Law Review, n.º 94. Whashington, 2017. p.1109. Recuperado de: https://openscholarship.wustl.edu/law_lawreview/vol94/iss5/5. Acesso em 10/01/2021.

FERNÁNDEZ DE LA MORENA, Berta. **Discriminación Algorítmica Estudio del sesgo en arquitecturas de aprendizaje profundo.** Universidad Autónoma de Madrid. Monografia de fim de curso. Madrid, 2019.

FOLLONE, Renata Aparecida; SIMÃO FILHO, Adalberto. A conexão da LGPD e CDC: a proteção de dados pessoais nas relações consumeristas e a sua concretização como direito fundamental. Em Anais do Congresso Brasileiro de Processo Coletivo e Cidadania. 2020. p. 937-959.

FRIEDE, Reis. "As prisões brasileiras e a condição humana do encarcerado". Revista Interdisciplinar de Direito, 2019, vol. 17, no 1, p. 215-230.

HABERMAS, Jürgen; MCCARTHY, Thomas; MCCARTHY, Thomas. T**he theory of communicative action.** Boston: Beacon press, 1984.

LLINARES, Fernando Miró. "Policia predictiva: utopia o distopia? Sobre les actituds cap a l'ús d'algorismes de big data per a l'aplicació de la llei". IDP: revista d'Internet, dret i política, 2020, no 30, p. 6-7.

MAISUECHE CUADRADO, Alberto. Utilización del Machine Learning en la Industriav4.0. Publicação em acesso aberto. Universidad de Valladolid. Valladolid. Recuperado de: https://cutt.ly/qgjnJ0x. Acesso em 10/01/2021.

MULHOLLAND, C. S. 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, v.19, nº 3(2018), p.162. Disponível em: https://doi.org/10.18759/rdgf.v19i3.1603 acesso em 12/01/2021.

NORVIG, Peter. **Artificial Intelligence: A Modern Approach. Ed. Prentice Hall. Nova Jersey, 2003, p. 712.**

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 -** LGPD. São Paulo: Saraiva Educação, 2018

PINO DIEZ, Raúl. I**ntroducción a la Inteligencia Artificial.** Universidad de Oviedo. Oviedo: 2001, p. 03.

POLIDO, Fabrício Bertini Pasquot et. al. Sigilo online, investigações criminais e cooperação internacional: contribuições para a ADC 51/2017. Instituto de Referência em Internet e Sociedade (IRISBH): Belo Horizonte, 2018. Disponível em: https://irisbh.com.br/wp-content/uploads/2018/08/Sigilo-online-investiga%C3%A7%C3%B5es-criminais-e-coopera%C3%A7%C3%A3o-internacional.pdf acesso em: 05/01/2021.

PROVOST, F. Data Science for Business: What you need to know about data mining and data - analytic thinking. O'Reilly Media, 2013, p. 22 y ss.

RAMIÓ, Carles. **Inteligencia artificial y administración pública: robots y humanos compartiendo el servicio público.** Los Libros de la Catarata, 2019.

RIBEIRO, Márcio Vinicius M. Nossos dados na era digital: Lei Geral de Proteção de Dados. Conhecimento Interativo, São José dos Pinhais/PR, V. 14, N. 2, p. 362-382, jul/dez. 2020.

RODRIGUES, G. LGPD penal: um remédio contra o solucionismo tecnológico na segurança pública? 11 nov 2020. Disponível em: https://irisbh.com.br/lgpd-penal-um-remedio-contra-o-solucionismo-tecnologico-na-seguranca-publica/ acesso em 10/01/2021.

SANTOS-HERMOSO, Jor**ge. Policía Predictiva en España**. Aplicación y retos futuros". Behavior & Law Journal, 6(1), 26-41.

SCHWAB, Klaus. **A quarta revolução industrial.** Edipro, 2019.

SELVA, Leonardo Vinicius Galvão. **A transcendental ameaça do direito penal do inimigo ao estado de direito: a lei antiterrorismo brasileira**. Profanações, 2020, vol. 7, p. 431-451.

SHAPIRO, Aaron. **Predictive policing for reform? Indeterminacy and intervention in big data policing**. Surveillance & Society, v. 17, n. 3/4, 2019. págs. 456-548.

STEYVERS, Mark. "Active Bayesian Assessment for Black-Box Classifiers". Cornel University. Disponível em: https://arxiv.org/pdf/2002.06532.pdf. Acesso em 15/01/2021.

SUÁREZ XAVIER, Paulo Ramón. **Gobernanza, Inteligencia Artificial y Justicia Predictiva:** los retos de la Administración de Justicia ante la Sociedad en Red. Tese de doutoral. Universidade de Málaga, 2020.

SUSSKIND, Richard; SUSSKIND, Daniel. **El futuro de las profesiones: cómo la tecnología transformará el trabajo de los expertos humano**s. Oxford University Press, Estados Unidos, 2015.

VILAR, Silvia Barona. "La sociedad postcoronavirus con big data, algoritmos y vigilancia digital,¿ excusa por motivos sanitarios?,¿ y los derechos dónde quedan?". Revista Boliviana de Derecho, 2020, no 30, p. 14-39.

WACQUANT, Loïc. **Las cárceles de la miseria. B**uenos Aires, 2000, págs. 124-125.

WADSWORTH, Christina; VERA, Francesca; PIECH, Chris. **Achieving fairness through adversarial learning:** an application to recidivism prediction. arXiv preprint arXiv:1807.00199, 2018.