UNILEÃO
CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO
CURSO DE GRADUAÇÃO EM DIREITO

TALLES BARBOSA DE LACERDA

CIBERCRIME NO BRASIL: A utilização da Inteligência Artificial como possibilidade de prevenção

JUAZEIRO DO NORTE-CE
2023

TALLES BARBOSA DE LACERDA

CIBERCRIME NO BRASIL: A utilização da Inteligência Artificial como possibilidade de prevenção

Trabalho de Conclusão de Curso – *Artigo Científico,* apresentado à Coordenação do Curso de Graduação em Direito do Centro Universitário Doutor Leão Sampaio, em cumprimento às exigências para a obtenção do grau de Bacharel.

Orientador: Prof. Esp. Francisco José Martins Bernardo de Carvalho

JUAZEIRO DO NORTE-CE
2023

TALLES BARBOSA DE LACERDA

CIBERCRIME NO BRASIL: A utilização da Inteligência Artificial como possibilidade de prevenção

Este exemplar corresponde à redação final aprovada do Trabalho de Conclusão de Curso de TALLES BARBOSA DE LACERDA

Data da Apresentação: 08/12/2023

BANCA EXAMINADORA

Orientador: Prof. Esp. Francisco José Martins Bernardo de Carvalho

Membro: Prof. Esp. Alyne Leite de Oliveira

Membro: Prof.

JUAZEIRO DO NORTE-CE
2023

CIBERCRIME NO BRASIL: A utilização da Inteligência Artificial como possibilidade

de prevenção

Talles Barbosa de Lacerda[1]
Francisco José Martins Bernardo de Carvalho [2]

RESUMO

É amplamente reconhecido por todos que a tecnologia adentrou as sociedades no mundo, tornando-se essencial em quase todas aas áreas das pessoas em geral. Dado essa facilidade com que a tecnologia torna a vida atualmente, isso traz consigo um fardo: a facilidade de ser enganados. Desde que a tecnologia se fez presente no cotidiano, os casos de cibercrimes aumentaram proporcionalmente, restando a adaptação penal para os casos em questões. Dito isso, este trabalho tem como objetivo principal fazer uma análise de qual é a relação entre a Inteligência Artificial (IA) e a prevenção do cibercrime, identificando como a IA pode ser aplicada para identificar ameaças cibernéticas, e analisar as suas principais técnicas na detecção dessas ameaças. Para entender essa importância, mister se faz entender a evolução da tecnologia na sociedade, até chegar ao ponto da criação das inteligências artificiais, entender como a legislação brasileira se formou para combater crimes cometidos nos meios virtuais, para, enfim, perceber como a Inteligência Artificial será tão importante na prevenção destes crimes. Para chegar a essa conclusão, foi feito uma pesquisa bibliográfica, onde inclui a legislação atual do ordenamento jurídico brasileiro, trabalhos acadêmicos na área de pesquisa, livros e artigos que trouxeram bastante informação importante acerca desse assunto tão necessário de se estudar nos tempos atuais. Diante de todo o exposto, concluiu-se que, sim, a Inteligência Artificial poderá ser utilizada para prevenir os cibercrimes na sociedade contemporânea.

Palavras Chave: Inteligência Artificial. Cibercrime. Prevenção.

ABSTRACT

It is widely recognized by everyone that technology has penetrated societies worldwide, becoming essential in nearly all areas of people's lives. Given the ease with which technology makes life today, it brings with it a burden: the ease of being deceived. Since technology became part of everyday life, cybercrime cases have increased proportionally, necessitating legal adaptation for such cases. That said, this work aims to provide a brief account of Artificial Intelligence and how it has the power to prevent cybercrimes. To understand this importance, it is essential to grasp the evolution of technology in society, leading to the creation of artificial intelligences, understanding how Brazilian legislation was formed to combat crimes committed in virtual environments, and finally, realizing how Artificial Intelligence will be crucial in preventing these crimes. To reach this conclusion, a bibliographic research was conducted, including the current legislation in the Brazilian legal system, academic research in the field, books, and articles that provided significant information on this much-needed subject in today's times. In light of all the above, it was concluded that, indeed, Artificial Intelligence can be used to prevent cybercrimes in contemporary society.

[1] Talles Barbosa de Lacerda – Graduando do Curso de Direito do Centro Universitário Doutor Leão Sampaio/Unileão; e-mail: tallesbarbosa2k18@gmail.com.
[2] Francisco José Martins Bernardo de Carvalho - Professor do Curso de Direito do Centro Universitária Leão Sampaio - Graduação em Direito pela Centro Universitário Paraíso do Ceará - Pós-Graduado em Direito Previdenciário e Trabalhista pela Universidade Regional do Cariri - Pós-Graduado em Direito Público pela Faculdade LEGALE - Pós-Graduado em Gestão Pública pela UECE - Graduando em Pedagogia pela UNINASSAU Recife - Formação Pedagógica R2 em História e Geografia pela UNIBF. Advogado inscrito na OAB CE n. 32800. E-mail: franciscocarvalho@leaosampaio.Edu.br.

Keywords: Artificial intelligence. Cybercrime. Prevention.

1 INTRODUÇÃO

A crescente presença da inteligência artificial está revolucionando a forma como se lida com o cibercrime, tornando-se uma peça fundamental na sua prevenção. 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).

A detecção precoce de ameaças é apenas um dos aspectos do papel da inteligência artificial na prevenção do cibercrime. Através da análise preditiva, a IA pode antecipar possíveis vulnerabilidades e pontos fracos em sistemas, permitindo que medidas preventivas sejam tomadas antes que um ataque ocorra. Além disso, a automação impulsionada pela IA pode aliviar a carga de trabalho das equipes de segurança, permitindo que elas se concentrem em atividades de maior complexidade enquanto as tarefas rotineiras são executadas por sistemas inteligentes (PORTA, 2023).

No entanto, é importante considerar que os avanços na inteligência artificial também podem ser usados pelos próprios criminosos. A chamada "IA adversária" envolve a criação de algoritmos capazes de contornar as defesas baseadas em IA explorando suas fraquezas. Portanto, à medida que a IA evolui como aliada na prevenção do cibercrime, é essencial um desenvolvimento contínuo de estratégias e tecnologias de segurança que acompanhem a sofisticação das ameaças digitais (PRINCE, 2023).

O principal motivo desta pesquisa é analisar qual a relação entre a Inteligência Artificial (IA) e a prevenção do cibercrime, identificar como a IA pode ser aplicada para identificar ameaças cibernéticas, analisar as suas principais técnicas na detecção dessas ameaças, como machine learning, deep learning, redes neurais e algoritmos genéticos.

Para ilustrar a eficácia dessas técnicas, apresentar-se-á estudos de casos e exemplos reais de como a IA tem sido implementada com sucesso na defesa contra ameaças cibernéticas. Essas histórias destacarão a importância da IA em cenários diversos, desde a proteção de infraestruturas críticas até a segurança de transações financeiras online.

No entanto, à medida que a IA se torna uma aliada indispensável na prevenção do cibercrime, surgem questões éticas e legais importantes. Explorar-se-á as implicações

relacionadas à privacidade, responsabilidade e transparência que acompanham o uso crescente da IA em segurança cibernética, garantindo um debate equilibrado sobre o tema.

Além disso, este trabalho também enfatizará a importância da educação e conscientização na prevenção do cibercrime. Não basta depender da tecnologia; os usuários desempenham um papel fundamental na segurança digital, e a compreensão das ameaças e das melhores práticas é essencial.

Finalmente, refletir sobre o futuro da IA na prevenção do cibercrime. Como essa tecnologia continuará a evoluir para enfrentar ameaças cada vez mais complexas? Quais desafios futuros podemos antecipar na batalha contra o cibercrime em um mundo em constante transformação? Este trabalho busca fornecer uma visão abrangente e atualizada sobre um dos temas mais críticos da nossa era digital, demonstrando como a IA desempenha um papel central na defesa contra um inimigo invisível que ameaça constantemente nossos sistemas e informações.

2 REFERENCIAL TEÓRICO

2.1 APRESENTAÇÃO BÁSICA À INTELIGÊNCIA ARTIFICIAL E SUAS PRINCIPAIS FUNÇÕES

2.1.1 CONTEXTO HISTÓRICO DA INTELIGÊNCIA ARTIFICIAL (IA)

O contexto histórico da Inteligência Artificial (IA) no aspecto da segurança de dados é fascinante e envolve uma progressão significativa ao longo de várias décadas. O início de tudo se deu na década de 1950, onde ocorreu a origem das IA, quando pesquisadores começaram a explorar a ideia de criar máquinas capazes de imitar a inteligência humana. No entanto, naquela época, a segurança de dados não era uma preocupação central, pois a IA estava em seus estágios iniciais de desenvolvimento (X2, 2020).

Com o decorrer dos anos, e com a percepção do que essas máquinas poderiam fazer, foi na década de 1960 que ocorreu o surgimento das primeiras redes de computadores. Com o advento das redes de computadores nesta década, a coleta e o compartilhamento de dados se tornaram mais comuns. Só aqui houve a necessidade de segurança de dados, uma vez que informações confidenciais podiam ser acessadas remotamente (SILVA, 2022).

De acordo com o autor Daniel Neves Silva (2022), eis o motivo da criação da internet:

> "A internet foi criada para estabelecer uma rede de informação e comunicação entre centros militares e de produção científica dos Estados Unidos. A intenção foi facilitar a troca de informações entre esses espaços e, consequentemente, consolidar um mecanismo de defesa contra os soviéticos, já que o contexto era da Guerra Fria." (SILVA, 2022, pág. 3).

Continuando com o progresso das Inteligências Artificiais, na década de 1970 surge a criptografia e segurança cibernética. Esse período, surgiram avanços fundamentais que moldaram o cenário de segurança digital. Um dos eventos mais notáveis foi a criação do algoritmo de criptografia RSA, por Ron Rivest, Adi Shamir e Leonard Adleman, em 1977 (NOVAGEO, 2022).

A RSA representa um dos sistemas pioneiros de criptografia de chave pública e goza de uma ampla aplicação na garantia da segurança da transmissão de dados. Neste método de criptografia, a chave usada para codificar é pública e se diferencia da chave para decodificar, que é mantida em sigilo (privada). A sigla do algoritmo "RSA" é formada pelos nomes iniciais de seus criadores: Ron Rivest, Adi Shamir e Leonard Adleman (NOVAGEO, 2022).

Esse algoritmo de chave pública revolucionou a forma como os dados são protegidos online, estabelecendo as bases para comunicações seguras na internet. Além disso, em 1976, o padrão Data Encryption Standard (DES) foi adotado pelo governo dos EUA, marcando uma tentativa inicial de regulamentar a criptografia (KLUSAITÉ, 2022).

A década de 1970 foi um período de descobertas cruciais e marcos no campo da criptografia e segurança cibernética, que pavimentaram o caminho para as complexas soluções de proteção de dados e redes que utilizamos atualmente. Esta década também foi marcada com o surgimento da internet, que emergiu simultaneamente com os primeiros computadores, nos Estados Unidos, com o propósito de conectar a comunidade acadêmica de cientistas e estudantes ao Governo Federal e às forças militares (PAESANI, 2014).

Isso ocorreu durante a Guerra Fria, um período marcado pelo conflito entre as duas principais superpotências, os EUA e a URSS, que competiam pela supremacia ideológica. Esse contexto impulsionou avanços tecnológicos significativos, como a corrida armamentista e a corrida espacial, áreas nas quais a busca pelo domínio era de extrema importância. Não há dúvida de que o progresso tecnológico resulta da colaboração entre entidades governamentais e instituições acadêmicas na pesquisa e desenvolvimento de conhecimentos científicos específicos (PAESANI, 2014).

Em 1980 ocorreu um grande aumento no crescimento das ameaças cibernéticas com a proliferação de computadores pessoais e redes empresariais, as ameaças cibernéticas começaram a se mostrar como um grande inimigo, já que computadores com conexão à internet eram empregados por governos, entidades financeiras e diversas esferas da sociedade. Isso resultou em um aumento substancial das chances de os cibercriminosos obterem informações preciosas ou, simplesmente, gerarem tumultos por meio de vírus e diferentes formas de software

malicioso (KLUSAITÉ, 2022).

A popularização da Internet na década de 1990 aumentou significativamente o compartilhamento de informações online, testemunhando um surto de expansão da internet, com um aumento constante no acesso global de pessoas à rede. Ao longo dessa década, um experimento na internet teve transformações marcantes que se tornaram mais disponíveis, simplificadas e adotadas em larga escala. Isso levou ao desenvolvimento de firewalls, sistemas de detecção de intrusões e outras tecnologias de segurança cibernética (TERRA, 2023).

Essa popularização foi um fenômeno transformador que revolucionou a forma como as pessoas se comunicam, acessam informações e realizam negócios. Essa era ficou marcada pelo crescimento exponencial da World Wide Web e por uma série de eventos que contribuíram para a disseminação da internet, como, por exemplo, o surgimento das redes sociais e os serviços de mensagens instantâneas (TERRA, 2023).

Com o passar da década, o acesso à internet se tornou mais acessível e comum nas casas das pessoas, enquanto a conexão discada de alta velocidade substituiu as lentas conexões dial-up. A internet se tornou um meio de comunicação global, e as pessoas começaram a compartilhar informações, trocar e-mails, participar de fóruns de discussão e explorar uma ampla gama de conteúdo online (GAIDIS, 2023).

Os anos 2000 testemunharam a crescente aplicação da IA e do aprendizado de máquina na segurança cibernética. Os sistemas de IA começaram a ser usados para identificar padrões de ataque, analisar grandes volumes de dados em busca de comportamento anômalo e automatizar a detecção de ameaças (GAIDIS, 2023).

Já na década de 2010, a IA começou a ser utilizada na prevenção e detecção de ameaças, com o aumento exponencial no volume de dados e o surgimento de ataques cibernéticos cada vez mais sofisticados, a IA 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).

Como citou Vinicius Gaidis (2023), com relação a detecção que as Inteligências Artificiais podem fazer:

> A IA tem um papel fundamental na detecção de ameaças cibernéticas. Algoritmos de aprendizado de máquina podem analisar grandes volumes de dados em tempo real, identificar padrões suspeitos e distinguir atividades maliciosas de comportamentos normais. A detecção de anomalias, a análise de comportamento e a identificação da presença de malwares são itens em que a inteligência artificial pode ser aplicada com sucesso. (GAIDIS, 2023, p. 1).

Uma das principais áreas em que a IA se destacou foi na detecção de ameaças cibernéticas. À medida que os cibercriminosos se tornaram mais sofisticados, a IA foi adotada

para analisar volumes massivos de dados e identificar comportamentos suspeitos. Sistemas de IA, como os sistemas de detecção de intrusão baseados em aprendizado de máquina, conseguiram identificar atividades maliciosas com maior precisão do que as soluções tradicionais (GAIDIS, 2023).

Além disso, a IA desempenhou um papel vital na análise de grandes conjuntos de dados para identificar vulnerabilidades em sistemas e aplicativos. Isso permitiu que as organizações corrigissem falhas de segurança antes que fossem exploradas por invasores.

Em termos de prevenção, a IA também foi usada para desenvolver sistemas de autenticação avançados, como a autenticação multifator (MFA) baseada em IA, que tornou mais difícil para os criminosos obter acesso não autorizado. Além disso, chatbots e assistentes virtuais foram usados para fornecer suporte ao cliente e orientação em tempo real, ajudando a evitar golpes e fraudes online (ECOTRUST, 2022).

A autenticação multifator (MFA), é uma arma bastante eficaz para a proteção dos dados, como cita o Blog EcoTrust (2022) sobre isso:

> Os primeiros passos para evitar esse tipo de situação são a utilização de senhas fortes e a variação das senhas para diferentes categorias de acesso.
> Ou seja, além de não utilizar senhas óbvias como datas ou expressões simples, também é necessário evitar a utilização da mesma senha para diversas atividades.
> Esses são cuidados básicos que precisam ser tomados, mas estão longe de serem suficientes para a proteção dos dados do seu negócio.
> Os cuidados e recursos de segurança da informação funcionam bem quando empregados conjuntamente, integrando uma cultura organizacional voltada para a segurança.
> Nesse sentido, a autenticação multifator, também conhecida como MFA, é um recurso altamente recomendável.
> Trata-se de uma medida de segurança que possibilita a exigência de um ou mais fatores de autenticação extras após a autenticação com usuário e senha (ECOTRUST, 2022, p. 2).

Foi somente nos dias atuais que se pôde, minimamente, ter uma noção do que as IA realmente tem o poder de fazer. A cada década que se passa, ocorre um avanço tecnológico extremo com relação à essas inteligências e tudo o que elas podem alcançar. A IA continua a evoluir na segurança de dados, incorporando técnicas avançadas de aprendizado de máquina, processamento de linguagem natural e análise de comportamento anômalo. Também se tornou parte integrante da resposta a incidentes, automatizando a mitigação de ameaças em tempo real.

O futuro da IA na segurança de dados trará desafios e oportunidades. A crescente sofisticação das ameaças exigirá uma IA cada vez mais avançada. Ao mesmo tempo, questões éticas, legais e de privacidade relacionadas à IA na segurança cibernética precisarão ser abordadas de forma abrangente.

Em resumo, a evolução da IA na segurança de dados é intrinsecamente ligada à expansão

da tecnologia da informação e das ameaças cibernéticas. A IA se tornou um pilar fundamental na proteção de dados e sistemas em um mundo cada vez mais digitalizado e interconectado.

2.1.2 FUNDAMENTOS DA INTELIGÊNCIA ARTIFICIAL EM SEGURANÇA CIBERNÉTICA

Os conceitos básicos da inteligência artificial (IA) e sua aplicação à segurança cibernética são fundamentais para entender como a IA desempenha um papel crucial na detecção e prevenção de ameaças cibernéticas. Ela procura emular a inteligência humana por meio de algoritmos que identificam padrões e utilizam esse processo para fazer previsões e identificar tendências. À medida que aprimorar a segurança cibernética se tornou um desafio crescente para as equipes de segurança de TI, soluções inteligentes e especializadas estão ganhando destaque na abordagem das vulnerabilidades em constante evolução (BERTOLLI, 2022).

Dado que a maioria das violações de segurança decorre de falhas humanas, podemos notar um aumento significativo nos ataques de phishing. Ao utilizar a IA para treinar sistemas a imitar o comportamento humano, torna-se possível reduzir as ocorrências de erros que resultam em riscos de segurança. Assim, a IA deve ser capaz de analisar informações originadas de diversas fontes, identificar ameaças em potencial e formular automaticamente as melhores respostas para incidentes (BERTOLLI, 2022).

Para entender melhor como funciona a IA, se faz necessário entender alguns conceitos básicos, como por exemplo, entender o que é o aprendizado de máquina, também conhecido como machine learning, que é uma subárea da IA que se concentra em desenvolver algoritmos e modelos que permitem que sistemas aprendam com dados e melhorem sua performance ao longo do tempo (SILVEIRA, 2023).

Na segurança cibernética, o aprendizado de máquina é usado para identificar padrões e comportamentos anômalos em dados de rede e sistemas. Isso ajuda na detecção de atividades suspeitas, como intrusões e ataques (SILVEIRA, 2023).

Há também a necessidade de se conhecer as redes neurais artificiais, que são modelos inspirados na estrutura do cérebro humano. Elas são usadas em deep learning, uma técnica de aprendizado de máquina, para tarefas complexas, como análise de imagens e processamento de linguagem natural. Na segurança cibernética, redes neurais podem ser empregadas para melhorar a detecção de malware e analisar o tráfego de rede em busca de comportamentos maliciosos (SILVEIRA, 2023).

O conceito de redes neurais artificiais é descrito por Emerson Alecrim (2004), que diz:

> Redes neurais artificiais são um conceito da computação que visa trabalhar no processamento de dados de maneira semelhante ao cérebro humano. O cérebro é tido como um processador altamente complexo e que realiza processamentos de maneira paralela. Para isso, ele organiza sua estrutura, ou seja, os neurônios, de forma que eles realizem o processamento necessário. Isso é feito numa velocidade extremamente alta e não existe qualquer computador no mundo capaz de realizar o que o cérebro humano faz (ALECRIM, 2004, pág. 1 e 2).

Já a ACF, análise de comportamento anômalo, envolve a criação de perfis de comportamento normal para sistemas e usuários. Qualquer desvio significativo desse comportamento é considerado anômalo e pode ser indicativo de uma ameaça. A IA é usada para automatizar a análise de comportamento, identificando atividades incomuns ou suspeitas que podem indicar um ataque (LOIK, 2021).

Existe também a função de processamento de linguagem natural (PLN), que é a capacidade que uma máquina tem de entender e processar linguagem humana. Na segurança cibernética, a NLP é usada para analisar e classificar automaticamente textos, como e-mails e mensagens, em busca de conteúdo malicioso, como phishing ou spam (KOVACS, 2021).

E por fim, a detecção em tempo real, que é a capacidade da IA na segurança cibernética de poder analisar grandes volumes de dados em tempo real. Isso significa que os sistemas de IA podem identificar ameaças instantaneamente e tomar medidas para bloqueá-las antes que causem danos significativos.

IA na segurança cibernética aproveita técnicas de aprendizado de máquina, redes neurais, análise de comportamento e processamento de linguagem natural para identificar e responder a ameaças cibernéticas. Ela é fundamental para a detecção precoce de atividades maliciosas, a adaptação às táticas em evolução dos cibercriminosos e a proteção dos sistemas e dados valiosos contra-ataques.

2.1.3 A IMPORTÂNCIA DO TREINAMENTO DE MODELOS DE IA COM DADOS HISTÓRICOS DE ATAQUES E ANOMALIAS

O treinamento de modelos de Inteligência Artificial (IA) com dados históricos de ataques e anomalias é de suma importância na detecção de ameaças cibernéticas. Essa abordagem permite que os sistemas de IA aprendam com o passado e reconheçam padrões sutis e comportamentos suspeitos que seriam difíceis ou impossíveis de serem identificados por meio de métodos tradicionais de segurança.

O treinamento com dados históricos é crucial para que os modelos de IA compreendam as táticas, técnicas e procedimentos (TTPs) usados por invasores no passado. Isso possibilita a identificação de variações ou adaptações dessas táticas, tornando a detecção de ameaças mais

eficaz. Além disso, esses modelos podem aprender a distinguir entre atividades normais e anômalas com base em padrões observados anteriormente. Com o treinamento adequado, a IA se torna capaz de tomar decisões em tempo real para proteger sistemas de informação (LOIK, 2021).

Alguns exemplos de detecção de atividades suspeitas e anômalas são bastante importantes para o funcionamento da IA. Pode-se dar vários exemplos dessas detecções, mas será citado as principais, como a detecção de acesso não autorizado, que basicamente é um modelo de IA treinado com dados históricos que pode identificar tentativas de acesso não autorizado a sistemas ou redes, mesmo que o invasor esteja usando credenciais roubadas. Ele reconhece o comportamento atípico do invasor, como horários incomuns de login ou locais de acesso não usuais (LOIK, 2021).

Há também a detecção de malware, que é quando a IA consegue analisar o comportamento de programas em execução e identificar comportamentos suspeitos que correspondam a atividades maliciosas, como a comunicação com servidores de comando e controle ou a modificação não autorizada de arquivos do sistema (GARRETT, 2021).

Para haver a detecção de um malware é necessário haver um antivírus instalado no computador, como relata Filipe Garrett (2021):

> A detecção de qualquer tipo de malware depende, sobretudo, de um software específico: o chamado "antivírus". Mesmo as opções gratuitas mais simples terão mecanismos de monitoramento em tempo real que são capazes de identificar traços de malwares assim que eles tentam se instalar no seu sistema. A ideia é usar esse monitoramento em tempo real para impedir que qualquer tipo de ameaça se instale no seu computador e provoque dores de cabeça no futuro. (GARRETT, 2021, pág. 1)

Modelos de IA podem também analisar e-mails para a detecção de phishing, como remetentes desconhecidos, links suspeitos ou anexos maliciosos. Eles também podem identificar tentativas de engenharia social com base em padrões linguísticos (GARRETT, 2021).

A IA pode examinar o tráfego de rede em busca de atividades anômalas, como varreduras de portas não autorizadas, tráfego suspeito em horários incomuns ou aumento súbito de transferência de dados, indicando possível vazamento de informações. Já em sistemas de informação, a IA pode identificar comportamentos de usuário que desviam do padrão histórico. Por exemplo, acessos frequentes a pastas sensíveis por um usuário que normalmente não tem esse privilégio podem levantar suspeitas (GARRETT, 2021).

2.2 O SURGIMENTO DO CIBERCRIME

O surgimento do cibercrime pode ser rastreado até as primeiras décadas da era digital,

quando os computadores começaram a se tornar mais comuns nas empresas e lares. Há rastros dessas ações desde a década de 1960, quando o cibercrime teve suas raízes com o surgimento dos primeiros computadores. Nesse período, a maioria dos incidentes estava relacionada a hackers e entusiastas que exploravam sistemas por diversão ou desafio pessoal, sem intenções maliciosas. No entanto, o conceito de segurança digital ainda estava em sua infância (BARROS, 2006).

À medida que os computadores se tornaram mais acessíveis, começaram a surgir os primeiros vírus de computador, Esse período viu um aumento nas atividades de hacking e na propagação de malware, como o infame Worm de Morris, que paralisou parte da Internet em 1988 (MALENKOVICH, 2013).

O aluno da Universidade de Cornell, Robert Tappan Morris, optou por "analisar a extensão da Internet". Para conduzir esse estudo, ele elaborou um programa altamente complexo que tinha a capacidade de se replicar pela rede sem ser interrompido. É evidente que essa capacidade se enquadra perfeitamente na definição de um vírus de computador. O worm Morris não tinha a intenção de causar danos, mas devido a um erro de programação, acabou resultando em múltiplas infecções a partir de um único computador, sobrecarregando o servidor e tornando-o inoperável (MALENKOVICH, 2013).

Com o crescimento da Internet e o aumento da conectividade, o cibercrime começou a se expandir. Surgiram grupos de hackers organizados e motivados financeiramente. Os primeiros incidentes de fraude cibernética e roubo de informações pessoais se tornaram mais comuns.

O cibercrime entrou em uma nova era, com ataques mais sofisticados. Surgiram botnets, redes de computadores zumbis controlados remotamente para realizar atividades maliciosas, como ataques de negação de serviço e spam. O crime cibernético passou a ser um empreendimento lucrativo (MALENKOVICH, 2013).

O cibercrime se tornou uma ameaça global com ataques de grande escala. O foco mudou para o roubo de dados financeiros, espionagem cibernética e ataques a infraestruturas críticas. Além disso, o cibercrime evoluiu com o uso de criptomoedas para extorsão e pagamento por serviços ilegais. Continuou a se adaptar e se sofisticar com o tempo, sendo motivado tanto por ganhos financeiros quanto por motivações políticas ou ideológicas (MALENKOVICH, 2013).

Exemplo disso é o WannaCry, que é um dos tipos de ransomware de criptografia, um modelo de software malicioso (malware) usado por cibercriminosos para extorquir dinheiro., Ele age criptografando arquivos importantes e impedem que você os leia ou bloqueia o seu acesso ao computador para que você não consiga usá-lo (LATTO, 2020).

A crescente dependência da sociedade na tecnologia digital significa que o cibercrime é uma ameaça persistente, exigindo constante inovação em segurança cibernética e esforços de aplicação da lei para combatê-lo.

2.2.1 ANÁLISE JURÍDICA DO CIBERCRIME NO BRASIL

A situação do cibercrime no Brasil, do ponto de vista jurídico, é complexa e desafiadora, refletindo os contínuos avanços tecnológicos e a evolução das táticas dos criminosos cibernéticos. A sua complexidade faz com que haja diversas formas de praticar um crime por meio das diversas tecnologias atualmente, e só algumas foram elencadas como crime no Brasil.

O Brasil possui uma estrutura jurídica sólida para combater o cibercrime. Dentre elas, pode-se citar a Lei 12.737/2012, conhecida como "Lei Carolina Dieckmann", a qual criminaliza invasões de dispositivos e violações de dados pessoais (BRASIL, 2012).

Essa lei foi criada em decorrência de ampla repercussão de um incidente envolvendo a atriz em 2011, no qual seu computador pessoal foi invadido, resultando na divulgação de 36 fotos íntimas nas redes sociais, depois que ela se decidiu a ceder às demandas de extorsão dos criminosos. Quando a lei completou uma década, Carolina Dieckmann aprovou suas reflexões sobre o assunto em suas redes sociais (ARAÚJO, 2023).

Segundo relata a autora Janaína Araújo (2023), ela traduz o que ocorreu naquele ano:

> A fim de garantir segurança no ambiente virtual, no mesmo ano, seis deputados federais apresentaram proposta para tratar sobre invasões de dispositivos eletrônicos e uso das informações obtidas. O projeto de lei prevendo os crimes decorrentes do uso indevido de informações e materiais pessoais relativos à privacidade de qualquer pessoa na internet, como fotos e vídeos, foi analisado pelos senadores, que enfatizaram a necessidade da medida também para combater as fraudes financeiras cometidas por meio eletrônico. (ARAÚJO, 2023, p. 2).

Com isso, a lei torna-se uma das mais importantes no âmbito dos crimes em ambientes virtuais, sendo também uma das pioneiras, dando início ao combate dos cibercrimes.

Além disso, a Lei 12.965/2014, o "Marco Civil da Internet," estabelece princípios e diretrizes para o uso da internet e responsabiliza provedores de serviços online. No entanto, a legislação enfrenta desafios na adaptação às novas ameaças cibernéticas, como o ransomware e os ataques de negação de serviço distribuído (DDoS) (ALVES, 2023).

O Marco Civil da Internet foi concebido com a finalidade de estipular princípios para a utilização da internet no Brasil, garantindo a liberdade de manifestação, a proteção da privacidade, a imparcialidade na gestão da rede e a responsabilidade dos participantes. Ele é uma lei pioneira que é extremamente reconhecida como um modelo internacional a ser seguido (ALVES, 2023).

O Brasil estabeleceu uma estrutura de combate ao cibercrime com a criação da Polícia

Federal (PF) e da Agência Nacional de Segurança Cibernética (ANSC). No entanto, a escassez de recursos e a complexidade das investigações cibernéticas continuam sendo obstáculos significativos.

A crescente dependência da sociedade na tecnologia digital trouxe consigo uma escalada das ameaças cibernéticas. No Brasil, assim como em muitas partes do mundo, as investigações cibernéticas se tornaram uma prioridade para combater o cibercrime, proteger a infraestrutura crítica e garantir a privacidade dos cidadãos.

Em primeiro lugar, a escassez de recursos se manifesta de várias maneiras. Uma delas é a falta de pessoal especializado em cibersegurança e investigações cibernéticas. A demanda por profissionais altamente qualificados na área supera em muito a oferta, tornando difícil para as agências de aplicação da lei e órgãos governamentais reunirem as equipes necessárias para combater o cibercrime de maneira eficaz (AGUIAR, 2023).

Além disso, a aquisição de tecnologia de ponta e ferramentas de segurança cibernética muitas vezes é dificultada pela falta de recursos financeiros. Investimentos em infraestrutura tecnológica são necessários para a investigação e prevenção do cibercrime, mas esses investimentos nem sempre são suficientes (AGUIAR, 2023).

A complexidade das investigações cibernéticas também é um desafio considerável. Os cibercriminosos operam com anonimato, muitas vezes de maneira transnacional, o que torna a atribuição de crimes cibernéticos uma tarefa árdua. Além disso, as técnicas de ofuscação e criptografia utilizadas pelos criminosos dificultam a identificação e a captura dos infratores (AGUIAR, 2023).

A natureza transnacional do cibercrime e a dificuldade em rastrear e identificar infratores tornam estes casos particularmente desafiadores para o sistema de justiça. A cooperação internacional é fundamental na investigação e no julgamento desses casos. As penas para crimes cibernéticos no Brasil podem variar, dependendo da gravidade do delito. No entanto, as punições muitas vezes são vistas como brandas e inadequadas para desestimular cibercriminosos.

O cibercrime está sempre evoluindo com novas ameaças, como ataques de phishing sofisticados, criptomoedas para pagamentos de resgates e invasões de dispositivos IoT (Internet das Coisas). Isso exige uma constante adaptação da legislação e das políticas de combate ao cibercrime.

Dito isso, pode-se concluir que o cenário do cibercrime no Brasil envolve uma estrutura legal e regulatória, esforços de aplicação da lei e desafios jurídicos em constante evolução. Embora o país tenha tomado medidas significativas para combater o cibercrime, ainda enfrenta

desafios na adaptação às novas ameaças e na garantia de punições adequadas para os criminosos. A cooperação internacional e investimentos em capacidades de resposta a incidentes cibernéticos são cruciais para enfrentar esse problema em constante mutação.

2.2.2 AS PRINCIPAIS LEIS QUE REGEM O CIBERCRIME NO BRASIL

No Brasil, várias leis abordam o cibercrime e regulam atividades relacionadas à segurança cibernética e ao uso da internet. Algumas leis que já foram citadas anteriormente como a Lei 12.737/2012 (Lei Carolina Dieckmann) e a Lei 12.965/2014 (Marco Civil da Internet) são bastante importantes, mas também podemos citar a Lei 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) e a Lei 9.296/1996 (Lei de Interceptações Telefônicas), que embora tenha sido criada antes do crescimento da internet, essa lei é relevante para investigações cibernéticas, uma vez que regulamenta a interceptação de comunicações telefônicas e telemáticas. Ela estabelece procedimentos legais para a obtenção de provas por meio da interceptação de comunicações.

Além dessas leis, o Brasil está constantemente atualizando sua legislação para lidar com os desafios em evolução do cibercrime. É importante mencionar que a cooperação internacional também desempenha um papel fundamental na investigação de crimes cibernéticos, pois muitas vezes eles envolvem jurisdições diferentes. As leis e regulamentos em constante evolução refletem o esforço contínuo para combater as ameaças cibernéticas e proteger os cidadãos e as organizações no ambiente digital.

Pode-se adentrar melhor em relação a Lei 13.709/2018 (Lei Geral de Proteção de Dados - LGPD), por ser uma das leis mais recentes, relacionadas à questões que dizem respeito às tecnologias atuais e como se proteger delas, caso necessário.

A autor Fernanda Nones (2022) fala de como a Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que estabelece direitos e regulamentos relacionados à proteção de dados pessoais. Os principais aspectos da LGPD são, principalmente a privacidade e proteção de dados e tem como objetivo proteger a privacidade dos cidadãos, regulamentando a coleta, o processamento e o armazenamento de dados pessoais, garantindo que as informações dos indivíduos sejam tratadas com segurança e responsabilidade (NONES, 2022).

Esta lei também define o que são dados pessoais e estabelece regras específicas para seu tratamento, incluindo informações como nome, endereço, e-mail, histórico de navegação na internet, entre outros. A LGPD exige que as empresas obtenham o consentimento dos titulares dos dados antes de coletar e processar suas informações pessoais. Os titulares têm o direito de retirar seu consentimento a qualquer momento (NONES, 2022).

Há também um detalhe bastante importante sobre esta lei, pois ela pode ser aplicável fora da territorialidade do Brasil, segundo a autora Fernanda Nones (2022):

> Há um detalhe importante sobre a LGPD: ela possui aplicação chamada extraterritorial. Mas afinal, o que isso quer dizer? Na prática, significa que a lei é aplicada independentemente da localização da sede ou da localização em que os dados são processados pelas empresas.
> Nesse caso, a lei é aplicável para empresas e organizações que processam dados pessoais de cidadãos brasileiros, independentemente da localização física da empresa. Se os dados pertencem a indivíduos localizados no Brasil, ou se os dados foram coletados no Brasil – casos em que o titular dos dados estava no Brasil no momento da coleta, a LGPD é válida.

A legislação concede aos titulares uma série de direitos, como acesso aos seus dados, correção de informações incorretas e o direito de solicitar a exclusão de seus dados. Empresas e organizações que coletam e processam dados pessoais devem implementar medidas de segurança para proteger essas informações e nomear um Encarregado de Proteção de Dados (DPO) para supervisionar o cumprimento da lei (NONES, 2022).

A LGPD exige que empresas notifiquem os órgãos reguladores e os titulares dos dados em caso de violação de dados pessoais, o que ajuda a proteger a privacidade e a segurança das informações. A lei também estabelece diretrizes para a transferência de dados pessoais para o exterior e promove a cooperação internacional em questões relacionadas à proteção de dados.

2.3 HACKER WALTER DELGATTI NETTO

Walter Delgatti Netto é conhecido por sua participação no caso da invasão dos celulares de autoridades brasileiras em 2019, e vazar conversas que dizem respeito ao processo da Operação Lava Jato, incluindo o do Ministro da Justiça, Sérgio Moro. Delgatti, um hacker autodidata, alegou que sua motivação era a transparência e a revelação de supostas irregularidades no governo, e foi condenado a 20 anos e um mês de prisão (G1, 2023).

No entanto, suas ações geraram um intenso debate sobre ética, privacidade e a linha tênue entre ativismo cibernético e crimes cibernéticos. Ele foi preso e enfrentou processos legais devido à invasão dos dispositivos, o que levantou questões sobre os limites da atuação dos hackers no cenário político e social (G1, 2023).

Delgatti se tornou um exemplo de como a cibersegurança e a proteção de dados são desafios cada vez mais relevantes na era digital, destacando a necessidade de legislação e segurança robustas para enfrentar ameaças cibernéticas (G1, 2023)

Segundo o Ponto Poder do Diário do Nordeste (2023), Walter Delgatti Netto começou a ser mais mencionado nos meios de comunicação a partir de 2019. Antes de se tornar conhecido como um hacker, ele teve um encontro com a lei em 2015, quando foi detido por falsidade

ideológica, após alegar ser um delegado e portar armas em seu veículo (PONTOPODER, 2023).

Dois anos depois, em 2017, ele foi alvo de uma investigação por falsificação de documentos e também tinha registros anteriores relacionados a estelionato (PONTOPODER, 2023).

Em 2019, ele passou a ser identificado como "o Hacker de Araraquara," fazendo referência à sua cidade de origem, e isso chamou a atenção da Polícia Federal. Desde então, ele acumulou diversas interações com as autoridades policiais (PONTOPODER, 2023).

Na decisão que abordou de maneira específica a Operação Spoofing, o juiz Ricardo Augusto Soares Leite, que atua como substituto na 10ª Vara Federal do Distrito Federal, declarou que a extensão das pessoas afetadas é de proporções significativas (G1, 2023).

Segundo o autor Tiago Tortella da CNN (2023), Delgatti já se encontrava preso, pois era suspeito de ter recebido da deputada federal Carla Zambelli (PL-SP) aproximadamente R$ 40 mil (quarenta mil reais) para invadir sistemas do Poder Judiciário (TORTELLA, 2023).

Em julho de 2023, ele foi libertado e retomou o uso de uma tornozeleira eletrônica, mas, no dia 2 de agosto, foi novamente detido. Nessa mesma data, a Polícia Federal realizou buscas e apreensões tanto no apartamento quanto no gabinete da deputada federal Carla Zambelli (PL-SP). Essa operação recebeu autorização do ministro do Supremo Tribunal Federal (STF) Alexandre de Moraes, que também ordenou a apreensão do passaporte da parlamentar e de recursos e propriedades avaliados em mais de R$ 10 mil (TORTELLA, 2023).

Walter Delgatti Netto, tornou-se um personagem central na discussão sobre cibercrime e segurança na sociedade. Sua relação com o cibercrime é notória devido a suas atividades ilícitas, que envolveram a invasão de dispositivos e contas de figuras públicas e autoridades, incluindo conversas privadas vazadas.

Essas ações, apesar de terem levado à exposição de informações confidenciais e à quebra da privacidade de muitos, também desencadearam debates importantes sobre segurança cibernética. Elas destacaram a necessidade de aprimorar a segurança digital tanto em nível individual como institucional. A sociedade passou a refletir sobre a vulnerabilidade de suas informações pessoais e a importância de proteger dados sensíveis em um mundo cada vez mais digital.

Além disso, a relação de Delgatti Netto com a segurança na sociedade está intrinsecamente ligada à investigação e punição de crimes cibernéticos. Sua prisão e o trabalho das autoridades para desvendar suas atividades demonstram a importância de um sistema legal eficaz na prevenção e resolução de crimes digitais.

Dito isso, o caso desse hacker ilustra a interseção entre cibercrime e segurança na

sociedade, destacando a necessidade contínua de proteger informações pessoais e de fortalecer a capacidade de resposta das autoridades a esses desafios crescentes no mundo digital.

4 CONSIDERAÇÕES FINAIS

Nos últimos anos, o Brasil e o mundo têm enfrentado desafios significativos em relação à segurança cibernética. O aumento das atividades criminosas no ambiente digital tornou evidente a necessidade de estratégias mais eficazes de prevenção e combate ao cibercrime. Nesse contexto, a Inteligência Artificial surge como uma poderosa aliada, oferecendo soluções inovadoras para a proteção de dados, sistemas e informações sensíveis.

O objetivo principal da pesquisa foi alcançado, visto que a Inteligência Artificial tem a capacidade de analisar grandes volumes de dados em tempo real, identificando padrões suspeitos e comportamentos anômalos. Esse processo é essencial na detecção precoce de ameaças cibernéticas, permitindo uma resposta mais ágil e eficaz por parte das autoridades e das empresas. Além disso, a automação de tarefas rotineiras na segurança cibernética possibilita uma alocação mais eficiente de recursos humanos para lidar com ameaças mais complexas.

Esta também pode ser uma grande aliada no combate do cibercrime, pois utilização da Inteligência Artificial na prevenção do cibercrime também envolve a criação de sistemas de defesa mais robustos, capazes de se adaptar rapidamente às novas estratégias dos criminosos. Essa flexibilidade é fundamental, uma vez que os cibercriminosos constantemente evoluem suas táticas e técnicas. A Inteligência Artificial pode ser treinada para aprender com novas ameaças e aprimorar constantemente sua eficácia na proteção de redes e sistemas.

Dito isso, pode-se confirmar que a Inteligência Artificial apresenta um grande potencial para fortalecer a segurança cibernética no Brasil. Seu uso estratégico, aliado a políticas de regulamentação adequadas e investimento em treinamento de profissionais, pode contribuir significativamente para a prevenção do cibercrime, protegendo informações críticas, empresas e cidadãos. À medida que o país enfrenta os desafios do mundo digital, a Inteligência Artificial se posiciona como uma ferramenta fundamental na construção de um ambiente virtual mais seguro e confiável para todos.

REFERÊNCIAS

AGUIAR, Renan de Sousa; NETO, Luís Gonzaga de Araújo; GUIDA, Maria dos Reis Ribeiro. **Crimes Cibernéticos:** Análise do Processo Investigatório e os Desafios para Combatê-los. Revista FT, 2023. Disponível em: <https://revistaft.com.br/crimes-ciberneticos-analise-do-processo-investigatorio-e-os-desafios-para-combate-los/>. Acesso em: 22 de

outubro de 2023.

ALECRIM, Emerson. **Redes Neurais Artificiais.** InfoWester, 2004. Disponível em: <https://www.infowester.com/redesneurais.php>. Acesso em: 18 de outubro de 2023.

ALVES, Jósis. **Lei nº 12.959/2014 (Marco Civil da Internet)**. Bolg GranCursos, 2023. Disponível em: <https://blog.grancursosonline.com.br/lei-marco-civil-da-internet/>. Acesso em: 24 de outubro de 2023.

ARAÚJO, Janaína. **Dez anos de vigência da Lei Carolina Dieckmann:** a primeira a punir crimes cibernéticos. Rádio Senado, 2023. Disponível em: <https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos#:~:text=Portanto%2C%20desde%20mar%C3%A7o%20de%202023,dispositivos%20inform%C3%A1ticos%20para%20instalar%20vulnerabilidades>. Acesso em: 13 de outubro de 2023.

BARROS, Antônio. **Conheça a evolução dos crimes cibernéticos.** Câmara dos Deputados, 2006. Disponível em: <https://www.camara.leg.br/noticias/89137-conheca-a-evolucao-dos-crimes-ciberneticos>. Acesso em: 30 de setembro de 2023.

BERTOLLI, Emilia. **Qual o papel da inteligência artificial (IA) na segurança cibernética.** Varonnis, 2022. Disponível em: <https://www.varonis.com/pt-br/blog/qual-o-papel-da-inteligencia-artificial-ia-na-seguranca-cibernetica>. Acesso em: 15 set. 2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Senado Federal, 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 12 de mai. 2023.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 28 de outubro de 2023.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 28 de outubro de 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 22 de outubro de 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 23 de outubro de 2023.

FELIPE, Leandra. **Cibercrimes causaram prejuízos de bilhões de dólares no mundo em 2016.** Agência Brasil, 2017. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2017-05/cibercrimes-causaram-prejuizos-de-bilhoes-de-dolares-no-mundo-em-2016>. Acesso em: 28 de setembro de 2023.

G1. **Saiba quem é Walter Delgatti Netto**, hacker da 'Vaza Jato' preso pela Polícia Federal. Disponível em: <https://g1.globo.com/politica/noticia/2023/08/02/saiba-quem-e-walter-delgatti-netto-hacker-da-vaza-jato-preso-pela-policia-federal.ghtml>. Acesso em:

GAIDIS, Vinicius. **A IA na segurança da informação:** aliada ou inimiga? Compugraf, 2023. Disponível em: <https://www.compugraf.com.br/blog/a-ia-na-seguranca-da-informacao-aliada-ou-inimiga/**>.** Acesso em: 29 de setembro de 2023.

KLUSAITÉ, Laura. **A História da Segurança Cibernética**. NordVPN, 2022. Disponível em: < https://nordvpn.com/pt-br/blog/historia-seguranca-cibernetica/>. Acesso em: 09 de outubro de 2023.

KOVACS, Leandro. **O que é processamento de linguagem natural?** TecnoBlog, 2021. Disponível em: <https://tecnoblog.net/responde/o-que-e-processamento-de-linguagem-natural-nlp/>. Acesso em: 19 de outubro de 2023.

LATTO, Nica. **O que é o WannaCry?** Academy, 2020. Disponível em: <https://www.avast.com/pt-br/c-wannacry>. Acesso em: 10 de outubro de 2023.

LOIK, Nayla. **A importância da análise de comportamento na segurança cibernética da sua organização.** ManageEngine Blog, 2021. Disponível em: <https://blogs.manageengine.com/portugues/2021/07/27/a-importancia-da-analise-de-comportamento-na-seguranca-cibernetica-da-sua-organizacao.html>. Acesso em 18 de outubro de 2023.

MALENKOVICH, Serge. **Caso Morris Worm completa 25 anos.** Kaspersky Daily, 2013. Disponível em: <https://www.kaspersky.com.br/blog/caso-morris-worm-completa-25-anos/1632/>. Acesso em: 29 de setembro de 2023.

NOVAGEO. **O que é Criptografia Assimétrica RSA** – algoritmo de chave assimétrica? NovaGeo Solutions, 2022. Disponível em: <https://www.novageo.pt/novageo/displayArticles?numero=38346&_que__criptografia_assimetrica_rsa_algoritmo_chave_assimetrica_?#:~:text=O%20RSA%20%C3%A9%20um%20dos,que%20%C3%A9%20secreta%20(privada).>. Acesso em: 16 de outubro de 2023.

PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil.** – 7. ed. – São Paulo: Atlas, 2014.

PONTOPODER. Walter Delgatti Neto**, hacker investigado por vazar conversas da Lava Jato, é condenado a 20 anos.** Diário do Nordeste, 2023. Disponível em: <https://diariodonordeste.verdesmares.com.br/pontopoder/walter-delgatti-neto-hacker-investigado-por-vazar-conversas-da-lava-jato-e-condenado-a-20-anos-1.3407453>. Acesso em: 18 de outubro de 2023.

PORTA, Daniel. **Como a Cibersegurança e os Cibercriminosos usam a Inteligência Artificial.** Danresa, 2023. Disponível em: <https://www.danresa.com.br/danresa-portal/inteligencia-artificial/como-a-ciberseguranca-e-os-cibercriminosos-usam-a-inteligencia-artificial-tudo-sobre-ciberseguranca-e-ia/>. Acesso em: 24 ago. 2023.

PRINCE, Daniel. **4 usos preocupantes que criminosos podem fazer da inteligência artificial.** Galileu Tecnologia, 2023. Disponível em: <https://revistagalileu.globo.com/tecnologia/noticia/2023/07/4-usos-preocupantes-que-criminosos-podem-fazer-da-inteligencia-artificial.ghtml>. Acesso em: 24 ago. 2023.

SILVA, Daniel Neves. **História da internet.** Brasil Escola, 2022. Disponível em: <https://brasilescola.uol.com.br/informatica/internet.htm>. Acesso em 07 de outubro de 2023.
SILVEIRA, Paulo. **O que é Machine Leanig?** Alura, 2023. Disponível em: <https://www.alura.com.br/artigos/machine-learning#:~:text=Machine%20Learning%2C%20por%20outro%20lado,tempo%2C%20sem%20serem%20explicitamente%20programados>. Acesso em: 22 de outubro de 2023.

TERRA, Rodrigo. **A evolução da internet:** da criação aos dias atuais. Makerzine, 2023. Disponível em: <https://www.makerzine.com.br/celular/a-evolucao-da-internet-da-criacao-aos-dias-atuais/>. Acesso em: 15 de setembro de 2023.

TORNELLA, Tiago. **Saiba quem é Walter Delgatti Neto**, o "hacker da Vaza Jato" que teria invadido sistema do Judiciário. Disponível em: **<**https://www.cnnbrasil.com.br/politica/saiba-quem-e-walter-delgatti-neto-o-hacker-da-vaza-jato-que-teria-invadido-sistema-do-judiciario/>. Acesso em: 18 de outubro de 2023.

X2. **História da Inteligência Artificial.** X2 Inteligência Artificial, 2020. Disponível em: <https://x2inteligencia.digital/2020/02/20/historia-da-inteligencia-artificial-2/>. Acesso em: 25 de setembro de 2023.