PUC

DEPARTAMENTO DE DIREITO

Inteligência Artificial e Direito Penal: A Seletividade na Era Digital

Por

Ana Luiza Feitosa Vieira

Orientadora: Victoria-Amalia Sulocki

2022.1

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO DE JANEIRO
RUA MARQUÊS DE SÃO VICENTE, 225 - CEP 22453-900
RIO DE JANEIRO – BRASIL

Inteligência Artificial e Direito Penal: A Seletividade na Era Digital

Por

Ana Luiza Feitosa Vieira

Monografia apresentada ao Departamento de Direito da Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) para a obtenção do Título de Bacharel em Direito.

Orientadora: Victoria-Amalia Sulocki

2022.1

Dedicatória

Esse é um momento muito especial. Desde criança já falava que queria ser juíza. E a conclusão do curso de Direito é o primeiro grande passo dessa caminhada linda e corajosa que se concretizará.

A elaboração do presente trabalho é resultado de uma comunhão, de uma rede de apoio que eu tenho o privilégio de ter. Com toda certeza Deus, familiares, amigos e professores me guiaram. É para essas pessoas que quero dedicar essa monografia.

Aproveito para dedicar também às tantas vidas que se foram na pandemia do COVID-19.

Agradecimentos

Tempo da minha formatura e de vir, publicamente, agradecê-los por tudo ao longo desses 10 períodos.

Primeiramente, agradecer a Deus: Tudo que vem dele é maravilhoso, até mesmo naquele momento que não pareça. A cada obstáculo superado, outros aparecerão. Por isso, sempre procurei construir pontes para novas pontes. A força que tenho para alcançar meus sonhos e torná-los realidade, sem dúvida, não vem do lado ou de trás, vem de cima.

Familiares: São nosso pilar; nosso porto-seguro para nos encorajar, chorar, conquistar, comemorar, ou seja, nos momentos bons e ruins estão com a gente. Pai e mãe, vocês são essenciais na minha formação. Sem a confiança e todo patrocínio, não teria Aninha encerrando essa fase de cabeça erguida e com sorriso no rosto de "dever cumprido".

Amigos: Quando entramos na faculdade, nos sentimos um pouco perdidos diante de uma nova realidade. Afinal, ali já não era mais a nossa escola, o nosso berço que no meu caso foi o GARRIGA e que sempre levarei no coração. Universidade tem um ar de independência que já demanda maiores responsabilidades e assusta. Mas, aos poucos nos identificamos com algumas pessoas e formamos vínculos afetivos que tornaram esse ciclo mais leve. Foi uma fase que exigiu a vontade extra de cada um em estar junto ("alô, zoom"), em um cenário onde o distanciamento social era para sobrevivência.

Vale frisar o apoio do meu trio fantástico "PAN-TA-NAL" que desde o "Primeiro Dia PUC" já estava lado a lado fazendo essa trajetória mágica e acolhedora.

Professores: Agradeço a PUC por proporcionar professores incríveis, em especial dois que, sem dúvida, marcaram minha caminhada acadêmica. O primeiro é o professor querido Pedro Marcos Nunes Barbosa que no segundo período veio mostrando diretrizes fundamentais para que eu pudesse chegar até aqui dedicada e confiante na minha atuação.

E a minha orientadora Victoria Sulocki. Lembro que já acompanhava ela antes mesmo de ser minha professora nas mobilizações pela defesa dos direitos humanos. A admiração só cresceu diante da garra e o vigor que ela entrega nas aulas com uma visão humana e sensível da realidade criminal contemporânea. Inclusive, foi a partir de uma dessas aulas de processo penal no quinto período que passei a refletir sobre o meu tema da monografia e desde então tenho pesquisado sobre, para hoje consolidá-lo.

Vítimas do COVID-19: as memórias trágicas dos últimos dois anos contribuíram para uma visão mais responsável e solidária para com o outro.

Resumo

As crescentes tendências na adesão de tecnologias programadas por Inteligência Artificial demandam maior atenção no seu alcance e reflexos no Poder Judiciário, em especial no Direito Penal que traz maior humanidade para as relações jurídicas. Os algoritmos se mostraram ferramentas de intelecto limitado, falível, enviesados com diferentes níveis de consciência e inconsciência, estereótipos, historias, memórias e preconceitos. É importante frisar que estas deficiências que estão presentes na construção coletiva da sociedade não são excluídas com a implementação das máquinas. O volume, a capacidade de processamento, a velocidade e a profundidade de intervenção atingidas por tecnologias digitais tornam esses erros ainda mais significativos e danosos. O lado sombrio digital, sem clareza do que e como está sendo processado, é um potencial instrumento de violação dos direitos e garantias fundamentais, as quais têm sido silenciadas em virtude da dificuldade de questionamentos. Dessa forma, é evidente não se tratar de meros erros matemáticos, uma vez que não desapega do substrato social contribuindo para a legitimação de uma seletividade digital.

Palavras-chave: Hipertecnologias; Inteligência Artificial; Criptopoder; Falhas; Transparência; Contraditório; Ampla Defesa; Presunção de Inocência; Seletividade Digital.

Sumário

Introdução

Observa-se que, há uma nova revolução acontecendo no mundo. Depois da Revolução Industrial, a revolução tecnológica veio para ficar. A tecnologia vem sendo inserida na sociedade contemporânea com a ideia de facilitar a vida em seus diversos aspectos. A Inteligência Artificial (IA) é certamente uma dessas ferramentas tecnológicas que atrelada ao Judiciário desempenha a melhor eficácia dos atos judiciais até a execução de funções como: tramitação e armazenamento de processos, acesso a documentos legais e aumento da produtividade.

A sofisticação informática tem influenciado o modo de viver das pessoas. Recentemente, circulam ideias que sugerem, por exemplo, a substituição de juízes por robôs justificando-se como meio de evitar as incertezas das mudanças de opinião, os erros, as falhas, as demoras e os custos.

No Brasil, se "sonha" com a eficiência das máquinas no Judiciário. Aos poucos, verifica-se o avanço da IA em setores administrativos do Poder Judiciário, ainda em fase teste, cujo desfecho final, será, inevitavelmente, pugnar pela adoção desse sistema em escalas cada vez maiores, beirando a substituição dos julgadores.

Contudo, é de suma importância frisar que há algo de perverso na equiparação da atividade jurisdicional de solucionar um conflito a uma linha de montagem da indústria capitalista, cujo único objeto é a maximização do lucro e a minimização dos "custos", sob a lógica desumanizante do fordismo primitivo.

Nesse sentido, a crescente aposta na força de algoritmos, que por ora se mostram aparentemente eficientes, revelam imensa carga de *criptopoder* do programador com fortes tendências a aumentar seu poder repressivo em detrimento da capacidade crítica do ser humano.

A produção de modelos e atos padronizados limita o campo de atuação das ciências humanas que, no Direito, principalmente na área penal, se guiam por normas, mas o peso subjetivo é de grande valia.

O uso das ferramentas em audiências e sentenças, sejam condenatórias ou absolutórias, bem como dos recursos, seja para admissibilidade ou para conhecimento, contribui para uma maior seletividade na era digital, justificada pela matemática e padrões, legitimando os prejuízos "programados" aos historicamente marginalizados.

Uma frase que muito diz é "a história do Direito Penal é a história da humanidade. Ela surge com o homem e o acompanha através dos tempos, isso porque o crime, qual sombra sinistra, nunca dele se afastou" (Magalhães Noronha). A partir disso, observa-se que a interação social nem sempre foi harmônica. Com isso, depreende-se o motivo já das primeiras manifestações da existência de um ordenamento jurídico em uma sociedade, ocorrerem na seara penal, por intermédio da função punitiva, em virtude da qual, confere-se ao grupo a capacidade de punir, garantir a prevalência de sua ordem e consequente continuidade.

Em breve síntese, o Iluminismo propiciou ao Direito Penal abandonar a vingança e adotar uma concepção mais humanitária, na qual os direitos humanos seriam respeitados e assegurados. Diante das barbaridades à época, vislumbrou-se a necessidade de conscientização e de ruptura com os convencionalismos e tradições ora vigentes.

Ocorre que, a discriminação tão arraigada na sociedade brasileira não cessou com as ideias progressistas da ciência criminal e foi se "aperfeiçoando" utilizando instrumentos, cada vez mais, sofisticados para manipular e ratificar esse fenômeno social, fosse por renda, raça, idade, local de residência. E o mais recente são os projetos experimentais da Inteligência Artificial na Justiça Brasileira.

Sendo assim, buscando demonstrar a influência direta, vale-se dizer, negativa da IA sobre o Direito Penal, o primeiro capítulo abordará a

informatização do Direito Penal, elucidando o significado, o surgimento da IA, os variados projetos experimentais, apontando também as diferentes frentes de responsabilização.

O segundo capítulo tratará do lado obscuro, sem transparência, oculto e complexo dos algoritmos que, frequentemente, significam segredo de negócios. E, justamente, por isso, no sentido de não serem auditáveis -não que seja tecnicamente impossível, mas por ser economicamente um dado sigiloso-, podem ser tendenciosos e preconceituosos. Quanto a isso, já cabe trazer o episódio da Microsoft que, em março de 2016, apresentou ao mundo a conta no Twitter *@TayandYou*, que era de sua "chatbot" - programas computacionais que simulam um humano na conversação com outras pessoas-[1]no qual o perfil ficou menos de um dia no ar, tendo sido desativado em razão das mensagens racistas, homofóbicas, misóginas realizadas após interagir com humanos e absorver deles esses entendimentos lamentáveis expressados publicamente na referida rede social. Aproveita-se o momento para registrar algumas referências à Lei Geral de Proteção de Dados Pessoais que trata de modo excepcional a matéria criminal.

Os algoritmos têm sido ferramentas que diminuem o ônus sobre as instituições, inexistindo paridade entre eles e as decisões humanas[2].

É fundamental questionar, assim, se é esse o objetivo que se espera encontrar nas inovações. Deve-se automatizar pela simples automação? Ou cabe uma reflexão ética sobre injustiças algorítmicas? Questioná-los e enfrentar decisões supostamente injustas, ou manter a ideia de que são processos livres de falhas, ignorando injustiças e outros males?

---

[1] MOREIRA, Isabela**. A Microsot criou um robô que interage nas redes sociais - e ela virou nazista.** Revista Galileu. Disponível em: <https://revistagalileu.globo.com/blogs/buzz/noticia/2016/03/microsoft-criou-uma-robo-que-interage-nas-redes-sociais-e-ela-virou-nazista.html>. Acesso em 10/03/2022.

[2] SANTOS, Coriolano Camargo; CHEVTCHUK, Leila. **Inteligência artificial, algoritmos e decisões injustas: é hora de revermos criticamente nosso papel em face da tecnologia**. Portal Migalhas. Disponível em <https://www.migalhas.com.br/coluna/direito-digital/268283/inteligencia-artificial--algoritmos-e-decisoes-injustas--e-hora-de-revermos-criticamente-nosso-papel-em-face-da-tecnologia>. Acesso em 14/05/2022.

E o terceiro capítulo, por sua vez, trará algumas das violações constitucionais presentes nessas hipertecnologias avançadas e o que poderia ser feito para ao menos minimizá-las.

Por fim, para seguir o roteiro e iniciar o presente trabalho, é necessário destacar que os algoritmos são criados por pessoas, ou seja, são reflexo da sociedade que os cerca, mas até que ponto se esforçará por uma sentença justa, considerando apenas dados estatísticos, fórmulas exatas, probabilidades.

O direito é uma ciência humana regida a acolher demandas humanas. O aumento significativo das decisões baseadas em *big data* e algoritmos, faz com que muitos processos sejam automatizados, inclusive decisões sobre a vida das pessoas.

Ante o exposto, se por um lado considera-se a IA uma grande aliada do aumento da produtividade do Poder Judiciário brasileiro, para tornar a justiça mais efetiva e com maior qualidade, por outro infere-se como mais um instrumento para legitimar a seletividade em marginalizar, cada vez mais, os marginalizados (redundância proposital para representar o limbo instaurado) e exaltar a minoria dominante.

1. A Informatização e Seus Reflexos no Direito Penal

1.1. O Significado e a Origem da Inteligência Artificial

Inicialmente, cabe esclarecer o significado de algoritmos. De acordo com Moschovakis[3], não há uma definição universal e consensualmente aceita, embora esse conceito exista há séculos.

Intuitivamente, pode-se dizer que "um algoritmo é uma sequência de regras que devem ser executadas na ordem exata para realizar determinada tarefa", um método lógico que pode ser aplicado a qualquer campo do conhecimento, como uma receita culinária, a leitura de uma partitura musical ou a solução de um problema matemático[4].

A inteligência artificial, por sua vez, é um ramo da ciência da computação que estuda e desenvolve agentes inteligentes, assim chamados porque são máquinas executando, de forma dita inteligente, tarefas consideradas significativamente difíceis. Trata-se de termo criado por John McCarthy em 1956[5].

Não obstante, conforme tese de doutorado defendida por Romulo Soares Valentini[6]:

> "Inicialmente, é necessário estabelecer o mecanismo de entrada de dados (input). Um algoritmo deve ter um ou mais meios para recepção dos dados a serem analisados. Em uma máquina computacional, a informação deve ser passada para o computador em meio digital (bits). Do mesmo modo, é necessário ter um mecanismo para a saída ou retorno dos dados trabalhados (output). Um algoritmo deve ter um ou mais meios para retorno dos dados, os quais devem estar relacionados de modo específico com o input. Por exemplo, um algoritmo de uma calculadora que receba as informações para somar 2+2 (input) irá retornar como resultado o número 4 (output). O output decorre do input, sendo papel do algoritmo fornecer o retorno dos dados corretos a partir dos dados de entrada. Uma vez que o algoritmo não faz nenhum juízo de valor para além de sua programação, é necessário que a relação de "correção" entre o input e o output seja definida de modo preciso e sem ambiguidade. **Por isso, os algoritmos precisam ter cada passo de suas operações cuidadosamente definido.** Assim**, cada passo da tarefa**

[3] MOSCHOVAKIS, 2001.
[4] OCDE, 2017, p. 08
[5] OCDE, 2017, p. 09
[6] VALENTINI, Romulo Soares. **Julgamento por computadores? As novas possibilidades da juscibernética no século XXI e suas implicações para o futuro do direito e do trabalho dos juristas**. Tese de Doutorado apresentada à Faculdade de Direito da Universidade Federal de Minas Gerais (UFMG). Belo Horizonte, 2018.

> **computacional deve seguir um roteiro de tarefas pré-determinado e o programa (computação dos dados) deve terminar depois que o roteiro seja cumprido**. O algoritmo tem que ser finito, ou seja, entregar algum retorno (output) após cumpridos todos os passos estabelecidos. Para cumprir a tarefa adequadamente, cada operação que o algoritmo tiver que realizar deve ser simples o suficiente para que possa ser realizada de modo exato e em um tempo razoável (finito) por um ser humano usando papel e caneta. Conclui-se, desse modo, que um **o algoritmo é um plano de ação pré-definido a ser seguido pelo computador, de maneira que a realização contínua de pequenas tarefas simples possibilitará a realização da tarefa solicitada sem novo dispêndio de trabalho humano"**. (grifo nosso)

Uma das ramificações da IA é o aprendizado de máquina (*machine learning*). Aqui, os computadores utilizam algoritmos para que, iterativamente, aprendam a partir dos dados previamente coletados e da experiência das iterações. Já em 1959, Arthur Samuel dizia que o "aprendizado de máquina fornece aos computadores a habilidade de aprender sem serem explicitamente programados".

Nesse contexto, verifica-se que, apesar desses conceitos existirem há algum tempo, nas últimas décadas tem sido crescente o desenvolvimento exponencial de capacidade de coleta, armazenamento e processamento de informações pelas máquinas. Sendo assim, o uso de algoritmos e IA se expandiu para todos os campos do conhecimento, apresentando resultados que aparentam ser progressivamente mais eficientes, eficazes e efetivos[7].

1.2. Inteligência Artificial Forte e Fraca

Faz-se necessário distinguir a Inteligência Artificial Forte e Fraca. Enquanto o objetivo da primeira (forte) é construir uma máquina que responda à inteligência geral humana, a segunda (fraca) busca emular a realização de tarefas específicas, sem raciocinar, basicamente simula a inteligência e não possui autoconsciência[8].

A IA forte está relacionada com o desenvolvimento de máquinas que tenham a capacidade de pensar e não apenas simular raciocínios programados. O software teria conhecimento intrínseco a si das razões de ter

[7] O'NEIL, 2016; WORLD ECONOMIC FORUM, 2018
[8] LÓPEZ DE MÁNTARAS BADIA; MESEGUER GONZÁLEZ, 2017

manipulado certos símbolos e talvez até teria que ter pensado ou manifestado emoções. Um exemplo que a IA Expert Academy aponta é "se uma máquina for submetida ao processo de escrever uma poesia, ela teria que ter consciência do que escreveu e não somente organizar as palavras para formar frases"[9].

Já a IA fraca está relacionada à construção de máquinas ou *softwares* de certa forma inteligentes, mas sem autoconsciência. Da mesma fonte IA Expert Academy é dado o caso de um "sistema especialista que existe um componente chamado motor de inferência, que é responsável por fazer o encadeamento das regras e tomar as decisões analisando múltiplas condições do tipo *se-então*. Neste caso, não existe um real raciocínio da máquina, pois ela necessita que especialistas humanos forneçam o conhecimento para que o software consiga executar e tomar suas decisões"[10].

Em síntese, há duas classificações em destaque sobre o tema:

a) a famosa divisão de Peter Searle entre programas que atingiriam um nível tal de inteligência a ponto de terem uma mente tal qual humanos, e programas que apenas seriam capazes de simular (criar um modelo) essa mente; e
b) aquela exposta por Ray Kurzweil e outros futuristas, que criaram uma separação mais quantitativa que qualitativa, definindo como Inteligência Artificial Forte aquela que é capaz de competir ou mesmo superar a mente humana em qualquer atividade, sem ter sido, portanto, projetada para uma função específica e bem delimitada. Ela também é chamada de inteligência artificial geral (*Artificial General Intelligence)* ou de singularidade tecnológica.

[9] **Conceitos sobre IA**. Expert Academy. Disponível em <https://iaexpert.academy/2017/01/17/ia-forte-x-ia-fraca/>. Acesso em 12/04/2022.
[10] Ibid.

Nesse sentido, cabe mencionar o experimento de Alan Turing que rejeitou a pergunta “as máquinas podem pensar?” e a substituiu por um teste comportamental.

Reportou a experiência em seu famoso ensaio “*Computing Machinery and Intelligence*”[11], sugerindo que em vez de perguntar se as máquinas podem pensar, deve-se perguntar se as máquinas podem passar por um teste de inteligência comportamental que chamou-se de teste de Turing. Este

> “consiste em fazer um programa desenvolver uma conversação (via mensagens digitadas online) com um interrogador por cinco minutos. O interrogador deve então adivinhar se teve a conversação com um programa ou uma pessoa; o programa passa pelo teste se enganar o interrogador durante 30% do tempo. Turing conjecturou que, por volta do ano 2000, um computador com espaço de armazenamento de 10 unidades poderia ser programado suficientemente bem para passar no teste. Ele estava errado- os programas ainda não conseguem enganar um juiz sofisticado”[12].

1.3. Alguns Projetos Concretos de Sucesso da Inteligência Artificial

O recorte temporal aqui se dará a partir dos anos 90, época marcada pela explosão da internet comercial. Programas que vasculhavam a rede automaticamente e classificavam resultados, como o protótipo do Google, nasceram nesse período. As máquinas foram sendo desenvolvidas para auxiliar nas atividades humanas.

Em 2002, a *iRobot* lançou o primeiro Roomba – assistente de limpeza autônomo que combina eficiência e especialização –, bem como um teclado de pré-configurações e sensores de posicionamento em operação conjunta[13].

Em setembro de 2018, a mesma empresa, Roomba iRobot, anunciou um novo robô aspirador que, agora, utiliza a IA para desviar de dejetos

---

[11] Turing, 1950

[12] RUSSEL, Stuart J; NORVIG, Peter. **Inteligência Artificial.** 3ª ed. Rio de Janeiro: Elsevier, 2013. p. 1195. Disponível em <https://www.cin.ufpe.br/~gtsa/Periodo/PDF/4P/SI.pdf>. Acesso em: 19/05/2022.

[13] **Lançado robô dedicado à limpeza doméstica.** Portal Inovação Tecnológica. Disponível em: <https://www.inovacaotecnologica.com.br/noticias/noticia.php?artigo=010180020924&id=010180020924>. Acesso em 19/05/2022.

deixados por animais domésticos, cães e gatos e foi considerado como o mais aguardado pelos consumidores[14].

Outro empreendimento maquinário de destaque veio em 2005, com a Boston Dynamics. O desenvolvimento do robô *Big Dog*, capaz de se movimentar por terrenos de difícil acesso para humanos, se deu em formas de cachorro e até humanoides, estando cada vez melhores em mobilidade e inteligência[15].

Há, ainda, o estudo da implementação da IA para aplicação em carros autônomos, o que demanda conexão da plataforma com vários sensores do próprio veículo e também com o tráfego em si, de semáforos a outros automóveis[16].

O aprendizado evoluído da IA foi aprimorado por projetos do *Google* que desde 2006 se dedicou em *deep learning* e em 2012, por exemplo, conseguiu treinar um algoritmo para reconhecer gatilhos em vídeos do *Youtube*.

Vale dizer que essa instrumentalização do *deep learning* é, segundo a *Wikipedia*,

> "um ramo do aprendizado de máquina baseado em um conjunto de algoritmos que tentam modelar abstrações de alto nível de dados usando um grafo profundo com várias camadas de processamento, compostas de várias transformações lineares e não lineares"[17].

Ademais, o *deep learning* pode ser integrado com outro processo, qual seja a visão computacional, cuja função depreende-se em permitir que um sistema lide com obtenção, compreensão e análise de imagens. Inclusive, a empresa *Affectiva* empregou isso em reconhecimento de rostos para

---

[14] GOGONI, Ronaldo. **Venni N1, o robô-aspirador capaz de evitar "presentinhos"**. Portal Meio Bit. Disponível em <https://tecnoblog.net/meiobit/393701/venii-n1-robo-aspirador-anti-coco/>. Acesso em 19/05/2022.

[15] ***Legacy Robots: The robots that built the groundwork for today's portfolio***. Portal Boston Dynamics. Disponível em: <https://www.bostondynamics.com/legacy>. Acesso em 19/05/2022.

[16] **Aplicação da inteligência artificial na gestão de frotas e seus benefícios**. Portal Infleet. Disponível em: https://infleet.com.br/blog/aplicacao-da-inteligencia-artificial-na-gestao-de-frotas-e-seus-beneficios. Acesso em 19/05/2022.

[17] **Aprendizagem Profunda.** Portal Wikipédia Brasil. Disponível em: <https://pt.wikipedia.org/wiki/Aprendizagem_profunda#cite_note-goodfellow2016-1>. Acesso em18/05/2022.

reconhecer emoções humanas e usa como publicidade "*Humanizing technology to bridge the gap between humans and machines*"[18].

No que tange ao âmbito jurídico – objeto do trabalho –, a IA foi implementada, inicialmente, com a criação do robô *Ross*[19], o primeiro advogado artificialmente inteligente do mundo. O procedimento se dava da seguinte forma: os advogados perguntavam questões jurídicas à *Ross* em linguagem natural, assim como se conversassem com um humano e a inteligência artificial as interpretava utilizando a lei, reunindo provas, referências e as responde rapidamente, de modo relevante e baseado em evidências. Foi incorporado, em novembro de 2017, à *Baker e Hosteller*-empresa famosa no ramo de falências, com sede em Nova Iorque-EUA. Todavia, veja, se por um lado agiliza na questão mecânica de reunir provas objetivas de acordo com as indagações trazidas, por outro, esse método carece de eficiência em situações que exigem o mínimo de subjetividade ou juízo de valor.

Não obstante, buscando espelhar que a aplicação da IA no mérito do campo jurídico demanda maior atenção ao binômio necessidade-adequação, segue tal abordagem no próximo subcapítulo.

1.4. Experiências da Inteligência Artificial no Direito Brasileiro

Dentre muitos programas de Inteligência Artificial que já operam, em todo território nacional, na área jurídica, podemos apontar alguns.

Primeiramente, a iniciativa do Tribunal de Justiça do Estado de Minas Gerais, desenvolveu um sistema para indexação automática de processos, a

[18] Tradução livre: "tecnologia de humanização para preencher a falha entre humanos e máquinas". Conforme: **Deep Learning**. Portal Affectiva. Disponível em: <https://www.affectiva.com/how/deep-learning-at-affectiva/>. Acesso em 18/05/2022.

[19] **Ross, o primeiro robô advogado do mundo**. Portal ICEV. Disponível em <https://www.somosicev.com/blogs/ross-o-primeiro-robo-advogado-do-mundo/>. Acesso em 19/05/2022.

fim de identificar com maior facilidade a existência de demandas repetitivas[20].

Do mesmo modo, o Tribunal Superior do Trabalho, em parceria com a Universidade de Brasília (UnB), elaborou um *software* que realizará a triagem automática de processos, bem como processamento de julgados envolvendo a questão jurídica para a sugestão de proposta de voto[21].

Atualmente,

> "há no mercado das empresas de tecnologia e startups de direito, as chamadas *legal techs ou lawtechs*, propostas de desenvolvimento de programas que façam análises acerca do mérito das alegações das partes, resumindo ao magistrado os principais pontos de cada peça e qual é a jurisprudência relacionada ao caso, bem como programas que alegam serem capazes de construir peças jurídicas com pouco ou nenhum auxílio humano".[22]

O Tribunal de Justiça do Rio de Janeiro, por sua vez, apresentou um sistema de inteligência artificial na execução fiscal de tributos municipais[23].

Tecnologias utilizadas nos EUA e em outros países, como o robô de IA da empresa IBM que auxilia na redação e análise de petições, já estão em uso em alguns escritórios maiores do Brasil[24].

No início de 2018, o Supremo Tribunal Federal anunciou o desenvolvimento de um programa de IA, batizado de *Victor*, também em parceria com a UnB[25]. O objetivo é ler os recursos extraordinários

---

[20] BRASIL. Tribunal de Justiça do Estado de Minas Gerais. **Gestão de precedentes é tema de encontro no TJMG**. Disponível em <http://www.tjmg.jus.br/portal-tjmg/noticias/gestao-de-precedentes-e-tema-de-encontro-no-tjmg.htm>. Acesso em 30/03/2022.

[21] RACANICCI, Jamile. **Judiciário desenvolve tecnologia de voto assistido por máquinas**. Disponível em: <https://www.jota.info/justica/judiciario-desenvolve-tecnologia-de-voto-assistido-por-maquinas-080120>. Acesso em: 30/03/2022

[22] CONJUR, 2017; CHIESI FILHO

[23] Disse o órgão que "o inovador sistema de inteligência artificial, testado pelo Tribunal de Justiça, realiza todas essas operações em apenas 25 segundos. É um mecanismo 1.400% mais rápido, com 99,95% de precisão.". Conforme: BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **TJRJ adota modelo inovador nas cobranças de tributos municipais**. Disponível em: <http://cgj.tjrj.jus.br/noticias/noticia/-/visualizar-conteudo/5111210/5771753>. Acesso em 28/03/2022.

[24] CHIESI FILHO, 2018

[25] BRASIL. Supremo Tribunal Federal. **Ministra Cármen Lúcia anuncia início de funcionamento do Projeto Victor, de inteligência artificial**. Disponível em: <https://stf.jusbrasil.com.br/noticias/620175789/ministra-carmen-lucia-anuncia-inicio-de-funcionamento-do-projeto-victor-de-inteligencia-artificial>. Acesso em 30/03/2022.

interpostos, identificando vinculações aos temas de repercussão geral, aumentando a velocidade de tramitação[26].

No Superior Tribunal de Justiça, destaca-se *o Projeto Sócrates*, uma IA criada para facilitar a identificação de demandas repetitivas[27].

Dessa forma, atualmente, observa-se que, a adoção da Inteligência Artificial se esgota em procedimentos administrativos e de admissibilidade, nos variados tribunais. Porém, é crescente a tendência em expandir a influência no mérito das decisões e sentenças e substituir julgadores humanos por juízes-robô. Por isso, há de se analisar as consequências desse fenômeno, principalmente no direito penal que exige maior humanidade.

1.5. Responsabilização Penal e Sistema de Inteligência Artificial

A priori, o Direito Penal é um conjunto de normas jurídicas destinadas a proteger a paz social a partir de medidas de segurança e imposição de penas[28].

O seu maior intuito é manter a ordem e promover a paz em uma sociedade democrática de Direito.

> " O Direito Penal foi criado para controlar os seres humanos e suas relações[...]. Entretanto, com o desenvolvimento dos meios tecnológicos, verifica-se que as

[26] Além disso, segundo a versão de 2020 do relatório "Justiça em Números", elaborado pelo Conselho Nacional de Justiça (CNJ) a partir de dados referentes ao ano de 2019, o Poder Judiciário terminou o ano com 77,1milhões de processos em tramitação a serem analisados por 18.091 magistrados e outros 436.207 profissionais, divididos entre servidores e auxiliares. O número de processos em tramitação no ano de 2019 foi 1,5 milhão a menos que no ano anterior, no entanto, apesar da redução ainda há um alto volume de casos. Com o objetivo de aplacar esse alto volume de processos, o Superior Tribunal Federal (STF) tem investido em Inteligência Artificial para assim acelerar a grande quantidade de processos. Victor, como é chamada a IA, foi desenvolvido em parceria com a Universidade de Brasília (UnB) "o que o torna o mais relevante Projeto Acadêmico brasileiro relacionado à aplicação de IA no Direito." Conforme: BRASIL. Supremo Tribunal Federal. **Inteligência artificial vai agilizar a tramitação de processos no STF**. Disponível em: <https://stf.jusbrasil.com.br/noticias/584499448/inteligencia-artificial-vai-agilizar-a-tramitacao-de-processos-no-stf>. Acesso em: 30/03/2022.

[27] A ferramenta identifica grupos de processos que possuem acórdãos semelhantes, o que contribuirá para o aprimoramento da política de incentivo ao instituto dos recursos repetitivos." (STJ, 2019, p. 17).

[28] ESTEFAM & GONÇALVES, 2020

> ofensas criminais não são cometidas apenas por humanos na contemporaneidade"[29].

Segundo Gabriel Hallevy[30] há três vertentes para lidar com o sistema de IA[31]:

- *The Perpetration-by-Another Liability Model (*O Modelo de Perpetração por Outro): esse modelo baseia-se no fato de a máquina não ser humana. Portanto, o sistema penal não pode ser aplicado. A IA seria apenas um instrumento. Este modelo assume que os programadores são os responsáveis, seja por meio de dolo ou culpa.[32]
- *Natural Probable Consequence Liability Model* (Modelo de Responsabilidade de Consequência Natural Provável): apesar de não existir intenção, a máquina comete um crime. Esta modalidade é aplicada quando a IA comete um crime que não foi previsto pelo programador.
- E, por último, *Direct Liability Model* (Modelo de Responsabilidade Direta): neste modelo, a IA é responsabilizada pelo ilícito. Não existe dependência entre a máquina e o programador ou usuário.[33]

Apesar da IA ser útil no ambiente jurídico, há quem questione acerca da possibilidade desta julgar casos concretos. Isso porque do outro lado tem seres humanos esperando por julgamento, e uma máquina, é, por ora, incapaz de sentir, e portanto, de decidir, por exemplo, sobre a liberdade de alguém. Senão vejamos:

> "A Inteligência Artificial como ferramenta é incrível, principalmente quando aplicada na automação de documentos jurídicos, gerenciamento de prazos e pesquisas jurídicas, mas o Direito Penal pode ser manipulado por algoritmos? Entendo que não. **Não há como excluir a sensibilidade humana de um julgamento, principalmente nos casos criminais, em que há uma série de circunstâncias que só seres humanos conseguem definir.** A liberdade para o ser humano é um bem absoluto e um robô jamais conseguirá distinguir o que é verdade e o que é mentira, a exemplo,

[29] FENELON, 2019, online
[30] Professor da Faculdade de Direito no Ono Academic College's School em Israel.
[31] HALLEVY, Gabriel. ***The Basics Models of Criminal Liability of AI Systems and outer circles***. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3402527>. Acesso em 28/03/2022.
[32] Hallevy, 2013.
[33] Hallevy, 2013.

> como num depoimento de uma testemunha ou no interrogatório de um réu no processo penal. Evidente que a Inteligência Artificial traz uma infinidade de informações, mas não podemos esquecer que informação não é conhecimento. Ou seja, mais tecnologia, mais informação, menos conhecimento, menos saber, menos sabedoria."[34] (Grifo nosso)

É imprescindível ressaltar que os dispositivos dependem das pessoas, pois necessita que estas os alimente com as informações. Além disso, há funções que são essencialmente humanas, principalmente as que exigem análise estratégicas e interações pessoais, como a do magistrado.

Esses processos estão intimamente relacionados ao desenvolvimento dos aludidos sistemas de inteligência artificial, em que máquinas são programadas para executar funções que originalmente demandariam raciocínio e empenho humano.

1.6. Projetos Brasileiros em andamento no Sistema de Justiça Criminal, em especial no Policiamento

1.6.1. Projeto Detecta

Em virtude do que foi apresentado, citar-se-á o projeto Detecta, em andamento pela Secretaria de Segurança Pública do Governo de São Paulo. Trata-se de um software utilizado na plataforma da CompStat[35], cujo sistema inspirado na experiência Domain Awareness System (DAS)[36], tem inrteface da Microsoft (*image analytics*[37] *& heatmaps*[38]). Durante a implantação, o projeto contou com o auxílio técnico e treinamento operacional de profissionais da Polícia de Nova Iorque (NYPD).

---

[34] Jirardi, 2020.
[35] CompStat (Compare Statistics) é o sistema mais conhecido é o, utilizado desde 1994 pela polícia de Nova York (Estados Unidos) para cruzar dados de segurança com informações geográficas – o que permite traçar um mapa detalhado da criminalidade e do policiamento na cidade.
[36] Situational awareness é um termo derivado da jargão militar e pode ser entendido como um regime de vigilância do campo operacional, por meio do monitoramento de diversos elementos e informações que podem contribuir para a gestão operacional, tanto tática quanto estratégica. Essa noção deriva dos esforços militares de coletar e produzir dados massivos, a partir de fontes públicas e privadas, para predizer e agir contra ameaças terroristas.
[37] Image Analytics é a capacidade dos computadores de reconhecer atributos dentro de uma imagem.
[38] Heatmap (ou mapa de calor) é um relatório gerado por ferramentas automáticas que utiliza as cores como referência para facilitar o entendimento.

Além de dados públicos de sistemas policiais e governamentais, ao sistema *Detecta* é inserido uma malha de dados da iniciativa privada, basta que haja um convênio.

O grande objetivo do projeto é ser um sistema de vigilância no rastreamento de suspeitos e compilação de dados, a partir de uma identificação automatizada de criminosos, contribuindo assim para a atividade policial.

> "O Detecta, adquirido pela primeira vez em 2014 pela Secretaria de Segurança Pública do estado, o Detecta foi um sistema da Microsoft inspirado na experiência do DAS (Domain Awareness System), fruto da parceria da empresa com o departamento de polícia de Nova York, cujo objetivo era o rastreamento de suspeitos e compilação de dados. Originalmente projetado para identificação e prevenção de ataques terroristas em solo norte-americano, o Detecta foi adquirido em função da promessa de ser um sistema de vigilância que permite a identificação automatizada de criminosos e que sincroniza várias fontes de dados para melhorar a atividade policial. Essa tecnologia organiza os dados de maneira georreferenciada. Entretanto, seu diferencial está na conjunção de reconhecimento de imagens com a construção de modelos estatísticos a partir da análise de grandes bancos de dados — predominantemente públicos. Por meio deles, deriva-se padrões criminais futuros, que serão incorporados no policiamento, aumentando a eficiência policial na guerra ao crime. Originário de concepções e parâmetros militaristas — que equivale a luta contra o crime à luta contra o terrorismo —, a implementação do DAS trouxe a acomodação de novos atores ao modelo de segurança pública, ao incorporar empresas e tecnologias oriundas do setor privado na esfera do provimento da segurança pública estatal. Desta feita, a instalação do sistema Detecta não se deu conforme o planejado. Em 2016, um relatório do Tribunal de Contas do Estado de São Paulo diagnosticou que o sistema não funcionava adequadamente, as funções de predição estavam inoperantes e havia baixa integração de bancos de dados. Em pesquisa de campo apresentada por Perón, Simões-Gomes e Nery (2019), a razão apresentada para tanto foi incapacidade logística e de custos — dificuldades que seriam sanadas no médio prazo, com a incorporação de atores privados. Tal integração, no entanto, não indica o fracasso da iniciativa, mas a configuração determinante de uma simbiose entre os setores público e privado para a operacionalização dessa política. A análise desses novos elementos é essencial para a compreensão do funcionamento do sistema. Em sua dimensão pública, o Detecta tornou-se um sistema abrangente de integração de dados e câmeras, em que a aquisição e instalação de novos aparelhos foram delegadas à iniciativa privada. Constam no sistema as câmeras públicas municipais do Radar (que contam com leitor automatizado de placas de veículos), as City Câmeras, bem como uma malha de aparelhos privados de cidadãos que buscam a adesão — seja individualmente, seja por intermédio de associações, seja em negócios e empresas privadas. Assim, vê-se que esses elementos a serem levados em consideração têm múltiplas filiações: desde projetos municipais (como o City Câmeras e o app SP+Segura), servidores públicos estaduais (Polícias Civil e Militar, Secretaria de Segurança Pública), a empresas nacionais ou transnacionais (como Microsoft, Genetec, Techvoz, Tacira e Aster) e usuários, associações e instituições (Sociedade de Amigos do Alto de Pinheiros e Universidade de São Paulo). Na leitura do setor privado (evidenciado na entrevista de um executivo da

> Microsoft), a integração e visualização dos dados pelo Estado seria dificultada pela falta de expertise, de recursos financeiros, bem como pela despadronização semântica entre as agências de segurança pública. Nesse sentido, a ideia central seria não só providenciar uma solução instantânea para a Secretaria Estadual de Segurança Pública, mas modificar a gestão e interação entre as agências de segurança, tanto as forças policiais, militares e civis, como o aparato judicial. Assim, seria possível constituir uma situational awareness, mediada por esses instrumentos de vigilância. (GOMES. Letícia Simões; 2019)"[39]

De acordo com a Cartilha de Adesão ao Sistema DETECTA, esse projeto experimental é como:

> "uma solução de *software*, com interface web, composta por uma infraestrutura de servidores que realizam funções inteligentes de correlacionamento de diversos tipos de eventos de interesse de segurança pública com as informações das bases de dados integradas à solução: veículos, pessoas (civil e criminal), atendimento 190, etc. Os dados dos eventos são encaminhados àsolução por intermedio dos seguintes tipos de equipamentos, provindo de sistemas pũblicos ou privados: LAP-Leitores Automáticos de Placas de Veiculos, Sistema de Videomonitoramento, Ferramentas de Vídeos Analíticos"[40].

O policiamento preditivo pode ser definido como uma "aplicação da modelagem por computadores a dados criminais passados para predizer atividade criminal futura"[41]. Ou seja, é o "uso de dados e análises para predizer o crime"[42].

A grande novidade é a expansão da lógica de análises estatísticas para uma situação com mais dados disponíveis e poder para analisá-los, o que em tese, transformaria tais policiamentos mais precisos, neutros e confiáveis.

Ocorre que, como pôde se verificar na prática, isso vem fortalecendo práticas discricionárias baseadas no julgamento subjetivo, o qual parece potencializá-los e legitimá-los por meio de montagens sociotécnicas, mediada por tecnologias e sistemas de vigilância.

---

[39] **Policiamento Preditivo, Controle Social e Desigualdades Raciais**. Disponível em: <https://anpocs.com/index.php/encontros/papers/43-encontro-anual-da-anpocs/spg6/spg32-1/12010-policiamento-preditivo-controle-social-e-desigualdades-raciais/file>. Acesso em: 13/05/2022.

[40] **Cartilha de Adesão ao Sistema Detecta (V3.0)**. Disponível em: <http://www.sapp.org.br/sapp/wp-content/uploads/Sistema_Detecta_cartilha_completa_v3.pdf.>. Acesso em 21/05/2021.

[41] BACHNER, apud JOH, 2014, p. 42, tradução livre

[42] SELBST, 2017, p. 114, tradução livre, notas omitidas

É evidente a carência da neutralidade. Dessa forma, constata-se, mais uma vez, a possibilidade da IA adquirir vieses e reproduzir discriminação. Dentre eles, elencam-se:

(a) a discricionariedade do programador no desenvolvimento do software (o grau de precisão e generalização das variáveis, as conexões causais e exemplos dados à máquina no processo de *machine learning*)[43];
(b) a confiabilidade dos dados (dado que muitos vêm de data brokers, i.e., terceiros que compilam e comercializam informações, outros vêm de bancos de dados do governo)[44];
(c) a natureza dos dados (como o banco sobre antecedentes criminais estão dentre os mais frequentes, assim como o de ocorrências)[45];
(d) a manipulação dos dados (em quais categorias crimes são agrupados e qual a sua priorização[46];
(e) a inserção dessas técnicas no processo de policiamento (se serve para alocação de recursos, para a formação de "listas de ameaças ("threat lists"), para investigação de suspeitos pré-identificados, etc.)[47].

É importante destacar a modelagem bastante heterogênea desses softwares em suas fontes. Todavia, alguns dados relativos a bancos de dados do Estado estão quase sempre presentes, tais como: fichas de antecedentes criminais, passagem pelo sistema carcerário, participação nos sistemas de assistência social, etc.

O considerado êxito nas apreensões de armas de fogo e interceptações por parte do *Detecta* tem sido garantido pelo aumento no número de câmeras de monitoramento. Conforme informações do Governo de São Paulo, o sistema foi adotado em 2014, e já em 2016 contava com mais de 500 novas câmeras de monitoramento.

[43] SELBST, 2017, p. 131
[44] MADDEN et. al, 2017
[45] SELBST, 2017; LUM; ISAAC, 2016
[46] SELBST, 2017
[47] Ibid.

Os números são surpreendentes. Atualmente o aparato logístico "conta com 3.144 câmeras em 1.497 pontos de todo o Estado de São Paulo. Desse total, 2.215 câmeras se encontram em 469 locais da cidade de São Paulo, em parceria com a prefeitura da capital e com a utilização de equipamentos da Companhia de Engenharia de Tráfego (CET)[48].

Conforme os índices criminais fornecidos pelo Governo de São Paulo, observa-se um resultado positivo e considerável em matéria de segurança pública durante o período de funcionamento do *Detecta*. O balanço dos resultados indica que, "no período de 2014 a 19 de abril de 2017, as imagens captadas contribuíram para a prisão de 4.731 pessoas em flagrante delito; interceptação de 3.320 veículos, apreensão de 276 armas de fogo e leitura de 20 bilhões de placas de automóveis. Na capital, durante o mesmo período, 2.942 pessoas foram detidas, 2.172 veículos interceptados e apreendidas 162 armas de fogo"[49].

Na prática, a função do sistema era identificar um suspeito através das câmeras espalhadas na área de atuação. Por exemplo, quando foge em um carro vermelho em que só se sabe parte do número da placa, o sistema poderá localizar todos os veículos com aquele número parcial, da mesma cor, e apresentar essas localizações em um mapa.

O sistema *Detecta* foi desenvolvido justamente para esse cruzamento ágil de informações, podendo por exemplo, fazer buscas de um determinado nome e localizar em um mapa todas as ocorrências relacionadas a ele, seja na Polícia Militar, na Civil ou no Detran. Enviar um alerta sempre que for registrado um crime com as mesmas características de outro que já está sendo investigado, mesmo que seja em regiões ou cidades diferentes.

---

[48] **Detecta monitora o Estado de SP com mais de três mil câmeras de vídeo.** Disponível em: <https://www.saopaulo.sp.gov.br/spnoticias/detecta-monitora-oestado-de-sao-paulo-com-3-mil-cameras-de-video/>. Acesso em 16/05/2022.

[49] **Detecta monitora o Estado de SP com mais de três mil câmeras de vídeo.** Disponível em: <https://www.saopaulo.sp.gov.br/spnoticias/detecta-monitora-oestado-de-sao-paulo-com-3-mil-cameras-de-video/>. Acesso em 16/05/2022.

É interessante notar que a maior parte dessas tecnologias usa como base crimes patrimoniais e/ou ligados ao tráfico de entorpecentes, coincidentemente ou não os tipos penais mais presentes nas bases de dados criminais e estatisticamente falando imputados a um grupo especifico marginalizado. Outras tipologias, como crimes tributários, estupro, tortura, sequestro, crime de ódio, violência doméstica não são abrangidos nesta contabilização.

Isso evidencia com clareza o nível radical da seletividade operada dentro do sistema penal[50]: na maioria dos crimes praticados contra o patrimônio público (crimes tributários e previdenciários, p. ex.), é tradição o ordenamento jurídico ser extremamente generoso, criando inúmeros mecanismos de extinção da punibilidade em razão da reparação do dano. Não por outra razão os crimes contra o patrimônio público sequer constam nas estatísticas carcerárias nacionais. A título de exemplo, segue o artigo 6º da lei 12.382/11, alterando o artigo 83, §4º da Lei nº 9.430/96, senão vejamos:

> "extingue-se a punibilidade dos crimes referidos no caput quando a pessoa física ou a pessoa jurídica relacionada com o agente efetuar o pagamento integral dos débitos oriundos de tributos, inclusive acessórios, que tiverem sido objeto de concessão de parcelamento."

Nesse contexto, Joh (2014) apontou que esses sistemas de inteligência artificial não estão preparados para alguns tipos de ocorrência, pois muitos deles não obedecem a padrões territoriais. A natureza dos dados, então, é essencial. Ao ensinar ao software o que é crime, recorre-se a uma gama duplamente restrita de dados: primeiro, ao ser um banco de dados de justiça criminal, filtra-se pelo sistema de registro oficial (há aqui um viés do que foi notificado enquanto tal, não correspondendo a uma amostra representativa nem universal dos delitos[51], que consolida vieses historicamente construídos na atividade policial.

---

[50] CARVALHO, Saulo. **O encarceramento seletivo da juventude negra brasileira**. 624 Rev. Fac. Direito UFMG, Belo Horizonte, n. 67, pp. 637, jul./dez. 2015. Disponível em: <www.direito.ufmg.br/revista/index.php/revista/article/download/1721/1636>. Acesso em 13/05/2022.

[51] RATTON JR, 1996; ADORNO, 1993

Hoje, o projeto perdeu suas aplicações práticas e viabilidade operacional, se resumindo à detecção de veículos em situações irregulares.

1.6.2. Projeto Córtex

O Córtex é uma tecnologia de inteligência artificial que utiliza a leitura de placas de veículos por milhares de câmeras viárias espalhadas, para, por exemplo, localizar veículos roubados e criminosos foragidos ou em fuga.

É um projeto lançado, também, de forma experimental desde o ano de 2018, pela Secretaria de Operações Integradas (Seop), o qual compartilha o sistema com outras instituições policiais.

Estima-se que o sistema utilize pelo menos 26 mil câmeras de monitoramento espalhadas nas vias públicas do país, localizadas em prédios e radares de velocidade.

No que tange ao seu *big data*, a ele são inseridos além de dados das Rais (Relação Anual de Informações Sociais do Ministério da Economia), os dados de Cadastro de Pessoas Físicas (CPF) da Receita Federal, com informações pessoais de todos os brasileiros registrados[52].

O banco de dados do sistema é alimentado por informações fornecidas por instituições policiais, que através de convênio, firma compromisso de compartilhar e alimentar o sistema, utilizando-se do acesso ao mesmo em colaboração operacional. Policiais civis e militares, desde que autorizados, têm acesso ao sistema, além de alguns integrantes das Guardas Municipais.

Cabe mencionar que, de acordo com a matéria do UOL[53], esse programa envia alertas de ocorrências e tem sido alimentado com dados sensíveis e informações sigilosas de cidadãos e empresas. Também pode possuir dados cadastrais e trabalhistas, como cargo, empregos e salários,

---

[52] **Sistema de inteligência do governo monitora 360 mil pessoas, diz revista**. Portal Uol. Disponível em <https://noticias.uol.com.br/politica/ultimas-noticias/2022/01/21/cortex-programa governo-vigiar-cidadaos-crusoe.htm>. Acesso em 16/05/2022.
[53] Ibid.

além da informação pessoais dos próprios funcionários como RG, CPF, endereço e dependentes.

Valendo-se de banco de dados federais e através de convênios com as polícias e outras entidades estaduais de justiça criminal, o programa pode ter acesso a bancos de dados públicos como boletins de ocorrência, passagens pela polícia, do Departamento Nacional de Trânsito (Denatran), do Sistema Nacional de Informações de Segurança Pública (Sinesp), Departamento Penitenciário (Depen), Cadastro Nacional de Pessoas Físicas (CPF) e Cadastro Nacional de Pessoas Jurídicas (CNPJ). Informações do sistema criminal como Cadastro Nacional de Foragidos e Banco Nacional de Mandados de Prisão. Tudo isso integrado em uma mesma plataforma, qual seja, o sistema Córtex.

Deve-se atentar ao risco do programa Córtex ser usado para "fins escusos", inclusive políticos[54]. Em tese, é uma ferramenta poderosa de combate ao crime. Na prática, o sistema pode ser usado para monitoramento e vigilância de cidadãos, organizações da sociedade civil, movimentos sociais, lideranças políticas e manifestantes, em uma escala sem precedentes.

Ademais, o delegado responsável pelo andamento do sistema experimental era Alfredo Carrijo, secretário da Seopi (Secretaria de Operações Integradas), o qual declara publicamente pertencer ao círculo íntimo da família Bolsonaro e, inclusive, trabalhou na segurança pessoal do presidente nas eleições de 2018 e a posse[55].

Nesse sentido, o diretor executivo da Transparência Brasil, Manoel Galdino[56], disse à Revista o que se segue: "Não há controle nenhum de quem acessa e os motivos pelos quais irá acessar. Isso é o mais grave. Com a

---

[54] **Sistema de inteligência do governo monitora 360 mil pessoas, diz revista**. Portal Uol. Disponível em <https://noticias.uol.com.br/politica/ultimas-noticias/2022/01/21/cortex-programa governo-vigiar-cidadaos-crusoe.htm>. Acesso em 16/05/2022.

[55] REBELLO, Aiuri. **Da placa de carro ao CPF**. Portal The Intercept Brasil. Disponível em: <https://theintercept.com/2020/09/21/governo-vigilancia-cortex/>. Acesso em: 19/05/2022.

[56] Ele é responsável por um projeto destinado a monitorar o uso de algoritmos e de ferramentas de inteligência artificial pelo governo.

quantidade de dados ofertados, poderá abrir brecha para perseguição de opositores e uso para fins pessoais. O próprio crime organizado pode ter acesso à ferramenta. Basta que haja um policial corrupto com acesso. A falta de um sistema para prevenir isso nos deixa bastante expostos".

Estudiosos especializados no campo digital e conhecedores das entrelinhas da Lei da Proteção Geral de Dados destacam que por se tratar de uma ferramenta de uso das polícias, o programa deveria ser submetido ao controle do Ministério Público, bem como por ser de inteligência, deveria de ser fiscalizada pela CCAI (Comissão de Controle da Atividade de Inteligência) do Congresso Nacional. No entanto, não há qualquer informação de que haja fiscalização nessas frentes.

O Sistema Córtex, por muito tempo, funcionou sem regulamentação. Apenas em 30 de setembro de 2021, o Ministro da Justiça Anderson Torres assinou a portaria nº 218/2021 que estabelece as regras de utilização[57]do sistema. No capítulo das definições, no artigo 4º, incisos VIII e IX da referida Portaria[58], o texto é genérico, não explica o que pode ser considerado um "alvo móvel", o que abre caminho para o uso indevido.

[57] BRASIL. Ministério da Justiça e Segurança Pública. **Portaria nº 218, de 29/09/2021**. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/operacoes-integradas/cortex/publicacoes/portaria-no-218-de-29-de-setembro-de-2021>. Acesso em: 16/05/2022.

[58] "Art. 4º Para os efeitos do disposto nesta Portaria, consideram-se: VIII - atuação policial com monitoramento de alvos móveis: atividade desempenhada pelo profissional de segurança pública que exige o monitoramento de alvos móveis em regime temporal definido, com vista à consecução da atribuição legal de seu órgão; IX - atuação policial com busca de informações de alvos móveis: atividade desempenhada pelo profissional de segurança pública que exige a busca de informações de alvos móveis durante a execução de suas funções, com vista à consecução da atribuição legal de seu órgão."

2. O Lado Obscuro dos Algoritmos

2.1. As Entrelinhas dos Algoritmos

No livro Algoritmos de Destruição em Massa, a autora Cathy O'Neil destaca que os algoritmos são construídos para modelar uma realidade e, a partir dos dados fornecidos, responder com o resultado que seus criadores assim desejarem, de modo a solucionar o problema posto. Entretanto, a autora pontua que, "apesar de terem uma reputação de imparcialidade", esses modelos, e, por consequência, os algoritmos, "refletem objetivos e ideologias".

Ainda, segundo ela, isso é em razão dos "valores e desejos" de seus criadores influenciarem suas escolhas, desde os dados que são coletados, passando pelas perguntas que vão direcionar o tratamento e análise destes, chegando até a própria definição do que pode ser considerado como sucesso do modelo.[59] Assim, "modelos são opiniões envelopadas em matemática".[60]

Dessa maneira, o mau uso dessas ferramentas pode vir a violar, como será visto no capítulo III, direitos fundamentais das pessoas[61], bem como contribuir com a precarização e mecanização do próprio Direito. Afinal, trata-se de um ramo do conhecimento intrinsicamente subjetivo e influenciado por ciências como Sociologia. Isto implica que não é uma tarefa trivial parametrizar e quantificar objetivamente, em termos matemáticos, conceitos jurídicos naturalmente definidos por intermédio da interpretação.[62]

As empresas e os especialistas têm optado por introduzir a IA aos poucos, começando pelas atividades que parecem, incialmente, mais objetivas e simples de serem automatizadas e analisadas por meio de algoritmos de IA.

---

[59] O'NEIL, 2016, cap. 1.
[60] Ibid.
[61] O'NEIL, 2016; EPIC, 2017
[62] STRECK, 2019a; idem, 2019b; idem 2019c

2.2. O Problema da Atribuição de Função Decisória à Robôs

É sabido que, há algum tempo, a questão dos vieses já tem estado presente nos grandes debates do Direito, principalmente, em relação às decisões judiciais.

Os vieses cognitivos são características inerentes ao ser humano, vez que o nosso cérebro possui recursos cognitivos limitados e por isso cria "atalhos" para a tomada de decisões. Todavia, a partir do momento que afetam juízes, tais vieses são extremamente danosos, pois interferem diretamente nos julgamentos, ao considerar fatores externos ao caso.

No processo de tomada de decisão o impacto do viés de confirmação (*confirmation bias*) é relevante, visto que o julgador tenderá a favorecer evidências que confirmem sua hipótese, descartando as que apontem para solução distinta.

A solução não avança, pois o problema é mascarado pelos próprios julgadores, os quais em sua maioria ainda se consideram imparciais e não desenvolvem técnicas capazes de superar o enviesamento – as técnicas de "desenviesamento" ou debiasing. O mesmo fenômeno pode ser verificado nas ferramentas de IA que, conforme previamente exposto, são consideradas por muitos como isentas.

O cerne da questão é que apesar do exposto acima, as decisões tomadas por humano são impugnáveis. É possível delimitar os fatores que ensejaram determinada resposta e o próprio decisor deve ofertar o iter que o induziu a tal resposta (arts. 93, IX, CF/1988 e 489 do CPC). Por outro lado, os algoritmos utilizados nas ferramentas de inteligência artificial são obscuros para a maior parte da população – algumas vezes até para seus programadores – o que os torna, de certa forma, inatacáveis. Em função disso, a atribuição de função decisória aos sistemas de inteligência artificial torna-se especialmente problemática no âmbito do Direito.

Não se nega as vantagens da utilização das máquinas para alguns atos da prática jurídica. Conforme demonstrado no subcapitulo sobre as "experiências da IA no Direito Brasileiro" a implementação de sistemas de IA para realização de pesquisas, classificação e organização de informações, vinculação de casos a precedentes, bem como elaboração de contratos tem se mostrado efetiva na prática por proporcionar maior celeridade e precisão.

Todavia, atribuir-lhes a função de tomar decisões, equivalente a um juiz, pode significar a ampliação ainda maior de desigualdades que permeiam nosso sistema Judiciário, respaldando-o, ademais, com um decisionismo tecnológico e "lógico".

Portanto, sob o prisma da sentença de mérito, Fenoll suscita quatro aspectos relevantes que não podem ser esquecidos quando se cogita da aplicação de uma inteligência artificial para julgamento: 1) a motivação da valoração probatória; 2) o procedimento probatório, notadamente a fase de admissão da prova aos autos; 3) a incidência dos standards — ou padrões — de prova[63]; e, por derradeiro, 4) a análise acerca da presunção de inocência[64].

Resta claro que, o perigo da IA está na simplificação de conceitos, uma vez que a máquina não é capaz de compreender o significado.[65] E, ao que parece, a fundamentação da decisão judicial continuará atuando como mecanismo de controle revisional de uma decisão de mérito proferida, no bojo do processo penal, por uma inteligência artificial, para fins de preservação da própria segurança jurídica.[66]

---

[63] Sobre o tema, cf. KNIJNIK, Danilo. **Os standards do convencimento judicial: paradigmas para o seu possível controle**. Revista Forense, Rio de Janeiro, n. 353, jan.-fev. 2001. p. 27. Não em sentido diferente, MORALES, Rodrigo Rivera. ***La Prueba: un análisis racional y práctico***. Madrid: Marcial Pons, 2011. p. 305. Um ser humano não pode pensar em probabilidades no exercício da atividade de julgar, mas uma inteligência artificial pode quantificar, por exemplo, 90% de certeza.

[64] FENOLL, Jordi Nieva. ***Inteligencia Artificial y Proceso Judicial***. Marcial Pons: Madrid, 2018. pp. 101-115.

[65] BOEING, Daniel Henrique Arruda; ROSA, Alexandre Morais da. **Ensinando um Robô a Julgar: pragmática, discricionariedade, heurísticas e vieses no uso de aprendizado de máquina no Judiciário.** Florianópolis: Emais Academia, 2020. Pp. 84-85.

[66] GALVÃO, Danyelle da Silva; PEIXOTO JUNIOR, Hélio; LOBO, Ricardo. **O artigo 489 do Novo Código de Processo Civil (Lei 13.105/2015) e suas implicações no Direito Processual Penal**. In: Revista dos Tribunais, v. 105, n. 971, set./2016, pp. 283-312. P. 284.

2.3. O Perigo da Parcialidade Programada das Máquinas

Os programadores, ao criarem um produto, devem selecionar as informações que serão fornecidas ao sistema de IA e que serão utilizadas para prever soluções e/ou resultados futuros. Portanto, elaboram, de modo que, sempre haja pontos cegos nos algoritmos, os quais refletem os objetivos, prioridades e concepções de seu criador. “Os modelos são, a todo tempo, permeados pela subjetividade do sujeito que os desenvolve”.

No desenvolvimento tecnológico podem ser ignoradas informações determinantes para correta análise da situação, influenciando negativamente nas respostas dadas pelo sistema. Como alerta Cathy O’Neil:

> “Algumas vezes esses pontos cegos não importam. Quando perguntamos ao Google Maps por direções, ele modela o mundo como uma série de estradas, túneis e pontes. Ele ignora os prédios, porque não são relevantes para sua tarefa. [...] outros (pontos cegos) são muito mais problemáticos.
> O modelo aplicado nas escolas de Washington, retornando para aquele exemplo, avalia os professores em grande parte com base nas notas de estudantes nos testes, mas ignora o quanto os professores engajam os estudantes, trabalham com habilidades específicas, lidam com a gestão da sala de aula ou ajudam seus alunos com problemas pessoais e familiares. O modelo é muito simples, sacrificando sua exatidão e diferentes percepções em prol da eficiência. No entanto, do ponto de vista dos administradores ele fornece uma ferramenta efetiva para investigar centenas de professores aparentemente com um baixo desempenho, mesmo que se corra o risco de interpretar incorretamente alguns deles”.

Concluída a elaboração do modelo, são fornecidos dados para o sistema, de maneira a possibilitar o *machine learning* (aprendizado de máquina), mediante o qual a máquina analisará as informações fornecidas, seguindo instruções estabelecidas pelo algoritmo, para encontrar padrões e, então, conseguir prever resultados.

A qualidade dos dados fornecidos aos sistemas de inteligência artificial também impactará os resultados, uma vez que os dados são coletados da sociedade que é permeada por desigualdades, exclusões e discriminações. Conforme estudo realizado por pesquisadores da Universidade de Oxford:

> “[...] o aprendizado de máquina pode confirmar **padrões discriminatórios** – se eles forem encontrados no banco de dados, então, por conseguinte, um sistema de

> classificação exato irá reproduzi-los. Deste modo, decisões enviesadas são apresentadas como resultado de um "algoritmo objetivo"[67].

Com isso, nota-se que as escolhas feitas na própria constituição dos sistemas de IA, refletem também as opiniões e prioridades dos criadores, influenciando diretamente as respostas do sistema.

Não se pode ignorar, assim, a impossibilidade de isenção completa, até mesmo ao se falar de inteligência artificial e de sistemas que, muitas vezes, são tratados como universais e "desenviesados", porquanto o ponto de partida é sempre uma atividade humana de seleção de informações e dados, fortemente relacionados com o contexto social de quem os produziu.

A partir dos vieses se apresentarem como característica intrínseca do pensar humano, pode-se concluir, de igual modo, que um algoritmo criado por seres humanos enviesados provavelmente padecerá do mesmo "mal", não de forma proposital, mas em decorrência das informações fornecidas ao sistema. Dessa maneira, surgem os chamados *vieses algorítmicos*, que ocorrem quando as máquinas se comportam de modos que refletem os valores humanos implícitos envolvidos na programação, é o caso da conta no twitter @tayandYou.

O fato dos algoritmos serem constituídos por informações selecionadas, por si só, não se constitui em um problema. Contudo, trata-se de um dado normalmente ignorado e que, quando aliado à falta de transparência dos algoritmos, bem como a sua possibilidade de crescimento exponencial, pode constituir um mecanismo perigoso de segregação ou erro, amparado pela pretensa imparcialidade da matemática.

Veja, a seletividade racial é uma constância na historiografia dos sistemas punitivos e, em alguns casos, pode ser ofuscada pela incidência de variáveis autônomas. No entanto, no Brasil, a população jovem negra,

---

[67] Tradução livre. No original, "*machine learning can reify existing patterns of discrimination - if they are found in the training dataset, then by design an accurate classifier will reproduce them. In this way, biased decisions are presented as the outcome of an 'objective' algorithm*". Conforme: GOODMAN, B.; FLAXMAN, S. R. ***European Union regulations on algorithmic decision-making and a "right to explanation"***. In: AI Magazine, 38(3), pp. 50-57.

notadamente vive na periferia dos grandes centros urbanos e tem sido alvo do encarceramento massivo, o que parece indicar que o racismo se infiltra como uma espécie de metarregra interpretativa da seletividade, situação que permite afirmar o racismo estrutural, não meramente conjuntural, do sistema punitivo. Esse quadro pode se agravar diante da legitimidade dada a um robô que em tese estaria isento de falhas e erros, quando na verdade reproduz padrões discriminatórios.

Outro caso bastante ilustrativo dessa dinâmica se deu no trabalho de campo descrito por Perón, Simões- Gomes e Nery (2019): a Universidade de São Paulo. O campus Butantã foi um perímetro integrado ao projeto experimental Detecta (citado no subcapítulo 1.6.1 do presente trabalho) no início de 2018, o qual permite o controle eletrônico do espaço a partir de um centro de monitoramento, integrado a câmeras e aplicativos.

No aplicativo, com interface para a comunidade universitária, há um 'botão de pânico' que pode ser acionado em caso de incidentes ou ocorrências. O alerta gerado é transmitido no centro de monitoramento, e a sua geolocalização ativa as câmeras dos arredores. Todavia, essa estrutura é mobilizada muito raramente. A rotina dos operadores do sistema se restringe ao monitoramento e observação das imagens gravadas e retransmitidas, que usam da sua experiência no ramo para diferenciar situações suspeitas. Situações essas que consistiam em jovens — negros — que não condiziam com o estereótipo do estudante universitário.

Os habitantes e circulantes habituais desses perímetros securitizados ganham proeminência nesse equipamento enquanto prosumidores[68] do sistema de vigilância. À medida que produzem dados, eles consomem as informações extraídas do agregado desses conteúdos.

[68] "Prosumidor" é um aportuguesamento do termo prosumer, que consiste na fusão das capacidades de consumidor e produtor (consumer + producer) em uma mesma pessoa. Essa noção deriva da criação e expansão de plataformas online que permitem e encorajam seus usuários a contribuir e compartilhar conteúdo com outros em tempo real, chamando a atenção para as modificações nas formas de interação entre usuários por meio de tecnologias digitais. (LUPTON, 2015, p. 10).

A possibilidade de sinalização de ocorrências e situações suspeitas ao poder público por meio dessas plataformas — como, no app SP+Segura, de cometimentos de delitos e infrações — alçam a percepção ordinária e destreinada ao status de dado registrado, que contribui para, de um lado, a desproporção numérica de dados contra suspeitos racializados, e de outro, a legitimação da figura do suspeito racializado e do indesejável.

A relação de prosumidor do sistema insere os usuários em um exercício ativo de vigilância e endereça o sentimento de insegurança e medo, apaziguando-o por meio de sua incorporação à atividade cotidiana. Assim, há o feedback constante para a geração contínua de dados — os quais podem ser úteis no desenvolvimento da interface preditiva do software.

O peso e relevância desses dados passados, a serem usados em um processo de *machine learning*, tem o potencial de estabelecer um curso de ação — ou a predição de um evento — em detrimento de outro.

Segundo os argumentos de Esposito "[data] only become significant when processed and presented in a context, producing information. Information requires data, but data are not enough to have information" (2017a, p. 4)[69]. A produção da informação está vinculada à sua projeção de futuro e intervenção no presente, a partir das imagens dele derivadas. A ressignificação, então, contribui para uma espécie de manufatura do futuro, já que o algoritmo visualiza o futuro existente pela intervenção algorítmica.

A busca por padrões e intervenção na vida social com base em projeções feitas a partir de dados passados pode gerar uma espécie de exponencialidade das tendências identificadas — o que se denomina *overfitting* na computação e que basicamente deriva da uma cegueira dos algoritmos para outras possibilidades além daquelas identificadas nos eventos passados.

[69] ESPOSITO, E. ***Algorithmic memory and the right to be forgotten on the web***. In: Big Data & Society, v. 4, n. 1, pp. 01-11.

2.4. Lei Geral da Proteção de Dados Pessoais e o Tratamento Excepcional ao Direito Penal

A Lei Geral de Proteção de Dados disciplina o direito do titular dos dados pessoais à proteção desses dados. Essa proteção também diz respeito ao tratamento automatizado dos referidos dados.

Não poderia, um estatuto dirigido à proteção da pessoa humana, ignorar o tratamento de dados pessoais com base em decisão realizada por meios automatizados, cada vez mais frequentes.

Como muito bem disciplina, o objetivo principal é tratar de toda e qualquer atividade que envolva o uso e o compartilhamento de dados pessoais. Senão vejamos, conforme artigo 1º da lei:

> "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".

Buscando-se tutelar os direitos fundamentais de liberdade e privacidade, a LGPD dispõe sobre a possibilidade de responsabilização dos agentes que violarem qualquer norma prevista em lei, os quais estão sujeitos a sanções administrativas aplicáveis pela autoridade nacional.

Diferentemente do que ocorreu em relação a outros termos técnicos, a LGPD foi omissa quanto ao conceito de decisão automatizada. O PLS nº 4.496/2019,[70] de autoria do senador Styvenson Valentim (Podemos/ RN), visa à inclusão no texto da LGPD da definição da expressão "decisão automatizada", nestes termos:

> "[...] é processo de escolha, de classificação, de aprovação ou rejeição, de atribuição de nota, medida, pontuação ou escore, de cálculo de risco ou de probabilidade, ou outro semelhante, realizado pelo tratamento de dados pessoais utilizando regras, cálculos, instruções, algoritmos, análises estatísticas, inteligência artificial, aprendizado de máquina, ou outra técnica computacional."

[70] BRASIL. Senado Federal. **Projeto de Lei nº 4.496/2019, de autoria do Senador Styvenson Valentim.** Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/138136>. Acesso em: 16/05/2022.

Tal definição não se limita aos casos e decisão por sistema de IA. Revela, na verdade, a amplitude da expressão.

A LGPD não discrimina em quais hipóteses o processamento totalmente automatizado pode ocorrer. Limitou-se a disciplinar, apenas, o direito à explicação quando a decisão automatizada é tomada sem qualquer interferência humana. Com isso, o tratamento de dados automatizados submete-se às regras gerais de utilização e tratamento de dados, especialmente aquelas previstas nos artigos. 7º e 11.

A previsão acerca do direito à explicação não é inédita em território nacional, pois a lei nº. 12.414/2011 (Lei do Cadastro Positivo) inclui, entre os direitos do cadastrado o de solicitar ao consulente a revisão de decisão realizadas exclusivamente por meios automatizados (art. 5º, VI). Todavia, a sua inserção no microssistema de proteção de dados pessoais ampliou o campo de aplicabilidade.

O direito à explicação, nos moldes do art. 20, é uma consequência do princípio da transparência, previsto no art. 6º, VI da LGPD. O *caput* do art. 20 confere ao titular dos dados o direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, desde que afetem seus interesses. Estão incluídas as decisões destinadas a definir o perfil pessoal, profissional, de consumo e de crédito ou os aspectos da personalidade do titular, bem como em alguns países o perfil dito “criminal”.

Conforme uma linha hermenêutica, a alteração do texto legal, retirando a pessoa natural como único titular dos dados a ter direito de solicitar revisão, suprimiu a possibilidade de revisão. Como consequência, a decisão automatizada seria revisada mediante outra decisão automatizada[71].

[71] MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. **Inteligência artificial e a lei de proteção de dados pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de *machine learning***. In: FRAZÃO, Ana. MOULHOLLAND, Caitlin (Coord.). **Inteligência artificial e direito: ética, regulação e responsabilidade**. São Paulo: Thomson Reuters (Revista dos Tribunais), 2019, pp. 265-290

Por outro lado, há a interpretação de que essa alteração significaria somente que as condições da revisão não se encontram detalhadas na LGPD, mas não há uma vedação a que ela seja realizada por pessoa natural. A lógica é de que haveria uma permissão – não a obrigatoriedade- para um pedido de revisão de decisão automatizada ser processado por outro sistema, também, automatizado, não um ser humano.

Necessário pontuar que, nesse caso a revisão por pessoa natural seria mais apta a corrigir eventuais discriminações decorrentes de processos algorítmicos e dar concretude aos princípios da transparência e da responsabilidade no tratamento de dados pessoais.

Nesse sentido, Carlos María Romeo-Casabona e Guillermo Lazcoz Moratinos em texto intitulado Inteligencia Artificial aplicada a la salud: ¿Qué marco jurídico?, em que os autores analisam o direito espanhol e o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27.4.2016 (GDPR):

> "Em conclusão, qualquer decisão amparada pelas informações fornecidas por um sistema baseado no processamento automatizado de algoritmos deve ser tomada e/ou supervisionada por um ser humano qualificado, para que ele possa avaliar sua decisão à luz da situação específica apresentada pela parte interessada (por exemplo, não limitar-se à exclusão de um paciente de um novo tratamento, pois de acordo com seu perfil não será benéfico para ele, mas reconsiderar a decisão proposta e garantir a conveniência de optar por outro tratamento alternativo talvez menos eficaz, mas com o potencial de proporcionar algum benefício para tratar a doença)."[72]

Os parâmetros legais para o exercício do direito à explicação podem não ser suficientes para assegurar a autonomia informativa do titular dos dados pessoais e para concretizar a principiologia sistematizada no art. 6º, em especial, os princípios do livre acesso (inc. IV) da transparência (inc. VI) e da não discriminação (inc. IX). Nesse ponto, a lei brasileira não reproduz o marco regulatório europeu que a inspirou.

---

[72] ROMEO-CASABONA, Carlos María; LAZCOZ MORATINOS, Guillermo. **Inteligência artificial aplicada à saúde: que marco legal?** P. 78. Disponível em: <https://www.fundacionmercksalud.com/wp-content/uploads/2020/03/1.3.-IA-APLICADA-A-LA-SALUD.-Carlos-M.-Romeo-Guillermo-azcoz.pdf>. Acesso em: 02/06/2022. Tradução livre.

Para conferir efetividade ao direito à explicação, é prevista a atuação da Autoridade Nacional, que passou a ser disciplinada pela LGPD, nos arts. 55-A a 55-L, por força da Lei nº 13.853/2019.

Seguindo a linha do §2º do artigo 20, se o titular ao exercer o direito à explicação, se deparar com a recusa do controlador em fornecer as informações solicitadas, sob o fundamento de segredo comercial e industrial, a Autoridade Nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

As professoras Caitlin Mulholland e Isabella Frajhof, sobre o art. 20 da LGDP, advertem:

> "Merecem ser feitas duas notas importantes sobre este artigo. A primeira refere-se ao fato de que a lei autoriza o pedido de revisão, mas não significa que, após a análise do controlador, o resultado final necessariamente será alterado. A segunda reconhece, à primeira vista a discricionariedade da autoridade nacional para realizar a auditoria apenas quando o controlador se negar a fornecer as informações elencadas no parágrafo primeiro."[73]

Com isso, verifica-se ser puramente discricionária a decisão da Autoridade Nacional de realizar ou não a auditoria. Sabedor de que a auditoria poderá não acontecer, o controlador pode preferir assumir o risco e não prestar as informações, alegando sempre segredo comercial ou industrial.

No que tange a responsabilização, as normas sobre ressarcimento de danos encontram-se na sessão III do capítulo IV da lei e adota a responsabilidade civil (objetiva e solidária) dos agentes de tratamento (controlador e operador), sem descurar da função compensatória:

> "O sistema de responsabilização civil da Lei Geral de Proteção de Dados Pessoais, previsto nos artigos 42 a 45 da Lei n. 13853/2018, mostra-se especialíssimo, configurando-se como a principal novidade da lei, e reflete a determinação do disposto no inciso X do art. 6º da Lei, que prevê o princípio da "responsabilização e prestação de contas, isto é, a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas". Como se vê, o legislador pretendeu aqui não apenas determinar o ressarcimento dos danos

[73] MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. **Inteligência artificial e a lei de proteção de dados pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de *machine learning***. In: FRAZÃO, Ana. MOULHOLLAND, Caitlin (Coord.). **Inteligência artificial e direito: ética, regulação e responsabilidade**. São Paulo: Thomson Reuters (Revista dos Tribunais), 2019. P. 272.

> eventualmente causados, mas também e, principalmente, buscou prevenir e evitar a ocorrência desses danos[74]"

Ocorre que, no ponto de vista criminal, a lei optou por nada dispor sobre o tema. De forma deliberada, o artigo 4º impede, expressamente, o tratamento de dados pessoais nos casos de: (a) segurança pública, (b) defesa pessoal, (c) segurança do Estado e/ou atividades de investigação e repressão de infrações penais[75].

Seguindo o Regulamento Geral de Proteção de Dados Europeus (GDPR)[76], o Brasil também adotou uma legislação geral com ampla aplicação nos mais diversos setores sociais e exclui de seu escopo de atuação o uso de inteligência artificial e de tratamento de dados pessoais para fins de persecução penal.

Enquanto no Brasil houve um vácuo regulatório a este respeito, na União Europeia o surgimento da Diretiva 2016/680 – tratamento dos dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais- ocorreu simultaneamente à criação do GDPR.

Na era das hipertecnologias, é imprescindível perquirir se o emprego da IA promove o direito à proteção de dados ou se, ao revés, serve a práticas discriminatórias, atingindo os direitos da pessoa ou dos grupos sociais que ela integra e representa.

Não obstante a LGPD não regular o uso da Inteligência Artificial para fins de persecução penal, apresenta níveis de garantias que devem ser

---

[74] MORAES, Maria Celina Bodin de. **LGPD: um novo regime de responsabilização civil dito "proativo"**. Civilistica.com, Rio de Janeiro, ano 8, n. 3, 2019. P. 02. Disponível em: <http://civilistica.com/lgpd-umnovo-regime/>. Acesso em: 28/01/2022.

[75] "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;"

[76] ***Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)***. Disponível em <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434>. Acesso em 16/05/2022.

seguidos por uma futura lei mais específica que vise a segurança dos dados pessoais dos indivíduos.

A existência dessa lei mais específica é necessária do ponto de vista da segurança jurídica, uma vez que é preciso viabilizar o tratamento de dados pelas autoridades de segurança pública com uma maior eficiência ao passo que possa também ser compatível com a garantia dos direitos fundamentais dos titulares de dados. Assim, visto que o uso de tecnologia de vigilância no contexto de investigações no processo penal é uma realidade que tende a se expandir cada vez mais, em novembro de 2019 uma Comissão de Juristas especializados na elaboração de um anteprojeto de lei, apresentou ao presidente da Câmara dos Deputados, um anteprojeto de lei sobre o tema em questão.

O anteprojeto tenta, ao mesmo tempo, equilibrar a necessidade de tornar mais eficiente as investigações penais através do uso de ferramentas tecnológicas, com a proteção dos indivíduos contra o abuso das autoridades públicas. Para isso, esse dispositivo estabelece um conjunto de princípios que se aplicam ao uso de inteligência artificial e ao tratamento de dados para fins de persecução penal. Dentre esses princípios, alguns são semelhantes aos elencados pela LGPD e outros como a licitude e a legalidade estrita são exclusivas desse dispositivo.

Diante do exposto, a inaplicabilidade da Lei Geral de Proteção de Dados (LGPD), que está em vigor desde o dia 18/09/2020, está condicionada ao tratamento em questão se destinar exclusivamente à segurança pública ou a outra(s) exceção(ões) prevista(s) na lei. Desse modo, a eventual demonstração de que os dados em questão também estão sendo tratados para finalidades outras, que extrapolam o escopo excepcionado pela LGPD, atrairia sua aplicação e, em caso de ilicitude, das sanções judiciais correspondentes. A presente opacidade do sistema, em particular quanto a suas finalidades, não permite afirmar o âmbito de aplicação da LGPD às operações dos mais variados sistemas de IA.

Em todo caso, tal inaplicabilidade seria apenas parcial: de acordo com o art. 4º, §1º, da LGPD, tratamentos de dados para fins de segurança pública ainda devem prever "medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular" previstos na LGPD. Soma-se a isso que essa inaplicabilidade parcial também não afasta outros instrumentos protetivos do sigilo dos dados dos cidadãos, como o Código do Processo Penal, o Marco Civil da Internet, a Lei 12.850/2013 e a Lei 9.296/96. Assim, o acesso pelos agentes de segurança deve estar balizado pelo devido processo legal e pelo respeito aos princípios e garantias constitucionais e infraconstitucionais existentes, assim como os direitos dos titulares de dados.

Por fim, é evidente a suma importância pela transparência dos dados.

3. Inteligência Artificial: Direito Penal em Face da Constituição Cidadã

3.1. Sem Transparência, Sem Garantias Constitucionais Penais: Devido Processo Legal, Ampla Defesa, Contraditório e Presunção de Inocência

Destaca-se a opinião de Cathy O'Neil em Algortimos de Destruição em massa, segundo a qual a ausência de transparência dos modelos torna seu funcionamento **invisível para todos**, salvo matemáticos e cientistas computacionais. Por isso, mesmo quando equivocados, o veredito dos algoritmos se torna imune a discordâncias e reclamações, perpetuando por vezes as desigualdades e contribuindo, inclusive, para o seu crescimento, por meio do feedback loop.

A EPIC – Eletronic Privacy Information Center[77]- publicou dados acerca do uso de algoritmos no Sistema de Justiça Criminal Norte Americana, no qual evidencia-se uma série de dúvidas, a partir da opacidade dos algoritmos usados, sendo esses programas não publicizados, além de não contarem em sua maioria com estudo prévio de validade, refletindo, com isso, na baixíssima taxa de credibilidade e confiabilidade das mencionadas ferramentas de IA no campo criminal.

> "Algoritmos de justiça criminal – às vezes chamados de métodos de 'avaliações de risco' ou 'baseados em evidências' – são ferramentas controversas que pretendem prever comportamentos futuros de réus e pessoas encarceradas. Essas técnicas proprietárias são usadas para fixar fiança, determinar sentenças e até mesmo contribuir para determinações sobre culpa ou inocência. No entanto, o funcionamento interno dessas ferramentas está em grande parte escondido da visão pública. Muitos algoritmos de 'avaliação de risco' levam em conta características pessoais como idade, sexo, geografia, histórico familiar e status de emprego. Como resultado, duas pessoas acusadas do mesmo crime podem receber fiança ou resultados de sentença severamente diferentes com base em insumos que estão além de seu controle – mas não têm como avaliar ou contestar os resultados. Como os algoritmos de justiça criminal têm sido mais utilizados nos níveis federal e estadual, eles também estão sob maior escrutínio. Muitos especialistas em justiça criminal denunciaram ferramentas de 'avaliação de risco' como opacas, não confiáveis e inconstitucionais. A Suprema Corte também está considerando se deve

[77] ***Algorithms in the Criminal Justice System***. Disponível em <https://epic.org/algorithmic-transparency/crim-justice/>. Acesso em 16/05/2022.

> tomar um caso sobre o uso de uma técnica secreta para prever uma possível reincidência" [78]

Um outro exemplo de sistema de IA que produz resultados eminentemente discriminatórios é o COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), mecanismo utilizado nos EUA para avaliar o risco de reincidência dos acusados no país. Os dados obtidos são utilizados, em alguns Estados, para a fixação da sentença do réu, sendo que, quanto maior o índice de reincidência, maior seria o tempo de reclusão do detento.

Quando o software ajudava os juízes nos tribunais dos Estados Unidos para formarem conclusões sobre o futuro dos réus a fim de condená-los, a análise era feita com base em informações de outras pessoas e supostamente prevendo a futura reincidência, o que é completamente contrário aos princípios da garantia do estado de inocência e o devido processo legal do direito penal, tirando a personalidade da condenação e da pena. Conforme o algoritmo se baseava no histórico de condenações anteriores ocorreu esse enviesamento. Sendo assim, os processos seriam considerados inquisitórios, pois o juiz não estaria sendo imparcial.

Em uma pesquisa realizada pela *ProPublica*[79], averiguou-se, no entanto, que o algoritmo utilizado tende a classificar erroneamente acusados negros como prováveis reincidentes e, por outro lado, enquadrar, também de forma equivocada, acusados brancos como indivíduos com baixo risco de reincidência. Senão vejamos:

> "Alguns dados sobre a utilização do COMPAS na Florida também trazem preocupação. Citam-se algumas conclusões de pesquisadores da ProPublica, que analisou 10.000 condenações em Broward County: (i) acusados negros frequentemente foram classificados com maior risco de reincidência do que efetivamente possuíam. Acusados negros que não reincidiram em um período de dois anos tinham o dobro de chance de serem erroneamente classificados como alto risco de reincidência, em relação aos acusados brancos (45% contra 23%); (ii) acusados brancos frequentemente foram classificados com menor risco do que

[78] ***Algorithms in the Criminal Justice System***. Disponível em <https://epic.org/algorithmic-transparency/crim-justice/>. Acesso em 16/05/2022.

[79] ***Machine Bias – There´s Software Used across the Country to Predict Future Criminals. And it´s Biased Against Black*.** Portal Propublica. Disponível em <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 16/05/2022.

> efetivamente possuíam. Acusados brancos que reincidiram em um intervalo de dois anos foram equivocadamente classificados como baixo risco reincidência em uma proporção quase duas vezes maior que os acusados negros (48% contra 28%); (iii) no tocante à reincidência especificamente para crimes violentos, acusados negros foram erroneamente classificados como alto risco em uma taxa duas vezes maior que acusados brancos."[80]

A empresa Northpointe, responsável pelo software, não disponibiliza ao público o algoritmo no qual se baseia o índice de reincidência do acusado, mas apenas as perguntas feitas ao indivíduo e utilizadas no cálculo, de modo que o réu não sabe por qual motivo possui um alto ou baixo indicador, tampouco de que forma suas respostas influenciam no resultado final.

Vale salientar que não se pergunta a raça do acusado no questionário, porém são realizadas perguntas que selecionam indivíduos pobres e, em sua maioria, negros, como prováveis reincidentes.

Não obstante a ferramenta de *risk assentment* ser considerada científica ou "imparcial" para alguns, a base de cálculo sobre a qual incidirá não o é, tendo em vista que a realidade da Justiça Criminal é a da seletividade. A pontuação que corresponde a cada item, determinada por dados empíricos, incorpora o viés seletivo do próprio sistema, eis que pontua negativamente, levando a pessoa a apresentar um *high risk*, o fato de pertencer a grupos sociais mais criminalizados, ou criminalizáveis, como negros, jovens e pobres.

Nesse ponto, verifica-se o risco da realização de analogias para a previsão de comportamentos quando faltam dados específicos sobre os resultados pretendidos. Não se pode precisar cientificamente quais características e indicadores fazem com que um indivíduo seja mais ou menos propenso à reincidência.

Assim, para que o algoritmo chegue a tal resultado, são utilizadas correlações entre dados, como a existência de parentes ou vizinhos condenados, o desempenho escolar, a convivência com usuários de drogas,

---

[80] TOVO, Antônio. **O Periculosômetro Digital**. Disponível em <https://www.ab2l.org.br/o-periculosometro-digital/>. Acesso em 16/05/2022.

entre outros, e a probabilidade de reincidência, o que carece de confirmação científica e acarreta resultados discriminatórios.

Ocorre que, esse método atenta frontalmente com os princípios do devido processo legal e da presunção de inocência, tendo em vista que já considera culpado pela colheita precoce e equivocada de circunstâncias pretéritas. Direciona de tal modo para a reincidência, uma das agravantes da pena, que o julgamento é por quem o indivíduo é e não pelo o que ele praticou.

A paridade de armas tecnológicas pressupõe a possibilidade efetiva de contraditório significativo sobre a qualidade, credibilidade e confiabilidade dos meios e trajetos empregados. Do contrário, não se trata de vantagem tecnológica, mas em verdade, de subtração das condições mínimas do dever de "informação" sobre o conteúdo da prova produzida, violadora do devido processo legal e da presunção de inocência.

Assim, viola-se tais princípios, uma vez que não são informados quais os critérios e parâmetros utilizados pelo algoritmo para enquadrar o sujeito como isso ou aquilo. Não é esclarecido quais variáveis são consideradas ou não, prejudicando, assim, eventual tese de correção ou mesmo, defensiva.

Ou seja, a partir da inobservância desses pilares do devido processo legal, há lacunas acerca da quebra da cadeia de custódia digital, o reconhecimento da ilicitude e/ou invalidade do material apresentado[81].

Os algoritmos, conforme demonstrado, vêm sendo produzidos, propositalmente, para não serem questionados e estabelecerem, com base em informações científicas e ocultas, verdades absolutas, o que é impensável no direito penal.

---

[81] PRADO, Geraldo. **Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital**. Disponível em: <https://www.conjur.com.br/dl/artigo-geraldo-prado.pdf>. Acesso em 20/05/2022. "violada a cadeia de custódia da prova digital incide imperiosa proibição de valoração da prova assim obtida. É o corpo de delito que se converte em algo juridicamente imprestável à luz do direito fundamental à integridade dos sistemas informáticos e o igualmente fundamental direito à confidencialidade, princípios constitucionais implícitos assim como o é o direito fundamental à autodeterminação informativa."

3.2. Ética nos Desenhos Autônomos da IA

Buscando promover a ética nos programas autônomos da Inteligência Artificial, o *Institute of eletrical and eletronics Engineer* (IEEE)[82] desenvolveram uma espécie de guia pontuando quais princípios devem nortear a aplicação das ferramentas, quais sejam:

> "- Princípio dos Direitos Humanos: Como garantir que os sistemas de IA não infrigem os direitos humanos? Ou seja, como deverão os sistemas computacionais ser desenhados de forma a respeitar a igualdade de direitos nos humanos? Por exemplo, quando os nossos sistemas são treinados com dados que, à partida, reflectem uma sociedade estratificada e desigual, não estaremos a perpetuar estas desigualdades reforçando ainda mais o que negativo existe?
> - Princípio da Responsabilidade: Como garantir que os sistemas de IA são "responsáveis"? Quando os sistemas são autónomos e executam acções de forma independente, sem o controlo humano, de quem é a responsabilidade da execução da acção? Como garantir a moralidade das acções executadas?
> - Princípio da Transparência: Como garantir que as decisões efectuadas pelas máquinas sejam transparentes para os humanos? Isto é, como garantir que seja possível descobrir a razão de uma dada acção, decisão ou escolha feita pelo sistema de IA? Quando as decisões são efectuadas por algoritmos complexos e baseados em dados, esta transparência pode não ser trivial. Por exemplo, um sistema autônomo pode decidir se uma pessoa deve ter crédito ou não com base no perfil da pessoa e nos dados. No entanto, não existe um conjunto de regras que dite a decisão. - Princípio da Educação e Consciência Pública: Como educar os cidadãos de forma a estarem cientes dos riscos da má utilização de sistemas IA?"[83]

Ademais, a Eletronic Privacy Information Center (EPIC) através da Public Voice publicou algumas recomendações que intitularam de uma *Universal Guideline for Artificial Intelligence:*

> "We propose these Universal Guidelines to inform and improve the design and use of AI. The Guidelines are intended to maximize the benefits of AI, to minimize the risk, and to ensure the protection of human rights. These Guidelines should be incorporated into ethical standards, adopted in national law and international agreements, and built into the design of systems. We state clearly that the primary responsibility for AI systems must reside with those institutions that fund, develop, and deploy these systems.
> 1. Right to Transparency. All individuals have the right to know the basis of an AI decision that concerns them. This includes access to the factors, the logic, and techniques that produced the outcome.
> 2. Right to Human Determination. All individuals have the right to a final determination made by a person.
> 3. Identification Obligation. The institution responsible for an AI system must be made known to the public.

---

[82] IEEE – Institute os Electrical and Electronics Engineer se apresenta como « the world´s largest technical professionalorganization dedicated to advancing technology for benefit of humanity ». Disponível em <https://www.ieee.org/>. Acesso em 22/05/2022.
[83] TRANCOSO, Isabel, PAIVA, Ana. 2018, Op. Cit. Pp. 172/173.

> 4. Fairness Obligation. Institutions must ensure that AI systems do not reflect unfair bias or make impermissible discriminatory decisions.
> 5. Assessment and Accountability Obligation. An AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks. Institutions must be responsible for decisions made by an AI system.
> 6. Accuracy, Reliability, and Validity Obligations. Institutions must ensure the accuracy, reliability, and validity of decisions.
> 7. Data Quality Obligation. Institutions must establish data provenance, and assure quality and relevance for the data input into algorithms.
> 8. Public Safety Obligation. Institutions must assess the public safety risks that arise from the deployment of AI systems that direct or control physical devices, and implement safety controls.
> 9. Cybersecurity Obligation. Institutions must secure AI systems against cybersecurity threats.
> 10. Prohibition on Secret Profiling. No institution shall establish or maintain a secret profiling system.
> 11. Prohibition on Unitary Scoring. No national government shall establish or maintain a general-purpose score on its citizens or residents.
> 12. Termination Obligation. An institution that has established an AI system has an affirmative obligation to terminate the system if human control of the system is no longer possible."[84]

No contexto criminal, de acordo com artigo da professora Victoria Amália Sulocki[85], é necessário que pelo menos cinco delas já se encontrem automaticamente, quais sejam: "a preocupação com processos e julgamentos justos e transparentes, a existência da autonomia e autodeterminação humana, a necessidade de estabelecer controles para maior precisão dos dados e da qualidade destes, a segurança e confiabilidade dos dados, e reduzir ao máximo seus objetos de aplicação, eis que julgar pessoas, por fatos, e não pela pessoa que é, foi ou será (impossível até mesmo na ficção) na seara criminal".

Indaga-se sobre a necessidade do desenvolvimento de operações matemáticas que dialoguem criticamente sobre os critérios aplicados e promovam o foco na ação de ser humano, enquadrando suas ferramentas no fundamento maior: o princípio da dignidade da pessoa humana.

---

[84] ***Universal Guidelines for Artificial Intelligence***. Portal The Public Voice. Disponível em: <https://thepublicvoice.org/ai-universal-guidelines/>. Acesso em: 16/05/2022.

[85] SULOCKI, Victoria. **Novas tecnologias, velhas discriminações: ou da falta de reflexão sobre o sistema de algoritmos na justiça criminal**. In: FRAZÃO, Ana de Oliveira; MULHOLLAND, Caitlin (coord.). **Inteligência Artificial e Direito: ética, regulação e responsabilidade**. São Paulo: Revista dos Tribunais, 2019. pp. 651-670.

3.3. Reconhecimento Facial Enviesado

Primeiramente, é necessário estabelecer a diferença entre reconhecimento facial que é uma das modalidades de reconhecimento de imagens, e o reconhecimento fotográfico, realizado diretamente por pessoas e utilizado frequentemente como ferramenta nas investigações.

A base trabalhada pelo reconhecimento facial é a biometria dos traços faciais humanos. Detecta traços geométricos medindo distância entre nariz, olhos, queixo e boca identificando até mesmo cicatrizes existentes na face como também o contorno do rosto, no qual é identificado pelo sistema operacional de forma algorítmica com código binário que são uma sequência numérica utilizada pelos computadores.

É possível realizar comparações de pontos estratégicos na face, são os pontos nodais, que detectam os indivíduos através de câmeras de segurança nas cidades, transportes públicos e órgãos públicos em geral. O êxito dos computadores em identificar os indivíduos a partir do rastreamento da captura de imagens- momento da ligação dos traços faciais- possui uma precisão de 96%.

Os avanços das hipertecnologias trouxe para sistemas de segurança, câmeras de celulares, aplicativos variados, a possibilidade de emprego do reconhecimento facial. No entanto, quando o emprego de tal ferramenta envolve grau de certeza maior com as questões delicadas como a identificação de pessoas em casos criminais, é preciso contextualizar melhor a hipótese, uma vez que os algoritmos associados a essa tecnologia estão longe de serem considerados confiáveis, conforme apresentado nesse trabalho.

Muito embora tramite na Câmara dos Deputados o projeto de Lei 9736/2018[86] que torna obrigatória a identificação por reconhecimento facial

[86] BRASIL. Câmara dos Deputados. **Projeto de Lei nº _, de 2018, de autoria do deputado Julio Lopes**. Disponível em < https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node01qpih0bpj4mfjc9w8t6pxcxfa8176821.node0?codteor=1643053&filename=PL+9736/2018>. Acesso em 13/03/2022.

de todo preso que ingressar em estabelecimento penal como medida de combater a criminalidade[87], especialistas apontam como um dos principais problemas do reconhecimento facial é o viés racista. O cientista político Pablo Nunes diz que:

> "Algoritmos não são produtos do nada, não se constroem no vácuo. São produzidos numa sociedade e refletem essa sociedade, são embutidos dos preconceitos e questões dessa sociedade, como o racismo. É inevitável que eles reproduzam o racismo, uma vez que não resolvemos esse problema na sociedade"[88].

Os algoritmos são produtos do intelecto limitado, falível, enviesados, com diferentes níveis de consciência e inconsciência, arquétipos, historias e memorias. Problemas estes que estão presentes na construção coletiva que não é excluída, apagada ou esterilizada. O volume, a capacidade de processamento, a velocidade e a profundidade da intervenção atingidas por tecnologias digitais tonem esses erros muito mais consideráveis. Ou seja, não se trata apenas de erros matemáticos, pois não desapega do substrato social.

O reconhecimento facial trata o que há de mais sensível: o rosto, a figura, a face de alguém, expressões, demonstração de emoções. O rosto é o dado mais pessoal, aquilo que identifica o homem entre a multidão.

A sensibilidade do dado biométrico, em especial sobre os rostos já está refletida nas obrigações legais relativas a esses. Há de aplicar os princípios da proporcionalidade, necessidade e minimização dos dados, de modo a compreender a cadeia de tratamento e ser, portanto, capazes de atribuir responsabilidades e prover informações integrais- sobre a tecnologia, sobre o criador, quem esteve presente no desenvolvimento, implementação e sob qual justificativa os tratamentos são realizados.

---

[87] BRASIL. Câmara dos Deputados. **Política pública de combate à criminalidade deve ser mais abrangente, diz Fórum de Segurança Pública**. 2019b. Disponível em: <https://www2.camara.leg.br/camaranoticias/noticias/SEGURANCA/574466-GOVERNO-QUER-LEI-PARA-REGULAR-VIGILANCIA-ESTATAL-POR-MEIO-DE-RECONHECIMENTO-FACIAL.html>. Acesso em: 13/03/2022.

[88] GUIMARÃES, Hellen. **Nos erros de Reconhecimento Facial, um "Caso Isolado" Atrás do Outro**. Revista Piauí, 2021. Disponível em: <https://piaui.folha.uol.com.br/nos-erros-de-reconhecimento-facial-um-caso-isolado-atras-do-outro/>. Acesso em: 27/02/2022.

No âmbito Judiciário, se valer do uso do reconhecimento facial com o intuito de identificar suspeitos e foragidos da polícia é problemático. Isso porque seria por intermédio de comparações em um banco de dados, onde ficam armazenados uma série de capturas fotográficas que não são totalmente eficazes devido ao ângulo, sombras, qualidade ruim e abrem margem a erros que podem causar sérios danos a um cidadão que não tenha praticado crime, mas que pelo reconhecimento facial precário poderia ser incriminado.

Destaca-se que as pessoas mais afetadas são as negras, tendo em vista a oposição das máquinas em reconhecer tonalidades de peles negras agravado pelo grande número de dados inseridos na IA por pessoas brancas.

É importante ressaltar que diante dos riscos e erros já documentados e conhecidos do reconhecimento facial, bem como sua banalização, submissão massiva da população as decisões sem conhecimento, com finalidades duvidosas, sequer definidas, o torna inadmissível nos dias atuais.

É constatado que a presença de um "Data Sets" viciado pode inluir na tomada de decisão e informação sobre crimes, de modo que a frequência de ocorrência numa localidade ou bairro contribuísse para um círculo vicioso do software.

> "A maioria dos sistemas de reconhecimento acial que existem são treinados em bancos de dados de otos. Os bancos de dados de Mugshot são desproporcionalmente alimentados com imagens digitalizadas de indivíduos negros e pardos, como resultado do excesso de policiamento e da criminalização desproporcional das comunidades negras e pardas."[89]

Atualmente, é interessante a lógica da inclusão de um elemento de aleatoriedade, o qual difunde um caráter modificativo. Pois, através dessa alteração é possível que o algoritmo que antes se concentrava em um determinado ambiente- como nas regiões pobres e de maior concentração populacional- se expanda para os crimes praticados em regiões favorecidas. A título de exemplo: se antes os policiais eram direcionados apenas para uma determinada região, com o sistema de aleatoriedade, a tendência é que em

[89] GARVIE; BEDOYA e FRANKLE, 2016

algum momento o software coloque esses policiais em uma região distinta. Sendo assim, torna-se possível que o "software" corrija as falhas nos dados progressivamente.

Isto posto, quando o desfecho é guiado pelos algoritmos e automatizado, deve-se considerar o contexto histórico e as implicações atuais para transformar a realidade assim como os julgamentos sobre eles em dados, do qual todos os sistemas tecnológicos são desenvolvidos.

O mais preocupante é a ausência de regulamentação que garanta as liberdades individuais e a transparência no uso da tecnologia e proteção de dados pessoais.

Ademais, restam dúvidas sobre a precisão do sistema. Em 2018, o Instituto Nacional de Padronizações e Tecnologia do Departamento do Comércio dos EUA[90] (NIST, na sigla em inglês) testou 127 algoritmos de 45 desenvolvedores e descobriu que, quando havia imagens de alta qualidade para comparação, os melhores algoritmos só falharam em 0,2% das vezes, um resultado 20 vezes melhor do que no teste semelhante feito em 2014. Contudo, entre ambientes privados e as consideradas "praças públicas" há diferença significativa: uma coisa é o celular reconhecer o rosto do dono, outra é aquele mesmo rosto ser identificado em uma multidão.

Em um experimento muito citado para mostrar que as minorias podem ser prejudicadas, a ONG norte-americana American Civil Liberties Union[91] revelou que o programa de reconhecimento facial da Amazon erroneamente identificou 28 membros do Congresso dos EUA como criminosos cadastrados em uma base de fotos pública. Quase 40% dos resultados errados

---

[90] GROTHER, Patrick; NGAN, Mei; HANAOKA, Kaynee. **Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification**. National Institute of Standards and Technology. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf>. Acesso em: 19/05/2022.

[91] SNOW, Jacob. ***Amazon's face Recognition falsely Matched 28 members o Congress with Mugshots***. ACLU of Northern California. Disponível em: <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>. Acesso em: 19/05/2022.

envolveram pessoas negras — algo desproporcional, já que somente 20% dos congressistas são negros.

No MIT, pesquisadores identificaram[92] que algoritmos para identificar o gênero com base no rosto classificaram mulheres de pele escura como homens em quase 35% das vezes. Para os homens com pele clara, a taxa de erro era menor que 1%.

Ora, o número elevado de "falsos positivos" pode gerar constrangimentos e apreensões, podendo, à sua maneira, intensificar as discriminações e racismos já latentes na sociedade. Uma questão que se sobressai é que essas tecnologias, na maior parte das vezes, são produzidas em países da Europa, Ásia e Estados Unidos e a fase de testagem se dá nos respectivos países que apresentam realidade diversa da brasileira. Ou seja, os treinamentos não correspondem às nossas características físicas ou hábitos, o que agrava a deficiência na eficiência da tecnologia.

[92] BUOLAMWINI, Joy; GEBRU, Timnit. ***Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification***. Disponível em: <http://proceedings.mlr.press/v81/buolamwini18a.html>. Acesso em: 19/05/2022.

Conclusão

O padrão humano de avaliação está longe de ser o ideal, sendo frágil a influencias. Em tese, os algoritmos estão buscando aperfeiçoar essas avaliações, mas não colecionam perfeição. De acordo com o estudo apresentado, verificou-se que as avaliações por *softwares* existem falhas humanas integradas. Fato é que essas informações podem ser utilizadas para aumentar a sentença e punir alguém pelo crime que ainda não cometeu, se os indivíduos ainda não cometeram crimes, não há no que se falar em um julgamento quanto à possibilidade de violar a lei novamente.

Considerando o exposto ao longo desse trabalho, são inegáveis as conquistas obtidas com o auxílio de ferramentas de Inteligência Artificial. No entanto, acrescenta-se à realidade contemporânea o aumento na implementação de artefatos para análise de comportamento humano, não se podendo esquecer que representam perigo à autonomia do ser humano, como indivíduo, e podem gerar sim mecanismos potencialmente discriminatórios em razão da possibilidade de manejo perverso de algoritmos.

É sabido que as decisões humanas não são neutras, as quais estão munidas de concepções ideológicas, políticas ou religiosas, de valores apreendidos e de experiências vividas. Por esse motivo, estão sujeitas a reproduzir os preconceitos de quem decide, e a tratar com igualdade ou discriminar pessoas ou grupos sociais que ela representa (pessoas com deficiência, indígenas, idosos, negros, entre outros). No entanto, não há certeza de que as decisões automatizadas- tomadas por máquinas dotadas de inteligência artificial- sejam mais sábias e melhores para o bem-estar da humanidade.

O sistema operacional da IA é elaborado, alimentado e concretizado por humanos que depositam suas vivências, ainda que indiretamente na seleção do que considerar ou desconsiderar, incluir ou excluir, sancionar ou vetar. As escolhas do criador são determinantes para o proceder da máquina

que a partir de padrões, reproduz em cadeia. A manipulação, ainda que intuitiva, está presente.

Nesse sentido, o uso de big data, então, é tratado como capaz de proporcionar de mais precisão, conferir potencialidades preditivas, as quais contribuem para o aumento da eficiência, segurança, geração de valor e gestão de recursos. "[*B]ig data sets are systems of knowledge (...) [they] are both the product of social and cultural processes and themselves act to configure elements of society and culture.*"[93]. Todavia, a própria manipulação desses dados envolve escolhas e a agência de indivíduos — seja na seleção, tratamento e organização dos dados, como no desenvolvimento, treinamento e aplicação do software. Tais decisões não estão isentas de subjetividade ou das percepções dos indivíduos sobre o mundo social.

A reflexão sobre a discriminação é atual e relevante, pois os sistemas de IA estão sendo utilizados, em muitos países, com os mais diversos objetivos. Exemplo é o policiamento preditivo que, mediante a análise de dados disponíveis, busca prever onde o crime poderá ocorrer[94]. Não obstante, os sistemas de predição e outros sistemas de IA não estão livres de distorções no resultado. Afinal, os dados são inseridos por programadores humanos que, mesmo involuntariamente, podem contaminá-los com seus preconceitos.

Verifica-se que é uma tarefa complexa a tentativa de corrigir os vieses existentes nas máquinas que utilizam *machine learning* e, se não for feito, pessoas podem ser afetas, como visto no caso do COMPAS nos EUA. Para que sejam corrigidos é necessário entender de onde vem e de onde surgem esses vieses.

De acordo com o MIT, os preconceitos podem aparecer antes mesmo dos dados serem coletados, ou em outras fases do procedimento de *Machine*

---

[93] Lupton, 2015, p. 116

[94] BRAGA, Carolina. **Discriminação nas decisões por algoritmos: polícia preditiva**. In: FRAZÃO, Ana. MOULHOLLAND, Caitlin (Coord.). **Inteligência artificial e direito: ética, regulação e responsabilidade.** São Paulo: Thomson Reuters (Revista dos Tribunais), 2019. Pp. 671-695

Learning. Assim sendo, elencam três pontos principais de como o viés pode ocorrer: (a) o enquadramento do problema, ou seja, nesse ponto o programador define o que o programa fará especificamente, pois se fugir de sua finalidade poderá ocorrer, como no caso do COMPAS, uma discriminação; (b) é no momento da coleta de dados, no qual o preconceito poderá surgir, onde o algoritmo poderá ser treinado com dados tendenciosos. E (c) na preparação dos dados, isto é, o viés pode ser incorporado durante a elaboração dos dados. Se no momento da elaboração forem utilizados dados sensíveis, como raça, cor, gênero ou outros fatores implícitos poderá haver esse enviesamento[95].

Considerando ser o principal aspecto do processo penal a constante tomada de decisão- vale dizer de todos os agentes processuais, não apenas dos magistrados-, há de se ponderar a lógica facilitadora da IA. Ocorre que, deve-se observar os comportamentos na tomada de decisão das máquinas, no campo do Direito, exigindo a supervisão humana apurada e atenta, a saber, pois elas não podem "decidir sozinhas", a partir dos critérios e preferências que elegerem, uma vez que a "razão humana" deve "supervisionar" o conjunto de dados (o *input*), construir o algoritmo (os critérios e o passo a passo da decisão), validar o modelo decorrente (acurácia, precisão etc.), justamente porque produzidas por algoritmos que se valem de heurísticas.

Se adotados no âmbito judiciário brasileiro, os resultados "sugeridos" pelas máquinas devem ser "validados" por agentes humanos, no controle das decisões. Diante da capacidade de processamento das máquinas, a velocidade e volume de processamento de dados impede o entendimento humano (p.ex. *Black Box*), como no caso de "veículos autônomos", contexto em que as discussões são complexas e devem ser tratadas.

---

[95] HAO, Karen. ***This is how AI bias really happens – and why it's so hard to fix***. Disponível em: <https://www.technologyreview.com/2019/02/04/137602/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix/>. Acesso em 19/05/2022.

Isso deriva da dificuldade de pedir às máquinas a explicação *step by step* do trajeto decisório, característica particular das máquinas.

Dessa forma, a inclusão das máquinas pode auxiliar a decisão judicial com aderência normativa e científica, mantendo o humano como o responsável único pelas deliberações (*accountability*). A máquina serve de apoio à decisão e não substitui o humano. Eis a diretriz defendida.

O grande objetivo do trabalho foi mostrar que por mais que não tenham no Brasil casos de robô com autonomia de decidir como juiz, há uma tendência cada vez mais forte de incorporar essa tecnologia inclusive na fase decisória- etapa de grande impacto, em especial no Direito Penal que comprometido com a efetivação dos direitos fundamentais e proteção dos bens jurídicos mais importantes ao seio social só encontra competência quando desenvolvida em estrita obediência a seu caráter fragmentário e subsidiário.

Por fim, é necessário reforçar a importância da sensibilidade humana nos julgamentos, considerando suas imperfeições, subjetividades e história única de cada parte processual.

Conclui-se, assim, que as decisões das máquinas não são 100% seguras e devem ser questionadas. Para tanto, é de suma importância a transparência dos dados, que estes sejam publicizados de maneira clara e acessível. E que se traduza a computação para que a pessoa mais leiga entenda e possa eventualmente saber seus direitos e responsabilidades perante essa tecnologia que mal-usada pode ser um “campo minado” para o Estado Democrático de Direito.

Referências Bibliográficas

Algorithms in the Criminal Justice System. Disponível em <https://epic.org/algorithmic-transparency/crim-justice/>. Acesso em 16/05/2022.

Aplicação da inteligência artificial na gestão de frotas e seus benefícios. Portal Infleet. Disponível em: https://infleet.com.br/blog/aplicacao-da-inteligencia-artificial-na-gestao-de-frotas-e-seus-beneficios. Acesso em 19/05/2022.

Aprendizagem Profunda. Portal Wikipédia Brasil. Disponível em: <https://pt.wikipedia.org/wiki/Aprendizagem_profunda#cite_note-good_fellow2016-1>. Acesso em 18/05/2022.

BOEING, Daniel Henrique Arruda; MORAIS DA ROSA, Alexandre. **Ensinando um Robô a Julgar: pragmática, discricionariedade, heurísticas e vieses no uso de aprendizado de máquina no Judiciário**. Florianópolis: EMais, 2020, pp. 73-106.

BOEING, Daniel Henrique Arruda; ROSA, Alexandre Morais da. **Ensinando um Robô a Julgar: pragmática, discricionariedade, heurísticas e vieses no uso de aprendizado de máquina no Judiciário.** Florianópolis: Emais Academia, 2020.

BRAGA, Carolina. **Discriminação nas decisões por algoritmos: polícia preditiva**. In: FRAZÃO, Ana. MOULHOLLAND, Caitlin (Coord.). **Inteligência artificial e direito: ética, regulação e responsabilidade.** São Paulo: Thomson Reuters (Revista dos Tribunais), 2019. Pp. 671-695

BRASIL. Advocacia-Geral da União (AGU). **Advocacia-Geral aposta em inteligência artificial e automação de processos para agilizar trabalhos jurídicos**. Disponível em: <http://www.agu.gov.br/page/content/detail/id_conteudo/230719>. Acesso em: 13/03/2022.

BRASIL. Câmara dos Deputados. **Apresentações dos participantes da audência pública sobre reconhecimento facial**. 2019a. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cctci/audiencias-publicas/copy_of_2018/2019-04-03-reconhecimento-facial/03-04-2019-ap-reconhecimento-facial>. Acesso em: 13/03/2022.

BRASIL. Câmara dos Deputados. **Governo quer lei para regular vigilância estatal por meio de reconhecimento facial**. 2019a. Disponível em: <https://www2.camara.leg.br/camaranoticias/noticias/SEGURANCA/5744

69-POLITICA-PUBLICA-DE-COMBATE-A-CRIMINALIDADE-DEVE-SER-MAIS-ABRANGENTE,-DIZ-FORUM-DE-SEGURANCA-PUBLICA.html>. Acesso em: 13/03/2022.

BRASIL. Câmara dos Deputados. **Política pública de combate à criminalidade deve ser mais abrangente, diz Fórum de Segurança Pública**. 2019b. Disponível em: <https://www2.camara.leg.br/camaranoticias/noticias/SEGURANCA/574466-GOVERNO-QUER-LEI-PARA-REGULAR-VIGILANCIA-ESTATAL-POR-MEIO-DE-RECONHECIMENTO-FACIAL.html>. Acesso em: 13.03.2022.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº _, de 2018, de autoria do deputado Julio Lopes**. Disponível em <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node01qpih0bpj4mfjc_9w8t6pxcxfa8176821.node0?codteor=1643053&filename=PL+9736/ 2018>. Acesso em 13/03/2022.

BRASIL. Ministério da Justiça e Segurança Pública. **Portaria nº 218, de 29/09/2021**. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/operacoes-integradas/cortex/publica coes/portaria-no-218-de-29-de-setembro-de-2021>. Acesso em: 16/05/2022.

BRASIL. Senado Federal. **Projeto de Lei nº 4.496/2019, de autoria do Senador Styvenson Valentim.** Disponível em: <https://www25.senado.leg.br/ web/atividade/materias/-/materia/ 138136>. Acesso em: 16/05/2022.

BRASIL. Superior Tribunal de Justiça. **Relatório do 1º ano de Gestão: Ministro João Otávio de Noronha**. Brasília, 2019. Disponível em: <http://www.stj.jus.br/sites/portalp/SiteAssets/documentos/noticias/Relat%C3%B3rio%20de%20gest%C3%A3o.pdf>. Acesso em: 19/05/2022.

BRASIL. Superior Tribunal Federal. **Inteligência Artificial vai Agilizar a Tramitação de Processos no STF**. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=380038>. Acesso em: 19/05/2022.

BRASIL. Supremo Tribunal Federal. **Inteligência artificial vai agilizar a tramitação de processos no STF**. Disponível em: <https://stf.jusbrasil.com.br/noticias/584499448/inteligencia- artificial-vai-agilizar-a-tramitacao-de-processos-no-stf>. Acesso em: 30/03/2022.

BRASIL. Supremo Tribunal Federal. **Ministra Cármen Lúcia anuncia início de funcionamento do Projeto Victor, de inteligência artificial**. Disponível em: <https://stf.jusbrasil.com.br/noticias/ 620175789/ministra-carmen-lucia-anuncia-inicio-de-funcionamento-do-projeto-victor-de-inteligencia-artificial>. Acesso em 30/03/2022.

BRASIL. Tribunal de Justiça do Estado de Minas Gerais. **Gestão de precedentes é tema de encontro no TJMG**. Disponível em <http://www.tjmg.jus.br/portal-tjmg/noticias/gestao-de-precedentes-e-tema-de-encontro-no-tjmg.htm>. Acesso em 30/03/2022.

BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **TJRJ adota modelo inovador nas cobranças de tributos municipais**. Disponível em: <http://cgj.tjrj.jus.br/noticias/noticia/-/visualizar-conteudo/5111210/5771753>. Acesso em 28/03/2022.

BUOLAMWINI, Joy; GEBRU, Timnit. ***Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification***. Disponível em: <http://proceedings.mlr.press/v81/buolamwini18a.html>. Acesso em: 19/05/2022.

CANÁRIO, Pedro. **Robôs permitem que juízes deixem de lado função de gestor de processos e varas**. Disponível em: <https://www.conjur.com.br/2017-ago-26/robos-permitem-juizes-deixem-lado-funcao-gestor>. Acesso em: 03/03/2022.

Cartilha de Adesão ao Sistema Detecta (V3.0). Disponível em: <http://www.sapp.org.br/sapp/wp-content/uploads/Sistema_Detecta_cartilha _completa_v3.pdf.>. Acesso em 21/05/2021.

CARVALHO, Saulo. **O encarceramento seletivo da juventude negra brasileira.** 624 Rev. Fac. Direito UFMG, Belo Horizonte, n. 67, pp. 623 - 652, jul./dez. 2015. Disponível em: <www.direito.ufmg.br/revista/index.php/revista/article/download/1721/1636>. Acesso em 14.05.2022.

CHIESI FILHO, Humberto. **Inteligência artificial é uma realidade e já afeta a área jurídica.** Revista Consultor Jurídico (CONJUR). Disponível em: <https://www.conjur.com.br/2017-set-15/chiesi-filho-inteligencia-artificial-afeta-area-juridica>. Acesso em: 31/03/2022.

Conceitos sobre IA. Expert Academy. Disponível em <https://iaexpert.academy/2017/01/17/ia-forte-x-ia-fraca/>. Acesso em 12/04/2022.

Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Disponível em <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434>. Acesso em 16/05/2022.

Deep Learning. Portal Affectiva. Disponível em: <https://www.affectiva.com/ how/deep-learning-at-affectiva/>. Acesso em 18/05/2022.

Detecta monitora o Estado de SP com mais de três mil câmeras de vídeo. Disponível em: <https://www.saopaulo.sp.gov.br/spnoticias/detecta-monitora-oestado-de-sao-paulo-com-3-mil-cameras-de-video/>. Acesso em 16/05/2022.

ESPOSITO, E. ***Algorithmic memory and the right to be forgotten on the web***. In: Big Data & Society, v. 4, n. 1, pp. 01-11

ESTEFAM, A.; GONÇALVES, V. E. R**. Direito Penal Esquematizado – Parte Geral**. 9º edição, São Paulo: Saraiva Educação, 2020.

FENELON, F. **Responsabilização Penal e Sistema de Inteligência Artificial: Um Tema Controverso**. Canal Ciências Criminais. Disponível em: <https://canalcienciascriminais.com.br/responsabilizacao-penal-e-sistemas-de-inteligencia-artificial/>. Acesso em: 19/04/2022.

FENOLL, Jordi Nieva. ***Inteligencia Artificial y Proceso Judicial***. Marcial Pons: Madrid, 2018.

FRAZÃO, Ana. **Algoritmos e Inteligência Artificial**. Jota. 16/5/2018. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/ constituicao-empresa-e-mercado/algoritmos-e-inteligencia-artificial-16052018>. Acesso em: 16/05/2022

FRAZÃO, Ana. **Dados, estatísticas e algoritmos**. Jota. 28/6/2017. 2017. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/ constituicao-empresa-e-mercado/dados-estatisticas-e-algoritmos-28062017>. Acesso em: 16/05/2022.

GALVÃO, Danyelle da Silva; PEIXOTO JUNIOR, Hélio; LOBO, Ricardo. **O artigo 489 do Novo Código de Processo Civil (Lei 13.105/2015) e suas implicações no Direito Processual Penal**. In: Revista dos Tribunais, v. 105, n. 971, set./2016, pp. 283-312.

GOGONI, Ronaldo. **Venni N1, o robô-aspirador capaz de evitar "presentinhos"**. Portal Meio Bit. Disponível em <https://tecnoblog.net/meiobit/393701/venii-n1-robo-aspirador-anti-coco/>. Acesso em 19/05/2022.

GONZÁLEZ, Pedro Meseguer; BADIA, Ramón López de Mántaras. **Inteligência Artificial. Los Libros de la Catarata**. 11 de novembro de 2017. Disponível em: <https://zoboko.com/read/inteligencia-artificial-

yq2dxqpp ?hash=71a2074807d78b6ae6cb4c4456e72348>. Acesso em: 10/02/2022.

GOODMAN, B.; FLAXMAN, S. R. ***European Union regulations on algorithmic decision-making and a "right to explanation"***. In: AI Magazine, 38(3), pp. 50-57.

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kaynee. **Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification**. National Institute of Standards and Technology. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf>. Acesso em: 19/05/2022.

GUIMARÃES, Hellen. **Nos erros de Reconhecimento Facial, um "Caso Isolado" Atrás do Outro**. Revista Piauí, 2021. Disponível em: <https://piaui.folha.uol.com.br/nos-erros-de-reconhecimento-facial-um-caso-isolado-atras-do-outro/>. Acesso em: 27/02/2022.

HALLEVY, G. **When Robots Kill: Artificial Intelligence Under Criminal Law.** 1ª edição. Boston: Northeastern University Press, 2013.

HALLEVY, Gabriel. ***The Basics Models of Criminal Liability of AI Systems and outer circles***. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3402527>. Acesso em 28/03/2022.

HAO, Karen. ***This is how AI bias really happens – and why it's so hard to fix***. Disponível em: <https://www.technologyreview.com/2019/02/04/137602/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix/>. Acesso em 19/05/2022.

JIRARDI, Alessandra. Inteligência **Artificial no Processo Penal**. Portal Jusbrasil. Disponível em: <https://alessandrajirardi.jusbrasil.com.br/artigos/847009808/inteligencia-artificial-no-processo-penal>. Acesso em: 30/03/2022.

JOH, E. E. Policing by numbers: **Big data and the 4th Amendment.** Washington Law Review, v. 89, 2014. Disponível em: https://digitalcommons.law.uw.edu/wlr/vol89/iss1/3/ Acesso em: 12/05/2022.

KNIJNIK, Danilo. **Os standards do convencimento judicial: paradigmas para o seu possível controle**. Revista Forense, Rio de Janeiro, n. 353, jan.-fev. 2001.

Lançado robô dedicado à limpeza doméstica. Portal Inovação Tecnológica. Disponível em: <https://www.inovacaotecnologica.com.br/noticias/noticia.php?artigo=010180020924&id=010180020924>. Acesso em 19/05/2022.

Legacy Robots: The robots that built the groundwork for today's portfolio. Portal Boston Dynamics. Disponível em: <https://www.bostondynamics.com/legacy>. Acesso em 19/05/2022.

***Machine Bias – There´s Software Used across the Country to Predict Future Criminals. And it´s Biased Against Black*.** Portal Propublica. Disponível em <https://www.propublica.org/article/ machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 16/05/2022.

MORAES, Maria Celina Bodin de. **LGPD: um novo regime de responsabilização civil dito "proativo"**. Civilistica.com, Rio de Janeiro, ano 8, n. 3, 2019. Disponível em: <http://civilistica.com/lgpd-umnovo-regime/>. Acesso em: 28/01/2022.

MORALES, Rodrigo Rivera. ***La Prueba: un análisis racional y práctico***. Madrid: Marcial Pons, 2011.

MOREIRA, Isabela**. A Microsot criou um robô que interage nas redes sociais - e ela virou nazista.** Revista Galileu. Disponível em: <https://revistagalileu.globo.com/blogs/buzz/noticia/2016/03/microsoft-criou-uma-robo-que-interage-nas-redes-sociais-e-ela-virou-nazista.html>. Acesso em 10/03/2022.

MOSCHOVAKIS, Y. N. ***What is an Algorithm?***. In: ENGQUIST, B.; SCHMID, W. (coord.). **Mathematics Unlimited – 2001 and Beyond**. Springer, pp. 919–936 (Part II). 2001. Disponível em <www.cs.cmu.edu/~-cdm/pdf/Moschovakis01.pdf>. Acesso em 23/4/2022

MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. **Inteligência artificial e a lei de proteção de dados pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de *machine learning***. In: FRAZÃO, Ana. MOULHOLLAND, Caitlin (Coord.). **Inteligência artificial e direito: ética, regulação e responsabilidade**. São Paulo: Thomson Reuters (Revista dos Tribunais), 2019, pp. 265-290

NORONHA, E. Magalhoões. **Direito Penal – Volume 1: Introdução e Parte Geral**. São Paulo: Editora Saraiva, 2003.

O'BRIEN, Matt; KANG, Dake. ***AI in the court: When algorithms rule on jail time.*** 31/1/2018. Disponível em: https://phys.org/news/2018-01-ai-court-algorithms.html. Acesso em: 05/03/2022.

O'NEIL, Cathy. ***Weapons of math destruction: how big data increases inequality and threatens democracy***. Nova York: Crown Publishers. 2016. Edição digital.

Organização para a Cooperação e Desenvolvimento Econômico (OCDE). ***Algorithms and collusion: Competition policy in the digital age*.** 2017. Disponível em <www.oecd.org/competition/algorithms--collusion-competition-policy-in-the-digital-age.htm>. Acesso em 17/2/2022

Policiamento Preditivo, Controle Social e Desigualdades Raciais. Disponível em: <https://anpocs.com/index.php/encontros/papers/43-encontro-anual-da-anpocs/spg6/spg32-1/12010-policiamento-preditivo-controle-social-e-desigualdades-raciais/file>. Acesso em: 13/05/2022.

PRADO, Geraldo. **Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital**. Disponível em: <https://www.conjur.com.br/dl/artigo-geraldo-prado.pdf>. Acesso em 10/05/2022

RACANICCI, Jamile. **Judiciário desenvolve tecnologia de voto assistido por máquinas**. Disponível em: <https://www.jota.info/justica/judiciario-desenvolve-tecnologia-de-voto-assistido-por-maquinas-080120>. Acesso em: 30/03/2022

REBELLO, Aiuri. **Da placa de carro ao CPF**. Portal The Intercept Brasil. Disponível em: <https://theintercept.com/2020/09/21/governo-vigilancia-cortex/>. Acesso em: 19/05/2022.

ROMEO-CASABONA, Carlos María; LAZCOZ MORATINOS, Guillermo. **Inteligência artificial aplicada à saúde: que marco legal?** P. 78. Disponível em: <https://www.fundacionmercksalud.com/wp-content/uploads/2020/03/1.3.-IA-APLICADA-A-LA-SALUD.-Carlos-M.-Romeo-Guillermo-azcoz.pdf>. Acesso em: 02/06/2022.

Ross, o primeiro robô advogado do mundo. Portal ICEV. Disponível em <https://www.somosicev.com/blogs/ross-o-primeiro-robo-advogado-do-mundo/>. Acesso em 19/05/2022.

RUSSEL, Stuart J; NORVIG, Peter. **Inteligência Artificial.** 3ª ed. Rio de Janeiro: Elsevier, 2013. p. 1195. Disponível em <https://www.cin.ufpe.br/~gtsa/Periodo/PDF/4P/SI.pdf>. Acesso em: 19/05/2022.

SAMUEL, Arthur. L. ***Some Studies in Machine Learning Using the Game of Checkers. IBM Journal of Research and Development***. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?-doi=10.1.1.368.2254&rep=rep1&type=pdf. Acesso em 9/5/2022.

SANTOS, Coriolano Camargo; CHEVTCHUK, Leila. **Inteligência artificial, algoritmos e decisões injustas: é hora de revermos criticamente nosso papel em face da tecnologia**. Portal Migalhas. Disponível em

<https://www.migalhas.com.br/coluna/direito-digital/268283/inteligencia -artificial--algoritmos-e-decisoes-injustas--e-hora-de-revermos-criticamente-nosso-papel-em-face-da-tecnologia>. Acesso em 14/05/2022.

SAVCHUK, Katia. ***Justice by the numbers: meet the statistician trying to fix bias in criminal justice algorithms***. 1/2/2019. Disponível em: https://psmag.com/social-justice/justice-by-the-numbers-meet-the-statistician-trying-to-fix-bias-in-criminal-justice-algorithms. Acesso em 8/5/2022.

Sistema de inteligência do governo monitora 360 mil pessoas, diz revista. Portal Uol. Disponível em <https://noticias.uol.com.br/politica/ultimas-noticias/2022/01/21/cortex-programa governo-vigiar-cidadaos-crusoe.htm>. Acesso em 16/05/2022

SKIBBA, Ramin. ***A Calculating Look at Criminal Justice***. Disponível em: https://undark.org/article/a-calculating-look-at-criminal-justice/. Acesso em: 8/5/2022.

SNOW, Jacob. ***Amazon's face Recognition falsely Matched 28 members o Congress with Mugshots***. ACLU of Northern California. Disponível em: <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>. Acesso em: 19/05/2022.

STRECK, Lenio Luiz. **Distopia: os algoritmos e o fim dos advogados: *kill all the lawyers*!** Revista Consultor Jurídico. 2019a. Disponível em: https://www.conjur.com.br/2019-mai-23/senos-incomum-distopia-algoritmos-fim-advogados-kill-all-the-lawyers. Acesso em 23/05/2022.

STRECK, Lenio Luiz. **Lawtechs, startups, algoritmos: Direito que é bom, nem falar, certo?** Revista Consultor Jurídico. 2019b. Disponível em: https://www.conjur.com.br/2019-mai-16/senso-incomum-lawtechs-startups-algoritmos-direito-bom-nem-falar-certo. Acesso em 16/05/2022.

STRECK, Lenio Luiz. **Que venham logo os intelectuais para ensinarem aos especialistas.** Revista Consultor Jurídico. 2019c. Disponível em: https://www.conjur.com.br/2019-mai-30/senso-incomum-venham-logo-intelectuais-ensinarem-aos-especialistas. Acesso em 30/05/2022.

SULOCKI, Victoria. **Novas tecnologias, velhas discriminações: ou da falta de reflexão sobre o sistema de algoritmos na justiça criminal**. In: FRAZÃO, Ana de Oliveira; MULHOLLAND, Caitlin (coord.). **Inteligência Artificial e Direito: ética, regulação e responsabilidade**. São Paulo: Revista dos Tribunais, 2019. pp. 651-670.

TALBOT, David; FOSSETT, Jeff. **Exploring the Role of Algorithms in Online Harmful Speech**. Berkman Klein Center for Internet & Society at Harvard University. Agosto/2017. Disponível em: <https://shorensteincenter.org/wp-content/uploads/2017/08/Harmful-Speech-Workshop-Summary.pdf>. Acesso em: 17/05/2022.

TOVO, Antônio. **O Periculosômetro Digital**. Disponível em <https://www.ab2l.org.br/o-periculosometro-digital/>. Acesso em 16/05/2022.

Universal Guidelines for Artificial Intelligence. Portal The Public Voice. Disponível em: <https://thepublicvoice.org/ai-universal-guidelines/>. Acesso em: 16/05/2022.

VALENTINI, Romulo Soares. **Julgamento por computadores? As novas possibilidades da juscibernética no século XXI e suas implicações para o futuro do direito e do trabalho dos juristas**. Tese de Doutorado apresentada à Faculdade de Direito da Universidade Federal de Minas Gerais (UFMG). Belo Horizonte, 2018.

VIEIRA, Leonardo. **A problemática da Inteligência Artificial e dos vieses algoritimicos: caso Compas**. Disponível em: <https://www.lcv.fee.unicamp.br/images/BTSym-19/Papers/090.pdf>. Acesso em: 19/05/2022.

WOJCIECHOWSKI, Paola Biachi; MORAIS DA ROSA, Alexandre. **Vieses da Justiça: como as herurísticas e vieses operam nas decisões penais e a atuação contraintuitiva**. Florianópolis: EMais, 2021.

WORLD ECONOMIC FORUM. ***AI is convicting criminals and determining jail time, but is it fair?***. Disponível em: <https://www.weforum.org/agenda/2018/11/algorithms-court-criminals-jail-time-fair/>. Acesso em: 08/04/2022.