PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO

Faculdade de Direito

MARCELA ZANELATO ALMEIDA

Projeto de pesquisa

O USO DA INTELIGÊNCIA ARTIFICIAL NA ERA DO CRIME DIGITAL

São Paulo - SP

2024

MARCELA ZANELATO ALMEIDA

O USO DA INTELIGÊNCIA ARTIFICIAL NA ERA DO CRIME DIGITAL

Projeto de Pesquisa apresentado ao Curso de Direito da Pontifícia Universidade Católica de São Paulo como um dos pré-requisitos para aprovação na disciplina de de Direito, sob orientação da Profa. Dra. Greice Patrícia Fuller.

São Paulo - SP

2024

AGRADECIMENTOS

Agradeço primeiramente a Deus, por ser a rocha firme em que me apoiei nos momentos de tempestade e a brisa suave que celebrou comigo cada conquista.

Sou extremamente grata a todos os meus professores que me ajudaram no meu progresso acadêmico, principalmente a professora Greice Patrícia Fuller, que tornou esse trabalho de conclusão de curso possível, que ajudou no meu crescimento acadêmico desde o inicio da faculdade, com muita dedicação, conselhos e ministrando aulas de forma inefável.

Aos meus pais, irmão, tios, e avó, pelo amor, incentivo e apoio incondicional, que foram essenciais para que eu pudesse superar os desafios e chegar até aqui, e que sempre me encorajaram a perseguir meus objetivos e me ajudaram a manter a motivação em momentos difíceis.

Ao meu amor, que foi a calmaria em meio à tempestade, obrigado por ser meu porto seguro e minha fonte inesgotável de apoio e carinho.

Aos meus amigos, que foram minha dopamina durante toda essa jornada.

E, finalmente, a todos que de alguma forma tocaram minha vida durante essa jornada.

RESUMO

Este trabalho explora o uso da inteligência artificial (IA) no combate a crimes digitais, abordando suas estratégias, expectativas e considerações éticas. À medida que a tecnologia avança, as ameaças cibernéticas se tornam mais sofisticadas, exigindo soluções inovadoras. O estudo analisa estratégias como a detecção avançada de deepfakes, autenticação multifatorial e sistemas de monitoramento em tempo real. Além disso, discute as expectativas em relação à análise preditiva de ameaças e à resposta automatizada a incidentes. A pesquisa também considera os desafios éticos, como a vigilância excessiva e o viés algorítmico, e enfatiza a necessidade de marcos regulatórios e educação em segurança cibernética. Por fim, o trabalho sugere a colaboração entre setores, incluindo empresas, instituições acadêmicas e governos, Estado, para desenvolver políticas de segurança eficazes e promover o uso responsável da IA.

Palavras Chave: Inteligência artificial; Crimes digitais; Segurança cibernética; Ética; Políticas de segurança

ABSTRACT

This paper explores the use of artificial intelligence (AI) in combating cybercrime, addressing its strategies, expectations, and ethical considerations. As technology advances, cyber threats become more sophisticated, requiring innovative solutions. The study analyzes strategies such as advanced deepfake detection, multifactor authentication, and real-time monitoring systems. In addition, it discusses expectations regarding predictive threat analysis and automated incident response. The research also considers ethical challenges, such as excessive surveillance and algorithmic bias, emphasizing the need for regulatory frameworks and cybersecurity education. Finally, the paper suggests collaboration among sectors, including companies, academic institutions and governments, State, to develop effective security policies and promote the responsible use of AI.

Keywords: Artificial intelligence; Cybercrime; Cybersecurity; Ethics; Security policies

SUMÁRIO

INTRODUÇÃO

Com o desenvolvimento e evolução da população, temos como consequência, o avanço e a popularização da internet. A internet permite cada vez mais o livre acesso às informações, traz o direito à expressão de diversas formas e possibilita o relacionamento e interação entre diversas pessoas pelo mundo inteiro.

A internet com certeza modificou e facilitou o modo de viver da sociedade, facilitando o trabalho, o convívio, a comunicação e demais atividades essenciais para o cotidiano. Conforme diversas pesquisas, a internet é utilizada por 5,4 bilhões de pessoas, de pessoas de diversas idades, classes sociais e sexo, representando uma grande quantidade da população mundial, seja o uso por notebook, seja por celular ou outros dispositivos móveis que se ligam com uma rede.

Contudo, a internet passou a ser utilizada também para o cometimento de crimes, principalmente por ser um método discreto, sem fronteiras e a facilidade de acessar qualquer arquivo, foto, vídeo e dados de qualquer lugar do mundo, o que é uma facilidade para os criminosos.

Diante dessa nova era digital e desse avanço desenfreado da internet e crimes digitais, a legislação brasileira possui a tarefa de se adequar a esses avanços tecnológicos para inibir os crimes cibernéticos, a fim de não virar refém de criminosos sem identidade certa, que se escondem por trás das redes.

Portanto, esta pesquisa tem como objetivo analisar a inteligência artificial sob diversos ângulos, como por exemplo o uso da IA como uma ferramenta poderosa no combate ao crime, visto que é uma segurança preditiva, onde algoritmos de Inteligencia artificial analisam grandes quantidades de dados produzidos, para identificar padrões e prever possível crimes e, principalmente, a descobrir os autores dos crimes, permitindo com que as autoridades ajam proativamente para evitar as

atividades criminosas. Além de analisar as qualidades do uso da IA, o trabalho traz as problemáticas que o uso da tecnologia pode trazer para o meio jurídico.

Além disso, a IA desempenha um grande e importante papel na coleta de evidências criminais, como a análise de gravações de áudios e vídeos feita por algoritmos de IA, sendo possível a extração de informações relevantes que podem ser usadas em processos judicias, além da possibilidades da utilização de drones equipados com Inteligência artificial para monitorar áreas de alto risco e difícil acesso.

Ademais, é necessário também observar, como o uso da IA pode ter implicações constitucionais significativas, por mais que a IA garanta em sua tecnologia uma maior eficiência e precisão no combate aos crimes, também levanta preocupações quanto ao direto à privacidade e a à intimidade, diretos estes, assegurados pela Constituição Federal em seu artigo 5º, inciso X.

Por esta razão, o assunto abordado é muito recente e curioso, visto que traz diversas questões em aberto quanto a utilização da inteligência artificial junto ao processo penal, que são essenciais para determinar o uso e limites da IA perante ao ordenamento jurídico, para que não infrinja direitos humanos e apenas sirva de melhoria e avanço para o Direito Penal.

Os capítulos desse trabalho irão abordar temas como o impacto da inteligência artificial nos crimes digitais, desde os aspectos teóricos para inteirar o leitor sobre como essa tecnologia funciona, até o seu uso para a prevenção e investigação de crimes digitais. Além disso irá abordar os Avanços e os Desafios na utilização da IA em crimes digitais, utilidades como o reconhecimento facial, análise de dados de redes sociais e as propostas de regulamentação da IA. O papel da sociedade civil na discussão sobre a ética da Inteligência artificial e a IA no sistema jurídico brasileiro, também serão temas desta obra,

1. IMPACTO DA INTELIGÊNCIA ARTIFICIAL NOS CRIMES DIGITAIS

A inteligência artificial é uma ferramenta poderosa que, embora traga muitos benefícios, também está sendo explorada por criminosos para cometer delitos, tornando a segurança digital um desafio ainda maior. A utilização da IA oferece aos criminosos uma série de ferramentas sofisticadas para realizar seus atos ilícitos,

incluindo a criação de *deepfakes*, engenharia social, ataques cibernéticos automatizados, desenvolvimento de malware adaptável e disseminação de *fake news*.

A criação de *deepfakes* é uma das formas mais notórias de como a IA está sendo usada para fins maliciosos. Essa técnica permite a elaboração de vídeos e áudios falsos, substituindo a imagem ou a voz de uma pessoa por outra. Os *deepfakes* podem ser utilizados para difamar indivíduos, manipular a opinião pública em campanhas eleitorais ou até mesmo para fraudes financeiras. Além disso, a engenharia social se beneficia da IA por meio da criação de bots que imitam pessoas reais, visando obter informações confidenciais ou realizar golpes. Outra aplicação alarmante da IA é a automação de ataques cibernéticos, que se tornam mais eficientes e difíceis de detectar. O desenvolvimento de malwares mais inteligentes, capazes de se adaptar às defesas de um sistema, torna a segurança digital ainda mais vulnerável. Por fim, a IA também pode ser utilizada para gerar e disseminar *fake news* em grande escala, manipulando a opinião pública e gerando instabilidade social.

Embora a IA não "cometa" crimes de forma "voluntária", é importante ressaltar que a responsabilidade pelos crimes recai sobre os indivíduos que a utilizam. Existem diversos exemplos práticos de como a IA pode ser utilizada para realizar atividades criminosas. Um caso notável envolve o uso de *deepfakes* em campanhas políticas, onde vídeos falsos foram criados para difamar adversários ou manipular a opinião pública. Criminosos também têm utilizado *deepfakes* para extorquir pessoas, criando vídeos falsos de indivíduos em situações comprometedoras. Além disso, *deepfakes* de executivos de empresas foram usados para enganar funcionários e autorizar transferências bancárias fraudulentas. Essa forma de desinformação é extremamente eficaz, pois muitas vezes é impossível perceber que se trata de uma falsificação.

Para combater os *deepfakes*, algumas medidas podem ser adotadas, como o uso de algoritmos criptográficos para inserir *hashes* em intervalos definidos durante o vídeo, a utilização de IA e blockchain para registrar uma impressão digital à prova de adulteração para vídeos e o emprego de programas que inserem elementos digitais especialmente projetados em vídeos, com o objetivo de ocultar padrões de pixels utilizados por softwares de detecção de rosto.[1]

[1] https://www.kaspersky.com.br/resource-center/threats/protect-yourself-from-deep-fake

Diante da crescente preocupação com o uso malicioso da IA, o Brasil tem buscado legislar sobre a questão. Um exemplo é o Projeto de Lei nº 1272, de 2023, que visa criminalizar a adulteração de vídeos e áudios utilizando técnicas de inteligência artificial. O projeto propõe a adição do artigo 308-A ao Código Penal, que estabelece penas de reclusão de dois a quatro anos, além de multa, para quem adulterar arquivos de vídeo ou áudio com a intenção de divulgar notícias falsas ou prejudicar pessoas físicas ou jurídicas. Se a divulgação ocorrer na internet ou em redes sociais, a pena pode variar de quatro a oito anos de reclusão. Essa legislação representa um passo significativo no enfrentamento dos crimes digitais e busca proteger tanto os cidadãos quanto as instituições contra as práticas maliciosas que emergem com o avanço da tecnologia.

> Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, passa a viger acrescido do seguinte art. 308-A: “Adulteração maliciosa de vídeos ou áudios Art. 308-A. Adulterar arquivos de vídeo ou de áudio, mediante clonagem da voz, substituição de rosto, sincronização labial ou outra ferramenta de inteligência artificial, com a intenção de divulgar notícias falsas ou prejudicar pessoa física ou jurídica. Pena – reclusão, de dois a quatro anos, e multa. § 1º Na mesma pena incide quem faz uso do vídeo ou do áudio, sabendo ser adulterado, para divulgação de notícia falsa ou para prejudicar pessoa física ou jurídica, se a conduta não constituir crime mais grave. § 2º Se o vídeo ou o áudio é divulgado na internet, redes sociais ou outro meio análogo: Pena – reclusão, de quatro a oito anos, e multa.”[2]

A promulgação dessa legislação é um passo significativo na luta contra os crimes digitais, estabelecendo uma base legal para responsabilizar os criminosos que utilizam *deepfakes* e outras ferramentas de IA de forma maliciosa. É um reflexo da necessidade de adaptar as leis às novas tecnologias e de proteger a sociedade dos abusos que podem advir de seu uso inadequado.

Diante do panorama atual, é fundamental que a sociedade esteja atenta ao uso da inteligência artificial e busque maneiras de mitigá-la, ao mesmo tempo em que aproveita seus benefícios. As discussões em torno do papel da IA na segurança digital e as implicações legais que a cercam são essenciais para garantir que essa tecnologia seja utilizada de maneira ética e responsável.

[2] https://legis.senado.leg.br/sdleg-getter/documento?dm=9292769&disposition=inline

1.1. Aspectos Teóricos da Inteligência Artificial

A inteligência artificial é um universo que agrupa todos os campos multidisciplinar que envolvem desenvolvimento de sistemas que são capazes de realizar tarefas que muitas vezes, requerem a inteligência do ser humano. As tarefas realizadas pela IA incluem raciocínio, percepções, reconhecimento de padrões, compreensão de diferentes linguagens e resolução de problemas complexos, para isso, a IA engloba diversas técnicas para que consiga entregar aquilo que propõe, como algoritmos simples e até mesmo algoritmos e redes neurais profundas e complexas.

Kaplan e Haenlein (2019), em seus trabalhos, conceituam a inteligência artificial como a habilidade de um sistema de interpretar corretamente dados externos, aprender a partir desses dados e utilizar esses aprendizados para atingir metas e objetivos específicos por meio de uma adaptação flexível. Os autores Poole e Mackworth (2017) definem inteligência artificial como um campo que estuda a síntese e a análise de agentes computacionais que agem de maneira inteligente. Em Russell e Norvig (2020), os autores definem o conceito de inteligência artificial como o estudo de agentes (inteligentes) que recebem preceitos do ambiente e agem.

É possível observar diferentes tipos de inteligência artificial, a que realiza tarefas mais especificas, tais quais reconhecimento de fala e tradução para outros idiomas, nesse caso, a IA não possui a consciência e entendimento para além do que foi solicitado à ela.

Além desta, temos a IA que possui a capacidade de interpretar, aprender e aplicar o conhecimento de forma parecida com os humanos, mas de forma mais rápida e mais dinâmica, permitindo também, que sistemas técnicos lidem com o problema e resolva, agindo com a maior eficácia para atingir o objetivo.

Entendendo a Inteligência artificial é possível observar que o seu maior objetivo é busca simular o raciocínio dos seres humanos em máquinas, a fim de solucionar problemas de acordo com o comportamento humano.

Sabendo da importância, e da possível utilização da inteligência artificial, é possível também, utilizá-la no direito penal, em atividades como sistema de vigilância com reconhecimento fácil e análise de comportamentos suspeitos, para alertar as

autoridades competentes, para prevenir um potencial crime, ou até mesmo o uso de algoritmos para decisões judiciais.

A inteligência artificial tem revolucionado diversos setores, inclusive o jurídico. Com o aumento da quantidade de dados disponíveis, o direito penal e constitucional se beneficia da capacidade da IA em processar e analisar informações de maneira rápida e eficiente

No artigo “A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and IA” (Um Direito a Inferências Razoáveis: Repensando a Lei de Proteção de Dados na era dos Big Data e IA) de Sandra Wachter e Brent Mittelstadt, publicado em 05 de outubro de 2018, analisa de que forma os algoritmos da Inteligência Artificial podem ser aplicados para prever os comportamentos de possíveis criminosos e fazer uma possível sentença judicial. Este artigo traz também, a necessidade da IA garantir que o sistema não traga questões como desigualdades, preconceitos determinando um padrão de pessoa para o potencial crime.

No Direito Penal, aumenta cada vez mais a aplicação da IA, a qual oferece ferramentas capazes de melhorar a eficácia e eficiência do sistema de justiça criminal no Brasil. Essa integração da inteligência artificial no direito penal não se limita apenas à vigilância e à análise preditiva, a IA pode desempenhar um papel crucial na otimização dos processos judiciais, permitindo uma triagem mais eficiente dos casos e a identificação de prioridades em meio a uma demanda crescente. Contudo, a utilização dessa ferramenta levanta diversas questões relacionadas à ética e a aplicação jurídica, que trataremos no decorrer desta pesquisa.

1.2. Fraudes de Identidade e o Papel da Inteligência Artificial e casos de crimes implicando Inteligência Artificial

A *Sumsub*, uma plataforma internacional de verificação que protege cada etapa da jornada do usuário, lançou recentemente o *Sumsub Identity Fraud Report 2023*. Este relatório, agora em sua terceira edição, analisa mais de dois milhões de tentativas de fraude em 224 países e territórios, abrangendo 28 segmentos. Embora o Brasil tenha apresentado uma taxa relativamente baixa de fraude de identidade em

comparação com os demais países da América Latina, ocupando a 20ª posição entre as nações analisadas, o volume de fraudes mais sofisticadas, impulsionadas pela inteligência artificial (IA), foi o mais alto da região.

O relatório destaca um aumento global de dez vezes no número de *deepfakes* detectados em todos os setores em apenas um ano. As variações regionais são notáveis: enquanto a América do Norte registrou um aumento impressionante de 1.740% no uso de *deepfakes*, a média na América Latina foi de 410%, a mais baixa entre todas as regiões do mundo. No entanto, no Brasil, o crescimento de *deepfakes* entre 2022 e 2023 foi o maior da região, com um aumento de 830%. Isso ilustra um quadro preocupante, onde o país, apesar de ter uma taxa de fraude de identidade mais baixa, enfrenta uma escalada significativa em fraudes sofisticadas.

Dentre os dados revelados, a Espanha foi identificada como o país mais atacado por *deepfakes*, com a ocorrência de um ataque a cada dez que acontecem globalmente. O relatório também revelou que o passaporte dos Emirados Árabes Unidos foi o documento mais falsificado no mundo, e que a mídia online se tornou o segmento mais explorado pelos fraudadores.

Pavel Kalaydin (2023), chefe de IA e machine learning da *Sumsub*, enfatiza que os fraudadores, dependendo de suas habilidades, podem tentar enganar os sistemas de verificação de diversas maneiras. As falsificações de documentos de identidade estão se tornando cada vez mais sofisticadas, exigindo um esforço maior para distinguir um documento falso de um original. De acordo com Guilherme Terrengui (2023), *head* de negócios em desenvolvimento na América Latina e Ibéria, apesar de todos os países latino-americanos terem registrado um aumento nas fraudes, a situação no Brasil, que quase duplicou (crescendo 1,8 vezes), ainda se manteve a mais baixa da região.

Terrengui também observa que, para o próximo ano, o Brasil deve concentrar esforços no combate à fraude impulsionada pela IA e na implementação de sistemas de prevenção de fraudes de ciclo completo. Isso é fundamental, pois o país teve quase tantos casos de *deepfake* quanto todos os outros países latino-americanos juntos, principalmente nos setores de criptomoedas, *fintechs e iGaming*.

À medida que a inteligência artificial deve se tornar o foco principal das regulamentações em 2024, a segurança da IA está se tornando parte integrante das operações empresariais. O relatório da *Sumsub* não apenas fornece dicas de prevenção de fraudes baseadas em IA, mas também oferece uma visão geral das regulamentações em andamento relacionadas à inteligência artificial. Os leitores encontrarão um resumo dos principais esforços para regular as *deepfakes* em quatro jurisdições-chave: China, União Europeia, Reino Unido e Estados Unidos.

Terrengui também aponta que websites de notícias, serviços de streaming, plataformas sociais e publicidade digital, que compõem o segmento de meios de comunicação online, foram os maiores alvos de fraudadores. Entre 2021 e 2023, esse setor registrou o maior aumento (274%) na taxa de fraude de identidade em todo o mundo. Para combater o aumento dos ataques no setor de mídia online, especialistas acreditam que as empresas devem implementar regras mais rigorosas, como a identificação obrigatória dos usuários. Essa abordagem é essencial para mitigar os riscos associados à crescente ameaça de fraudes baseadas em inteligência artificial e proteger tanto os consumidores quanto as instituições contra os impactos dessas práticas maliciosas.

Embora a inteligência artificial (IA) em si não possua vontade ou intenção, suas aplicações têm levantado preocupações sobre a possibilidade de utilização em atividades criminosas que podem parecer, à primeira vista, "voluntárias". Isso se deve ao fato de que sistemas de IA, especialmente aqueles com capacidade de aprendizado autônomo, podem ser programados ou treinados para realizar ações que resultam em violações legais ou éticas. Aqui estão alguns exemplos de como a IA pode estar envolvida em crimes de forma que poderia ser interpretada como "voluntária".

Um dos casos mais discutidos envolve a utilização de sistemas de IA para automatizar fraudes financeiras. Por exemplo, algoritmos de machine learning podem ser usados para desenvolver software que identifica vulnerabilidades em sistemas de segurança financeira, permitindo que criminosos realizem transferências não autorizadas ou manipulem dados financeiros. Embora a IA não tenha a capacidade de agir por conta própria, os resultados de suas operações podem causar prejuízos

financeiros significativos a indivíduos e empresas, levantando questões sobre responsabilidade e intenção.

Outro exemplo é a criação de *deepfakes*, onde a IA é utilizada para gerar vídeos ou áudios que imitam pessoas reais de maneira convincente. Essa técnica tem sido empregada em situações de extorsão, onde criminosos produzem vídeos falsos de uma pessoa em situações comprometedores para coagi-la a pagar quantias em dinheiro. Embora o software de *deepfake* em si não "decida" criar esses vídeos, a intenção por trás de sua utilização é claramente criminosa, e a capacidade de a IA produzir esses conteúdos de maneira rápida e convincente intensifica a gravidade do problema.

Um dos cenários de potencial aplicação de viés discriminatório pelos algoritmos que se utilizam de inteligência artificial é no campo da persecução penal.

No trabalho de Yarovenko, Shapovalova e Ismagilov (2021), os autores destacam as possíveis consequências problemáticas do uso de ferramentas modernas de hardware e de software e dos métodos de fixação de penas e de reconhecimento facial pelo Estado. Conforme o estudo destaca, o reconhecimento facial pode auxiliar as autoridades na localização de pessoas procuradas e na confirmação de autoria e de materialidade de crimes, porque permite objetivar e otimizar a produção da prova. Nesse sentido, a inteligência artificial, em conjunto com outras técnicas, permite analisar características, construir perfis e revelar relacionamentos entre diversas variáveis e atores de delitos.

No trabalho de Catiane Steffen, intitulado "A Inteligência Artificial e o Processo Penal: A Utilização da Técnica na Violação de Direitos" (2022), aborda uma das preocupações mais relevantes no uso de inteligência artificial (IA) no campo da persecução penal: o risco de viés discriminatório. Baseando-se no estudo de Yarovenko, Shapovalova e Ismagilov (2021), o texto enfatiza os potenciais efeitos problemáticos do uso de tecnologias modernas, como softwares de reconhecimento facial e métodos de fixação de penas. Esses algoritmos, ao serem empregados pelo Estado, podem reforçar desigualdades e gerar decisões enviesadas que violam direitos fundamentais, especialmente em um contexto em que o próprio treinamento dos algoritmos pode reproduzir preconceitos sociais. Assim, o alerta da autora é

crucial para refletir sobre os limites e as consequências da implementação dessas ferramentas em um campo tão sensível como o penal, exigindo mecanismos rigorosos de controle e revisão para mitigar esses riscos.

Além disso, a utilização de *chatbots* e assistentes virtuais baseados em IA para realizar fraudes, como *phishing*, tem crescido. Esses sistemas podem ser programados para interagir com usuários de maneira a enganar pessoas, levando-as a fornecer informações pessoais ou financeiras. Embora a IA não tenha vontade própria, as ações resultantes podem ser vistas como voluntárias, na medida em que são projetadas para enganar e prejudicar.

Por último, a utilização de veículos autônomos, que incorporam IA, levanta preocupações éticas e legais. Em casos de acidentes causados por falhas no sistema de IA, a questão de responsabilidade se torna complexa. Se um veículo autônomo causar um acidente por falha em seu sistema de decisão, isso levanta questões sobre a intencionalidade do "comportamento" do veículo, mesmo que a IA não tenha consciência ou intenção.

Esses exemplos demonstram como a IA, embora não tenha vontade própria, pode ser manipulada por indivíduos com intenções maliciosas, resultando em atividades criminosas que desafiam a compreensão tradicional de responsabilidade legal e ética. A discussão sobre a "vontade" da IA nas suas ações levanta questões importantes para legisladores, pesquisadores e desenvolvedores, especialmente à medida que a tecnologia continua a evoluir e se integrar em mais aspectos da vida cotidiana.

1.3. Uso de inteligência artificial na prevenção e investigação de crimes digitais.

A IA começou a ser utilizada em 2010, na prevenção e detecção de ameaças, com o surgimento de ataques cibernéticos cada vez mais sofisticados, a Inteligência Artificial se tornou fundamental na prevenção e detecção de ameaças cibernéticas. Ela pode analisar rapidamente grandes conjuntos de dados para identificar comportamentos maliciosos e ameaças em tempo real (GAIDIS, 2023).

A inteligência artificial (IA) tem se mostrado uma ferramenta poderosa na luta contra os crimes digitais, oferecendo uma gama de estratégias e abordagens que ajudam na identificação, prevenção e investigação de atividades criminosas no ambiente cibernético. A capacidade da IA de processar grandes volumes de dados rapidamente e identificar padrões complexos a torna uma aliada valiosa nesse esforço.

Uma das principais aplicações da IA na segurança cibernética é a detecção de ameaças em tempo real. Os algoritmos de IA podem analisar o tráfego de rede e identificar comportamentos anômalos que sugerem um ataque em andamento. Essa capacidade de resposta rápida é crucial, pois permite que as organizações reajam de forma imediata a possíveis invasões, minimizando os danos. Além disso, a análise de malware é outro aspecto importante, onde a IA pode ser utilizada para examinar o código malicioso, identificar novas variantes e desenvolver defesas mais eficazes. A autenticação biométrica, como o reconhecimento facial e de voz, também é aprimorada por meio da IA, tornando esses sistemas mais seguros e confiáveis.

O gerenciamento de incidentes é outro campo onde a IA demonstra seu valor. Ela pode automatizar tarefas relacionadas à resposta a incidentes, como a análise de logs e a identificação da raiz do problema, permitindo que as equipes de segurança concentrem seus esforços em tarefas mais estratégicas. Outro ponto relevante é a previsão de ataques, onde modelos de machine learning podem ser treinados para identificar padrões que indicam a probabilidade de um ataque, permitindo que as empresas se preparem antecipadamente para possíveis ameaças.

A análise de dados é um dos pilares da segurança cibernética baseada em IA. Ao examinar grandes volumes de dados, os algoritmos de IA conseguem identificar padrões e correlações que seriam difíceis de detectar pela análise humana. Exemplos dessa utilização incluem a análise de logs de sistemas, redes e aplicativos para identificar atividades suspeitas e detectar intrusões, além da análise de e-mails para reconhecer tentativas de *phishing* e outras formas de engenharia social. A IA também é utilizada para monitorar redes sociais, ajudando a identificar a propagação de desinformação e outras ameaças.

A detecção de padrões é outra área onde a IA se destaca. Ela é capaz de identificar padrões complexos em grandes conjuntos de dados, como comportamentos que podem indicar a presença de um intruso em uma rede ou padrões de tráfego anômalos que podem sugerir um ataque em andamento. Através da identificação desses padrões, a IA pode auxiliar na prevenção de ataques, bloqueando tráfego malicioso e isolando sistemas comprometidos, evitando assim a propagação de malware.

A capacidade da IA de analisar grandes volumes de dados em tempo real permite identificar padrões suspeitos e comportamentos anômalos em sistemas de redes e plataformas online. Além disso, algoritmos de aprendizado de máquina conseguem aprimorar constantemente suas habilidades de detecção, adaptando-se às novas táticas dos criminosos cibernéticos (PORTA, 2023).

Além disso, a IA pode ser utilizada para atualizar sistemas de defesa em tempo real, reconhecendo novas ameaças e implementando contramedidas de forma rápida e eficiente. Em suma, a IA está revolucionando a forma como empresas e agências governamentais combatem os crimes digitais. A automação de tarefas, a identificação de ameaças em tempo real e a análise de grandes volumes de dados possibilitam que as organizações se protejam de maneira mais eficaz contra os ataques cibernéticos.

2. DESAFIOS E AVANÇOS NA UTILIZAÇÃO DA IA EM CRIMES DIGITAIS.

À medida que a utilização de inteligência artificial na segurança cibernética avança, surgem novos desafios e oportunidades. Sistemas de hacking autônomos, por exemplo, de acordo com o IBSEC[3] demonstram a capacidade de realizar ataques cibernéticos de forma autônoma, utilizando técnicas como LFI (*Local File Inclusion*), CSRF (*Cross-Site Request Forgery*), XSS (*Cross-Site Scripting*) e SQL *Injection*. Essas tecnologias são testadas em ambientes controlados, como *sandboxes*, para validar sua eficácia, o que torna a defesa contra esses ataques ainda mais complexa.

O uso de redes neurais e aprendizado de máquina também está em evolução, sendo empregado para detectar e explorar vulnerabilidades em sistemas de segurança. A automação de testes de penetração, por meio da integração de modelos de LLM

(*Large Language Model*) com ferramentas como Kali Linux, facilita a detecção contínua e eficiente de falhas de segurança. Além disso, agentes LLM são utilizados para interagir com sistemas operacionais, realizar testes de penetração e mitigar ameaças, simulando ataques e fortalecendo as defesas cibernéticas.

A implementação de leis de escala para modelos de linguagem neural sugere que o desempenho dos sistemas de segurança melhora com o aumento do tamanho dos modelos, permitindo a análise de grandes volumes de dados e a identificação de padrões anômalos. Monitorar propriedades emergentes em modelos de IA é essencial para detectar novas capacidades de ataque, fornecendo insights valiosos para reforçar as defesas cibernéticas.

Por outro lado, a integração de inteligência artificial em malwares cria novas ameaças que exigem defesas mais robustas. A análise dessas integrações é crucial para antecipar ataques e desenvolver contramedidas efetivas. Avaliar e reforçar os controles de egresso é igualmente importante para identificar e gerenciar chamadas de saída para serviços LLM, prevenindo o uso não autorizado de recursos de rede para atividades maliciosas.

Além disso, ferramentas que simulam ações de operadores de ameaças reais, utilizando automação e IA, ajudam a preparar as equipes de segurança para cenários de ataque realistas, aumentando a eficácia das respostas. O treinamento e a conscientização em cibersegurança se tornam fundamentais para a formação contínua de profissionais e usuários finais sobre as ameaças de segurança cibernética e as melhores práticas para mitigá-las. Este tipo de treinamento contribui para aumentar a resiliência contra-ataques de engenharia social e outras ameaças comuns.

Em conclusão, a utilização da inteligência artificial na prevenção e investigação de crimes digitais representa uma revolução na forma como as organizações abordam a segurança cibernética. Embora existam desafios significativos a serem enfrentados, as oportunidades para melhorar a segurança e responder a ameaças em tempo real são imensas, tornando a IA uma aliada indispensável na luta contra os crimes digitais.

O uso da inteligência artificial (IA) na prevenção e investigação de crimes digitais é um campo em rápido crescimento, mas não sem seus desafios éticos.

Embora a IA traga benefícios significativos, como a capacidade de processar grandes volumes de dados e identificar padrões complexos, a sua aplicação suscita preocupações em várias áreas, incluindo privacidade, responsabilidade e transparência. Portanto, é essencial discutir esses desafios para garantir que a tecnologia seja utilizada de forma responsável e benéfica para a sociedade.

Um dos principais desafios éticos relacionados ao uso da IA em crimes digitais é a questão da privacidade. Para que a IA funcione eficazmente, ela requer grandes volumes de dados, o que pode resultar em uma coleta massiva de informações. Essa coleta indiscriminada pode violar a privacidade dos indivíduos, especialmente quando se lida com dados pessoais sensíveis. Além disso, a vigilância em massa, impulsionada pela IA, pode criar um ambiente onde as liberdades individuais são restringidas em nome da segurança. O uso de IA para a criação de perfis psicológicos detalhados pode levar a manipulações ou discriminações, levantando ainda mais preocupações éticas.

Outro aspecto crítico é a questão da responsabilidade. Muitos algoritmos de IA operam como "caixas pretas", onde o processo de tomada de decisão é complexo e opaco. Isso dificulta a atribuição de responsabilidade em casos de erros ou abusos. Além disso, os vieses algorítmicos representam um grande risco; se os dados utilizados para treinar os algoritmos forem tendenciosos, isso resultará em decisões injustas, perpetuando desigualdades. À medida que as máquinas se tornam mais autônomas, a responsabilidade por suas ações torna-se uma questão complexa e debatida.

A transparência também é um aspecto fundamental nesse contexto. A falta de clareza sobre como os algoritmos de IA operam dificulta a identificação e correção de vieses e erros. Além disso, a concentração do desenvolvimento e controle da IA em mãos de poucas organizações pode levar a um desequilíbrio de poder e à criação de sistemas que não são auditáveis, tornando a supervisão e a responsabilidade mais difíceis de alcançar.

Outros desafios éticos incluem a manipulação da opinião pública por meio da disseminação de notícias falsas, o que pode minar a confiança nas instituições, e o

desenvolvimento de armas autônomas, que levanta questões sobre a ética de permitir que máquinas tomem decisões de vida ou morte.

Para enfrentar esses desafios éticos e garantir que a IA seja utilizada de forma responsável, é necessário estabelecer algumas diretrizes. A transparência deve ser um pilar central, com algoritmos de IA sendo auditáveis e claros em seu funcionamento. A responsabilidade deve ser claramente definida, estabelecendo quem é responsável pelas ações dos sistemas de IA. A proteção da privacidade dos indivíduos é imprescindível, assim como o compromisso em evitar discriminações.

Por fim, uma colaboração ampla entre pesquisadores, desenvolvedores, governos e a sociedade civil é crucial para desenvolver normas e padrões éticos que guiem a utilização da IA. Em resumo, embora a IA ofereça um potencial extraordinário para melhorar a segurança e a eficiência na luta contra crimes digitais, é fundamental que seu uso seja acompanhado por uma reflexão ética profunda, visando o bem-estar de todos.

O uso da inteligência artificial na segurança pública e na justiça criminal já resultou em vários casos que geraram debates éticos significativos. Entre eles, destacam-se:

2.1. Reconhecimento Facial

As tecnologias que utilizam de características biométricas englobam identificação baseada em aspectos fisiológicos (Face, digitais, geometria dos dedos e das mãos, irís, retina, etc.) e também baseada em traços comportamentais (forma de andar, padrão de digitação e assinaturas). (NUNES, 2016, p.21)

Os sistemas de reconhecimento facial têm sido amplamente utilizados por agências de segurança para identificar suspeitos em multidões. Embora possam ser eficazes em alguns contextos, esses sistemas levantam preocupações sobre a vigilância em massa.

A possibilidade de erros nos algoritmos pode levar à detenção de pessoas inocentes, exacerbando questões de justiça social e discriminação racial. Estudos mostram que esses sistemas tendem a ser menos precisos em identificar pessoas de

cor, o que pode resultar em preconceitos institucionais, visto que detecção facial é realizada com base em vários estímulos: cor de pele, formato do rosto ou cabeça, aparência da face, ou a combinação destes

2.2. Algoritmos de Previsão de Crimes

Algumas cidades adotaram algoritmos para tentarem reconhecer o local de maior incidência de crimes, na esperança de direcionar os recursos policiais de forma mais eficiente.

No entanto, essas ferramentas têm sido criticadas por reforçar preconceitos raciais e discriminar comunidades marginalizadas. A utilização de dados históricos, que muitas vezes contêm viés, pode perpetuar ciclos de vigilância desproporcional e criminalização de grupos já vulneráveis.

2.3. Análise de Dados de Redes Sociais

Agências de inteligência têm utilizado a análise de dados de redes sociais para identificar potenciais terroristas ou criminosos. Embora essa abordagem possa ajudar na identificação de ameaças, levanta sérias questões sobre a privacidade e a liberdade de expressão. A coleta e análise de informações pessoais sem o consentimento dos indivíduos podem resultar em violações dos direitos humanos e em um clima de medo e censura.

2.4. Propostas de Regulamentação para a IA

Diante dos desafios éticos apresentados pelo uso da Inteligência artificial, diversos países e organizações internacionais estão propondo regulamentações para garantir seu desenvolvimento e uso responsáveis, a fim de evitar discriminações, preconceitos, erros no judiciário e outros erros que podem ser irreparáveis. Nas propostas em estudos estão os seguintes quesitos:

a) Transparência

Uma das propostas mais urgentes é exigir que os sistemas de IA sejam transparentes, permitindo que se compreenda todo o processo para chegar a

determinadas decisões. Isso inclui a disponibilização de informações sobre os dados utilizados e os critérios que guiam as decisões dos algoritmos.

b) Responsabilidade

É fundamental estabelecer mecanismos que responsabilizem desenvolvedores e usuários de IA por suas ações. Isso envolve a criação de marcos legais que definam claramente as responsabilidades em casos de erro ou abuso, garantindo que as vítimas possam buscar reparação.

c) Não Discriminação

Proibir a criação e o uso de sistemas de IA que discriminem indivíduos ou grupos é uma proposta essencial. Isso requer uma avaliação rigorosa dos algoritmos e dos dados utilizados para evitar preconceitos raciais, de gênero ou socioeconômicos.

d) Privacidade

Garantir a proteção dos dados pessoais utilizados para treinar e alimentar sistemas de IA é crucial. Regulamentações devem ser implementadas para salvaguardar a privacidade dos indivíduos e impedir a coleta indevida de dados.

Sendo necessário a correlação com a Lei nº 13.709/ 20218, proteção de dados pessoais (LGPD), uma vez que está lei busca a proteção de todos os dados pessoais e, muitas vezes, para treinar e alimentar sistemas de inteligência artificial é inevitável o uso de dados próprios.

e) Auditoria

Estabelecer mecanismos de auditoria é essencial para garantir que os sistemas de IA sejam utilizados de forma ética, responsável e conforme todos os procedimentos de regulamentação. Auditorias regulares e independentes podem ajudar a identificar e corrigir vieses, além de garantir a conformidade com as regulamentações propostas.

3. O PAPEL DA SOCIEDADE CIVIL NA DISCUSSÃO SOBRE A ÉTICA DA IA

Como já observado, a inteligência artificial emergiu de forma transformadora na sociedade moderna em diversos aspectos, desde as resoluções mais simples até a as mais complexas e criação de mecanismos.

O uso da Inteligência Artificial também pode levar à discussões sobre questões éticas, que geralmente envolvem: o uso ou reuso de dados em contextos, momentos e para propósitos diferentes dos quais ele foi inicialmente consentido (Herschel & Miori, 2017); a ausência de transparência, veracidade e clareza dos termos de consentimento (Weinhardt, 2020), e a falta de entendimento único com relação ao que se constitui um dado público, diferenciando-o visivelmente de um dado privado (Weinhardt, 2020).

A sociedade civil desempenha um papel fundamental na discussão sobre a ética da IA contribuindo para um debate mais equilibrado e inclusivo. Como forma de garantia a ética, as seguintes ações são cruciais:

3.1. Aumentar a Conscientização

Organizações da sociedade civil, pesquisadores e cidadãos podem promover a conscientização sobre os riscos e benefícios da IA. Informar o público sobre como a IA pode afetar suas vidas é essencial para um debate público mais informado e para a pressão por regulamentações adequadas.

Além disso, essa grande necessidade de informação, se da pelo fato de que diversas pessoas utilizam a inteligência artificial para apreender dados, divulgação de dados pessoais daqueles que apenas tentam utilizar a IA para soluciona problemas.

Sempre que possível, o utilizados dos dados pessoais das pessoas deve obter o consentimento das pessoas em estudo em relação ao uso de seus dados. Consentimento é entendido como a “expressão livre, específica, inequívoca e informada da vontade do titular, por meio da qual ele aceita e autoriza o tratamento dos dados pessoais que lhe correspondam” (Rede Ibero-americana de Proteção de Dados, 2017).

3.2. Participar de Processos de Tomada de Decisão

A participação ativa em processos de tomada de decisão é vital para influenciar a criação de políticas públicas e regulamentações relacionadas à IA. A sociedade civil pode fornecer insights valiosos e experiências do mundo real que informam o desenvolvimento de normas éticas.

3.3. Desenvolver Alternativas

Propor soluções tecnológicas e sociais que minimizem os riscos e maximizem os benefícios da IA é uma tarefa importante. A sociedade civil pode contribuir com inovações que priorizem a ética e os direitos humanos, ajudando a moldar o futuro da tecnologia de forma mais responsável, Responsabilidade é entendida como prontidão para prestar contas sobre suas próprias ações ou atividades, criações ou pessoas sob sua responsabilidade, aceitando as consequências desses atos (Oliver, 1994)

3.4. Monitorar o Uso da IA

Acompanhar o desenvolvimento e o uso da IA é crucial para denunciar abusos e violações dos direitos humanos. Organizações da sociedade civil podem desempenhar um papel de vigilância, garantindo que a tecnologia seja usada para o bem comum e não como uma ferramenta de opressão.

4. IA NO SISTEMA JURÍDICO BRASILEIRO: OPORTUNIDADES E DESAFIOS

A introdução de IA no sistema jurídico brasileiro tem potencial para transformar significativamente a forma como a justiça é administrada. Um dos principais benefícios que a IA pode proporcionar é a celeridade processual. Com sistemas capazes de analisar grandes volumes de documentos em curto espaço de tempo, a expectativa é que a carga de trabalho dos juízes e advogados seja aliviada, permitindo que se concentrem em aspectos mais estratégicos e interpretativos dos casos.

À medida que a inteligência artificial (IA) se torna cada vez mais sofisticada e acessível, o desafio de combater seu uso malicioso em crimes digitais cresce proporcionalmente. Este capítulo explora as estratégias de combate a esses crimes, as expectativas em relação às IAs na prevenção de problemas e as considerações sobre os investimentos necessários para implementar soluções eficazes.

Importante destacar que são necessárias estratégias de combate ao uso malicioso, estratégias tais como: Detecção Avançada de *Deepfakes*: O desenvolvimento de algoritmos capazes de identificar conteúdo manipulado por IA é crucial. Empresas e pesquisadores estão trabalhando em técnicas que analisam inconsistências sutis em vídeos e áudios, como padrões de piscadas não naturais ou micro expressões faciais inconsistentes; Autenticação Multifatorial Aprimorada: Para combater ataques de *phishing* e engenharia social potencializados por IA, é essencial implementar sistemas de autenticação mais robustos. Isso pode incluir o uso de biometria avançada, tokens de segurança física e análise comportamental do usuário.; Sistemas de Detecção de Anomalias baseados em IA: Implementação de sistemas de monitoramento em tempo real que utilizam IA para identificar padrões de comportamento anômalos em redes e sistemas, permitindo a detecção precoce de atividades maliciosas e; Educação e Conscientização: Programas de treinamento abrangentes para usuários finais, funcionários e executivos sobre as ameaças emergentes relacionadas à IA e as melhores práticas de segurança cibernética.

Com essa visão da IA, é possível visualizar e criar expectativas na prevenção de problemas, tais quais: Análise Preditiva de Ameaças: Espera-se que as IAs sejam capazes de analisar vastos conjuntos de dados para prever potenciais ameaças antes que elas se concretizem, permitindo uma abordagem mais proativa na segurança cibernética.; Resposta Automatizada a Incidentes: Sistemas de IA que podem detectar, classificar e responder a incidentes de segurança em tempo real, reduzindo significativamente o tempo de resposta e mitigação de danos; Evolução Contínua das Defesas: IAs que aprendem e se adaptam constantemente a novas ameaças, atualizando automaticamente os sistemas de defesa para proteger contra táticas de ataque em evolução; Detecção de Vulnerabilidades em Código: Ferramentas de IA que podem analisar código-fonte em busca de vulnerabilidades de segurança, ajudando os desenvolvedores a criar software mais seguro desde o início e; Simulação Avançada de Ataques: IAs capazes de simular ataques complexos em ambientes controlados, permitindo que as organizações testem e aprimorem suas defesas de forma mais eficaz.

4.1. Otimização de Processos e Redução de Prazos:

Como mencionado por Heloisa Rodrigues da Rocha, a Advocacia-Geral da União (AGU) e tribunais superiores, como o STJ e o STF, já estão implementando ferramentas de IA para a classificação de processos e localização de documentos importantes para os casos. Isso se traduz em uma redução significativa dos prazos processuais, com maior agilidade no trâmite dos processos. Além disso, a IA pode auxiliar na análise de jurisprudência, identificando rapidamente os precedentes mais relevantes para um determinado caso, o que é crucial em um sistema como o brasileiro, onde a uniformidade de decisões é um princípio fundamental.

4.2. A IA e a Redução de Erros Judiciais:

Outro aspecto promissor é a capacidade da IA de ajudar a minimizar erros judiciários. Por meio da análise precisa e imparcial de dados, a IA pode identificar inconsistências em depoimentos, provas ou documentos, contribuindo para uma decisão mais justa. Além disso, tecnologias como o machine learning podem ser treinadas para detectar padrões de comportamento ou de fraude que, de outra forma, passariam despercebidos por humanos.

> A implementação da IA no sistema de justiça criminal oferece tanto oportunidades quanto desafios significativos. Embora a tecnologia tenha o potencial de melhorar a eficiência e a precisão das operações policiais e judiciais, é fundamental que se abordem os vieses e as injustiças inerentes ao uso desses sistemas. A prudência e a ética devem guiar a adoção de IA, com uma ênfase contínua na eliminação de preconceitos e na promoção da justiça equitativa. Para evitar a perpetuação de um sistema de justiça racista e discriminatório, é essencial que as tecnologias de IA sejam desenvolvidas e implementadas com uma compreensão profunda das suas implicações sociais. A transparência, a responsabilidade e a inclusão de diversas perspectivas no processo de desenvolvimento são fundamentais para garantir que a

> IA contribua para um sistema de justiça mais justo e humanizado.[3]

O trecho citado aborda de forma crítica a implementação da inteligência artificial (IA) no sistema de justiça criminal, destacando tanto as oportunidades quanto os desafios éticos que acompanham essa adoção. Embora a tecnologia possa trazer maior eficiência e precisão às operações policiais e judiciais, é crucial reconhecer que os sistemas de IA, se mal implementados, podem replicar e até intensificar preconceitos e injustiças presentes nos dados utilizados para seu treinamento.

O alerta para os vieses algorítmicos é especialmente pertinente em um contexto onde o sistema de justiça já enfrenta críticas por ser seletivo e, muitas vezes, racista. Esses algoritmos, se baseados em dados históricos permeados por discriminação racial e social, podem perpetuar essas desigualdades, resultando em decisões prejudiciais a grupos marginalizados. Portanto, o texto enfatiza que a adoção de IA deve ser guiada pela ética e pela prudência, buscando eliminar preconceitos e promover uma justiça equitativa.

Para que isso aconteça, o desenvolvimento dessas tecnologias deve ser feito de forma transparente e com responsabilidade, com a inclusão de perspectivas diversas, especialmente aquelas de grupos que historicamente sofreram com o sistema de justiça. Somente com essa abordagem inclusiva e consciente será possível garantir que a IA contribua para um sistema de justiça mais justo e humanizado, em vez de agravar as desigualdades já existentes.

4.3. O Risco de Viés Algorítmico:

Por outro lado, conforme argumentado por críticos do uso de IA no direito, existe um risco significativo de viés algorítmico. Se os sistemas de IA forem treinados com base em dados históricos que contenham preconceitos, como discriminações raciais ou sociais, essas falhas podem ser replicadas nas decisões automatizadas. Um exemplo disso é o uso de algoritmos preditivos nos EUA para auxiliar na

---

[3] Vista do Desafios éticos ao uso da inteligência artificial no sistema de justiça criminal: https://ibccrim.org.br/?gad_source=1&gclid=Cj0KCQiAuou6BhDhARIsAIfgrn5J5lKOjkQf8rPilnF3Rsb9-LMDRK4IhUT7_9b92-IXsV0jzIcFzWwaAkBUEALw_wcB

determinação de penas e na concessão de fianças, onde já se verificou que esses sistemas tendem a discriminar minorias raciais. No Brasil, onde o sistema penal já enfrenta críticas por ser seletivo, a implementação de IA sem as devidas salvaguardas pode agravar ainda mais as desigualdades.

4.4. IA e a Autonomia do Judiciário:

Outra questão relevante é a possível redução da autonomia do magistrado frente ao uso de sistemas de IA. Embora essas ferramentas possam auxiliar na coleta e organização de informações, a decisão final deve permanecer sob o controle humano. Como apontado por acadêmicos, confiar cegamente em algoritmos para decisões críticas, como a sentença de um réu, pode representar uma ameaça ao princípio da liberdade de convencimento do juiz, que é basilar no direito brasileiro. Além disso, existe o perigo de uma padronização excessiva, que pode desconsiderar nuances importantes de cada caso individual.

4.5. Transparência e Controle:

O uso da IA pode afetar negativamente não só a nossa segurança e liberdade, mas uma ampla gama de outros Direitos Humanos, especialmente

Quando as decisões são tomadas com base em sistemas de IA de alto risco, sem que exista, transparência e explicabilidade, que são os dois dos requisitos fundamentais para uma conceção de IA ética, sendo esta entendida como tendo em consideração as normas morais, os valores e a salvaguarda dos Direitos Humanos, de acordo com os critérios expressos no relatório elaborado pelo Grupo Independente de Peritos de Alto Nível sobre a IA “Orientações éticas para uma IA de confiança”, podem afetar negativamente a segurança e a liberdade dos Direitos Humanos. (Comissão Europeia, 2019).

Para garantir que a IA seja usada de maneira justa e eficaz no direito penal, é fundamental que haja transparência nos processos e que os algoritmos utilizados sejam auditáveis e passíveis de escrutínio público. É importante que as partes envolvidas no processo tenham o direito de entender como a IA chegou a determinadas conclusões e que possam contestar eventuais decisões com base nessas tecnologias.

4.6. As Legal Techs no Brasil:

No Brasil, as legal techs, empresas focadas no desenvolvimento de tecnologias jurídicas, já estão trabalhando em soluções para otimizar o trabalho de advogados e tribunais. Como destacado por Rocha (2017), algumas dessas empresas já oferecem ferramentas que analisam o mérito de petições e resumem os principais pontos das alegações, além de fornecer jurisprudências relacionadas aos casos. Embora essas tecnologias representem um avanço importante, é necessário cuidado na sua adoção, pois a automação excessiva pode prejudicar o caráter humano das decisões judiciais.

A incorporação de IA no sistema jurídico brasileiro pode trazer inúmeros benefícios, desde a aceleração de processos até a redução de erros judiciais. No entanto, é essencial que a implementação dessas tecnologias seja feita com cautela, levando em conta os riscos de viés algorítmico, a manutenção da autonomia judicial e a necessidade de transparência e controle sobre os algoritmos utilizados. O futuro da justiça brasileira dependerá de um equilíbrio cuidadoso entre a inovação tecnológica e a preservação dos princípios fundamentais do direito.

A experiência de outros países, como os Estados Unidos, pode servir de alerta e inspiração, mostrando que, embora a IA tenha o potencial de melhorar o sistema de justiça, sua adoção deve ser acompanhada de um debate profundo sobre ética, responsabilidade e justiça social. Assim, o Brasil tem a oportunidade de moldar um futuro no qual a IA trabalhe em benefício de todos, garantindo uma justiça mais eficiente e acessível, sem abrir mão dos direitos e garantias fundamentais.

4.7. IA na Prevenção e Investigação de Crimes Digitais

a IA tem se mostrado uma aliada poderosa na luta contra os crimes digitais. Instituições financeiras, em particular, têm sido pioneiras no uso de IA para detecção de fraudes.

O HSBC, por exemplo, implementou um sistema de IA desenvolvido pela startup Quantexa para combater a lavagem de dinheiro. Em 2018, o banco relatou que o sistema ajudou a identificar 680 milhões de dólares em transações potencialmente fraudulentas que haviam passado despercebidas pelos métodos tradicionais de detecção.

Na área de análise de malware, a empresa de segurança cibernética Cylance (agora parte da BlackBerry) desenvolveu um sistema de IA capaz de prever e prevenir ataques de malware desconhecidos. Em um teste realizado em 2019, o sistema conseguiu bloquear com sucesso o ransomware WannaCry em ambientes simulados, demonstrando o potencial da IA na proteção proativa contra ameaças cibernéticas emergentes.

A investigação forense digital também tem se beneficiado enormemente da IA. Um caso notável ocorreu em 2019, quando a polícia do Reino Unido utilizou IA para analisar 29 milhões de arquivos relacionados a um caso de tráfico de drogas. O sistema de IA conseguiu processar e categorizar os arquivos em apenas 24 horas, uma tarefa que teria levado meses se realizada manualmente. Isso permitiu que os investigadores identificassem rapidamente evidências cruciais, levando à condenação dos criminosos envolvidos.

No campo da previsão de crimes, o Departamento de Polícia de Los Angeles (LAPD) implementou em 2015 um sistema de IA chamado PredPol para prever áreas de alta criminalidade. Embora controverso devido a preocupações com vieses algorítmicos, o LAPD relatou uma redução de 13% nos crimes violentos nas áreas onde o sistema foi implementado durante o primeiro ano de uso.

Estes casos ilustram o poder transformador da IA tanto para perpetrar quanto para combater crimes digitais. À medida que a tecnologia continua a evoluir, é crucial que pesquisadores, legisladores e profissionais de segurança trabalhem em conjunto para desenvolver estratégias eficazes de mitigação de riscos e aproveitar o potencial positivo da IA na segurança cibernética.

A complexidade e a rápida evolução deste campo destacam a necessidade de uma abordagem multidisciplinar, que combine expertise técnica, considerações éticas e uma compreensão profunda das implicações sociais do uso da IA em contextos de segurança digital. Somente através de esforços coordenados e uma vigilância constante poderemos esperar manter-nos à frente das ameaças emergentes e garantir um ambiente digital mais seguro para todos.

4.8. O Futuro da IA no Direito Penal Brasileiro

Considerando os avanços tecnológicos e as demandas por maior eficiência e celeridade no sistema judiciário, é razoável prever que a utilização da IA no direito penal brasileiro se intensifique nos próximos anos. No entanto, é fundamental que essa implementação seja acompanhada de um amplo debate sobre os seus impactos sociais, éticos e legais.

Para garantir que a IA seja utilizada de forma benéfica e responsável, é necessário:

- Desenvolver mecanismos de controle e supervisão: É fundamental estabelecer normas e protocolos que garantam a transparência, a imparcialidade e a explicabilidade dos algoritmos utilizados.
- Promover a educação e a capacitação: Advogados, juízes e demais operadores do direito precisam ser preparados para lidar com as novas tecnologias e compreender seus limites e potencialidades.
- Garantir a proteção dos direitos fundamentais: A utilização da IA não pode comprometer direitos como o devido processo legal, a presunção de inocência e a ampla defesa.

Em suma, o futuro da IA no direito penal brasileiro é promissor, mas repleto de desafios. Ao navegar por esse novo cenário, é fundamental que se busque um equilíbrio entre a inovação tecnológica e a proteção dos direitos fundamentais, garantindo que a justiça seja exercida de forma justa e eficiente.

> Um exemplo é o software desenvolvido pela (Advocacia-Geral da União AGU) para auxiliar os advogados públicos a localizarem documentos e informações relacionadas a um processo que lhes seja distribuído (AGU, 2013). Também há experiências no Superior Tribunal de Justiça e no Supremo Tribunal Federal, para auxiliar na classificação de processos (CONJUR, 2018b; STF, 2018). Aplicações semelhantes estariam sendo desenvolvidas de igual modo em parceria com o Tribunal de Justiça do Estado de Minas Gerais TJMG) e com o Tribunal Superior do Trabalho (TST). 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 (CHIESI FILHO, 2018). Há, ainda, 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 (CONJUR, 2017; CHIESI FILHO, 2017; CONJUR, 2018a). Como tem ocorrido na maioria dos países, essas propostas também receberam duras críticas de acadêmicos, de associações de advogados, de magistrados e da sociedade civil (CHIESI FILHO, 2017; FRAZÃO, 2017; CONJUR, 2018c; FRAZÃO, 2018; NUNES, RUBINGER, MARQUES, 2018; STRECK, 2019a; idem, 2019b; idem 2019c). [4]

O trecho mencionado discute o uso crescente de tecnologias de inteligência artificial (IA) no sistema jurídico, tanto no Brasil quanto em outros países. Iniciativas como o software desenvolvido pela Advocacia-Geral da União (AGU) e as experiências em tribunais superiores demonstram a adoção de IA para melhorar a eficiência, como na classificação de processos e na busca de informações relacionadas a processos. Além disso, parcerias com tribunais, como o Tribunal de Justiça de Minas Gerais (TJMG) e o Tribunal Superior do Trabalho (TST), também reforçam essa tendência.

Outro ponto relevante é a utilização de robôs de IA, como o da IBM, que auxilia na redação de petições e na análise de mérito. Essa tecnologia já é adotada em grandes escritórios de advocacia no Brasil. As legal techs e lawtechs também oferecem soluções tecnológicas que buscam agilizar o trabalho jurídico, com ferramentas que resumem os principais pontos de um processo e sugerem jurisprudências aplicáveis, além de criarem peças jurídicas com pouca ou nenhuma intervenção humana.

Porém, o uso da IA na justiça não está isento de críticas. Acadêmicos, advogados, magistrados e a sociedade civil têm expressado preocupação com o impacto dessas tecnologias. As críticas envolvem questões sobre a qualidade das decisões automatizadas, a possível desumanização do processo decisório e o risco de que esses sistemas perpetuem vieses presentes nos dados com os quais foram treinados. A resistência também reflete o temor de que a IA substitua, de forma inadequada, o papel dos seres humanos em decisões que, por sua natureza, exigem sensibilidade e julgamento ético.

---

[4] ROCHA, Heloisa Rodrigues da. In Dubio Pro… Algoritmo? – Lições para o Brasil Sobre o Uso da Inteligência Artificial nas Decisões Penais nos Estados Unidos. Eixo 1 - Futuro da Justiça no Brasil – 1º Lugar. - https://bdjur.stj.jus.br/jspui/bitstream/2011/147043/dubio_algoritmo_licoes_rocha.pdf

Em suma, o uso de IA no sistema jurídico, embora tenha o potencial de aumentar a eficiência e a precisão, também traz à tona preocupações sobre a equidade, a transparência e a responsabilidade. Essas questões precisam ser cuidadosamente consideradas para garantir que a adoção dessas tecnologias não comprometa a justiça e os direitos das partes envolvidas.

Esse trecho, extraído do trabalho “In Dubio Pro… Algoritmo? – Lições para o Brasil Sobre o Uso da Inteligência Artificial nas Decisões Penais nos Estados Unidos”, da autora Heloisa Rodrigues da Rocha, destaca o dilema entre o progresso tecnológico e a necessidade de preservar os valores fundamentais da justiça no Brasil.

4.9. Considerações sobre Investimentos

O investimento necessário para implementar soluções de IA no combate a crimes digitais pode ser substancial, mas é cada vez mais visto como essencial[5]:

1. Custos Iniciais vs. Benefícios a Longo Prazo: Embora o investimento inicial em tecnologia de IA e treinamento possa ser alto, os benefícios a longo prazo em termos de prevenção de perdas e proteção da reputação podem justificar os custos.

2. Escalabilidade: Soluções baseadas em IA tendem a ser altamente escaláveis, o que pode resultar em economias significativas à medida que as operações crescem.

3. Necessidade de Expertise: O investimento não se limita apenas à tecnologia, mas também à contratação e treinamento de especialistas em IA e segurança cibernética, o que pode representar um custo significativo.

4. Infraestrutura de Dados: A implementação eficaz de soluções de IA requer uma infraestrutura de dados robusta, o que pode necessitar de investimentos adicionais em armazenamento e processamento de dados.

[5] file:///C:/Users/marcela.almeida/Downloads/Uso-responsavel-da-IA-para-politicas-publicas-manual-de-formulac%C3%A3o-de-projetos.pdf

5. Colaboração e Compartilhamento de Custos: Parcerias entre empresas, instituições acadêmicas e governos podem ajudar a distribuir os custos de pesquisa e desenvolvimento de soluções de IA para segurança cibernética.

6. Regulamentação e Conformidade: À medida que novas regulamentações sobre o uso de IA são implementadas, as organizações precisarão investir em conformidade, o que pode aumentar os custos gerais.

Embora o investimento em soluções de IA para combater crimes digitais possa ser substancial, ele é cada vez mais visto como uma necessidade estratégica. A crescente sofisticação das ameaças cibernéticas torna a adoção de tecnologias avançadas de defesa não apenas desejável, mas essencial para a sobrevivência e prosperidade das organizações na era digital. O desafio está em equilibrar os investimentos com os riscos potenciais e os benefícios esperados, sempre considerando o panorama em constante evolução das ameaças cibernéticas e das capacidades da IA.

A implementação de sistemas de inteligência artificial (IA) no combate aos crimes digitais, embora promissora e potencialmente eficaz, levanta uma série de questões éticas e sociais que merecem uma análise cuidadosa. À medida que as tecnologias de IA se tornam mais sofisticadas e onipresentes nas estratégias de segurança cibernética, é crucial considerar não apenas sua eficácia técnica, mas também seu impacto mais amplo na sociedade e nos direitos individuais.

Um dos principais pontos de preocupação é o potencial de vigilância excessiva. Sistemas de IA projetados para detectar atividades criminosas online podem, inadvertidamente, infringir a privacidade de usuários inocentes. Por exemplo, algoritmos de detecção de anomalias, se não forem adequadamente calibrados, podem sinalizar comportamentos online legítimos, mas incomuns, levando a investigações desnecessárias e potencialmente prejudiciais. Este cenário levanta questões sobre o equilíbrio entre segurança e privacidade, um debate que se intensifica à medida que as capacidades de monitoramento se expandem.

Outro aspecto crítico é o risco de viés algorítmico. As IAs são treinadas com dados históricos que podem refletir preconceitos sociais existentes. No contexto da segurança cibernética, isso pode levar a uma aplicação desproporcional de medidas

de segurança contra certos grupos demográficos. Por exemplo, sistemas de IA usados para prever atividades criminosas online podem inadvertidamente direcionar mais recursos de investigação para comunidades já marginalizadas, perpetuando ciclos de discriminação. A transparência no desenvolvimento e implementação desses sistemas, bem como auditorias regulares para identificar e corrigir vieses, são essenciais para mitigar esses riscos.

A questão da responsabilidade e prestação de contas também emerge como um desafio significativo. Quando decisões críticas sobre segurança cibernética são tomadas ou influenciadas por sistemas de IA, determinar a responsabilidade em caso de erros ou danos se torna complexo. Quem deve ser responsabilizado se um sistema de IA falhar em detectar uma ameaça séria ou, inversamente, se ele gerar um falso positivo que resulte em danos à reputação ou perdas financeiras para um indivíduo ou organização? Estabelecer estruturas claras de governança e responsabilidade é crucial para manter a confiança pública e garantir o uso ético dessas tecnologias.

Além disso, há preocupações sobre o potencial de abuso de poder. Tecnologias de IA avançadas para combater crimes digitais, se caírem em mãos erradas, podem ser usadas para fins maliciosos, como espionagem em larga escala ou supressão de dissidência política. Isso sublinha a necessidade de regulamentações robustas e mecanismos de supervisão para garantir que essas ferramentas sejam usadas de maneira ética e dentro dos limites legais.

O impacto dessas tecnologias na dinâmica de poder entre estados e indivíduos também merece consideração. À medida que governos e grandes corporações adquirem capacidades cada vez mais sofisticadas de monitoramento e análise baseadas em IA, existe o risco de um desequilíbrio de poder, onde a privacidade e a autonomia individuais são progressivamente erodidas em nome da segurança coletiva.

Por outro lado, o uso ético e responsável de IA no combate aos crimes digitais tem o potencial de criar uma internet mais segura e confiável para todos. Pode ajudar a proteger populações vulneráveis contra exploração online, reduzir perdas financeiras devido a fraudes cibernéticas e preservar a integridade de sistemas críticos de infraestrutura. O desafio está em desenvolver e implementar essas

tecnologias de uma maneira que maximize seus benefícios sociais enquanto minimiza os riscos éticos.

Para abordar essas questões, é essencial um diálogo contínuo e multidisciplinar envolvendo tecnólogos, legisladores, especialistas em ética e representantes da sociedade civil. A criação de marcos regulatórios flexíveis, que possam se adaptar ao rápido ritmo de avanço tecnológico, é crucial. Esses marcos devem não apenas estabelecer limites claros para o uso de IA em segurança cibernética, mas também promover a inovação responsável neste campo.

Educação e transparência também desempenham um papel vital. O público deve ser informado sobre como essas tecnologias estão sendo usadas, seus potenciais benefícios e riscos, e os mecanismos de proteção em vigor. Isso não apenas ajuda a construir confiança, mas também capacita os cidadãos a participar de forma mais significativa nos debates sobre o uso dessas tecnologias.

CONCLUSÕES

Os capítulos deste trabalho abordam a crescente relevância da inteligência artificial (IA) no combate aos crimes digitais, refletindo sobre as estratégias discutidas, as expectativas em relação às tecnologias emergentes e os investimentos necessários para garantir a eficácia das soluções propostas. À medida que a IA se torna uma ferramenta fundamental na luta contra atividades maliciosas online, a necessidade de um enfoque estratégico se torna evidente. Este trabalho destacou a importância de adotar métodos proativos, como a detecção avançada de deepfakes, autenticação multifatorial e sistemas de monitoramento em tempo real, que são cruciais para enfrentar a evolução das ameaças cibernéticas.

Além das estratégias, as expectativas em relação à IA na prevenção de crimes digitais trazem à tona um potencial significativo para transformar a segurança cibernética. O uso de análise preditiva, resposta automatizada a incidentes e simulações de ataques complexos representa um avanço promissor que pode aumentar a resiliência das organizações contra ameaças emergentes. No entanto, é importante reconhecer que, para que essas expectativas se concretizem, é necessário um compromisso contínuo com a inovação e a adaptação das tecnologias de

segurança. A evolução constante das defesas é essencial para acompanhar as táticas em constante mudança dos cibercriminosos.

Outro aspecto crucial discutido ao longo deste trabalho é a consideração dos investimentos necessários para implementar soluções eficazes de IA. Embora os custos iniciais possam ser elevados, os benefícios a longo prazo em termos de proteção contra fraudes, perda de dados e danos à reputação justificam o investimento. Além disso, a escalabilidade das soluções de IA pode oferecer economias significativas à medida que as operações crescem, reforçando a importância de ver a segurança cibernética como uma prioridade estratégica para as organizações. A colaboração entre empresas, instituições acadêmicas e governos também pode ajudar a compartilhar os custos e fomentar a pesquisa e desenvolvimento de novas tecnologias.

Entretanto, é fundamental que o uso da IA na segurança cibernética seja acompanhado por uma análise cuidadosa das implicações éticas e sociais. A vigilância excessiva, o viés algorítmico e a questão da responsabilidade em casos de falhas nas tecnologias de IA são preocupações que não podem ser ignoradas. É imperativo estabelecer um equilíbrio entre a segurança e a proteção dos direitos individuais, garantindo que as soluções adotadas não apenas previnam crimes, mas também respeitem a privacidade e a dignidade das pessoas. A transparência nas operações de segurança e a realização de auditorias regulares são medidas essenciais para mitigar os riscos associados ao uso de IA.

Por fim, o futuro do combate aos crimes digitais com o apoio da inteligência artificial depende de um diálogo contínuo entre todos os stakeholders envolvidos. Tecnólogos, legisladores, especialistas em ética e a sociedade civil devem colaborar para criar marcos regulatórios flexíveis que garantam o uso responsável e ético das tecnologias de IA. A educação e a conscientização sobre o uso dessas ferramentas são cruciais para promover uma internet mais segura e confiável. Assim, ao abordar as questões éticas e sociais associadas ao uso da IA, podemos construir um ambiente digital que não apenas protege, mas também respeita os direitos fundamentais dos cidadãos, promovendo uma convivência mais harmônica entre segurança e liberdade.

O estudo revelou que a implementação de estratégias avançadas, como a detecção de deepfakes, autenticação multifatorial e sistemas de monitoramento em tempo real, é crucial para enfrentar as crescentes ameaças cibernéticas. A análise preditiva de ameaças e a resposta automatizada a incidentes se destacaram como abordagens promissoras, demonstrando que a IA pode não apenas identificar atividades maliciosas, mas também mitigar os danos de forma eficaz. Além disso, a integração de tecnologias como blockchain para verificação de integridade e a importância da educação e conscientização foram identificadas como componentes fundamentais na construção de um ambiente digital seguro.

À medida que as organizações se adaptam a um panorama de ameaças em constante evolução, a necessidade de investimentos em tecnologias de segurança se torna evidente. Embora os custos iniciais possam ser substanciais, os benefícios a longo prazo em termos de proteção contra fraudes e danos à reputação justificam esses gastos. O estudo também destacou a importância da colaboração entre diferentes setores, incluindo empresas, instituições acadêmicas e governos, como uma estratégia eficaz para compartilhar custos e impulsionar a pesquisa e o desenvolvimento de soluções inovadoras. No entanto, a implementação dessas tecnologias deve ser acompanhada por uma análise cuidadosa das questões éticas e sociais associadas, garantindo que os direitos individuais sejam respeitados e protegidos.

Com base nas descobertas deste trabalho, há várias sugestões para futuras pesquisas e o desenvolvimento de políticas de segurança. Primeiramente, é fundamental realizar estudos adicionais sobre o impacto das tecnologias de IA nas práticas de segurança cibernética, especialmente no que diz respeito à identificação e mitigação de vieses algorítmicos. A realização de auditorias regulares e a implementação de diretrizes para garantir a transparência e a responsabilização são áreas que merecem maior atenção. Além disso, a criação de programas educacionais que abordem tanto a conscientização sobre ameaças cibernéticas quanto as melhores práticas de segurança é uma prioridade para preparar usuários e profissionais para os desafios emergentes.

Outra sugestão importante é a necessidade de desenvolver marcos regulatórios que promovam o uso responsável da IA na segurança cibernética. As

políticas devem ser flexíveis o suficiente para se adaptarem ao rápido avanço das tecnologias, ao mesmo tempo que estabelecem limites claros para proteger a privacidade e a liberdade dos indivíduos. A colaboração internacional é vital nesse contexto, uma vez que crimes digitais frequentemente transcendem fronteiras, exigindo uma abordagem global para a segurança cibernética.

Por fim, este trabalho enfatiza a importância de um diálogo contínuo entre tecnólogos, legisladores e a sociedade civil. A participação ativa de todos os stakeholders é essencial para garantir que as soluções de IA não apenas combatam crimes digitais, mas também promovam um ambiente digital mais seguro e ético. O futuro da segurança cibernética deve ser construído sobre uma base de confiança, transparência e respeito pelos direitos individuais, garantindo que a tecnologia sirva para o bem comum e contribua para a proteção da sociedade como um todo.

REFERÊNCIAS BIBLIOGRÁFICAS

https://wearesocial.com/blog/2018/01/global-digital-report-2018/. Acesso em 27 de setembro de 2024

file:///C:/Users/DAKI/Downloads/ssrn-3248829.pdf. Acesso em 08 de setembro de 2024

BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro. Forense. 2019. Acesso em 08 de setembro de 2024

Identity Fraud Report 2023 - Statistics & Trends | Sumsub. Sumsub. Disponível em:<https://sumsub.com/fraud-report 2023/?utm_source=pr&utm_medium=article&utm_campaign=fraud_report2023>. Acesso em 6 outubro 2024.

Vista do Desafios éticos ao uso da inteligência artificial no sistema de justiça criminal. Ibccrim.org.br. Disponível em: <https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1242/1071>. Acesso em 19 outubro 2024.

Educação | IBSEC - 10 Estratégias Atuais para Proteger-se Con...2986. Ibsec.com.br. Disponível em: <https://ibsec.com.br/10-estrategias-para-proteger-se-contra-hackers-autonomos-e-ia-maliciosa/>. Acesso em 2 outubro 2024.

SENADO FEDERAL. [s.l.: s.n., s.d.]. Disponível em: <https://legis.senado.leg.br/sdleggetter/documento?dm=9292780&disposition=inline>. Acesso em 2 outubro 2024.

EMERJ ; DE, Rio. A Inteligência Artificial e o Processo Penal: A Utilização da Técnica na violação de Direitos. n. 1, p. 105–129, 2023. Disponível em: <https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista_v25_n1/revista_v25_n1_105.pdf>. Acesso em 2 outubro 2024.

ROCHA, Heloisa Rodrigues da. In Dubio Pro… Algoritmo? – Lições para o Brasil Sobre o Uso da Inteligência Artificial nas Decisões Penais nos Estados Unidos. Eixo 1 - Futuro da Justiça no Brasil – 1º Lugar. Disponível em: https://www.stj.jus.br/publicacaoinstitucional/index.php/RCSTJ/author/proofGalleyFile/6405/6530. Acesso em 05 de outubro de 2024.

WACHTER, Sandra; MITTELSTADT, Brent.*A right to reasonable inferences: re-thinking data protection law in the age of big data and IA**. Columbia Business Law Review***, 2019. Disponível em:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829. Acesso em 05 de outubro de 2024.

[1] **JORNAL DO ESTADO DE MINAS INTERNACIONAL**: https://www.em.com.br/app/noticia/internacional/2023/09/12/interna_internacional,1560532/um-terco-da-populacao-mundial-continua-sem-acesso-a-internet.shtml#:~:text=Desde%20a%20%C3%BAltima%20contagem%20da,5%2C4%20bilh%C3%B5es%20de%20pessoas. Acesso em 25 de outubro de 2024

SENADO FEDERAL PROJETO DE LEI N° 1272, DE 2023. Acesso em 25 de outubro de 2024

IBSEC – Instituto Brasileiro de Cibersegurança. Acesso em 25 de outubro de 2024

YAROVENKO, Vasily; SHAPOVALOVA, Galina; ISMAGILOV, Rinat. Some problems of using the facial recognition system in law enforcement activities. Правовое государство теория и практика, [s. l.], v. 17, n. 1, p. 189-200, mar. 2021. Disponível em: https://pravgos.ru/index.php/journal/article/view/160. Acesso em 25 de outubro de 2024

https://ibccrim.org.br/?gad_source=1&gclid=Cj0KCQiAuou6BhDhARIsAIfgrn5J5lKOjkQf8rPilnF3Rsb9-LMDRK4IhUT7_9b92-IXsV0jzlcFzWwaAkBUEALw_wcB.Acesso em 25 de outubro de 2024

KAPLAN, Andreas; HAENLEIN, Michael. A brief history of artificial intelligence: on the past, present, and future of artificial intelligence, California Management Review, Califórnia, v. 61, n. 4, p. 5-14, ago. 2019. Disponível em: https://journals.sagepub.com/doi/10.1177/0008125619864925. Acesso em: 25 de outubro de 2024

POOLE, David; MACKWORTH, Alan. Artificial intelligence foundations of computational agents. Cambridge: Cambridge University Press, 2017. Acesso em 25 de outubro de 2024

RUSSELL, Stuart; NORVIG, Peter. Artificial intelligence: a modern approach. New Jersey: Pearson. 2020. Acesso em 25 de outubro de 2024

https://bdjur.stj.jus.br/jspui/bitstream/2011/147043/dubio_algoritmo_licoes_rocha.pdf. Acesso em 25 de outubro de 2024

https://www.terra.com.br/noticias/deepfakes-crescem-830-no-brasil-em-um-ano-aponta-estudo,601f3d28caa943b3728390a82f13cc2b0x3pdhbk.html. Acesso em 20 de novembro de 2024.

https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista_v25_n1/revista_v25_n1_105.pdf. Acesso em 20 de novembro de 2024.

Comissão Europeia. (2013). Regulamento (UE) nº 1291/2013. https://eur-lex.europa.eu/eli/reg/2013/1291/oj. Acesso em 27 de novembro de 2024.

file:///C:/Users/marcela.almeida/Downloads/Uso-responsavel-da-IA-para-politicas-publicas-manual-de-formulac%C3%A3o-de-projetos.pdf. Acesso em 27 de novembro de 2024.

NUNES, L. F. M. Reconhecimento Facial Biométrico Em Nuvens de Pontos Tridimensionais. 2016. Disponível em:< file:///C:/Users/User/Downloads/2016_LuisFelipeMeloNunes_tcc.pdf>. Acesso em 28 de novembro de 2024.

GAIDIS, Vinicius. A IA na segurança da informação: aliada ou inimiga? Compugraf, 2023. Acesso em 28 de novembro de 2024

PORTA, Daniel. Como a Cibersegurança e os Cibercriminosos usam a Inteligência Artificial. Danresa, 2023. Acesso em 28 de novembro de 2024.

https://www.kaspersky.com.br/resource-center/threats/protect-yourself-from-deep-fake. Acesso em 28 de novembro de 2024.

WEINHARDT, M. (2020). Ethical issues in the use of big data for social research. Historical Social Research. https://www.ssoar.info/ssoar/handle/document/68212. Acesso em 28 de novembro de 2024.

HERSCHEL, R, & Miori, V. M (2017). Ethics & big data. Technology in Society. Acesso em 28 de novembro de 2024.

Oliver, D. (1994). Law, politics and public accountability. The search for a new equilibrium. Public Law, 238-238. Acesso em 28 de novembro de 2024.