INTERFACE TECNOLÓGICA

O PAPEL TRANSFORMADOR DA INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA

THE TRANSFORMATIVE ROLE OF ARTIFICIAL INTELLIGENCE IN SECURITY

Erik Henrique Leite – erik.leite016@gmail.com
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

Douglas Francisco Ribeiro – douglas.ribeiro16@fatec.sp.gov.br
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

DOI: 10.31510/infa.v20i1.1669
Data de submissão: 20/03/2023
Data do aceite: 29/05/2023
Data da publicação: 30/06/2023

RESUMO

A revolução trazida pela Inteligência Artificial (IA) na forma como armazenamos dados sensíveis, como dados bancários, fotos e e-mails, bem como na interação com nossas máquinas. Reconhecendo que toda evolução possui seus aspectos positivos e negativos, abordaremos de maneira abrangente as implicações dessa transformação, fornecendo informações claras sobre como manter-se seguro ao aproveitar os benefícios dessa tecnologia. Além disso, dedicaremos uma seção do artigo para explorar as consequências da IA e a crescente dependência de dados, destacando os desafios e as considerações éticas associadas ao seu uso no contexto da segurança. Esperamos que esse projeto proporcione uma compreensão mais aprofundada dos efeitos da IA no cenário de segurança, oferecendo diretrizes importantes para lidar de forma eficaz com as implicações e desafios decorrentes dessa evolução tecnológica.

Palavras-chave: Armazenamento de dados. Dependência de dados. IA (Inteligência Artificial)

ABSTRACT

The revolution brought by AI in the way we store sensitive data, such as banking information, photos, and emails, as well as in our interaction with machines. Recognizing that every evolution has its positive and negative aspects, we will comprehensively address the implications of this transformation, providing clear information on how to stay safe while harnessing the benefits of this technology. Furthermore, we will dedicate a section of the article to explore the consequences of AI and the growing dependency on data, highlighting the challenges and ethical considerations associated with its use in the context of security. We hope that this project will provide a deeper understanding of the effects of AI in the security landscape, offering important guidelines to effectively deal with the implications and challenges arising from this technological evolution.

Keywords: Data storage. Data dependency. AI (Artificial Intelligence).

1. INTRODUÇÃO

A Inteligência Artificial (IA) é um campo em rápido crescimento (NG,2007) que tem demonstrado um grande potencial no domínio da segurança. Envolve o uso de algoritmos avançados e modelos estatísticos para analisar dados e identificar padrões, anomalias, e potenciais ameaças.

No contexto dos sistemas de segurança, a IA pode ser utilizada para melhorar a detecção de ameaças, os tempos de resposta e as capacidades de tomada de decisões. Ao analisar grandes volumes de dados de várias fontes, tais como câmeras de segurança, registos de acesso, e redes de sensores, a IA pode identificar e responder a potenciais ameaças em tempo real.

Uma das aplicações mais significativas da IA na segurança está no desenvolvimento da análise preditiva (MESQUITA,2012). A análise preditiva pode analisar padrões de dados e identificar potenciais riscos de segurança antes que estes ocorram. Isto é especialmente útil na proteção de infraestruturas críticas, onde a detecção precoce de potenciais ameaças é fundamental.

Outra aplicação importante da IA na segurança está no desenvolvimento de algoritmos de aprendizagem de máquinas. Estes algoritmos podem aprender com incidentes de segurança passados e desenvolver modelos preditivos que podem ser utilizados para identificar potenciais ameaças à segurança. A aprendizagem de máquinas também pode ser utilizada para automatizar tarefas de segurança de rotina, tais como monitorização e actualização de software de segurança, libertando recursos humanos para tarefas mais complexas. (BERTOLLI,2022)

Globalmente, a utilização de IA em sistemas de segurança tem demonstrado grande promessa na melhoria da detecção de ameaças, tempos de resposta e capacidades de tomada de decisões. À medida que a tecnologia continua a avançar, podemos esperar ver mais desenvolvimentos neste campo e um enfoque contínuo no aumento da segurança através da utilização de IA. (BERTOLLI,2022)

2. INTELIGÊNCIA ARTIFICIAL E SEGURANÇA

A Inteligência Artificial (IA) pode ser uma ferramenta valiosa na segurança da informação, pois pode ajudar as organizações a detectar, prevenir, e responder a ameaças à segurança em tempo real. O uso de IA na segurança da informação envolve a aplicação de algoritmos de aprendizagem de máquinas, técnicas de análise de dados, e análise preditiva para identificar

potenciais ameaças e tomar as ações apropriadas para as atenuar (GARCIA; GUTIERREZ; SILVA, 2022).

Apresentam-se a seguir algumas das formas como a IA trabalha com a segurança da informação: a análise comportamental, a análise de rede, a análise de logs, e a análise de vulnerabilidades. A análise comportamental utiliza algoritmos de aprendizagem de máquina para analisar o comportamento dos usuários e identificar atividades suspeitas (IBRAHIM et al., 2019). A análise de rede utiliza técnicas de inteligência artificial para identificar padrões de tráfego suspeitos na rede (SABARAD; DAWANE, 2021). A análise de logs envolve a análise de registros de eventos do sistema para identificar atividades suspeitas (SILVA et al., 2021). A análise de vulnerabilidades utiliza a IA para identificar vulnerabilidades nos sistemas e aplicativos (GARCIA et all, 2022). Dito isso, a alguma fatores que podem ser analisados para melhorias em questão de vulnerabilidade, como, detectação de ameaças, anomalias entre outros que serão citados abaixo.

- Detecção de Ameaças: Os algoritmos de IA podem analisar grandes volumes de dados de várias fontes tais como tráfego de rede, registos, e sensores para identificar padrões e anomalias que possam indicar um potencial ameaça à segurança. Isto permite às organizações detectar potenciais ameaças mais rapidamente e com maior precisão.
- Detecção de anomalias: Os algoritmos de IA podem detectar padrões de comportamento anómalos que se desviam da norma. Isto ajuda a identificar ameaças que de outra forma poderiam passar despercebidas pelos sistemas de segurança tradicionais.
- Análise Predicativa: A IA pode analisar dados históricos para desenvolver modelos preditivos que identificam ameaças potenciais antes que estas ocorram. Isto ajuda as organizações a tomar medidas proativas para prevenir incidentes de segurança.
- Resposta e Remediação: Os algoritmos de IA podem responder a incidentes de segurança em tempo real. Por exemplo, um sistema de IA pode isolar automaticamente uma máquina infectada ou negar o acesso a um utilizador com uma tentativa de login suspeita. Isto ajuda a reduzir o impacto dos incidentes de segurança.
- Automatização de Tarefas de Segurança: A IA pode automatizar tarefas de segurança de rotina, tais como actualização de software, monitorização do tráfego de rede, e identificação de vulnerabilidades. Isto permite que as equipas de segurança se concentrem em questões de segurança mais complexas.

- Inteligência de Ameaças: A IA pode analisar grandes volumes de dados de inteligência de ameaças para identificar potenciais ameaças à segurança. Isto ajuda as organizações a manter-se à frente de ameaças novas e emergentes.

Basicamente, o uso de IA na segurança da informação pode ajudar as organizações a detectar, prevenir, e responder às ameaças à segurança de forma mais eficaz. À medida que o cenário de ameaças continua a evoluir, podemos esperar ver sistemas de IA mais avançados que irão melhorar a segurança dos dados e bens sensíveis das organizações. (GARCIA, GUTIERREZ, DA SILVA, 2022, p. 15-30).

3. A UTILIZAÇÃO DE INTELIGÊNCIA ARTIFICIAL EM APLICAÇÕES E SUA SEGURANÇA

De acordo com Gandomi e Haider (2015), a Inteligência Artificial (IA) tem se tornado cada vez mais presente em diversas aplicações, desde assistentes virtuais em smartphones até carros autônomos. Segundo Sezer et al. (2018), a IA pode melhorar significativamente as capacidades dessas aplicações, fornecendo sistemas mais inteligentes e com maior capacidade de resposta. Entretanto, com o aumento do uso de IA, crescem também as preocupações com a segurança desses sistemas, conforme alertam Sharma e Bali (2020). Dentre as principais preocupações estão as vulnerabilidades e ameaças cibernéticas que podem comprometer a integridade e a confidencialidade dos dados. Assim, é fundamental adotar medidas de segurança adequadas para garantir a proteção desses sistemas e a privacidade dos usuários envolvidos. Apresentam-se a seguir algumas das formas como a IA estar a ser utilizada em aplicações:

- Linguagem de Processamento Natural (PNL): de acordo com Jurafsky e Martin (2009), "Processamento de Linguagem Natural (PNL) é um subcampo da Inteligência Artificial (IA) que envolve o uso de algoritmos para analisar e compreender a linguagem humana (p. 5). A PNL é utilizada em diversos sistemas, como assistentes virtuais, para permitir aos usuários interagir com estes sistemas utilizando a linguagem natural.
- Visão por computador: A visão por computador é outro subcampo da IA que envolve o uso de algoritmos para analisar e interpretar dados visuais de câmaras e outros sensores. A visão por computador é utilizada em aplicações tais como carros auto conduzidos e sistemas de segurança para ajudar estes sistemas a interpretar o mundo à sua volta. (NG,2007)

- Análise Predicativa: A análise preditiva envolve a utilização de modelos estatísticos e algoritmos de aprendizagem de máquinas para analisar dados históricos e identificar padrões que podem ser utilizados para prever eventos futuros. Como afirmam Kim e Koo (2021), a análise preditiva é uma ferramenta importante em várias aplicações, incluindo detecção de fraudes e previsão financeira.
- Robótica: Parafraseando Sousa: A robótica é uma área da inteligência artificial que envolve o uso de robôs para desempenhar tarefas humanas. A robótica é aplicada em setores como manufatura, logística e cuidados de saúde. (SOUSA, 2023)."A robótica é uma área da inteligência artificial que envolve o uso de robôs para executar tarefas que são tipicamente realizadas por humanos. A robótica é utilizada em aplicações tais como o fabrico, logística, e cuidados de saúde" (SOUSA, 2023).

Embora a IA ofereça muitos benefícios nestas aplicações, há também preocupações com a segurança. Os sistemas de IA podem ser vulneráveis a ataques tais como envenenamento de dados, onde os atacantes manipulam os dados usados para treinar algoritmos de IA para produzir resultados incorretos. Os ataques adversariais, em que os atacantes manipulam os dados introduzidos para enganar os sistemas de IA, são também uma preocupação.

Segundo Al-Jarrah et al. (2020), para abordar as preocupações com segurança em sistemas de Inteligência Artificial (IA), é fundamental que as organizações implementem medidas de segurança robustas. Entre as principais medidas, destaca-se a segurança dos dados utilizados para treinar algoritmos de IA e processados pelos sistemas de IA. Para isso, é necessário adotar técnicas de criptografia de dados, bem como implementar controles de acesso e monitorar a utilização desses dados, conforme recomendado por Chang et al. (2020). Além disso, é importante avaliar regularmente a segurança dos sistemas de IA e atualizar as medidas de segurança conforme necessário, conforme ressaltado por Sharma e Bali (2020**).** Sistemas de monitorização: As organizações devem monitorizar os seus sistemas de IA para detectar anomalias e potenciais ameaças à segurança. Isto inclui a monitorização do tráfego de rede e dos registos do sistema para identificar atividades suspeitas. Implementar as Melhores Práticas: As organizações devem implementar as melhores práticas de segurança de IA incluindo manter o software atualizado, utilizar métodos de autenticação fortes, e implementar planos de backup e recuperação de dados.

Outra forma de utilizar é Realização de auditorias regulares: As organizações devem realizar auditorias regulares aos seus sistemas de IA para assegurar que estão seguros e que cumprem os requisitos de conformidade regulamentar.

A IA também pode ser utilizada para automatizar tarefas de segurança de rotina. Por exemplo, os algoritmos de IA podem ser usados para monitorizar e atualizar software de segurança, libertando recursos humanos para tarefas mais complexas.

A IA pode ser usada para melhorar a encriptação de dados e o controlo de acesso. Os algoritmos de IA podem ser usados para identificar padrões nos padrões de acesso aos dados e ajudar a desenvolver mecanismos de controlo de acesso mais seguros. A IA pode também ser usada para desenvolver algoritmos de encriptação mais robustos que podem ajudar a proteger os dados contra o acesso não autorizado.

A IA ofereça muitos benefícios nas aplicações, as organizações devem implementar medidas de segurança robustas para proteger os seus sistemas de IA contra ameaças à segurança. Como a IA continua a tornar-se mais prevalente nas aplicações, é essencial que as organizações tomem medidas para proteger estes sistemas para proteger os seus dados e bens. (GARCIA, 2022)

4. APLICAÇÕES DA INTELIGÊNCIA ARTIFICIAL

Há diversas aplicações de segurança com inteligência artificial que estão cada vez mais presentes no nosso dia a dia, algumas delas são:

Verificação de identidade: "O reconhecimento biométrico é amplamente utilizado para a identificação de indivíduos, especialmente em sistemas de autenticação e segurança, como acesso a edifícios e controle de fronteiras" (SHEN et al., 2020, p. 372).

Antivírus: “os antivírus modernos fazem uso de técnicas de inteligência artificial para analisar o comportamento de programas em execução e detectar atividades maliciosas" (SANTOS; DE SOUZA, 2019, p. 69).

Assistente virtual: “O sistema é protegido por mecanismos de segurança de reconhecimento de voz que impedem que pessoas não autorizadas utilizem o dispositivo" (SHAO et al., 2021, p. 16).

Controle de acesso: “A tecnologia de reconhecimento facial é uma das tecnologias biométricas mais utilizadas para autenticação e controle de acesso" (LI et al., 2020, p. 523).

Monitoramento de câmeras: “os sistemas de segurança por vídeo usam a análise de vídeo para detecção de atividades suspeitas ou indesejadas, permitindo que os agentes de segurança tomem medidas apropriadas" (GUL et al., 2020, p. 198).

Detecção de fraude: “A aplicação de técnicas de aprendizado de máquina tem sido uma das principais soluções para a detecção de fraudes em transações financeiras" (PINHEIRO et al., 2018, p. 323).

Detecção de invasão: “as soluções de detecção de intrusão baseadas em inteligência artificial podem detectar as atividades maliciosas na rede, e impedir a ação dos invasores" (LEE et al., 2019, p. 1677).

Detecção de invasão: Sistemas de detecção de intrusão que utilizam aprendizado de máquina para identificar atividades suspeitas na rede.

3. Quais as consequências a IA traz.

Como tudo em nossa vida, desde atitudes até pensamentos nos trazem consequências, com a Inteligência artificial não seria diferente, há pesquisadores que apresentam pontos significativos sobre o tema, como por exemplo citados por Hinton e Bostrom:

- Falta de transparência: Alguns sistemas de IA são tão complexos que não é possível entender como eles tomam suas decisões, o que torna difícil responsabilizar as partes envolvidas em caso de problemas. Isso pode ser particularmente preocupante quando a IA é utilizada em áreas como diagnósticos médicos ou tomada de decisões judiciais.
- Dependência de dados: A IA depende de dados para aprender e tomar decisões, mas esses dados podem estar incompletos, desatualizados ou serem de qualidade ruim. Isso pode levar a decisões incorretas ou falhas no sistema. (HINTON, 2021).
- Segurança cibernética: A IA pode ser vulnerável a ataques cibernéticos, como invasões ou manipulação de dados, o que pode levar a danos aos sistemas ou a comprometimento de dados sensíveis. (HINTON, 2021).
- Ética: A IA pode ser utilizada para fins antiéticos, como o monitoramento de atividades pessoais ou a criação de armas autônomas. (BOSTROM, 2014)

Para mitigar esses riscos, é importante que as organizações implementem medidas de segurança e governança rigorosas em suas aplicações de IA. Isso pode incluir monitoramento constante de desempenho e tomada de decisões da IA, transparência na tomada de decisões, diversidade de dados de treinamento e auditoria de sistemas de IA. (DAMILANO, 2019, p. 81).

4. O uso da Inteligência Artificial na segurança de dados.

Existem várias vantagens em utilizar softwares que utilizam inteligência artificial para proteger dados, incluindo:

- Detecção mais rápida de ameaças: "A análise em tempo real dos dados com o uso de inteligência artificial permite detectar e responder a possíveis violações de segurança com maior rapidez e eficácia." (LOPES, 2020.)
- Maior precisão na identificação de ameaças: "Os algoritmos de aprendizado de máquina permitem que as soluções de segurança aprendam com o tempo e identifiquem padrões de comportamento que seriam difíceis de detectar com soluções de segurança tradicionais." (ALMEIDA, 2020.)
- Redução de falsos positivos: "As soluções de inteligência artificial conseguem analisar grandes volumes de dados, reduzindo o número de alertas falsos e permitindo que a equipe de segurança concentre seus esforços em ameaças reais." (BORGES, 2021.)

5. Problemas e desafios para o uso da Inteligência Artificial na segurança de dados.

Embora a inteligência artificial (IA) ofereça muitas vantagens e possibilidades, há também algumas desvantagens e desafios a serem considerados:

As tecnologias de IA são criadas a partir de dados e algoritmos que podem ter preconceitos implícitos. Isso pode levar a decisões discriminatórias ou injustas que afetam determinados grupos. (DAMBROS, 2020)

• Dependência: A dependência de algoritmos de IA pode fazer com que as pessoas confiem demais em soluções tecnológicas, sem questionar a sua precisão ou limitações. (MCGREGOR, 2019.)

• Interoperabilidade: A IA pode produzir resultados difíceis de interpretar, o que pode dificultar a compreensão dos processos de tomada de decisão. (CHEN, et al. 2018.)

• Custos: A implementação de soluções de IA pode exigir investimentos significativos em termos de infraestrutura, dados e treinamento de pessoal. (LEE, et al. 2019.)

• Ética: A implementação de tecnologias de IA levanta questões éticas, incluindo questões de privacidade, direitos autorais e de propriedade intelectual. (TADDEI, 2020.)

• Desemprego: A automação de processos de trabalho pode levar à eliminação de empregos que são rotineiros e previsíveis, embora possa haver oportunidades para novos empregos. (RODENBORN, et al 2020.)

5 CONCLUSÃO

Com base neste estudo, conclui-se que a inteligência artificial (IA) é uma tecnologia poderosa que está sendo cada vez mais utilizada em sistemas de segurança para proteger dados e prevenir ameaças. Embora a IA ofereça muitas vantagens, como eficiência, precisão e rapidez, ela também apresenta riscos, como vieses e discriminação, falta de transparência, dependência de dados, vulnerabilidade a ataques cibernéticos e questões éticas.

Portanto, é importante que as organizações que utilizam a IA em sistemas de segurança implementem medidas de segurança e governança rigorosas para mitigar esses riscos. Essas medidas incluem monitoramento constante da IA, transparência na tomada de decisões, diversidade de dados de treinamento e auditoria dos sistemas de IA. Com essas medidas, a IA pode ser uma ferramenta poderosa para a segurança de dados e prevenção de ameaças, desde que utilizada de forma responsável e ética.

Além disso, ao abordar a questão da dependência de dados, é importante garantir práticas robustas de gerenciamento de dados, incluindo backup e redundância de dados, verificação de integridade dos dados e protocolos de proteção de dados. Ao reduzir a dependência de uma única fonte de dados e estabelecer procedimentos seguros de manipulação de dados, as organizações podem minimizar o impacto da dependência de dados e aprimorar a segurança dos sistemas de IA.

Constatado isso, é fundamental reconhecer tanto os aspectos positivos quanto as limitações e riscos potenciais da IA na área de segurança. Para obter benefícios significativos enquanto mitigam os desafios relacionados, as organizações devem implementar medidas de segurança apropriadas e adotar práticas responsáveis. É essencial encontrar um equilíbrio entre a dependência de dados, a segurança e as considerações éticas, a fim de aproveitar plenamente o potencial da IA na proteção de dados e prevenção de ameaças. Através dessas ações, a IA pode ser uma ferramenta poderosa e confiável para impulsionar a segurança cibernética e proporcionar um ambiente mais seguro para as organizações e seus dados sensíveis.

REFERÊNCIAS

ALI, Maj. Inf. RAJA ASAD. NTELIGÊNCIA ARTIFICIAL: IMPLICAÇÕES NA SEGURANÇA NACIONAL E DESAFIOS JURÍDICOS. ESCOLA DE COMANDO E ESTADO MAIOR DO EXÉRCITO ESCOLA MARECHAL CASTELLO BRANCO, p. 25, 2020.

CINQUE, A.R.R. Segurança da Informação na Inteligência Artificial. Faculdade de Tecnologia de Americana, [S.l.] p. 17. Publicado em: 3 dezembro 2018.

DAMILANO, Cláudio Teixeira. Inteligência artificial e inovação tecnológica: as necessárias distinções e seus impactos nas relações de trabalho. Brazilian Journals Publicações de Periódicos, São José dos Pinhais, Paraná, [S. l.], p. 4, 16 out. 2019.

DE LIMA, SILVA, LUZ, SILVA, LIMA, ANDRADE, SILVA, Sidney Marlon Lopes, Heverton Kleidson, João Henrique da Silva, Samuel Lopes de Paula, Hercília Juliana do Nascimento, Anna Beatriz Augusta de, Alisson Marques da. Antivirus endowed with Artificial Neural Network in order to Detect Malwares Preventively. Departamento de Computação, Universidade de Pernambuco -Empresa Bidweb Security IT–Recife, Brasil, [S. l.], p. 2, 21 dez. 2021.

GARCIA, GUTIERREZ, DA SILVA, Caio Cruz Alfonso, Carolina de Carvalho, Nathan Brito. Inteligência Artificial Aplicada a Reconhecimento de detecção de Ataque Cibernético. Escola de Engenharia Mauá do Centro Universitário do Instituto Mauá de Tecnologia, São Caetano do Sul, p. 15-30, 2 jan. 2022.

LEE, Kai-Fu. AI Superpowers: China, Silicon Valley, and the New World Order. [S. l.]: Harper Business; Illustrated edição, 2018. 272 p. 20 – 256 25 setembro 2018.

MORAIS, Tiago de Lima Caiadas. A APLICAÇÃO DA INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA DA FRONTEIRA MARÍTIMA. 30 jul. 2022. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/42455/1/183%20GNR%20Inf_Tiago%20de%20Lima%20Caiadas%20Morais.pdf. Acesso em: 17 mar. 2023.

MONTEIRO, GIORDANO, POSSAMAI, GABRIELLE TEXEIRA, LUCAS AZAMBUJA, Vinicius Avila. O USO DA INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA DAS CRIPTOMOEDAS. 2019. Disponível em: http://raam.alcidesmaya.edu.br/index.php/projetos/article/view/115. Acesso em: 19 mar. 2023.

MUELLER, John Paul. Aprendizado de máquina para leigos. [S. l.]: Alta Books, 2020a. 432 p. 30 – 443, 8 de outubro 2019.

MUELLER, John Paul. Inteligência artificial Para Leigos - edição de bolso. [S. l.]: Alta Books, 2020. 227 p. 1-227,01 de setembro 2020.

OLIVEIRA, Vânia Filipa Moreira Queirós de. Cibe segurança e Inteligência Artificial: Como garantir a segurança de um Sistema de Informação. Repositório Universidade Nova, MGI, p. 1 - 91, 13 maio 2021.

QUAL o papel da inteligência artificial (IA) na segurança cibernética. 26 set. 2022. Disponível em:https://www.varonis.com/pt-br/blog/qual-o-papel-da-inteligencia-artificial-ia-na-seguranca-cibernetica. Acesso em: 8 mar. 2023.