FACULDADE DE TECNOLOGIA PADRE DANILO DE OLIVEIRA OHL

AMANDA SILVEIRA LEMOS

JOÃO VICTOR MINGUETTI

MARIANE DE SOUSA MASCARENHAS

USO DE INTELIGÊNCIA ARTIFICIAL PARA DETECTAR CRIMES NA DARK WEB

BARUERI

2025

FACULDADE DE TECNOLOGIA PADRE DANILO DE OLIVEIRA OHL

AMANDA SILVEIRA LEMOS
JOÃO VICTOR MINGUETTI
MARIANE DE SOUSA MASCARENHAS

USO DE INTELIGÊNCIA ARTIFICIAL PARA DETECTAR CRIMES NA DARK WEB

Projeto de pesquisa apresentado à banca examinadora da Faculdade de Tecnologia de Barueri como requisito parcial para obtenção do título de tecnólogo em Gestão de Tecnologia da Informação.

Orientador: Prof.ª Jayr Figueiredo de Oliveira

BARUERI

2025

SUMÁRIO

1. LISTA DE ABREVIATURAS

AI	***Artificial Intelligence*** **(Inteligência Artificial)**
AI Act	***Artificial Intelligence Act*** **(Regulamento Europeu de IA)**
DL	***Deep Learning*** **(Aprendizado Profundo)**
IA	**Inteligência Artificial**
IEEE	***Institute of Electrical and Electronics Engineers***
LGPD	**Lei Geral de Proteção de Dados (Lei nº 13.709/2018)**
LSTM	***Long Short-Term Memory*** **(Memória de Curto e Longo Prazo)**
ML	***Machine Learning*** **(Aprendizado de Máquina)**
RNN	***Recurrent Neural Network*** **(Rede Neural Recorrente)**
SciELO	**Scientific Electronic Library Online**
Tor	***The Onion Router*** **(Roteador em Camadas, utilizado para navegação anônima)**
US$	**Dólar Americano**

VPN	***Virtual Private Network*** **(Rede Privada Virtual)**
XAI	***Explainable Artificial Intelligence*** **(Inteligência Artificial Explicável)**

2. RESUMO

O presente artigo analisa o uso da Inteligência Artificial (IA) na detecção e combate de crimes cibernéticos na dark web, destacando seu potencial como ferramenta tecnológica para investigações em ambientes digitais anônimos. A pesquisa, de natureza qualitativa e exploratória, fundamenta-se em revisão bibliográfica e estudo de caso do modelo DarkBERT, desenvolvido para identificar padrões criminosos em fóruns ocultos. O estudo aborda o funcionamento da dark web, os principais tipos de crimes cibernéticos e a aplicação de técnicas de Machine Learning e Deep Learning na segurança digital. Também discute os desafios éticos, legais e técnicos da utilização da IA nesse contexto, especialmente no Brasil, onde há lacunas estruturais e legislativas. Conclui-se que, embora a IA represente um avanço promissor no rastreamento e prevenção de atividades ilícitas, seu uso deve estar alinhado a princípios de transparência, ética e governança responsável, exigindo a atuação conjunta de profissionais qualificados e políticas públicas voltadas à cibersegurança.

Palavras-chave: Inteligência Artificial. Dark Web. Crimes Cibernéticos. Cibersegurança. Machine Learning.

3. ABSTRACT

This article examines the use of Artificial Intelligence (AI) in detecting and combating cybercrimes on the dark web, emphasizing its potential as a technological tool for investigations in anonymous digital environments. The research, qualitative and exploratory in nature, is based on a bibliographic review and a case study of the DarkBERT model, developed to identify criminal patterns in hidden forums. The study explores the structure of the dark web, the main types of cybercrimes, and the application of Machine Learning and Deep Learning techniques in digital security. It also discusses the ethical, legal, and technical challenges of using AI in this context, particularly in Brazil, where structural and legislative gaps persist. The findings indicate that although AI represents a promising advancement in tracking and preventing illicit activities, its implementation must align with

transparency, ethical governance, and human oversight, supported by skilled professionals and public policies aimed at strengthening cybersecurity.

Keywords: Artificial Intelligence. Dark Web. Cybercrime. Cybersecurity. Machine Learning.

4. INTRODUÇÃO

Por volta do século XX, o mundo passou por diversas mudanças sociais e tecnológicas, dentre elas, o surgimento do computador utilizado na Segunda Guerra Mundial (1939-1945), criado por John Eckert e John Mauchly. O ENIAC foi o primeiro passo, rumo ao que hoje conhecemos como tecnologia moderna. Essa mesma tecnologia assumiu um papel fundamental no desenvolvimento social, econômico e científico, trazendo praticidade, acessibilidade em conhecimentos gerais e transformando profundamente as formas de comunicação, trabalho e aprendizado (CERUZZI, 2003; CASTELLS, 2003).

A partir desse marco, a sociedade passou a vivenciar uma revolução digital, em que os processos se tornaram cada vez mais automatizados e integrados. Com o avanço da internet e das tecnologias da informação, novas possibilidades surgiram. Desde a criação de sistemas de gestão e bancos de dados até o surgimento da inteligência artificial e da computação em nuvem. Assim, o computador deixou de ser apenas uma ferramenta de cálculo para se tornar um elemento essencial no cotidiano das pessoas e nas organizações, impulsionando a inovação e moldando o mundo contemporâneo.

Entretanto, é inegável que esse ambiente também abriu espaço para novas formas de criminalidade. À medida que a sociedade se digitalizou, surgiram práticas ilícitas como o comércio ilegal de dados pessoais, a falsidade ideológica e diversas modalidades de fraude virtual. Essas ações passaram a se disseminar com facilidade, muitas vezes sobrepondo-se às atividades legítimas e comprometendo a confiança nas interações online.

Esses setores da internet com menor visibilidade, comumente denominados como *camadas profundas da web* ou *deep web*, exigem métodos de acesso específicos, o que restringe significativamente a entrada de usuários comuns (CASTELLS, 2003). Essa limitação técnica, inicialmente criada para garantir privacidade e segurança na troca de informações, passou a ser explorada por

organizações criminosas e grupos ilícitos. Conforme aponta Recuero (2014), o ambiente digital reflete as dinâmicas sociais existentes, o que inclui a migração de práticas ilegais para o meio virtual. Assim, essas áreas tornaram-se refúgio para o tráfico de drogas e armas, a comercialização de dados pessoais, fraudes financeiras e a disseminação de conteúdos ilegais, incluindo pornografia infantil.

Segundo Souza e Silva (2018), a estrutura descentralizada e o uso de ferramentas de anonimato, como o navegador Tor e redes criptografadas, dificultam a identificação e o rastreamento de usuários nessas camadas da web. Essa característica amplia a complexidade das investigações e desafia a atuação de órgãos reguladores e forças policiais. A ausência de mecanismos eficazes de monitoramento e a falta de cooperação internacional em matéria de cibersegurança têm contribuído para o fortalecimento dessas redes ilícitas, exigindo novas estratégias legais e tecnológicas para o enfrentamento do cibercrime.

Acompanhando o avanço dos computadores e da internet, por volta da década de 1940, Alan Turing propôs a possibilidade dos computadores apresentarem comportamentos humanos, originando assim o conceito de "Teste de Turing" (TURING, 1950). Mas apenas em 1956, durante a conferência de Dartmouth, os pesquisadores John McCarthy e Marvin Minsky estabeleceram a IA como um campo de estudo formal, cunhando o próprio termo “Inteligência Artificial” (MC CARTHY *et al.*, 1956).

Nas décadas seguintes, programas especializados em xadrez, resolução de problemas e sistemas especialistas demonstraram que algoritmos poderiam replicar aspectos do raciocínio humano. Essa trajetória culmina hoje no uso de aprendizado profundo (*deep learning*), que permite que máquinas identifiquem padrões complexos em grandes volumes de dados, abrindo possibilidades inéditas em áreas como segurança digital, análise de comportamento e prevenção do cibercrime (GOODFELLOW; BENGIO; COURVILLE, 2016).

A capacidade de aprendizado de uma máquina ao fazer análise de dados significativos, e de identificar padrões antecipando comportamentos ou ações suspeitas, trouxe o olhar dos estudiosos para que ela passasse a ser treinada para

esse tipo de serviço. A detecção de atividades criminosas utilizando IA traria uma nova visão para o combate do cibercrime, aumentando a eficiência do rastreamento de usuários suspeitos, movimentações que seguem um padrão e até mesmo na detecção de comportamentos humanos que podem ser julgados como potencialmente de risco.

A proposta desta pesquisa é investigar de forma aprofundada o uso da Inteligência Artificial (IA) no combate ao cibercrime, buscando compreender as tecnologias aplicáveis a diferentes contextos e seus respectivos limites. Além disso, pretende-se discutir os impactos sociais e éticos decorrentes da adoção dessas ferramentas, especialmente no que diz respeito à segurança e à confiabilidade dos sistemas automatizados. O foco do estudo concentra-se na análise de métodos e sistemas baseados em IA voltados ao monitoramento e à detecção de crimes cibernéticos, com ênfase em ambientes de acesso restrito, como a *dark web*, onde o anonimato e a criptografia representam desafios adicionais à atuação das autoridades.

O principal desafio identificado nesta pesquisa refere-se ao cenário contemporâneo em que o cibercrime evolui em ritmo superior à capacidade das instituições públicas de supervisionar e conter as ameaças digitais. Essa disparidade evidencia um descompasso entre o avanço das tecnologias empregadas em atividades ilícitas e os mecanismos de defesa desenvolvidos pelos órgãos reguladores. Nesse contexto, o presente trabalho busca contribuir para a discussão sobre o uso ético e responsável da IA, considerando não apenas sua eficiência técnica no rastreamento e detecção de crimes, mas também os riscos e implicações que seu uso pode representar para a sociedade digital contemporânea.

5. OBJETIVOS

O foco dos objetivos dessa pesquisa, são em grande maioria, analisar a eficiência da aplicação das técnicas da inteligência artificial na detecção e no combate de crimes digitais na camada mais escondida da web, conhecida como dark web. A pesquisa também se foca em buscar compreender o processo no qual essas tecnologias serão aplicadas para detectar padrões de comportamento suspeitos, uma vez que a IA é treinada, ela poderá identificar atividade suspeita, distribuições ilegais de dados e até mesmo fóruns que violem outras diretrizes legais, como, por exemplo, distribuição de pornografia infantil, tráfico humano quebrando a segurança e as altas camadas de irrastreabilidade.

Isto posto, o presente escrito pretende fazer descrições técnicas a respeito da estrutura da dark web, seu funcionamento, seus métodos de acesso, dando destaque aos recursos que permitem que seu anonimato seja impecável. Logo depois, analisar os cibercrimes que são mais críticos e que ocorrem com maior frequência nesse ambiente, assim como as dificuldades para serem investigados e, por fim, descrever sobre a Inteligência Artificial, apresentando também abordagens como Machine Learning e Deep Learning.

6. JUSTIFICATIVA

A crescente complexidade e expansão dos crimes cibernéticos na dark web têm se tornado uma ameaça concreta à segurança digital, à privacidade de dados e à integridade de sistemas públicos e privados. Este ambiente oculto da internet, por sua própria arquitetura técnica, dificulta a rastreabilidade de ações ilícitas, favorecendo atividades como tráfico de dados, armas, drogas, abuso infantil e fraudes financeiras. A utilização de tecnologias de anonimato, como a rede Tor, impõe barreiras substanciais à atuação de autoridades e sistemas tradicionais de investigação, exigindo soluções inovadoras que combinem alto desempenho técnico com respeito a princípios éticos e legais.

Diante desse cenário, o uso de inteligência artificial se destaca como uma abordagem promissora e necessária para pesquisadores, autoridades e órgãos responsáveis pela segurança digital. Algoritmos de aprendizado de máquina e modelos de linguagem treinados com dados oriundos da dark web, como o DarkBERT, têm demonstrado capacidade real de identificar padrões criminosos, classificar ameaças e apoiar investigações com precisão elevada, mesmo diante de volumes massivos e não estruturados de informação. A viabilidade técnica dessas ferramentas, aliada à sua escalabilidade, indica que a IA pode desempenhar papel central no combate aos crimes digitais, especialmente em ambientes onde a ação humana é limitada ou ineficaz.

A relevância desta pesquisa, sendo à comunidade acadêmica e científica e às autoridades, está no seu potencial de contribuir para o fortalecimento da segurança cibernética, a proteção e identificação de usuários vulneráveis e também no aprimoramento de políticas públicas voltadas ao enfrentamento de crimes digitais. Ao investigar a aplicação da IA nesse contexto, o trabalho busca ampliar a discussão acadêmica sobre as interações entre tecnologia, ética e direito digital, promovendo uma reflexão sobre os limites e possibilidades do uso de sistemas inteligentes em atividades de monitoramento e investigação.

7. DARK WEB

A dark web protagoniza um dos temas mais complexos e controversos na área da tecnologia, mais especificamente no campo da segurança da informação. Diferentemente do que se conhece como surface (superfície da internet) acessada por navegadores mais comuns, a dark web é uma camada profunda da deep web, por esse motivo não há como ser acessada pelos meios convencionais, sendo necessário softwares específicos, como o Tor, para ser acessada (TURING, 2013).

Turing (2013) relembra que o projeto Tor foi iniciado pela Marinha dos Estados Unidos na intenção de proteger comunicações governamentais e que em 2002 foi liberado como um software livre, desse modo, acredita-se que essa camada da deep web surgiu como uma parte do desenvolvimento das tecnologias de navegação anônima por volta da década de 90. Por oferecer uma grande segurança de privacidade, o Tor começou a ser utilizado por ativistas, jornalistas e outros usuários que buscavam esse anonimato, infelizmente essa ferramenta também passou a ser utilizada por criminosos o que levou ela a ser conhecida como dark web (OKYERE-AGYEI, 2025)

Para Turing (2013) a dark web, ao longo dos anos, se tornou um ambiente onde tanto a liberdade de expressão quanto o cibercrime andam lado a lado. "A dark web permite que usuários mantenham o anonimato quase total, o que atrai desde dissidentes políticos até criminosos" (TURING, 2013, p. 15). Na obra "dark web Demystified" podemos ter uma visão inicial clara sobre como as operações, os protocolos e a ambiguidade de seu uso acontecem, sendo uma obra fundamental para uma compreensão em larga escala desse fenômeno tecnológico.

Sob o olhar de Okyere-Agyei (s.d.), a essa camada profunda da dark web é composta por outras muitas camadas de segurança e criptografia que ocultam a identidade dos usuários e servidores, dessa forma, existe uma enorme dificuldade no rastreamento de ações criminosas. "As atividades ilícitas prosperam na dark web devido à sua natureza descentralizada e anônima" (OKYERE-AGYEI, s.d.). Essa complexa construção tecnológica permite que conteúdos ilegais circulem e sejam

distribuídos com relativa segurança e liberdade, o que representa um desafio constante para os órgãos responsáveis que precisam lidar com crimes cibernéticos.

Do ponto de vista jurídico, fazer uso de ferramentas como malwares para coletar provas digitais também se insere nesse debate. A Universidade de Coimbra realizou um estudo, no qual, "o uso de malware pela autoridade policial levanta sérias questões quanto à legalidade e à admissibilidade das provas colhidas" (UNIVERSIDADE DE COIMBRA, s.d., p. 22). Isso porque seriam utilizados meios que não possuem credibilidade para coletar provas que seriam cruciais na resolução desse dilema, que vem ocorrendo há muito tempo entre segurança pública e privacidade individual.

Fábio Serapião (2024) publicou uma reportagem no Estadão no qual se fala sobre as investigações que se baseiam em padrões de comportamento e as correlações para que o anonimato seja rompido, segundo o veículo, "os agentes conseguiram, por meio de técnicas de rastreamento digital, encontrar os verdadeiros operadores de páginas escondidas na dark web" (SERAPIÃO, 2024). Para complementar, a Polícia Federal brasileira já utiliza tecnologia de ponta para identificar usuários da dark web, mesmo quando protegidos pelos softwares que sustentam o anonimato.

Segundo Santos *et al.* (2022), "a estrutura do mercado negro digital na dark web opera com mecanismos próprios de reputação, pagamento via criptomoedas e controle de qualidade dos produtos ilícitos" (p. 9). Dessa forma, podemos perceber que não é apenas as camadas de segurança e anonimato que tornam as coisas desafiantes para as autoridades, a operação nesse espaço digital tem uma facilidade de comercialização e com o baixo risco de punições, além das suas estruturas de comunicação profundamente enraizadas nessa camada da web, o incentivo para o crescimento desses mercados continua forte e aumentando a uma velocidade maior do que os órgãos responsáveis podem reagir.

É importante destacar que, apesar de seu uso frequente para atividades criminosas, a dark web também serve como espaço de resistência e liberdade de expressão em contextos de repressão. Jornais independentes, fóruns de discussão

política e canais de denúncias utilizam a dark web para proteger suas fontes e suas informações. Conforme Turing (2013), que discorreu a respeito dos dois lados existentes no uso da dark web, isso é algo que não pode ser ignorado. Do contrário, devemos sempre lembrar que além da criminalidade instaurada nesse ambiente, há usuários que apenas buscam compartilhar suas ideias, princípios e visões com maior liberdade e segurança.

No campo da Ciência da Informação, a distinção entre deep web e dark web faz toda diferença, uma vez que uma faz parte da outra. Segundo Santos *et al.* (2022), "a deep web corresponde a conteúdo não indexados pelos mecanismos de busca, mas a dark web é intencionalmente escondida e acessível apenas por navegadores específicos" (SANTOS *et al.*, 2022, p. 6). A compreensão dessa diferença conceitual é essencial para evitar generalizações equivocadas sobre o que é considerado legal ou ilegal dentro desses ambientes.

A problemática começa com o crescimento dos golpes nas redes sociais oriundos de perfis anônimos, golpes financeiros e outros tipos de delitos que acabam sendo protegidos pelo sistema de segurança que o anonimato prevê. De acordo com reportagem de Giovana Frioli, no Estadão Verifica (2025), perfis conhecidos como "contas dark" trabalham atraindo milhões de seguidores e promovem fraudes financeiras, muitas vezes utilizando o anonimato digital para escapar de punições.

Tanto o anonimato quanto a ausência de uma regulamentação que seja efetiva tornam a dark web num espaço propício não apenas para crimes, mas também para desafios éticos e morais. Situações como tráfico humano, pornografia ilegal e terrorismo encontram na dark web um canal de disseminação, uma vez que não há supervisão de um órgão responsável ou regras que restringem esses comportamentos. Esses crimes sempre envolvem pessoas reais, e quando as autoridades têm dificuldade em controlar a situação, é possível perceber uma fragilidade e até mesmo descredibilização para com esses órgãos.

Dessa forma, compreender a dark web exige uma abordagem multidisciplinar que envolva muitas áreas além da tecnologia, como, por exemplo, o direito, a ética e a

informação. Trata-se de um fenômeno que não pode ser reduzido a uma situação única ou específica, pois envolve interesses legítimos e ilegítimos coexistindo em um mesmo espaço digital.

8. CRIMES CIBERNÉTICOS

Com o avanço das tecnologias digitais, a internet passou a fazer parte do dia a dia das pessoas, facilitando muitas tarefas e comunicação em geral. Mas, com essa dependência crescente, também aumentaram os crimes cibernéticos — ações ilegais que usam a tecnologia para invadir sistemas, violar dados, cometer fraudes e aplicar golpes dos mais variados tipos. Segundo Maia e Costa (2023):

> Os crimes cibernéticos, geralmente, ocorrem por motivos relacionados ao lucro, ou seja, com a finalidade de obterem resultado monetário. No entanto, tais crimes, podem causar danos psicológicos de difícil reparação para às vítimas. (MAIA e COSTA; 2023; p. 112)

Maia e Costa (2023, p.112) apontam que “dentre os crimes cibernéticos mais comuns podemos apontar o hacking e invasão de sistemas, phishing, o ransomware, as fraudes financeiras, a disseminação de malware, e o assédio cibernético”. Os crimes cibernéticos citados, apesar de diferentes, são praticados no meio digital e usam dela tecnologia, causando danos aos usuários a partir de dados vazados de indivíduos e/ou empresas.

Esses ataques comprometem informações sigilosas, confiança do usuário, funcionamento de empresas e em alguns casos, causam perdas financeiras significativas a partir do roubo de identidade, o que também podem acarretar problemas emocionais da pessoa e insegurança para navegar na internet.

Assim sendo, é notável que com o avanço e evolução da tecnologia, é preciso que existam ferramentas igualmente avançadas para realizar a detecção de possíveis ameaças e alerta de prevenção aos usuários. A criação ou reforço em leis já existentes se torna indispensável e necessária para haver um controle maior dos crimes

cibernéticos, como exemplo a identificação dos autores dos crimes e a motivação, como citado no Boletim Conteúdo Jurídico:

> O Brasil ainda enfrenta grandes problemas em relação à estrutura de redes e segurança, pois a medida que a tecnologia avança os crimes virtuais aumentam proporcionalmente e ainda somos um país com escassez de mão de obra qualificada para esse trabalho, porém os esforços não são nulos e existem diversos programas e iniciativas para evitar tais atrocidades. (JURÍDICO. *Boletim Conteúdo*, v. 1223, ano XVI, p. 47.)

É compreensível que a partir do aumento dos casos de crimes cibernéticos, os setores responsáveis são sobrecarregados e muitas vezes acabam não acompanhando os avanços da tecnologia e os novos desafios a serem enfrentados. As principais dificuldades de acompanhar este avanço são a lentidão e a ineficiência de detectar ou penalizar os crimes cometidos por não obter dados e ferramentas suficientes para realizar as análises necessárias para fazer a identificação dos autores dos crimes e como agir a partir disso.

Por conta de os crimes cibernéticos serem em sua grande maioria realizados de forma anônima ou fazendo o uso de redes internacionais, a detecção desses crimes se torna ainda mais complicada, ainda mais envolvendo a política de outros países. Uma ferramenta usada para mascarar a identidade do infrator é a VPN, que são redes privadas virtuais e possuem uma criptografia avançada, sendo mais um obstáculo para encontrar outra maneira de detectar as ameaças cibernéticas, evitando novamente a necessidade de resposta rápida e eficaz para a resolução dos casos. Vale lembrar que cada país tem sua legislação e procedimentos que podem variar conforme os níveis dos crimes cometidos.

De acordo com Borges e Novais (2024, p.4954), “a evolução tecnológica pode criar novas vulnerabilidades e desafios de privacidade que as leis existentes podem não abordar adequadamente”. O investimento em ferramentas como a Inteligência Artificial para identificar e atuar na prevenção de tais crimes se torna uma opção cada vez mais relevante, já que é uma ferramenta que é rápida e pode trazer resultados a partir da análise de uma série de dados em grande volume.

No Brasil, a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, tipifica crimes informáticos. Tal lei foi importante para dar a devida prioridade a assuntos que se trate de invasão da privacidade digital. A lei proíbe o acesso de terceiros a informações e dados sensíveis de pessoas no meio digital sem a devida autorização, estando o usuário conectado ou não à internet. No entanto, estudos mostram que sua aplicação apresenta lacunas, dificultando a análise mais assertiva e eficiente às vítimas de tal crime. Como apontam Bispo e Binto (2023):

> A problemática está relacionada com os crimes virtuais que continuam a ocorrer diariamente e com o avanço tecnológico as agências responsáveis pela aplicação da lei não estão sendo eficiente para reprimir os infratores. (BISPO e BINTO; 2023; p. 355)

Além das barreiras políticas, a falta de mais legislações robustas e eficientes voltadas para os crimes cibernéticos no Brasil é preocupante, pois nas leis atuais possuem falhas que podem ser o motivo dos casos e impunidade aos criminosos. Tais falhas nas leis dificultam a atividade de autoridades competentes por trazer limitações que possam comprometer a resolução dos casos.

A criação da lei e suas falhas se dão a falta da compreensão das necessidades, exigências e análises devidas para que os crimes cometidos fossem levados a sério a partir da gravidade deles. De acordo com Bispo e Binto (2023):

> A principal crítica ao sistema jurídico é a sua incapacidade de impor sanções mais severas àqueles que cometem crimes cibernéticos. As penalidades estabelecidas pela lei para acesso não autorizado a informações e hackers são relativamente brandas, com penas que variam de três meses a um ano de prisão. Isto é amplamente considerado inadequado para desencorajar futuros infratores[...] (BISPO e BINTO; 2023; p. 363)

A Lei Geral de Proteção de Dados nº 13.709/2018, também conhecida como LGPD, é bastante referenciada por conta de se tratar da proteção de dados pessoais, principalmente tratando-se do meio virtual, em que o usuário acaba não sabendo o que ocorre com seus dados, uma vez que fornecidos a uma empresa ou até mesmo cadastro em alguns sites. A LGPD tem o objetivo de evitar possíveis usos indevidos

dos dados sensíveis de pessoas que forneceram após confiar suas informações a terceiros (BISPO e BINTO; 2023; p.364).

A internet é um campo muito vasto quando se trata de dados, as informações podem ser tanto coletadas quanto vazadas rapidamente. Possuir leis que protejam os dados é essencial para um ambiente digital controlado e bem estruturado, visando a privacidade e a confiança dos usuários.

Além da preocupação do uso indevido dos dados informados, também surge a preocupação de como esses dados estão sendo protegidos. A fragilidade da proteção dos dados é uma das causas que podem favorecer os criminosos a ter o acesso mais fácil e roubar os dados em questão.

A possibilidade de usar a Inteligência Artificial como ferramenta ao combate dos crimes cibernéticos vem se tornando uma realidade necessária e atual.

> O investimento em tecnologia desempenha um papel crucial na prevenção e combate aos crimes cibernéticos. Isso envolve uma alocação de recursos para desenvolver sistemas de segurança cibernética robustos, atualizados e proativos. Isso inclui o aprimoramento de firewalls, sistemas de detecção de intrusões e criptografia de dados. (MAIA e COSTA; 2023; p.122)

De acordo com Maia e Costa (2023, p. 122), “os governos devem investir em treinamento e capacitação para seus especialistas em segurança cibernética, para estarem preparados para enfrentar ameaças em constante evolução”. Portanto, utilizar as ferramentas tecnológicas disponíveis para combater as ameaças digitais e pessoas capacitadas para enfrentar futuras ameaças podem trazer resultados e resoluções de forma rápida e ainda mais eficiente.

Investir também na educação da população sobre ameaças tecnológicas atualmente também se torna necessária em relação a sua própria vivência com a tecnologia. Os crimes cibernéticos no ambiente digital podem impactar a todos, não importando a idade do usuário nem a classe social. A importância de manter uma

senha segura, verificar se está acessando um site confiável e não fornecer seus dados sensíveis sem a necessidade, dão à pessoa um controle a mais sobre seus dados.

É importante destacar que, embora os benefícios da IA sejam expressivos, seu uso deve estar aliado a diretrizes éticas e jurídicas, respeitando a Lei Geral de Proteção de Dados (LGPD), estabelecendo limites e sendo transparentes para com os usuários das tecnologias digitais a fim de garantir que os dados sejam coletados e protegidos com responsabilidade, gerando a confiança do usuário no meio digital.

Compreender a importância da responsabilidade do uso da Inteligência Artificial de forma ética é essencial para um bom funcionamento e aproveitamento de tal ferramenta. A ausência de instruções, punições e limitações direcionadas ao uso da IA para certas atividades acabam gerando consequências, um exemplo é a capacidade do usuário conseguir “treinar” o algoritmo da IA para conseguir as informações que deseja, mesmo que a IA em questão não seja permitida a compartilhar a informação por questões de direitos autorais e/ou invasão de privacidade pedindo acesso a dados sensíveis de terceiros, evidenciando a necessidade da regulamentação o mais rápido possível para evitar uma crise de segurança.

9. APLICAÇÃO DA INTELIGÊNCIA ARTIFICIAL EM INVESTIGAÇÕES CRIMINAIS

A inteligência artificial, definida por Russel e Norvig (2022) como "o estudo de agentes que percebem o ambiente e tomam ações" (RUSSELL; NORVIG, 2022, p. 7), possui ampla aplicação em diversas áreas, incluindo a segurança cibernética. A IA pode ser estruturada em diferentes abordagens, como o aprendizado supervisionado, não supervisionado e por reforço. Essas abordagens permitem que os sistemas aprendam com dados e tomem decisões baseadas em padrões, mesmo em contextos complexos e dinâmicos.

Sistemas de IA conseguem, assim, identificar anomalias, correlacionar eventos e automatizar processos investigativos que seriam difíceis de realizar manualmente em

tempo hábil, potencializando o trabalho de investigação em ambientes de difícil rastreamento.

9.1. Machine Learning

O avanço das técnicas de Machine Learning (ML) tem desempenhado um papel fundamental no aprimoramento de sistemas de segurança cibernética, especialmente na detecção de atividades suspeitas em ambientes complexos como a dark web. Conforme os conceitos apresentados por Bishop (2006) e Mitchell (1997), o aprendizado de máquina busca desenvolver algoritmos capazes de reconhecer padrões e identificar comportamentos anômalos com base na análise de grandes volumes de dados. Isso possibilita uma resposta mais rápida e precisa a potenciais ameaças.

Nesse contexto, a aplicação de abordagens de ML supervisionados, como Random Forest e Decision Tree, ajudam na detecção automática de atividades ilícitas em redes anônimas, como a autora Nezhad (2023) diz “Tais métodos podem ajudar profissionais de segurança cibernética, organizações e agências governamentais para detectar e prevenir crimes cibernéticos na dark web” (NEZHAD, 2023, p. 13).

Os testes realizados com as abordagens de ML tem apresentado resultados positivos na detecção de tráfego malicioso, conforme demonstrado por Nezhad (2023):

> Com base nos resultados dos experimentos realizados neste projeto, pode-se concluir que ambos os algoritmos Random Forest e Decision Tree (J48) têm um bom desempenho na detecção de tráfego VPN e Tor. (NEZHAD, 2023, p. 33)

Essas técnicas também são utilizadas para monitorar o comportamento de usuários em tempo real, avaliando, por exemplo, o tempo de permanência em determinados sites, volume de dados trafegados e a frequência de comunicações entre determinados endereços.

Os dados utilizados para esse treinamento foram obtidos do dataset

CIC-Darknet 2020, reconhecido por sua variedade de tipos de tráfego. A autora também destaca que o pré-processamento dos dados, incluindo a remoção de valores nulos, normalização e randomização, é essencial para reduzir o viés e melhorar a capacidade de generalização dos modelos de aprendizado de máquina (NEZHAD, 2023, p. 24).

Ainda segundo a autora, “embora os estudos atuais tenham atingido alta precisão na detecção de tráfego do Darknet, ainda há espaço para melhorias” (NEZHAD, 2023, p. 33), indicando o potencial de aperfeiçoamento contínuo das soluções baseadas em IA.

9.2. Deep Learning

Goodfellow, Bengio e Courville (2016) mencionam que” O aprendizado profundo permite que o computador construa conceitos complexos a partir de conceitos mais simples.” (GOODFELLOW; BENGIO; COURVILLE, 2016, p. 5), uma habilidade essencial para aplicações em ambientes como a dark web, que envolvem grandes volumes de dados não estruturados, como postagens em fóruns, imagens, e comunicações criptografadas.

Também segundo Goodfellow, Bengio e Courville (2016):

> As seções restantes deste capítulo discutem várias abordagens propostas para reduzir a dificuldade de aprender dependências de longo prazo (em alguns casos, permitindo que um RNN aprenda dependências em centenas de etapas), mas o problema do aprendizado de dependências a longo prazo continua sendo um dos principais desafios no aprendizado profundo. (GOODFELLOW; BENGIO; COURVILLE, 2016, p. 403)

Essa característica é essencial para detectar comunicações com linguagens codificadas ou disfarçadas, comuns na dark web.

Mesmo com tais limitações, modelos de deep learning têm ganhado destaque por sua capacidade de lidar com grandes volumes de dados textuais. As redes LSTM, por exemplo, conseguem identificar padrões linguísticos em mensagens publicadas em

fóruns de hackers, que indicam intenções maliciosas.

Adewopo et al. (2022) demonstra que:

> O LSTM teve uma acurácia de 94%, precisão de 90% e uma taxa de verdadeiro positivo de 91%, que é o melhor resultado de algoritmos de aprendizado profundo na identificação de textos anômalos de ameaça cibernética e previsão de exposições de vulnerabilidades que alavancam a discussão no fórum de hackers. (ADEWOPO et al., 2022, p. 10).

Tais resultados reforçam o uso dessas técnicas para sistemas de alerta precoce e prevenção de incidentes de segurança, elevando o grau de automação na identificação de comportamentos suspeitos.

9.3. Estudo de caso: DarkBERT

O DarkBERT é um modelo de linguagem natural treinado exclusivamente com dados coletados da dark web. De acordo com Yoon (2023), o DarkBERT é um modelo de IA especializado em crimes cibernéticos, projetado para atuar como um analista profissional capaz de identificar vazamentos de dados e categorizar ameaças de forma autônoma.

Além disso, o autor destaca:

> Além do caso de uso introduzido brevemente nesta postagem do blog, também temos vários projetos de pesquisa em andamento. Um chatbot disfarçado que pode se comunicar com os cibercriminosos para realizar uma investigação ativa em nome de agentes humanos, motores de inferência de crimes cibernéticos que podem provavelmente prever as ameaças em potencial etc. (YOON, 2023, p. 1).

Esses avanços apontam para uma nova era de automação e escalabilidade na análise da criminalidade digital, viabilizando investigações mais eficazes mesmo em ambientes altamente anônimos como a dark web.

Diante disso, percebe-se que a dark web, os crimes cibernéticos e a inteligência

artificial se entrelaçam em um cenário repleto de desafios e oportunidades. Enquanto o anonimato e a falta de regulamentação favorecem práticas ilícitas, o avanço das tecnologias de IA surge como uma importante aliada no enfrentamento desses problemas, ainda que envolva questões éticas e jurídicas.

10. METODOLOGIA

Para a realização deste trabalho, foi adotada a estrutura metodológica proposta por Soares (2020) em seu artigo “Pesquisa científica: uma abordagem sobre o método qualitativo”, publicado na Revista Ciranda. Segundo a autora, uma pesquisa qualitativa busca desenvolver conceitos, ideias e interpretações a partir dos dados obtidos, possuindo um caráter exploratório e subjetivo. Essa abordagem usa de métodos como observação direta e análise de documentos ou discursos, permitindo compreender de forma mais profunda sobre o conteúdo estudado.

Seguindo essa linha, a presente pesquisa adota uma abordagem qualitativa, de caráter descritivo e exploratório, visando compreender como a Inteligência Artificial (IA) pode ser utilizada para detectar crimes na dark web. A escolha dessa metodologia se justifica por permitir não apenas descrever os aspectos técnicos das tecnologias analisadas, mas também refletir sobre suas implicações sociais, éticas e legais em ambientes digitais de difícil rastreamento.

A investigação possui caráter bibliográfico e secundário, fundamentando-se em materiais já publicados sobre o tema. Foram consultadas fontes científicas e acadêmicas, como artigos, livros, relatórios e legislações disponíveis em bases como Google Scholar, SciELO e IEEE Xplore, priorizando publicações recentes, dos últimos cinco anos.

Durante o desenvolvimento da pesquisa, foi adotada uma postura interpretativa e reflexiva, permitindo que as ideias surgissem a partir do conteúdo estudado. O processo metodológico foi estruturado em etapas: (1) levantamento e seleção das referências bibliográficas, (2) categorização das fontes, (3) interpretação e síntese das informações coletadas, e (4) estudo de caso de experiências práticas, como o modelo DarkBERT e outras soluções de IA aplicadas à cibersegurança.

O estudo de caso tem como finalidade observar como sistemas de IA vêm sendo empregados na identificação de crimes em ambientes anônimos, analisando seus resultados, limitações e desafios éticos. Essa etapa complementou a análise teórica,

aproximando o estudo de situações reais e evidenciando o impacto da tecnologia na prevenção e investigação de crimes digitais.

Em todas as etapas, foi necessário manter uma análise sensível ao contexto social e tecnológico, entendendo que a relação entre tecnologia e sociedade é interdependente. Assim, a metodologia qualitativa permitiu não apenas reunir informações, mas também refletir sobre seus significados e consequências.

Por fim, os resultados esperados são de natureza teórica e interpretativa, visando ampliar a compreensão sobre o papel da Inteligência Artificial no combate aos crimes cibernéticos. É esperado que a pesquisa contribua para o debate acadêmico sobre o uso ético e responsável dessas tecnologias e para o fortalecimento da segurança digital em um cenário de constante evolução tecnológica.

11. INTELIGÊNCIA ARTIFICIAL E CIBERSEGURANÇA NO CONTEXTO BRASILEIRO

O ambiente digital brasileiro possui um cenário que apresenta uma significativa expansão das atividades maliciosas. Segundo o Relatório Global Threat Landscape da Fortinet (2025), apenas no primeiro semestre de 2025, aproximadamente 314,8 bilhões de atividades suspeitas foram detectadas, demonstrando a crescente complexidade e volume dos ataques cibernéticos no país. Com esses números, é possível reforçar a vulnerabilidade estrutural que as redes brasileiras oferecem, bem como a urgência de ferramentas e procedimentos tecnológicos avançados, como a inteligência artificial, que poderia ser utilizada para detecção de ameaças em larga escala.

Complementarmente, o Relatório Brazil Threat Landscape (2024), elaborado pela SOCRadar, foi capaz de identificar o número significativo de 91 atores suspeitos que publicaram em torno de 629 vezes em comunidades da dark web, com ameaças direcionadas especificamente às empresas brasileiras. O setor público sozinho representou 10,65% das atividades observadas na dark web, também foram registrados 248 incidentes de ransomware, que tinham pelo menos 166 organizações brasileiras como alvo.

Esses dados deixam a mostra que o foco dessas atividades ilegais são instituições nacionais, e que o uso de ferramentas avançadas como a IA pode ser um grande facilitador e instrumento estratégico para analisar tanto padrões de comportamento nos fóruns, quanto para prever novos ataques, possibilitando medidas preventivas ao invés de ações que reparam danos.

Tais indicadores quantitativos colocam ainda mais em evidência a posição que o Brasil se encontra, sendo posicionado entre os países com maior incidência de ameaças cibernéticas, evidenciando a relevância do uso de tecnologias baseadas em IA para fortalecer a ciberdefesa e reduzir a exposição de dados sensíveis em redes ocultas. Os dados expostos mostram não apenas a magnitude das ameaças digitais no Brasil, mas também a limitação dos métodos tradicionais de investigação diante da dimensão e da velocidade dos ataques.

Entretanto, essa lacuna também serve como propulsor no desenvolvimento de novas soluções baseadas, especialmente, em inteligência artificial. Sendo capaz de processar uma enorme quantidade de informações e identificar padrões complexos como característica marcante, as ferramentas que utilizam IA como base de processos se estabelecem como elementos cruciais nas operações envolvendo rastreamento de atividades ilícitas, levando a maneira como as autoridades e instituições de segurança lidam com ameaças cibernéticas a um patamar mais sofisticado.

Isto posto, as ferramentas de Inteligência Artificial (IA) vêm se consolidando como instrumentos essenciais na detecção, previsão e mitigação de atividades criminosas online, transformando como autoridades e instituições de segurança lidam com ameaças digitais. De acordo com dados da Statista (2024), cerca de 57% das organizações que utilizam IA em sistemas de segurança aplicam essas tecnologias para detecção de anomalias e comportamentos suspeitos. Esse movimento reflete a crescente confiança em modelos de aprendizado de máquina e redes neurais para auxiliar na análise de grandes volumes de dados digitais e na identificação de atividades ilícitas.

Modelos como o DarkBERT (YOON et al., 2023), desenvolvido com base em textos extraídos da dark web, representam um marco relevante nessa área, pois são capazes de interpretar o vocabulário e o contexto linguístico específicos de fóruns ilegais, possibilitando a identificação automática de conteúdos relacionados a tráfico de dados, armas, drogas e exploração sexual. Sua capacidade de compreender nuances semânticas e contextos obscuros torna-o um aliado estratégico nas investigações cibernéticas complexas.

Além disso, algoritmos tradicionais de Machine Learning, como Random Forest, Decision Tree e Long Short-Term Memory (LSTM), são amplamente explorados em tarefas de reconhecimento de padrões de tráfego anônimo e análise de fluxos de dados criptografados (NEZHAD, 2023; ADEWOPO et al., 2022). Relatórios recentes da MixMode (2024) indicam que, em média, 51% dos alertas de segurança cibernética podem ser tratados por sistemas de IA sem supervisão humana, embora esses

mesmos sistemas ainda geram quase dez mil falsos positivos por semana, o que evidencia a necessidade de verificação humana constante.

A eficácia dessas ferramentas, contudo, está diretamente vinculada à qualidade, diversidade e atualização dos dados utilizados em seu treinamento. No ambiente da dark web, endereços, fóruns e protocolos de comunicação são constantemente modificados, o que pode comprometer a precisão dos modelos e gerar resultados incorretos ou desatualizados. Além disso, a escassez de bases de dados abertas e auditáveis dificulta a reprodutibilidade e validação científica dos resultados. O mercado global de IA voltado à cibersegurança reflete esse crescimento e desafio: em 2024, o setor foi avaliado em US$ 24,82 bilhões, com projeção de atingir US$ 146,52 bilhões até 2034 (PRECEDENCE RESEARCH, 2024).

Modelos fundamentados em Deep Learning caracterizam-se pela opacidade algorítmica, isto é, pela dificuldade de compreender seus processos decisórios internos. Essa falta de aplicabilidade levanta questões éticas, jurídicas e de credibilidade (LIMA et al., 2022; KIRAT et al., 2022). No contexto das investigações criminais, tal limitação pode comprometer a transparência e a validade das decisões automatizadas empregadas como provas ou indícios, sobretudo quando não há supervisão humana qualificada.

Dessa forma, embora as ferramentas de Inteligência Artificial representem avanços técnicos expressivos, é fundamental reconhecer que não substituem o olhar humano, mas o complementam. A presença de profissionais qualificados, como peritos digitais e analistas de dados, é indispensável para validar resultados, interpretar padrões e evitar erros provenientes de sistemas automatizados. Para garantir o uso responsável dessas tecnologias, é essencial adotar mecanismos de aplicabilidade (Explainable AI – XAI), capazes de tornar as decisões algorítmicas compreensíveis, auditáveis e passíveis de contestação, assegurando assim a governança ética e o respeito aos direitos fundamentais nas práticas de investigação digital.

Seguindo essa linha de raciocínio, percebe-se a diferença de maturidade entre os países na aplicação da inteligência artificial. Cerca de 70% dos investimentos voltados para soluções de inteligência artificial ao nível mundial estão relacionados à segurança digital, em regiões como América do Norte e Europa, enquanto a América Latina representa apenas 5% desses números (STATISTA, 2025). Essa diferença expõe não apenas diferenças econômicas, mas também o déficit da capacidade técnica e institucional de cada país na integração tecnológica aos sistemas de cibersegurança.

Em um cenário comparativo, identifica-se que os países com maior estrutura técnica no uso de IA no que tange a segurança digital se mantém em posições de liderança nos índices internacionais. Por exemplo, o Government AI Readiness Index 2023 da Oxford Insights atribui aos Estados Unidos e Singapura pontuações superiores a 80/100 em tecnologia, infraestrutura de dados e governança, enquanto o Brasil sustenta uma média inferior, se estabelecendo em torno de 45,08 no segmento tecnologia (OXFORD INSIGHTS, 2023).

No que se refere ao mercado de IA aplicada à cibersegurança, outro relatório mostra que, em 2025, a América do Norte representa cerca de 38% do mercado global, enquanto o Brasil contribui com cerca de 4% da fatia regional das Américas (INDUSTRY RESEARCH.BIZ, 2025). Ainda de acordo com levantamentos recentes, na América Latina o Brasil lidera em “readiness” de IA com pontuação de 65,89 segundo o “AI Governance Statistics 2025”, superando Chile (63,19) e Uruguai (62,21), porém essa posição ainda fica aquém das nações mais avançadas em IA (AI GOVERNANCE STATS, 2025).

Muito embora o progresso e a mobilização rumo a utilização da IA do Brasil sejam positivos, o país segue enfrentando uma distância significativa em relação aos outros países no que tange a infraestrutura, grandes investimentos e facilidade na integração plena dessas tecnologias. Como consequência, o sucesso no desenvolvimento e a eficácia das soluções brasileiras no combate aos crimes cibernéticos utilizando IA não depende apenas de inovação técnica, mas do sucesso

em mobilizar recursos, políticas governamentais internas e da própria competência humana a nível nacional para lidar com as mudanças que viriam atreladas às essas novas soluções.

Ocupando uma posição logo atrás dos EUA, Reino Unido e Alemanha, o Brasil está em 44ª colocado entre 60 países avaliados a respeito do nível de desenvolvimento e aplicação da inteligência artificial, segundo o relatório *Global AI Index* (TORTOISE MEDIA, 2024). Outra revista, intitulada como *AI Readiness Index* (OXFORD INSIGHTS, 2023) complementa esse raciocínio ao colocar o Brasil em 52º lugar dentre 181 países, indicando uma adoção ainda limitada da IA em políticas públicas e práticas de segurança digital.

Esses indicadores apontam que embora o país tenha avançado em pesquisas e iniciativas privadas, a adoção prática da IA na cibersegurança brasileira se encontra em estágio emergente. Em contraposição, países com maior investimento e tradição tecnológica aplicam modelos de aprendizado de máquinas e redes neurais para prevenir ataques, detectar vulnerabilidades e automatizar respostas a incidentes. A diferença de maturidade tecnológica reforça a importância de fortalecer o ecossistema nacional de inovação e de impulsionar parcerias entre o governo e o setor privado para consolidar uma estratégia integrada de defesa digital baseada em IA.

É essencial discutir também as regulamentações e políticas de inteligência artificial implementadas em diferentes regiões do mundo e a forma em que elas influenciam a adoção ética, segura e transparente dessas tecnologias. A comparação entre iniciativas internacionais e as propostas brasileiras auxiliam a compreensão dos desafios legais e éticos envolvidos e dos caminhos possíveis para o desenvolvimento de uma política nacional robusta de IA aplicada à segurança cibernética.

No contexto brasileiro, existem alguns avanços legislativos relevantes - como o Marco Civil da Internet Lei n.º 12.965/2014), a Lei Carolina Dieckmann (Lei n.º 12.737/2012) e a Lei Geral de Proteção de Dados (Lei n.º 13.709/2018), entretanto, ainda não há uma regulamentação específica para o uso de IA. O projeto de lei n.º

2.338/2023 propõe o Marco Legal da Inteligência Artificial e está em tramitação, o projeto busca definir princípios de transparência, não discriminação e segurança, aproximando o Brasil de padrões internacionais como o AI Act Europeu - regulamento europeu que estabelece regras harmonizadas para o desenvolvimento, a comercialização e o uso de sistemas de IA no mercado da European Union.

A diferença entre os contextos internacionais e nacionais evidencia que a consolidação da IA como ferramenta estratégica de cibersegurança depende de avanços técnicos e de mecanismos legais e éticos capazes de garantir sua aplicação responsável. A ausência de uma regulação específica no Brasil pode acarretar desaceleração do uso de IA em investigações digitais e no monitoramento da dark web, enquanto países com marcos regulatórios definidos avançam em direção a uma integração segura e ética entre tecnologia e política pública.

12. CONSIDERAÇÕES FINAIS

O presente estudo reforça que o uso de IA pode ser essencial para a identificação e enfrentamento de crimes cibernéticos, com foco nos que ocorrem na dark web. Embora o anonimato e a criptografia dificultem a identificação e as investigações, as ferramentas baseadas em IA como algoritmos de Machine Learning, Deep Learning e modelos linguísticos como o DarkBERT podem ser grandes aliados para a detecção e realizar as análises em ambientes digitais de difícil rastreamento.

A dark web representa uma camada mais profunda da internet, podendo ser acessada apenas por ferramentas específicas, como o Tor, que garantem o anonimato do usuário e suas atividades nela. Apesar de sua criação ter sido voltada à liberdade de expressão, acabou se tornando um ambiente propício à prática de crimes, que também dificulta a ação de agentes nela e o monitoramento.

Nesse contexto, a crescente onda de crimes cibernéticos praticados no ambiente digital, abrange desde fraudes financeiras, distribuição de conteúdo impróprio, tráfico humano, até vazamento de dados. Tais crimes vêm sendo impulsionados pela expansão e digitalização de serviços que envolvem o tratamento e armazenamento de dados sensíveis. A ausência da revisão das políticas voltadas à proteção de crimes cibernéticos aos usuários causa a desconfiança e insegurança no ambiente virtual.

Diante desse cenário, a Inteligência artificial surge como solução para o enfrentamento de ameaças cibernéticas, pois é uma tecnologia que, se bem aplicada e estudada, pode fazer a identificação por analisar padrões em grandes volumes e atuar de forma preditiva. Dessa forma, a IA não apenas amplia a capacidade de investigação das autoridades, como também contribui para a construção de um ambiente digital mais seguro, ético e confiável.

No contexto brasileiro, o crescimento de crimes digitais reforça a necessidade de urgência no revigoramento das leis já existentes para realizar a adoção de tecnologias que aprimorem a segurança digital e que haja transparência com o uso das

ferramentas aos usuários. As políticas públicas devem incentivar a capacitação de profissionais especializados em cibersegurança que foquem no desenvolvimento de soluções com as ferramentas disponibilizadas de forma ética e responsável, podendo transformar um ambiente digital mais seguro e confiável.

Apesar dos avanços globais na aplicação de tecnologias inteligentes, o Brasil ainda enfrenta limitações significativas na consolidação de uma infraestrutura sólida voltada à cibersegurança. O país carece de investimentos consistentes em pesquisa, inovação e capacitação de profissionais especializados capazes de lidar com as complexidades do ambiente digital contemporâneo. Essa ausência de estruturação e de políticas públicas eficazes torna o território nacional mais vulnerável a ataques cibernéticos e a práticas ilícitas digitais, refletindo um cenário de defasagem em relação às potências tecnológicas internacionais.

Nesse contexto, a Inteligência Artificial pode se tornar uma aliada estratégica na prevenção, detecção e monitoramento contínuo de atividades ilegais, sobretudo na dark web, onde o anonimato e a criptografia dificultam a atuação das autoridades. No entanto, o uso dessas ferramentas deve ser conduzido com cautela, uma vez que, embora apresentem alta capacidade de processamento e resposta, são baseadas em algoritmos suscetíveis a manipulações, vieses e falhas. Tais limitações podem comprometer a precisão das análises e interferir na tomada de decisões críticas em segurança digital.

Por essa razão, a presença de profissionais especializados e qualificados no Brasil é indispensável para garantir a transparência e a confiabilidade no uso das ferramentas de Inteligência Artificial, assegurando que os dados coletados sejam devidamente validados e utilizados de forma ética, rastreável e responsável nas decisões voltadas à segurança digital e à prevenção de crimes cibernéticos. O fortalecimento da formação técnica e científica desses profissionais, aliado à criação de políticas de incentivo e programas de capacitação, constitui passo essencial para a consolidação de um ecossistema digital seguro e sustentável.

Dessa forma, a Inteligência Artificial consolida-se como um importante aliado na prevenção e no monitoramento contínuo das atividades ilícitas na dark web, contribuindo para a identificação antecipada de ameaças e para a proteção de dados sensíveis. Contudo, o uso dessas tecnologias requer cautela, uma vez que, apesar de sua rapidez e eficiência, os algoritmos que as orientam podem apresentar vieses, falhas ou vulnerabilidades passíveis de manipulação, comprometendo a precisão e a confiabilidade dos resultados.

Nesse sentido, a atuação de profissionais especializados e devidamente capacitados é indispensável para garantir a transparência, a auditabilidade e a ética no uso das ferramentas de Inteligência Artificial. Esses especialistas desempenham papel essencial na validação e interpretação dos dados, assegurando que as decisões baseadas em IA sejam tomadas de maneira responsável e alinhadas aos princípios de segurança digital e de proteção dos direitos individuais.

Além da qualificação técnica, é imprescindível que haja uma base ética sólida e uma regulamentação consistente, de modo a assegurar que o uso da IA seja não apenas eficaz, mas também seguro, confiável e socialmente legítimo. A ausência desses elementos configura uma lacuna técnica e normativa que compromete a fiscalização e o controle das práticas em ambiente digital, dificultando a consolidação da IA como ferramenta estratégica e responsável no combate aos crimes cibernéticos.

REFERÊNCIAS

ADEWOPO, Victor; GONEN, Bilal; ELSAYED, Nelly; OZER, Murat; ELSAYED, Zaghloul Saad. **Deep learning algorithm for threat detection in hackers fórum (deep web).** *arXiv*, Ithaca, 3 fev. 2022. Disponível em: <https://arxiv.org/abs/2202.01448>. Acesso em: 25 maio 2025.

ADEWOPO, I. O. *Machine Learning Models for Dark Web Threat Intelligence: LSTM-based*

BISHOP, Christopher M.. **Pattern Recognition and Machine Learning**. Nova Iorque, Ny: Springer, 2006. 778 p. (Information Science and Statistics).

BISPO, Adrielle da Silva; BINTO, Emanuel Vieira. CRIMES CIBERNÉTICOS: da ineficácia da lei carolina dieckmann na prática de crimes virtuais. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S.L.], v. 9, n. 11, p. 354-369, 4 dez. 2023. Revista Ibero-Americana de Humanidades, Ciencias e Educacao. http://dx.doi.org/10.51891/rease.v9i11.12291. Disponível em: <https://periodicorease.pro.br/rease/article/view/12291>. Acesso em: 20 abr. 2025.

BORGES, Matheus Barroso; NOVAIS, Thyara Gonçalves. DESAFIOS DA LEGISLAÇÃO BRASILEIRA EM RELAÇÃO AOS CRIMES CIBERNÉTICOS: uma análise das deficiências atuais. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S.L.], v. 10, n. 5, p. 4936-4956, 24 maio de 2024. Revista Ibero-americana de Humanidades, Ciencias e Educacao. http://dx.doi.org/10.51891/rease.v10i5.14142. Disponível em: <https://periodicorease.pro.br/rease/article/view/14142>. Acesso em: 20 abr. 2025.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União, Brasília, DF, 3 dez. 2012.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. **Projeto de Lei nº 2.338, de 2023.** Institui princípios, direitos e deveres para o uso da Inteligência Artificial no Brasil. Brasília, DF: Senado Federal, 2023. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9854001. Acesso em: 8 nov. 2025.

BRITO, Sabrina. Google avisará se seus dados foram vazados na dark web. **O Estadão.** [S. l], p. 1-1. 7 de maio de 2025. Disponível em: <https://www.estadao.com.br/link/cultura-digital/google-avisara-se-seus-dados-foram-vazados-na-dark-web-gratuitamente-nprei/>. Acesso em: 25 maio 2025.

CASTELLS, Manuel. ***A sociedade em rede*.** 17. ed. São Paulo: Paz e Terra, 2003. (A Era da Informação: Economia, Sociedade e Cultura, v. 1).

CORREIA, Pedro Miguel Alves Ribeiro; SANTOS, Susana Isabel da Silva. A ação do Estado em matéria de cibersegurança: estudo de percepções no caso português. **Simbiótica. Revista Eletrônica**, [S.L.], v. 5, n. 2, p. 01-20, 9 ago. 2019. Universidade Federal do Espírito Santo. http://dx.doi.org/10.47456/simbitica.v5i2.23142. Disponível em: <https://periodicos.ufes.br/simbiotica/article/view/23142>. Acesso em: 3 out. 2025.

DEODATO, Bruno Rogério Leandro. **A INVESTIGAÇÃO CRIMINAL EM AMBIENTE DIGITAL E A UTILIZAÇÃO DE MALWARE COMO MEIO DE OBTENÇÃO DE PROVA**: entre a ineficácia e a ilegalidade. 2024. 144 f. Dissertação (Mestrado) - Curso de Direito, Universidade de Coimbra, Coimbra, 2024. Disponível em: <https://hdl.handle.net/10316/118220>. Acesso em: 25 maio 2025.

DEY, Maitrayee. **AI Governance Statistics By Market Size, Corporate Governance and Adoption, Funding, Trends And Facts (2025)**. 2025. Disponível em: https://electroiq.com/stats/ai-governance-statistics. Acesso em: 8 nov. 2025.

DEY, Maitraye. **AI Governance Statistics 2025 – Global and Latin America**

Rankings. New York: AI Governance Stats Lab, 2025. Disponível em: https://electroiq.com/stats/ai-governance-statistics/. Acesso em: 8 nov. 2025.

FRIOLI, Giovana. 'Contas dark': perfis anônimos de saúde com 42 milhões de seguidores aplicam golpes no Instagram. **O Estadão.** [S. L.], p. 1-1. 17 maio 2025. Disponível em: <https://www.estadao.com.br/estadao-verifica/contas-dark-perfis-anonimos-de-saude-com-42-milhoes-de-seguidores-aplicam-golpes-no-instagram/>. Acesso em: 25 maio 2025.

GOODFELLOW, Ian; BENGIO, Yoshua; COURVILLE, Aaron. **Deep Learning**. [S. L.]: The Mit Press, 2016. 775 p.

HANKINS, Emma; NETTEL, Pablo Fuentes; MARTINESCU, Livia; GRAU, Gonzalo; RAHIM, Sulamaan. **Government AI Readiness Index 2023**. 2023. Disponível em: https://oxfordinsights.com/wp-content/uploads/2023/12/2023-Government-AI-Readiness-Index-1.pdf. Acesso em: 8 nov. 2025.

INDUSTRY RESEARCH. BIZ. **Artificial Intelligence-Based Cybersecurity Market – Regional Outlook 2025.** London: Industry Research Biz, 2025. Disponível em: https://www.industryresearch.biz/market-reports/artificial-intelligence-based-cybersecurity-market-104058. Acesso em: 8 nov. 2025.

JURÍDICO. ***Boletim Conteúdo Jurídico*.** Brasília, DF, v. 1223, ano XVI, 2024. 235 f. ISSN 1984-0454.

KIRAT, D. et al. ***Explainability in Cybercrime Detection Systems****: Challenges and Prospects. IEEE Security & Privacy*, v. 20, n. 4, p. 45–54, 2022.

LIMA, R. et al. ***Ethical and Legal Aspects of AI in Criminal Investigations****. ScienceDirect – Forensic Science International: Digital Investigation*, v. 42, 2022.

LAB, Fortinet Research. **Global Threat Landscape Report – 1st Semester 2025**. São Paulo: Fortinet Research Lab, 2025. Disponível em:

<https://www.ecommerceupdate.org/en/news/risco-digital-314-bilhoes-de-atividades-maliciosas-sao-detectadas-no-brasil-no-1o-semestre-de-2025/>. Acesso em: 7 nov. 2025.

MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. CRIMES CIBERNÉTICOS. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S.L.], v. 9, n. 10, p. 109-126, 31 out. 2023. Revista Ibero-Americana de Humanidades, Ciencias e Educacao. http://dx.doi.org/10.51891/rease.v9i10.11580. Disponível em: <https://periodicorease.pro.br/rease/article/view/11580>. Acesso em: 20 abr. 2025.

MC CARTHY, John; MINSKY, Marvin L.; ROCHESTER, Nathaniel; SHANNON, Claude E. ***A proposal for the Dartmouth Summer Research Project on Artificial Intelligence.*** Hanover, NH: Dartmouth College, 1956.

MITCHELL, Tom M.. **Machine Learning**. [S. L.]: McGraw-Hill, 1997. 432 p.

MIXMODE. **State of AI in Cybersecurity Report 2024**. Santa Barbara: MixMode Inc., 2024.

NEZHAD, A. **Machine Learning Approaches for Secure Network Monitoring**. ACM Digital Library, 2023.

NEZHAD, Sahra Zangeneh. **Dark Web Traffic Detection Using Supervised Machine Learning**. 2023. 36 f. Dissertação (Mestrado) - Curso de Engenharia, The Department Of Electrical And Computer Engineering, University Of Victoria, Vitória, 2023. Disponível em: <http://hdl.handle.net/1828/15070>. Acesso em: 25 maio 2025.

NEZHAD, M. *Detection of Encrypted and Anonymous Traffic Using Random Forest and Decision Tree Algorithms*. **IEEE Transactions on Information Forensics and Security**, v. 18,

OKYERE-AGYEI, Stanley. *Even Though I Walk Through the Shadows... The Dark Web – A Review.* In: **Research Nexus in IT, Law, Cyber Security & Forensics.** [S.I.:] AIMS/CRP Book Chapter Series, 2022. p. 209-214. DOI: 10.22624/AIMS/CRP-BK3-P34. Disponível em: <https://www.isteams.net/ITlawbookchapter2022>. Acesso em: 6 nov. 2025.

PRECEDENCE RESEARCH. **Artificial Intelligence in Cybersecurity Market Size, Growth and Trends 2024–2034**. Ontario: Precedence Research, 2024.

RECUERO, Raquel. ***Redes sociais na internet*.** 2. ed. Porto Alegre: Sulina, 2014.

RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence**: **a modern approach.** 4. ed. [S. L.]: Pearson, 2020. 1136 p.

SERAPIÃO, Fábio. **PF tem tecnologia para identificar usuários da "dark web".** *Estadão*, São Paulo, 2025. Disponível em: <https://www.estadao.com.br/politica/blog-do-fausto-macedo/pf-tem-tecnologia-para-identificar-usuarios-da-dark-web/>. Acesso em: 25 maio 2025.

SOARES, Simaria de Jesus. **PESQUISA CIENTÍFICA: uma abordagem sobre o método qualitativo.** Revista Ciranda, [S.L.], v. 3, n. 1, p. 1-13, 13 jan. 2020. Disponível em: <https://www.periodicos.unimontes.br/index.php/ciranda/article/view/314>. Acesso em: 22 out. 2025.

SOCRADAR. **Brazil Threat Landscape Report 2024**. Ancara (Ankara), Turquia: Socradar Cyber Threat Intelligence Team, 2024. Disponível em: <https://socradar.io/wp-content/uploads/2024/10/SOCRadar-Brazil-Threat-Landscape-Report-2024.pdf>. Acesso em: 7 nov. 2025.

SOUZA E SILVA, Adriana de. ***Cultura móvel: comunicação e novas práticas sociais*.** São Paulo: Paulus, 2018.

STATISTA. **Artificial Intelligence in Cybersecurity – Market Revenue by Region (2025).** Hamburg: Statista Research Department, 2025. Disponível em: https://www.statista.com/topics/12001/artificial-intelligence-ai-in-cybersecurity/?srsltid=AfmBOop_FAixjUAt1rQ84-Z9ok8tEZHi89CFIi9r4fQr8EnS3JZnnJgc#topicOverview. Acesso em: 8 nov. 2025.

STATISTA. **Global Use of Artificial Intelligence in Cybersecurity by**

Application Area 2024. Statista Research Department, 2024.

TORTOISE MEDIA. **The Global Artificial Intelligence Index 2024.** London: Tortoise Intelligence, 2024. Disponível em: https://www.tortoisemedia.com/2024/09/18/the-global-artificial-intelligence-index-2024/. Acesso em: 8 nov. 2025.

TURING, Alan M. **Computing machinery and intelligence.** *Mind*, Oxford, v. 59, n. 236, p. 433–460, 1950.

TURING, Alan M. ***Dark web demystified*.** [S.l.]: CreateSpace Independent Publishing Platform, 2013.

UNIÃO EUROPEIA. **Regulation (EU) 2024/1689 of the European Parliament and of the Council – Artificial Intelligence Act.** Strasbourg: European Parliament, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689. Acesso em: 8 nov. 2025

VIGNOLI, Richele Grenge; MONTEIRO, Silvana Drumond. Deep Web e Dark Web: similaridades e dissiparidades no contexto da ciência da informação. **Transinformação**, [S.L.], v. 32, p. 1-12, 21 ago. 2020. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/2318-0889202032e190052. Disponível em: <https://www.scielo.br/j/tinf/a/8QrnXfB7VXrG4G6ywmhZngK/?format=html&lang=pt>. Acesso em: 25 maio 2025.

YOON, Changhoon. **Introducing DarkBERT: Combating cyber crimes at scale with AI**. 2023. Disponível em: <https://medium.com/s2wblog/introducing-darkbert-combating-cyber-crimes-at-scale-with-ai-5821e2ff74e3>. Acesso em: 25 maio 2025.

YOON, S. et al. DarkBERT: A Language Model for the Dark Web. **Proceedings of the Association for Computational Linguistics**, v. 61, p. 4521–4534, 2023.