JNT - FACIT BUSINESS AND TECHNOLOGY JOURNAL - ISSN: 2526-4281 - QUALIS B1
ANO 2025 – MÊS DE MAIO - FLUXO CONTÍNUO – Ed. 62. Vol. 1. Págs. 211-219
DOI: 10.5281/zenodo.15476200

CAPES

CNPq
Conselho Nacional de Desenvolvimento Científico e Tecnológico

TÉCNICAS DE PREVENÇÃO E DETECÇÃO DE CRIMES CIBERNÉTICOS UTILIZANDO INTELIGÊNCIA ARTIFICIAL

TECHNIQUES FOR THE PREVENTION AND DETECTION OF CYBER CRIMES USING ARTIFICIAL INTELLIGENCE

Elcio Alves dos SANTOS[1]
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: chefe.elc@gmail.com
ORCID: http://orcid.org/0009-0002-8113-2015

Wesley Oliveira CUNHA
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: wocbrasil@gmail.com/wesley.cunha@unitpac.edu.br
ORCID: http://orcid.org/0009-0008-7799-5946

RESUMO

As inovações tecnológicas, como a inteligência artificial (IA), não foram criadas para serem utilizadas apenas em um setor da sociedade, mas sim como ferramentas facilitadoras para a coletividade. Para Anabela Miranda Rodrigues, a revolução digital trouxe possibilidades relevantes para o Direito, como o uso de dados digitais como prova no processo penal, novos métodos de investigação e até a criação de uma justiça preditiva, capaz de antecipar resultados com base em padrões. A aplicação dessas ferramentas no combate ao crime tem se mostrado promissora, especialmente diante do aumento dos ataques cibernéticos. A relevância social do estudo está em evidenciar como o uso da inteligência artificial pode contribuir para a proteção de dados, a identificação de comportamentos suspeitos em tempo real e a rastreabilidade de ações criminosas no ambiente digital.

Palavras-chave: Cibersegurança. Crimes Cibernéticos. Inteligência Artificial.

ABSTRACT

Technological innovations, such as artificial intelligence (AI), were not created to be used solely in one sector of society, but rather as facilitating tools for the community as a whole. According to Anabela Miranda Rodrigues, the digital revolution has brought significant possibilities to the field of Law, such as the use of digital data as evidence in

criminal proceedings, new methods of investigation, and even the development of predictive justice, capable of anticipating outcomes based on patterns. The application of these tools in crime prevention has proven to be promising, especially in light of the increase in cyberattacks.

The social relevance of this study lies in demonstrating how the use of artificial intelligence can contribute to data protection, the identification of suspicious behavior in real time, and the traceability of criminal actions in the digital environment.

Keywords: Artificial Intelligence. Cybersecurity. Cybercrimes.

INTRODUÇÃO

No Brasil, os crimes cibernéticos ganharam força durante o período da pandemia, nos anos de 2020 e 2021[1].

Houve aumento significativo no número de usuários de redes e mídias sociais o que também levou ao crescimento de atividades suspeitas e maliciosas que demoraram a ser devidamente tipificadas pelo ordenamento jurídico brasileiro.

A era digital trouxe inúmeras oportunidades, mas também trouxe à tona desafios[2]. No que diz respeito à segurança da informação, o resguardo da privacidade dos usuários e o convívio social, tornou-se difícil pois as inovações tecnológicas vêm superando a capacidade de adaptação das legislações.

Os crimes cibernéticos, como fraudes online, invasões de sistemas e roubo de dados, têm se proliferado, e a inteligência artificial, com suas capacidades, tais como monitoramento em tempo real, identificação de padrões de ataques, rastreamento, surgem como uma abordagem promissora para enfrentar essas ameaças.

O presente projeto foi desenvolvido por meio de uma pesquisa de cunho bibliográfico, descritiva, de abordagem qualitativa, o tema e o objetivo do projeto foram pensados com o intuito de investigar técnicas de prevenção e detecção de crimes cibernéticos, assim como quais habilidades da Inteligência Artificial podem ser utilizadas para o melhor resguardo dos direitos dos usuários.

Para alguns autores, como se verá a seguir, é urgente a necessidade de relacionar a Inteligência Artificial (IA) ao direito, bem como atualizar e preparar os

legisladores para a especificação das situações jurídicas, a fim de tutelar os bens jurídicos no contexto digital, como privacidade, liberdade de comunicação e dignidade.

A relevância social do projeto se dá pelo fato de que o uso de ferramentas tecnológicas, visa facilitar qualquer atividade a ser desempenhada, e no contexto de prevenção e detecção de crimes poderá ser utilizada para a identificação do autor do crime e preservação das provas, tarefas incumbidas ao Estado ou ao ofendido, na ação penal.

Diante disso, este trabalho contempla além desta introdução, a metodologia, o referencial teórico com os seguintes tópicos: A importância da Inteligência Artificial (IA) para a cibersegurança, estudos de casos, resultados das aplicações da Inteligência Artificial e, por fim, a bibliografia.

REFERENCIAL TEÓRICO

A Importância da Inteligência Artificial para a Cibersegurança

Primeiramente, faz-se necessário conceituar Inteligência Artificial (IA). Trata-se de um conjunto de tecnologias de computadores capaz de realizar tarefas que exigem inteligência humana, por exemplo ver, entender, analisar, comparar, fazer reconhecimento, etc. Ademais, cibersegurança, são as ações que buscam evitar invasão ou destruição de sistemas, redes e dispositivos.

> A Cibersegurança é por vezes alvo de atividades ilícitas, tal como, o acesso a informação que se encontra reservada e é confidencial a entidades externas de determinada organização e que por conseguinte, não devem ser tornadas públicas, estas são guardadas em sistemas computacionais ou em redes de informação. Efetuar alterações à informação, isto é, alterar ou apagar informação à qual não se tem autorização para modificar. Por vezes, ocorre uma utilização exagerada ou abusiva dos recursos computacionais, ou seja, um recurso tem uma utilização exagerada relativamente a uma exploração acima do esperado e sofre de uma utilização abusiva quando é utilizado por quem não deve ter acesso ao recurso (Zúquete, 2018, p. 25).

O ambiente digital é por vezes meio pelo qual ocorrem crimes cibernéticos, tais como os citados por Zúquete[3], acessar informações confidenciais, alterar ou apagar informações, portanto, para detectar as ameaças e analisar os padrões de comportamento, é indispensável o papel da Inteligência Artificial (IA) na

cibersegurança, uma vez que detecta ameaças e reage a atividades suspeitas que indicam violação de segurança por meio de abordagens específicas.

Dentre as abordagens mais utilizadas o Machine Learning analisa grandes volumes de dados, identifica anomalias e classifica-as pelo nível de periculosidade. Já as Redes Neurais correlacionam padrões para prever futuros ataques.

Sabendo disso, entende-se que o investimento nessas técnicas pode mitigar as ameaças cibernéticas, que são em grande parte sequestro de dados e informações.

Estudos de Caso

O caso da IBM que utiliza inteligência artificial e aprendizado de máquina para acelerar a identificação e mitigação de ameaças.

A ferramenta vem processando cerca de 15 mil novos documentos todos os meses, identificando padrões de comportamento e alertando sobre atividades maliciosas em tempo real[4].

Um exemplo de sua aplicação é o IBM QRadar, que integra Inteligência Artificial (IA) e automação para fornecer visibilidade e priorização de ameaças, ajudando as equipes de segurança a responder de maneira mais eficiente, reduzindo o tempo de resposta a incidentes e a precisão dos alertas[5].

> Os sistemas cognitivos podem reconhecer o rico significado contextual desse conhecimento [no caso as ameaças] e aplicar dados gerados por máquinas tradicionais para ajudar os analistas a entender melhor o que estão vendo", afirmou Jeb Linton, arquiteto de segurança da IBM para o Watson, em entrevista (TI Rio Notícias, 2023).

Outro exemplo é o Google Cloud Platform (GCP) que desenvolveu o Security Command Center (SCC) capaz de monitorar os ambientes de nuvem onde são armazenados dados de segurança para identificar vulnerabilidades e tentativas de ciberataques.

Com isso, faz-se necessário o treinamento de dados atualizados, considerando as hipóteses de falsos positivos e os métodos que devem ser adotados para manter a privacidade e segurança dos dados armazenados.

A partir das ferramentas citadas acima, é possível enfrentar crimes como o estelionato digital previsto no art. 171, caput, do Código Penal e § 2º-A, que frequentemente ocorre ao enviar e-mails ou mensagens fraudulentas que simulam

empresas legítimas, pedindo informações pessoais ou bancárias, criar páginas falsas em plataformas de venda e contatar contatos de telefone[6].

Resultados das Aplicações da Inteligência Artificial

Os resultados da implementação da Inteligência Artificial (IA) para a prevenção de crimes cibernéticos são significativos, promovendo a segurança digital. A Inteligência Artificial (IA) vem identificando e mitigando as ameaças antes mesmo de causarem danos comprometedores.

> Sendo os sistemas de IA dotados de perigos, é natural que os ditos 'critérios correctivos à teoria da adequação', em especial os do risco permitido e os comportamentos lícitos alternativos, em sede de imputação objectiva, logrem uma aplicação mais ampla, sendo exactamente este o ponto mais sensível na interligação que sempre terá de existir entre o mundo da técnica que está na base da IA e o mundo do Direito que não pode voltar as costas à sua adequada regulamentação (Souza, 2024, p. 176)[7].

Segundo Souza (2024), os sistemas de Inteligência Artificial (IA) apresentam perigos, como violações aos direitos humanos e, consequentemente, riscos relacionados à discriminação algorítmica, violação de privacidade e decisões automatizadas injustas. Contudo, em outras regiões, como na Europa, observa-se um alinhamento mais claro entre as tecnologias de Inteligência Artificial (IA) e princípios éticos e de segurança, viabilizado por regulamentações rígidas[8].

Nesse cenário, é possível afirmar que há alternativas mais eficazes e menos invasivas do que as práticas humanas em processos investigatórios para prevenir e detectar ciberataques. Além disso, objetivos como a proteção e recuperação de dados costumam ser alcançados com maior rapidez, pois as respostas da Inteligência Artificial (IA) tendem a ser automatizadas e proativas.

Ante a devida regulamentação, em casos de julgamento de ações humanas em processos criminais, a tecnologia poderá contribuir para distinguir entre culpa humana e falha do sistema. Essa distinção é essencial para garantir uma imputação penal justa, reconhecendo quando o erro decorre de negligência do agente humano ou de uma falha técnica imprevisível.

Nesse contexto, a Inteligência Artificial (IA) pode ser uma aliada importante, pois oferece transparência processual e rastreabilidade, permitindo o registro

detalhado das etapas de decisão automatizada. Isso facilita a reconstrução dos fatos, a identificação da origem de eventuais erros e a responsabilização adequada.

Logo, as implementações de Inteligência Artificial (IA) devem ser mais amplas, sempre em conformidade com as legislações vigentes, de modo a identificar e enfrentar atividades ilícitas, responsabilizando o indivíduo nos moldes da lei.

METODOLOGIA

O presente artigo trata-se de uma pesquisa de revisão bibliográfica, com abordagem descritiva e qualitativa.

Segundo Fonseca (2002, p. 32), esse tipo de pesquisa é realizado a partir do levantamento de referências teóricas previamente analisadas e publicadas em meios escritos e eletrônicos, como livros e artigos científicos[9].

O objetivo da pesquisa foi investigar as ferramentas tecnológicas, com ênfase na Inteligência Artificial, que se mostram úteis para a prevenção e detecção de crimes cibernéticos.

De acordo com Minayo (2008), a metodologia científica abrange não apenas os métodos utilizados, mas também as técnicas para operacionalização do conhecimento e a criatividade do pesquisador, suas experiências, habilidades e sensibilidades. A autora destaca que os métodos não devem ser compreendidos apenas como técnicas aplicadas, mas como expressão das concepções teóricas que orientam a leitura da realidade[10].

O tema escolhido para o desenvolvimento deste estudo foi a aplicação de técnicas de prevenção e detecção de crimes cibernéticos com o uso da Inteligência Artificial.

O problema central levantado consistiu em analisar como as ferramentas de Inteligência Artificial (IA) podem contribuir para prevenir condutas ilícitas no ambiente digital, identificar ameaças com maior precisão e apoiar a responsabilização penal adequada nos casos em que haja envolvimento de decisões automatizadas.

As etapas da pesquisa compreenderam o levantamento e a análise de bibliografia especializada sobre o tema, disponível em artigos científicos, livros e revistas acadêmicas.

Os bancos de dados utilizados para a coleta do material teórico foram: Biblioteca Eletrônica Científica SciELO, Periódicos Eletrônicos em Psicologia (PEPSIC) e Google Acadêmico. Por meio dessa revisão bibliográfica, buscou-se realizar uma análise crítica das técnicas de proteção digital, dos mecanismos baseados em IA voltados à segurança cibernética e das abordagens que equilibram eficiência tecnológica e responsabilidade jurídica.

RESULTADOS E DISCUSSÃO

Diante de todo o exposto neste trabalho, é possível formular a seguinte discussão: "As técnicas de prevenção e detecção de crimes cibernéticos a partir da Inteligência Artificial (IA) no Brasil estão condicionadas a quais aspectos?" A resposta para esse questionamento está refletida na forma como esse conjunto de tecnologias é aplicado e regulamentado.

Ferramentas como o IBM Watson e técnicas de Processamento de Linguagem Natural (PLN) já são utilizadas em diversos setores, como o varejo de moda, redes de fast food e, inclusive, na área da saúde, para diagnósticos, agendamentos e análise de grandes volumes de informação.

Até mesmo plataformas como a Google Cloud Platform (GCP) têm se mostrado eficazes no arquivamento e recuperação de dados, contribuindo para a integridade da informação e a prevenção de fraudes digitais.

Essas soluções demonstram que a IA não apenas auxilia na proteção de sistemas, mas também oferece respostas rápidas e proativas diante de ameaças cibernéticas.

No entanto, para que essas ferramentas sejam eficazes na realidade brasileira, é essencial considerar a infraestrutura tecnológica disponível e a existência de um marco regulatório que garanta o uso ético e seguro da IA.

CONCLUSÃO

Neste diapasão conclui-se que as práticas anteriormente adotadas nas ações de combate aos crimes cibernéticos tornaram-se não só obsoletas, bem como, tem exigido das empresas responsáveis pela segurança, uma demanda maior de insumos

tecnológicos nos combates aos crimes virtuais, uma vez evidenciado que se trata de um período irreversível na humanidade.

Imperioso destacar, que os pontos evidenciados neste artigo, retrata o temor global a respeito da segurança no meio virtual, haja visto que além do crescimento assustador e vertiginoso da era digital, há a adesão do poder estatal de tais ferramentas na mesma velocidade, o que força os meios legais de segurança atuarem com maior presteza e seriedade.

Portanto, este artigo alerta para a vital necessidade de agir do estado e empresas responsáveis pela prestação de serviços tecnológicos da era virtual, atuando na fiscalização das ações, bem como, na cobrança contínua de ferramentas e meios legais que cumpram as normas elencadas na Lei Geral de Proteção de Dados, como a do Código do Consumidor, principal parte prejudicada com os crimes cibernéticos.

Exigindo de ambos prestadores e reguladores, investimentos constantes, atrelados com políticas públicas de informações periódicas para a sociedade a respeito do manuseio e formas de segurança ao acessar determinados sites, seja pelos próprios meios virtuais, escolas, universidades, órgãos públicos e privados e eventos voltados a conscientização do uso do meio virtual.

REFERÊNCIAS

[1] FREITAS, Rayssa Viana; LOIOLA JUNIOR, Edisio do Ó. Crimes cibernéticos durante a pandemia de COVID-19. **Revista Acadêmica de Iniciação Científica**, v. 1, n. 1, p. 58–69, 2023. Disponível em: <https://wyden.periodicoscientificos.com.br/index.php/raic/article/view/316>. Acesso em: 30 abr. 2025.

[2] ANIMA EDUCAÇÃO. Cibersegurança e os desafios do Direito Digital. **Revista Direito em Foco**, v. 12, n. 2, 2022. Disponível em: https://portaldeperiodicos.animaeducacao.com.br/index.php/RDFG/article/view/13928/7708. Acesso em: 1 dez. 2024.

[3] ZÚQUETE, André. **Segurança em Redes Informáticas**. 6. ed. Lisboa: FCA - Editora de Informática, 2021.

[4] WIRED. **IBM's Watson Now Fights Cybercrime in the Real World**. 6 dez. 2016. Disponível em: <https://www.wired.com/2016/12/ibm-watson-for-cybersecurity-beta>. Acesso em: 30 abr. 2025.

[5] TI RIO NOTÍCIAS. **IBM desenvolve projeto de segurança cibernética que utiliza recursos do Watson**. 18 nov. 2016. Disponível em: <https://www.ti.rio/ibm-desenvolve-projeto-seguranca-cibernetica-que-utiliza-recursos-do-watson>. Acesso em: 30 abr. 2025.

[6] CORDEIRO, C. D. Crimes cibernéticos e investigação policial. **Ministério Público do Estado do Piauí**, **2022**. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 1 dez. 2024.

[7] SOUZA, Maique. **A regulação da inteligência artificial e novos contornos para caracterização da responsabilidade civil**. Academia.edu, 2023. Disponível em: <https://www.academia.edu/118219054/A_Regula%C3%A7%C3%A3o_Da_Intelig%C3%AAncia_Artificial_e_Novos_Contornos_Para_Caracteriza%C3%A7%C3%A3o_Da_Responsabilidade_Civil.> Acesso em: 30 abr. 2025.

[8] RODRIGUES, Luis Gabriel Pereira; VIEIRA, Vinícius Garcia. **Regulamentação da inteligência artificial: garantia dos direitos fundamentais na Constituição Federal de 1988. Anais do 7º Congresso Internacional de Direito e Contemporaneidade**: mídias e direitos da sociedade em rede, Santa Maria, RS, 30 out. a 31 out. 2024. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2024/12/7.11.pdf. Acesso em: 30 abr. 2025.

[9] FONSECA, João José Saraiva. **Metodologia da Pesquisa Científica**. 2. ed. São Paulo: Atlas, 2002.

[10] MINAYO, Maria Cecília de Souza (Org.). **Pesquisa Social**: Teoria, Método e Criatividade. 29. ed. Petrópolis, RJ: Vozes, 2010.