P.PORTO

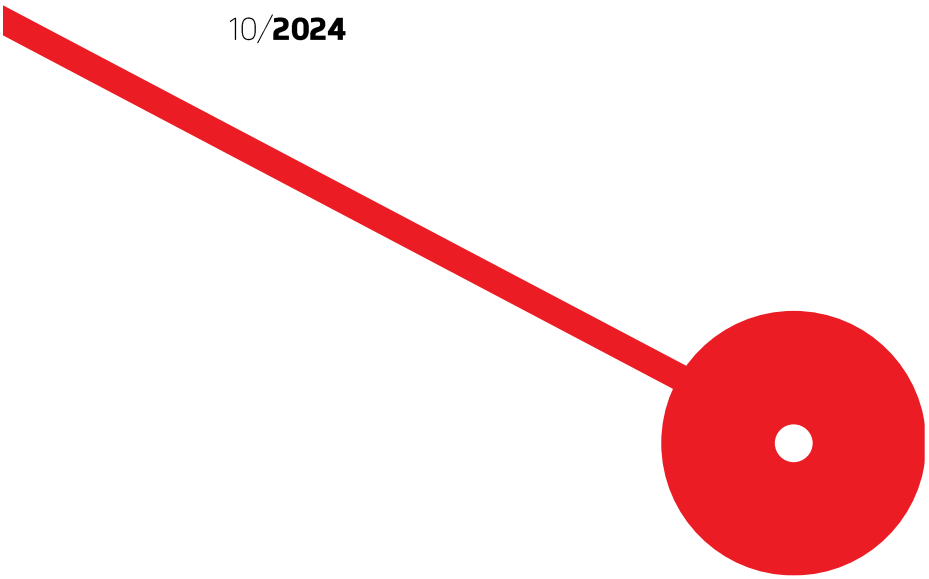
INSTITUTO
SUPERIOR
DE CONTABILIDADE
E ADMINISTRAÇÃO
DO PORTO
POLITÉCNICO
DO PORTO

M MESTRADO CONTABILIDADE E FINANÇAS

O Papel da Inteligência Artificial na Cibersegurança e a sua Eficiência no Mercado das Criptomoedas

Ana Margarida Martins Pereira

10/**2024**



Esta versão contém as recomendações e comentários do júri

Ana Margarida Martins Pereira. O Papel da Inteligência Artificial na Cibersegurança e a sua Eficiência no Mercado das Criptomoedas
10/**2024**

P.PORTO

INSTITUTO
SUPERIOR
DE CONTABILIDADE
E ADMINISTRAÇÃO
DO PORTO
POLITÉCNICO
DO PORTO

M MESTRADO CONTABILIDADE E FINANÇAS

O Papel da Inteligência Artificial na Cibersegurança e a sua Eficiência no Mercado das Criptomoedas

Ana Margarida Martins Pereira

Dissertação de Mestrado apresentado ao Instituto Superior de Contabilidade e Administração do Porto para a obtenção do grau de Mestre em Contabilidade e Finanças, sob orientação de Professor Doutor Adalmiro Álvaro Malheiro de Castro Andrade Pereira.

Ana Margarida Martins Pereira. **O Papel da Inteligência Artificial na Cibersegurança e a sua Eficiência no Mercado das Criptomoedas**
10/**2024**

Agradecimentos

Gostaria de agradecer a todos os que me apoiaram e contribuíram para a realização da presente dissertação. Primoridialmente, agradeço ao meu orientador, Professor Doutor Adalmiro Pereira, pela sua orientação e disponibilidade em prol dos melhores resultados, bem como a sua confiança e apoio em todas as dificuldades e conquistas. Um agradecimento especial aos meus pais pelo apoio incondicional ao longo de todo o processo. Agradeço também às minhas amigas, em especial à Andreia Barroso, por todo apoio, dedicação e dicas que contribuíram para a elaboração desta dissertação de mestrado.

Resumo:

Com o avanço das tecnologias, vivemos numa era cada vez mais digital, o que tem levado a uma aumento substancial na procura de soluções de cibersegurança. A exposição frequente nos media de casos de burlas e fraudes tem vindo a gerar uma maior preocupação dos indivíduos e empresas, que enfrentam um cenário de crescimento contínuo do cibercrime. À medida que os ataques, tanto pessoais quanto empresariais, aumentam, torna-se essencial que as organizações ajustem os seus processos e comportamentos para se protegerem contra ameaças futuras. A cibersegurança deve ser analisada em cinco categorias: identificação, proteção, deteção, resposta e recuperação. É fundamental para as empresas validar toda a sua rede, os acessos que fornecem aos colaboradores, o armazenamento dos dados, a monitorização contínua, a verificação e identificação dos sistemas de deteção, a rapidez na análise, a criação de automatismos de resposta e, essencialmente, o planeamento de recuperação, uma vez que, quanto maior o tempo de recuperação, maiores serão os custos para as entidades. Uma das ferramentas que pode melhorar a *performance* dos processos nas cinco áreas será a Inteligência Artificial (IA). Contudo, trata-se de uma tecnologia com um investimento elevado. Tendo em conta a dicotomia do custo-benefício da IA, foi realizado este estudo de metodologia qualitativa, com o objetivo de compreender a cibersegurança na atualidade e em que medida a IA beneficiará a cibersegurança. Um dos setores também vulneráveis a ataques é o mercado de criptomoedas, que será analisado. A análise será sustentada por relatórios de diversas empresas que entrevistaram executivos e líderes no departamento de segurança de diversos países. Os resultados obtidos indicam que, embora o investimento em IA seja elevado, uma aposta maior na tecnologia poderá reduzir os custos associados a ciberataques. Conclui-se ainda que o investimento em IA e cibersegurança aumenta o valor do negócio.

Palavras chave: Cibersegurança; Inteligência Artificial; Criptomoedas; Ataques Cibernéticos

Abstract:

With technological advancements, we are living in an increasingly digital era, which has led to a substantial rise in demand for cybersecurity solutions. Frequent media exposure to cases of scams and fraud has heightened concerns among individuals and companies, who now face a continuously growing cybercrime landscape. As both personal and corporate attacks increase, it becomes essential for organizations to adjust their processes and behaviors to protect against future threats. Cybersecurity should be analyzed in five categories: identification, protection, detection, response, and recovery. It is crucial for companies to validate their entire network, the access they provide to their employees, the storage of their data, continuous monitoring, verification and identification of detection systems, speed of analysis, the creation of automated response mechanisms, and, essentially, recovery planning, since the longer the recovery time, the greater the costs for entities. One of the measures that could improve the *performance* across these five areas is Artificial Intelligence (AI). However, it requires significant investment. Considering the cost-benefit dichotomy of AI, this qualitative study was conducted to understand modern cybersecurity and assess the extent to which AI can benefit cybersecurity. One sector also vulnerable to attacks is the cryptocurrency market, which will be analyzed. The analysis will be supported by reports from various companies that interviewed executives and leaders in the security departments in different countries. The results indicate that, although investment in AI is substantial, a greater commitment to this technology can reduce the costs associated with cyberattacks. It is also concluded that investing in AI and cybersecurity enhances business value.

Key words: Cybersecurity; Artificial Intelligence; Cryptocurrencies; Cyber Attacks

Índice Geral

Índice de Figuras

Índice de Gráficos

Índice de Tabelas

Lista de Siglas e Abreviaturas

CERT	Computer Emergency Response Team
CNCS	Centro Nacional de Cibersegurança
DDoS	Distributed Denial-of-Service
EUROPOL	European Union Agency for Law Enforcement Cooperation
IA	Inteligência Artificial
IBM	International Business Machines Corporation
iOS	iPhone Operating System
LLM	Large Language Model
MFA	Multi-Factor Authentication
NIST	Instituto Nacional de Padrões e Tecnologias
PGR	Procuradoria-Geral da República
PKI	Public Key Infrastructure
PwC	PricewaterhouseCoopers
SMS	Short Message Service
TIC	Tecnologias da Informação e Comunicação

CAPÍTULO - INTRODUÇÃO

A presente dissertação, elaborada para conclusão dos estudos no Mestrado de Contabilidade e Finanças do Instituto Superior de Contabilidade e Finanças pretende investigar "O Papel da Inteligência Artificial na Cibersegurança e a sua Eficiência no Mercado das Criptomoedas".

A segurança tem um impacto cada vez mais relevante na vida das pessoas, das organizações e da comunidade (CNCS, 2024). O número de incidentes de cibercrimes tem aumentado nos últimos anos e prospera-se que o aumento continue. Além disso, é observado um aumento na sofisticação dos crimes e no impacto que provocam. Neste sentido, é necessário avaliar a perceção das entidades relativamente aos riscos, na eventualidade de sofrerem ataques (CNCS, 2024).

A IA proporciona a utilização de máquinas capazes de processar, aprender e planear de forma semelhante à dos seres humanos, através de sistemas inteligentes (Sadiku *et al*., 2020). A utilização desta tecnologia trará benefícios, como a economização de recursos, a redução de tempo nas análises e na padronização e verificação de tendências (Das & Sandhane, 2021).

O aproveitamento da cibersegurança aliado à IA poderá acarretar diversas mais-valias para as empresas, especialmente no apoio aos profissionais de segurança cibernética em soluções capazes de defender contra ataques mais sofisticados (Adi *et al*., 2022).

Tendo em conta este contexto, o principal objetivo do estudo é compreender a cibersegurança na sua atualidade e em que medida a IA beneficiará a cibersegurança. Perante este objetivo, foram definidas as seguintes questões:

1. A cibersegurança é um tema presente?
2. A cibersegurança constitui uma preocupação generalizada?
3. A IA consegue combater os problemas atuais?

De modo a dar resposta a estas questões, foi realizada uma análise qualitativa através da análise de 15 relatórios de 12 entidades. Os relatórios são fundamentados em entrevistas realizadas a executivos e líderes no departamento de segurança, provenientes de diversos setores de atividade e a diferentes países. Relativamente à cibersegurança e à segurança cibernética, foram analisados relatórios de 2021 a 2024. No que concerne às criptomoedas e à segurança cibernética, foram considerados relatórios de 2017 a 2024.

Os objetivos secundários deste estudo consistem na verificação do estado atual da cibersegurança, analisar as consequências que os países estão a enfrentar com ataques cibernéticos, averiguar de que forma os países se estão a proteger e quais as práticas que estão a utilizar, bem como validar se a IA está a conseguir combater esses problemas e o estado do mercado criptográfico.

A estrutura da presente dissertação é composta por quatro capítulos. O primeiro capítulo é referente à revisão de literatura, que se encontra subdividida em duas partes. Na primeira parte, será abordada a IA e a cibersegurança, que inclui uma explicação sobre a IA, os seus objetivos e propósitos. Seguir-se-á uma análise da segurança cibernética, a intensificação dos ciberataques e a deteção de fraudes. Para finalizar a primeira parte, será evidenciado o papel da IA na segurança cibernética. No que concerne à segunda parte, o foco será o tema das criptomoedas, na qual é evidenciado o seu histórico, definições e evoluções. De seguida, é realizada uma análise da influência da IA nas criptomoedas. A segunda parte concluir-se-á com a discussão sobre os crimes cibernéticos no mercado das criptomoedas.

O capítulo dois é composto pela metodologia, na qual se descreve a metodologia aplicada, os objetivos e as questões que o estudo pretende responder.

O terceiro capítulo constitui o estudo de caso, que, por sua vez, é subdividido em três secções. A primeira secção inicia-se com os relatórios de segurança cibernética e IA, apresentado primeiramente o caso português e, posteriormente, os dados a nível mundial. De seguida, são referidos os relatórios sobre criptomoedas e segurança cibernética, destacando o apoio da IA. Por fim, será realizada a análise dos dados obtidos.

O quarto capítulo é dedicado às conclusões, onde serão evidenciadas as considerações finais, as limitações do estudo e as sugestões futuras para futuras investigações.

1 Inteligência Artificial e Cibersegurança

1.1 Inteligência Artificial, Benefícios e Propósitos

Rafi *et al*. (2017), no seu estudo, evidenciam o aparecimento da IA em 1952. Nesse ano foi criado por Newell e Simon o primeiro software através de IA denominado o "solucionador geral de problemas". A IA é sinónimo de sofisticação e permite obter os melhores serviços com o mínimo de intervenção humana. A fonte e o detalhe dos dados são a base para a IA compreender os pedidos e tomar decisões acertadas. Em primeiro lugar, procede-se à identificação das necessidades, seguido da reflexão do processamento para o tratamento do pedido e, por fim, advém a execução (Rafi *et al*., 2017).

Wilson (2023) no seu livro, evidencia o início da IA em 1956, por John McCarthy, através do seu Projeto sobre a IA do Dartmouth College. Inicialmente, a IA consistia no raciocínio e na resolução de problemas. Na década de 80, surge a aprendizagem das máquinas, caracterizada pelo tratamento de dados através de computadores, que originou os algoritmos. A partir de 2010, o foco consiste nas redes neurais, devido à numerosa quantidade de dados e aprendizagens, bem como pelos avanços computacionais que, atualmente, instruem as máquinas a ter comportamentos e a realizar as atividades características do cotidiano dos humanos.

Sadiku *et al*. (2020) consideram a IA um ramo tecnológico que reproduz a inteligência humana. Defendem que as máquinas são capazes de processar, aprender e planear da mesma forma que os seres humanos, através de sistemas inteligentes. Neste sentido, apresenta como principal objetivo a réplica das funções cognitivas do ser humano e a realização das suas atividades diárias. São exemplo, o reconhecimento facial e de voz pelos assistentes virtuais, ou veículos que contêm a capacidade de substituir o condutor (Sadiku *et al*., 2020).

A utilização da IA permitirá economizar recursos e diminuir o tempo gasto na leitura e padronização dos dados. Adicionalmente, a IA analisa as anomalias, conseguindo detetar os mais ínfimos detalhes. No entanto, o controlo da IA advém do ser humano e da informação que este o transmite, bem como o insere. Ou seja, a IA apresenta uma excelente capacidade, mas é desenvolvida pela forma que o ser humano a configurou (Das & Sandhane, 2021). A IA está presente em diversas áreas, como por exemplo na área da saúde, através dos assistentes virtuais e diagnósticos mais precisos através da correlação dos algoritmos (Wilson, 2023). No ramo industrial será possível aumentar a

produtividade, reduzir os erros humanos, e adicionalmente, irá permitir que as máquinas apresentem maior precisão, realizem tarefas repetitivas com menor dificuldade e trabalhem um maior número de horas. Nos transportes, é possível verificar a automatização através dos veículos autónomos. Nas finanças, é exequível realizar facilmente negociações, analisar dados rapidamente e tomar decisões no momento. Em relação ao entretenimento, a IA foca-se na personalização com base nas preferências dos consumidores e na aposta na realidade virtual (Wilson, 2023).

Atualmente, a eficácia e a eficiência são fundamentais na execução dos processos, bem como a rapidez e a tomada de decisões no momento (Rafi *et al*., 2017). A IA apresenta diversos proveitos, por exemplo, permite às pessoas maior liberdade de tarefas, pois executa atividades rotineiras e repetidas. Além disso, o detalhe das máquinas diminuiu os erros do ser humano e tornou-as mais ágeis nos procedimentos. O reconhecimento dos padrões é outra vantagem da IA, promovendo perspetivas futuras mais confiáveis (Rafi *et al*., 2017).

Sadiku *et al*. (2020) destacam, no seu estudo, diversas ferramentas que são usadas para atingir os propósitos da IA. Entre elas encontram-se os sistemas especializados, as redes neurais, os processadores de linguagem natural, os robôs, a lógica difusa, a aprendizagem de máquina, a aprendizagem profunda e a procura/análise dos dados. Os sistemas especializados correspondem a sistemas que têm por base o conhecimento. Com eles será possível a tomada de decisão, baseada na interpretação de dados que são processados tendo em conta as regras estipuladas. As redes neurais permitem reconhecer padrões e procedem a cálculos matemáticos, sendo usadas para análises de risco, gestão e monitorização ao nível da saúde e assistência. Os processadores são utilizados para traduzir e interpretar a comunicação entre pessoas. Neste sentido, os objetivos centram-se nos idiomas, reconhecimento da fala e análise de texto. Os robôs conseguem imitar/exercer as mesmas capacidades dos humanos e são utilizados em diversas áreas. A lógica difusa representa o raciocínio através da incerteza nas informações e pela junção dos dados. A aprendizagem das máquinas envolve previsões e interpretação dos dados, ou seja, analisa e interpreta a informação de modo a prever casos futuros. A aprendizagem profunda descodifica os problemas por camadas, de modo a resolver algo complexo. Por fim, a descoberta de dados, simboliza o reconhecimento de padrões e de novas fontes de informação (Sadiku *et al*., 2020).

Na atualidade, a IA é imprescindível, na medida em que proporciona diversos benefícios na vida do ser humano, seja na casa, no carro ou nos dispositivos (Sadiku *et al*., 2020). A pesquisa e utilização de IA torna a vida e o ambiente mais seguro e produtivo. Dos proveitos com a IA podem enumerar-se o reconhecimento e processamento rápido e pormenorizado, a capacidade de previsão, a deteção de comportamentos maliciosos e de padrões, o registo de anomalias e o ampliamento das defesas sobre todos os problemas encontrados, e fundamentalmente, a capacidade de identificação e a sua facilidade de reação. Por contrapartida, a IA também contém processos negativos para a sociedade e as empresas, uma vez que quem efetua os ataques também tirará proveito da IA, o que o tornará os ataques mais eficientes, eficazes e perigosos. Para além disso, um grande desafio de quem pretende implementar a IA diz respeito ao custo. Embora venha a ser muito compensativo aproveitar das enormes vantagens da IA é necessário avaliar o seu custo-benefício. A IA requer elevados recursos, formação, melhoria contínua e a base de informação deve ser abundante e pormenorizada de modo a alcançar o maior número de soluções possíveis (Sadiku *et al*., 2020).

Rafi *et al*. (2017) também evidenciam alguns impactos negativos, tais como, a despesa avultada, o tempo despendido na criação dos sistemas, a elevada sofisticação e a numerosa quantidade de base de dados necessárias para o sistema avaliar o meio envolvente e agir em prol do melhor resultado. Por outro lado, podem atuar na redução de profissionais, dado que é possível substituir o seu trabalho pelas máquinas, permitindo às organizações beneficiar de maior rentabilidade pelo aumento da capacidade horária de trabalho (Rafi *et al*., 2017).

1.2 Segurança Cibernética

Segundo os autores Kaur *et al*. (2023) o termo cibersegurança corresponde a um conjunto de tecnologias, processos e práticas em prol da proteção e defesa de redes, dispositivos e dados sobre possíveis ataques, danos e acessos que não foram autorizados. O crescente aumento do uso de tecnologias, cada vez mais sofisticadas, e a interligação de sistemas, gera uma maior procura pela cibersegurança. Para além disso, o aumento de ataques cibernéticos implicou a adoção de novas medidas para suportar as falhas na proteção. Neste sentido, surgiram ferramentas de segurança cibernética, através de IA, com o objetivo de atingir uma maior eficiência e controlo (Kaur *et al*., 2023).

A cibersegurança pode ser considerada fundamental para a sociedade atual, uma vez que, protege os indivíduos, as organizações e o governo contra os ataques e crimes cibernéticos. Estamos perante uma era cada vez mais digital, onde medidas robustas são fundamentais para obter uma maior proteção (Shanthi *et al*., 2023).

Kaur *et al*. (2023) evidenciam o sistema de cibersegurança proposto pelo Instituto Nacional de Padrões e Tecnologias (NIST) que identifica as soluções necessárias em virtude da proteção, deteção, reação e defesa contra os possíveis ataques cibernéticos. O NIST pormenoriza as práticas a fim de melhorar a capacidade de segurança em qualquer organização, tendo como foco quatro elementos, sendo eles as funções, as categorias, as subcategorias e as referências informativas. Estes elementos permitem fornecer a visão da gestão cibernética por um período temporal longo, a identificação das necessidades, a categorização breve e clara da IA sobre a cibersegurança. A estrutura do NIST consiste na identificação, proteção, deteção, resposta e recuperação. Ao nível da identificação, corresponde à gestão do negócio e do meio envolvente, à avaliação do risco e à estratégia de gestão de risco. Relativamente à proteção são geridos os controlos de acessos, identificados os processos e procedimentos sobre a proteção da informação e aplicada a tecnologia de proteção. Em virtude da deteção são validadas as anormalidades e os eventos decorrentes, é feita uma monitorização contínua da segurança e deteção de processos em risco. No que diz respeito à resposta são pré-definidas as medidas a tomar, o planeamento que se deve realizar e as melhorias necessárias para prevenção de casos semelhantes no futuro. Por fim, a recuperação consistirá na criação de um plano para recuperar de eventuais ataques, reduzindo os custos inerentes e o reforço com relatórios (Kaur *et al*., 2023).

O cibercrime é considerado um problema crescente, sendo necessário atenção redobrada sobre os processos e comportamentos. Estar ciente dos riscos é crucial e o uso de sistemas de combate é imprescindível para enfrentar os mais diversos crimes e atuar na prevenção a médio e a longo prazo. O recurso à cibersegurança permitirá proteger os sistemas e as informações confidenciais (Chakraborty *et al*., 2022).

1.3 A Intensificação dos Ciberataques e a Deteção de Fraudes

A entidade International Business Machines Corporation (IBM), no seu relatório de 2023, afirma que a segurança dos dados deveria ser prioridade para as empresas. Entre os fatores

mais comuns que resultam em ataques cibernéticos bem-sucedidos, estão a entrada nos perímetros da rede, as exigências dos serviços na nuvem sobre as práticas de cibersegurança, as sofisticações dos cibercrimes, a falta de competência na cibersegurança e a falta de conhecimentos por parte dos colaboradores. Um problema recorrente nas organizações é a adoção de medidas apenas para cumprir requisitos legais, o que resulta numa proteção ineficaz dos dados. As organizações devem definir planos estratégicos para proteger o seu negócio. Entre as práticas que os autores consideram mais importantes para a segurança, encontra-se, a análise e a classificação dos dados confidenciais armazenados na *cloud,* a avaliação dos riscos, a proteção através de encriptação, as monitorizações contantes, a análise dos padrões que permitem validar atividades maliciosas, os sistemas de resposta no momento dos ataques e a criação de relatórios simples para facilitar a compreensão entre todos (IBM, 2023).

Os analistas cibernéticos não devem ignorar as vulnerabilidades que encontrarem e, posteriormente, não as corrigir (IBM, 2023). Esta postura trará consequências, colocando em risco a empresa em que trabalham. Os cibercriminosos procuram sempre os pontos de entrada considerados mais acessíveis e, esses pontos, são as vulnerabilidades das empresas. O tratamento dos problemas implica a realização de testes, de forma a evitar um círculo vicioso em que a correção de um problema, gera outro. A rapidez com que esses testes são realizados, poderá determinar se a empresa corre, ou não, o risco de ser atacada. É essencial monitorizar os acessos, de forma a que as equipas de Tecnologia da Informação, consigam saber como, quando e quem acedeu aos dados, para avaliar se todos os acessos são necessários ou se devem ser mais restritos (IBM, 2023).

De acordo com o primeiro relatório da Grant Thornton (2021), em 2014, houve um custo de cibercrime na Irlanda de 630 milhões de euros. Comparativamente com 2020, o custo económico do cibercrime da Grant Thornton foi de 9,6 mil milhões de euros. O início da crise da Covid-19 desencadeou um aumento exponencial dos crimes, devido à adesão dos indivíduos ao teletrabalho com os seus próprios dispositivos. Nestas condições, os cibercriminosos conseguem mais facilmente ter acesso e invadir dispositivos, dados e ambientes operacionais. Além disso, os golpes por *email* e as fraudes online duplicaram face ao ano anterior. Alguns dos fatores que contribuíram para o aumento do cibercrime prenderam-se com a inexistência de restrições no acesso remoto a documentos para os colaboradores, o uso da mesma senha nos dispositivos pessoais e de trabalho, a troca de dados e relatórios com informação confidencial através de *emails* pessoais, a inexistência

de formação ou orientação sobre proteção contra ataques cibernéticos e, principalmente, a elevada quantidade de empregadores que solicitaram aos seus colaboradores o uso de dispositivos pessoais para a atividade laboral. As empresas devem priorizar a segurança cibernética, especialmente com o crescimento progressivo do trabalho remoto, dado que exige mais esforços para proteger os seus dados (Grant Thornton, 2021).

Um setor que sofreu um enorme aumento nos ataques de ransomware foi o bancário. Ransomware é um tipo de código de software malicioso que prejudica os sistemas dos computadores das vítimas, armazenando dados sobre elas para posterior chantagem, com o objetivo de receberem um pagamento (Grant Thornton, 2021). Contudo, apesar do aumento do cibercrime, muitas pessoas e instituições não se preocupam com o tema, acreditando que a probabilidade de serem afetadas é mínima. Esta opinião formada deve-se à falta de perceção da dimensão de pessoas e empresas prejudicadas, uma vez que os lesados tentam manter a situação em sigilo. O sigilo é motivado pelo medo de perda de reputação, por desconhecerem onde denunciar o ataque e pela falta de consciência de que foram alvo de um ataque (Grant Thornton, 2021).

Os indivíduos que praticam o crime cibernético fazem-no, maioritariamente, pelo ganho financeiro (Grant Thornton, 2021). No entanto, existem outros fatores, destacando-se os que se consideram ativistas, os oportunistas, os profissionais e os chamados "da nação". Os ativistas atuam por razões ideológicas promovendo a sua religião, a sua política e a sua causa, utilizando para o efeito as redes como forma de protesto para se fazerem ouvir e gerar discussão. Os oportunistas, por sua vez, atacam principalmente pessoas mais vulneráveis. Embora não obtenham grandes ganhos, realizam um número maior de ataques a alvos menores. Os profissionais fazem parte de redes de crime organizado, focando-se em alvos elevados, nomeadamente, grandes empresas do setor financeiro, para obter recompensas substanciais e tendem a correr menos riscos. Os "da nação" são os criminosos mais sofisticados, especializados em ataques políticos ou militares, para obterem informações confidenciais. Em menor escala, ocorrem os crimes cometidos por organizações que procuram obter dados de organizações rivais para atingirem vantagem competitiva, um tipo de crime conhecido como espionagem cibernética (Grant Thornton, 2021).

O cibercrime afeta todos e Grant Thornton (2021) considera a existência de três custos: diretos, indiretos e de defesa. Os custos diretos representam o impacto imediato, isto é, o custo monetário e os danos causados às entidades ou aos indivíduos. Os custos indiretos

são os danos à reputação, seja do indivíduo ou da empresa, a perda de confiança sobre quem foi atacado, a perda de oportunidades de negócios futuros e a redução de receita. Os custos de defesa envolvem despesas com prevenção, resposta a ataques e medidas para minimizar os problemas (Grant Thornton, 2021).

1.4 O Papel da Inteligência Artificial na Segurança Cibernética

Shanthi *et al*. (2023) referem que a história da IA na segurança cibernética remonta ao final da década 80 e início da década 90, aquando do desenvolvimento de sistemas baseados em regras e conhecimentos replicados de processos de tomada de decisão, por forma a detetar os intrusos e responder a ataques. Atualmente, a IA é cada vez mais utilizada na segurança, dando origem ao crescimento da fonte de informação, à sofisticação das ameaças e ao avanço das tecnologias (Shanthi *et al*., 2023).

As ferramentas de IA são cada vez mais utilizadas na deteção e prevenção de ataques cibernéticos, uma vez que têm capacidades avançadas, rapidez na deteção de anomalias e oferecem mais soluções para combater os crimes (Sadiku *et al*., 2020). Sadiku *et al*. (2020) evidenciam quatro áreas aplicacionais da IA, sendo elas a defesa automatizada, a segurança cognitiva, a formação sobre o adversário e a monitorização paralela e dinâmica. A defesa automatizada é proveitosa pela sua autonomia, autoaprendizagem, facilidade de ação, capacidade de defesa em processos complexos e, fundamentalmente, por oferecer proteção 24 horas por dia. A área da segurança cognitiva baseia-se na imitação dos comportamentos do cérebro humano. A formação sobre o adversário foca-se no desenvolvimento de sistemas que compreendam o lado dos crimes e recriam ataques e vulnerabilidades com o objetivo de aprimorar a sua defesa. A monitorização envolve o acompanhamento constante dos comportamentos (Sadiku *et al*., 2020).

Capgemini Research Institute (2019) realizou uma pesquisa a 850 executivos sobre a IA na segurança cibernética. Nesta pesquisa, demonstraram que nas áreas de serviços públicos, seguros, automobilística, venda a retalho, banca e telecomunicações, mais de 50% das respostas afirmam que já não são capazes de responder aos ataques cibernéticos sem o apoio da IA. Um em cada cinco executivos confirmou que a sua organização já sofreu ataques cibernéticos, através de acesso a redes, dispositivos ou dados. Entre os tipos de ataques que mais aumentaram, destacam-se os que ocorrem através de serviços na nuvem e na rede de *Internet of Things*, também denominados de objetos inteligentes.

Estes dispositivos são incorporados com sensores, software e conectividade de rede, o que permitirá a recolha e partilha de dados. A aposta da IA na segurança cibernética é mais intensificada na segurança de rede, seguida da segurança de dados e posteriormente da segurança de endpoint (Capgemini Research Institute, 2019).

A IA permite a redução de custos na deteção e resposta a ataques, uma vez que tem maior capacidade de perceção dos padrões e reutilizam as diversas ameaças para identificar novas ameaças (Capgemini Research Institute, 2019). Esta capacidade gera uma redução de tempo na identificação de problemas, bem como a pesquisa necessária para a defesa. Em relação aos analistas cibernéticos, a IA na segurança cibernética é extremamente benéfica, uma vez que melhora a sua precisão e eficiência, reduzindo a carga de trabalho nas análises e interpretações de todos os dados e incidentes, permitindo apenas iniciar a análise pelos algoritmos fornecidos pela IA. Segundo os autores, as organizações devem concentrar as suas iniciativas de segurança cibernética na pontuação de risco na rede, nomeadamente, através da deteção de intrusos, análise comportamental das máquinas, deteção de fraude e deteção de *malware*. A pontuação permitirá estimar o risco e os limites, priorizando ameaças de alto risco, para uma defesa mais rápida e eficaz. A deteção da intrusão consiste na atuação em tempo real, valorizando a deteção, análise e defesa na compreensão dos comportamentos e nos algoritmos de aprendizagem, alcançando a maior rede de dados. A análise dos comportamentos das máquinas permite diferenciar as ações de atividade humana e as ações de máquinas, de modo a bloquear ataques cada vez mais sofisticados com maior precisão. A deteção de fraude incide sobre perdas financeiras, como por exemplo, a aposta em aprendizagens pormenorizadas de transações. Por fim, a deteção de *malware*, consiste na utilização de ferramentas e técnicas de identificação de problemas e possíveis falhas, detetando diversas intrusões e priorizando o limite do custo e dos impactos nos negócios (Capgemini Research Institute, 2019).

Adi *et al*. (2022) destacam, no seu estudo, que a IA permite aos profissionais de segurança cibernética desenvolver as melhores soluções, com o propósito de derrotar os mais sofisticados ataques aos seus sistemas. Adicionalmente, referiu que ambos os lados beneficiam da IA, dado que estão cada vez mais bem preparados para defender eficazmente os ataques, assim como, os adversários se encontram cada vez mais fortes nos ataques.

A IA poderá acelerar as vulnerabilidades dos sistemas informáticos, além de permitir sequenciar os passos dos *hackers* aquando da realização de ataques cibernéticos, bem como aumentar as suas aptidões sobre códigos maliciosos que atacam os sistemas, permitindo perceber o lado de quem ataca (Abbas *et al*., 2023). Pelo lado da defesa, a IA deverá ser capaz de detetar os intrusos e atividades anômalas, antecipar o ataque e descobrir o modo de defesa mais apropriado para cada situação, além de ser rápido e eficaz na prevenção e antecipação de comportamentos suscetíveis a falhas (Abbas *et al*., 2023).

O futuro da IA na segurança cibernética é avaliado pelos constantes avanços nos sistemas, que originam diversos benefícios, como a rapidez e precisão na resposta aos ataques, a sofisticação na pesquisa sobre ameaças de modo a neutralizá-las eficazmente, automatização e atualização de tarefas e de políticas, foco na proteção da nuvem e análise cada vez mais pormenorizada dos padrões de todas as ameaças que surgem (Shanthi *et al*., 2023). Por outro lado, os desafios da IA também serão cada vez maiores, uma vez que os ataques tendem a ser mais eficientes e sofisticados pelo uso do poder da IA. Nesse sentido, a disponibilidade limitada de dados pode prejudicar o desempenho dos sistemas. A complexidade do sistema pode afetar a compreensão e aceitação do processo para mais pessoas, o que prejudicará a tomada de decisão. A vulnerabilidade do sistema tende a provocar falsos alarmes e falhas nas previsões. A dificuldade de compreensão dos termos éticos e legais, e a quantidade de recursos necessários alinhado com os custos (Shanthi *et al*., 2023).

Segundo Das e Sandhane (2021), é necessário que as empresas estabeleçam defesas de cibersegurança com recurso à IA, uma vez que os *hackers* também tiram proveito desta tecnologia. A IA permite análises mais precisas e eficientes, reforça soluções, adapta-se a todos os problemas e cria soluções. A amplitude e sofisticação das redes dificulta o trabalho do ser humano, sendo a IA benéfica nesta questão. O aumento substancial das ameaças cibernéticas e o aproveitamento da inteligência sofisticada para fins ilícitos, implica uma defesa mais eficiente, sendo imprescindível adotar medidas de segurança cibernética aprimoradas (Das & Sandhane, 2021).

Capgemini Research Institute (2019), no seu relatório, cria o roteiro para a implementação de IA na segurança cibernética, iniciando-o pela criação de dados na plataforma. Seguido pela seleção das iniciativas de segurança cibernética, com a finalidade de aceleração e maximização dos benefícios. Em terceiro lugar, evidenciam os apoios externos, a

colaboração entre profissionais, seguido pela análise, priorização e respostas célebres, de modo a melhorar a *performance* da segurança. Em penúltimo lugar, denotam a importância da formação dos analistas cibernéticos, para que possam compreender os algoritmos de IA e detetar ameaças de forma eficiente. Por fim, a definição das funções e das responsabilidades, o monitoramento dos algoritmos e a identificação da tolerância ao risco (Capgemini Research Institute, 2019).

Pupillo *et al*. (2021) evidenciam que, de modo a reforçar a segurança dos sistemas de IA, devem ser realizados testes antes e após a implementação do sistema, com a finalidade de avaliar os riscos e garantir a ação adequada. É essencial monitorizar os sistemas e métodos ao longo do tempo, além de documentar todas as fases do processo do sistema e dos seus componentes para fortalecer a análise. A documentação permitirá de forma ágil e rápida perceber o que mudou, quando mudou e o propósito para a mudança. Além disso, o acompanhamento contínuo dos dados e parâmetros da utilização da IA, a validação das capacidades do sistema, as especificações nas conclusões e a aprimoração das prevenções são estratégias que fortalecem os sistemas e a segurança. Através do seu estudo, foi possível perceber que os incidentes de segurança atingiram o seu pico em 2019, com ataques cada vez mais sofisticados, que aproveitaram as vulnerabilidades dos sistemas remotos. A Covid-19 levou a que mais de 900 mil mensagens de *spam* fossem enviadas em apenas um ano. Neste sentido, a aposta na IA ajudará a combater os diversos riscos existentes, através da melhoria na resiliência, na resposta aos ataques e na robustez diante dos desafios. A resiliência simboliza a persistência e a tolerância aos ataques, através da aposta na deteção de anomalias. Em relação à resposta, esta baseia-se na autonomia dos sistemas, pela sua capacidade de reação sem depender do humano, assim como, na identificação de ataques e o seu grau para contra-atacar. A melhoria da robustez consiste na capacidade de aguentar a configuração definida, mesmo após o processamento de entradas erradas, através de automatismos, realização de testes e correções. Ou seja, as máquinas têm capacidade para verificar e validar processos autonomamente (Pupillo *et al*., 2021).

Um dos principais focos do uso da IA na cibersegurança assenta no detalhe sobre a identificação das situações ambientais, consideradas como indesejadas, e nas ações que se devem aplicar (Kaur *et al*., 2023). Apresenta, neste sentido, como fonte principal o raciocínio, o planeamento, a aprendizagem, a comunicação e a perceção das ações. Sendo uma área considerada ampla, deverá apresentar diversas abordagens sobre a aplicação, as

consequências e os métodos a aplicar (Kaur *et al*., 2023). A utilização da IA na cibersegurança é impulsionada pela velocidade do impacto nas organizações, pela complexidade das operações e pela dificuldade de competência na segurança, sendo necessário apostar na automatização (Pupillo *et al*., 2021). A automatização permite ajudar as equipas de segurança a verificar o ataque, avaliar a sua escala, projetar o seu desenvolvimento e definir as ações que devem ser tomadas (Pupillo *et al*., 2021).

O investimento na segurança baseada na IA, permite aprimorar de forma mais precisa as ameaças, construir um histórico das informações que beneficiará a tomada de decisão, melhorar os automatismos, redefinir as prioridades e analisar as vulnerabilidades para alterar o circuito de possíveis problemas (Wilson, 2023). No que diz respeito aos riscos da segurança baseada na IA, é importante considerar a privacidade dos dados e a incapacidade de atuar perante as falhas dos sistemas. O desenvolvimento de práticas protetivas, como a aposta em medidas de segurança ao longo de todos os projetos, a identificação constante e correção de vulnerabilidades, a execução contínua de testes de segurança e o cruzamento de informação, permitirá proteger os sistemas. Neste sentido, a implementação da IA permite antecipar cenários, atualizações e evoluções, rapidez e eficiência nas respostas e o desenvolvimento de estratégias com fundamentos a longo prazo (Wilson, 2023).

Morovat e Panda (2020) evidenciam, no seu estudo, as abordagens que consideram mais comuns da utilização da IA na cibersegurança. Em primeiro lugar, referem a deteção e a classificação de ameaças, conseguida pela análise dos dados e reconhecimento de padrões que provocam o risco de ataque, garantindo a resposta no imediato. Em segundo lugar, a pontuação de riscos na rede, onde o uso da abordagem consiste na priorização de recursos. As priorizações são fundamentadas com as pontuações de risco que, por sua vez, são subdivididas em secções da rede com o propósito de automatizar processos e registos nas redes mais vulneráveis a ataques cibernéticos. Por último lugar, referem a automatização e otimização das análises realizadas pelas pessoas, com o objetivo de efetuar as tarefas diárias e repetitivas, realizadas pelo ser humano (Morovat & Panda, 2020).

Péter Bagó, professor assistente e chefe de departamento na Universidade Corvinus de Budapeste, perante a sua experiência e estudos na área, escreveu uma publicação sobre a segurança cibernética e a IA (Bagó, 2023). No seu estudo, indica algumas regras de segurança que considera fundamentais para as empresas aplicarem, sendo elas:

1. Utilização de senhas fortes, com pelo menos oito caracteres que devem incluir letras maiúsculas e minúsculas, números e caracteres especiais;
2. Autenticação em duas etapas, que sejam dois fatores distintos como por exemplo, a senha e um código individual;
3. Atualizações de software;
4. Firewall e proteção contra vírus;
5. Sistemas de *backup* de segurança de dados, para garantir os dados em caso de perda ou roubo;
6. Formação aos colaboradores sobre os riscos e as práticas de segurança;
7. Monitorização contínua para ajudar na deteção de ameaças e conseguir responder no imediato.

Bagó (2023) no seu estudo indica também as soluções em que a IA pode contribuir no setor financeiro:

1. Os sistemas de IA têm capacidade para recolher e analisar grandes quantidades de dados e identificam ameaças desconsideradas por outros sistemas enviando um alerta para os especialistas na área;
2. A IA elabora relatórios identificando as áreas mais vulneráveis que devem ser melhoradas;
3. A IA pode ser programada para respostas automatizadas, assim se por exemplo algum criminoso tentar aceder aos dados a IA pode desativar contas ou acessos bem como modificar as palavras-passe;
4. O sistema de IA é atualizado constantemente com as informações mais recentes e aprende com as situações ocorridas, fazendo distinções e prioridades para responder adequadamente aos novos ataques;
5. Monitorizam as redes e os controles de segurança;
6. A facilidade com que comparam e analisam um enorme volume de dados permite analisar anomalias rapidamente;
7. Detetam ataques de phishing, podendo identificar *emails* maliciosos e aplicações falsas;
8. A utilização de IA e tecnologias na nuvem melhora as soluções de segurança pela sua eficiência, reposta a possíveis incidentes e redução dos impactos;
9. Utilização de IA em soluções de identificação, como por exemplo em reconhecimento facial ou de voz e dados biométricos.

De acordo com o relatório da Traficom (2024), as chaves para o sucesso da IA na segurança cibernética são:

1. Concentração na raiz dos problemas

É primordial definir o problema que se pretende resolver. De seguida, é necessário conhecer os desafios na resolução desse problema, as capacidades que a IA proporcionará e se a solução é compatível com o problema.

2. Vínculo entre a IA e os objetivos de negócios

Os objetivos de negócios devem ser identificados e a utilização da IA deverá ir de encontra a esses objetivos. Devem ser avaliadas a precisão, os custos e a taxa de sucessos e erros, de modo a recalcular os desenvolvimentos ao longo do tempo.

3. Identificação dos requisitos para a sua aplicabilidade

Deverá ser analisado o sistema no global, as suas necessidades, os seus componentes e verificar a aplicabilidade da integração com a IA. Perante o orçamento estipulado, deverão ser realizados projetos capazes de se integrar e resolver todas as fragilidades.

4. Relevância, disponibilidade e qualidade dos dados

A vasta gama de dados pode não ser suficiente para combater diversos problemas. É importante ter os dados essenciais ao problema e de qualidade, para permitir realizar os desenvolvimentos, as suas validações e executá-los em produção. A aposta deverá consistir em qualidade, consistência e integridade dos dados.

5. Conhecimento sobre os seus dados e a sua evolução

As mudanças, ao longo do tempo, alteram a distribuição dos dados, sendo necessário monitorizá-la. Para além disso, devem ser desenvolvidas soluções para combater as mudanças, sem perder o desempenho atual.

6. Evitar complexidade

As soluções de IA também apresentam falhas, sendo mais difícil combatê-las em processos complexos. Neste sentido, na inicialização da integração da IA, processos mais simples permitem atuar mais eficazmente, conhecer todo o processo e reduzir os problemas.

7. Realização de testes antecipadamente

Devem ser realizados testes nos ambientes de desenvolvimento e, posteriormente, no ambiente de produção. O comportamento em ambiente de desenvolvimento nem sempre será o mesmo que no ambiente produtivo, uma vez que os dados são diferentes nos ambientes, podendo provocar discrepâncias nas precisões.

8. Flexibilidade sobre as opções e nas respostas

Os sistemas de IA devem ser agregados com outros sistemas, uma vez que trarão um leque maior de respostas e apresentarão maior flexibilidade na escolha e adaptabilidade. Cada sistema terá diferentes componentes que, agregados, trarão mais benefícios do que se atuassem de forma autónoma.

9. Atenção aos custos de processamento

A formação, capacidade de armazenamento e as previsões, acarretam custos elevados para as organizações. Neste sentido, antes de se avançar será necessário fazer as análises necessárias aos dispositivos pretendidos e as estratégias de otimização a adotar.

10. Desenvolvimento de competências cruzadas

A aposta em analistas com elevada formação, conhecimento e prática, é fundamental para desenvolver soluções de IA eficazes. Será necessário envolver a capacidade dos analistas de segurança e os analistas de dados para colaborarem eficientemente na resolução dos problemas na organização.

11. Desenvolvimento de ferramentas e processos para tarefas periódicas

Sistematização de processos, automatização de tarefas diárias e repetitivas, é um ponto fulcral para melhorar a *performance* dos projetos.

Em suma, o poder da cibersegurança através da IA é conseguido através das atualizações e pesquisas constantes, na aposta da maior quantidade de informação, no desenvolvimento de estratégias a curto e longo prazo, na definição das políticas aplicáveis e no alinhamento da proteção (Wilson, 2023).

2 Criptomoedas

2.1 Histórico, Definições e Evolução

A criptomoeda para Narciso (2020), é considerada como um ativo digital ou virtual para troca de moeda. Apresenta como características a segurança, o anonimato e a

acessibilidade, uma vez que apenas necessita de acesso a *internet*. Segundo Pernice e Scott (2021), um sistema de criptomoeda pode ser considerado uma emissão de *tokens* como meio de troca, que será contabilizado pelo livro digital. Os *tokens*, por sua vez, são instrumentos digitais ao portador, dado que as transferências são realizadas pela pessoa que possui uma chave privada, permitindo realizar uma transação de saída.

Barão (2022) explicita o significado da palavra criptomoeda, sendo "cripto" algo fechado ou secreto, e "moeda" um meio de troca por transações. Além disso, considera como um meio de investimento que não é controlado ou regulamentado, não existe intermediários ou custos referentes a comissões.

Nogueira (2020), no seu estudo, indica que a primeira criptomoeda moderna foi denominada de Bitcoin e foi evidenciada por Satoshi Nakamoto em 2008. Permitia a descentralização, era baseada na tecnologia *blockchain* e apresentava anonimato total para quem pretendia comprar ou vender (Nogueira, 2020). A tecnologia *blockchain* é a base de dados que contém os registos efetuados, garantindo a maior segurança e o não rastreamento (Narciso, 2020). Barão (2022) identifica *blockchain* como uma rede com alto nível de segurança, transparência e sem tolerância para erros nas operações. A chave privada garante a titularidade da transação na rede, permitindo despender de determinado montante para transferi-lo para outro indivíduo (Narciso, 2020). Cada transação é validada por um grupo, e qualquer pessoa consegue ter a noção dos procedimentos realizados dentro da rede. Foca-se na clareza de informação, assim como na restrição por utilizador (Nogueira, 2020).

A criptomoeda representa um meio alternativo de transferência de dinheiro sem registos (Zaghloul *et al*., 2020). A criptomoeda Bitcoin foi lançada no mercado em 2009 e as primeiras transações foram realizadas em 2010. Com o passar dos anos ganhou poder no mercado e atualmente é considerada uma moeda virtual de confiança e legítima para efetuar pagamentos (Nogueira, 2020).

As transações da bitcoin utilizam protocolos criptográficos, de modo a fornecedor um processo seguro, preservando as entidades do comprador e do vendedor (Zaghloul *et al*., 2020). As transações são armazenadas num banco de dados que contém todas as transações realizadas e as verificações necessárias. Após o sistema da bitcoin muitos outros foram criados. No entanto, o mercado das criptomoedas é considerado volátil, uma vez que os preços das moedas variam bastante, oscilando entre diversas subidas e descidas

e, noutros casos, pela entrada e saída do mercado por diversas moedas (Zaghloul *et al*., 2020).

O aumento da procura das criptomoedas tem levado cada vez mais empresas a desenvolverem a sua própria carteira digital, bem como a sua própria criptomoeda (Nogueira, 2020). Entre as vantagens desse movimento estão o controlo realizado pela rede, a segurança e rapidez nas transferências, a oportunidade de investimento e o reconhecimento. Relativamente às suas desvantagens, encontra-se o alto investimento necessário e os riscos associados, como a forte volatilidade e os financiamentos ilegais (Nogueira, 2020).

As vantagens evidenciadas por Barão (2022) consistem na facilidade e rapidez no envio dinheiro para qualquer lugar, sem custos ou taxas associadas, bem como a inexistência de intermediários e proteção contra a inflação. No que diz respeito às desvantagens, ressalta o risco abrangente aos investidores e a possibilidade de uso para finalidades ilícitas (Barão, 2022).

Chhatwani e Parija (2023) mencionam que o valor das criptomoedas depende dos investidores, o que torna o mercado mais volátil, especulativo e arriscado. A privacidade entre transações não permite compreender de forma direta as características dos investidores, no entanto, os autores destacam-nos como racionais, confiantes e que fundamentam as suas decisões através de preconceitos comportamentais (Chhatwani & Parija, 2023).

2.2 A Influência da IA nas Criptomoedas

Sabry *et al*. (2020) evidenciam a utilização de IA nos sistemas de negociação para a previsão do mercado de ações e na previsão do preço da moeda, facilitando a tomada de decisão aos investidores. Além disso, esses sistemas identificam comportamentos e padrões com maior eficácia, permitindo a previsão e proporcionando maior atenção a gastos ou ações suspeitas. A integração da IA às criptomoedas permitirá agilizar os serviços através da rapidez nos processos, redução de erros causados por cálculos humanos e minimizar o risco nas previsões a longo prazo (Sabry *et al*., 2020).

Segundo Choithani *et al*. (2024) a combinação das criptomoedas com a IA proporcionará um avanço no processamento da informação aumentará a sua visibilidade. A flutuação de

preços das criptomoedas representa um dos maiores desafios para os analistas e a IA permitirá atenuar esses desafios, melhorando as previsões, especialmente a curto prazo. Nos últimos anos, as criptomoedas tiveram uma procura elevada e são cada vez mais estudadas por investidores. No entanto, como o seu surgimento é considerado recente, provoca falhas na base de dados e resulta em informações menos precisas (Choithani *et al*., 2024).

As criptomoedas apresentam vários desafios que podem ser ultrapassados com a IA, conforme descrito pelos autores Sabry *et al*. (2020). Em primeiro lugar, no seu estudo, indicam que a previsão de preços é complexa, uma vez que o valor das criptomoedas é influenciado por fatores como a estabilidade política do país, fóruns, a demanda, bem como as tendências atuais. Além disso, o preço dos concorrentes e o estado do mercado também desempenham um papel importante. A IA permitirá facilitar a análise dessas influências, utilizando fontes de informação pormenorizada e séries temporais. Em segundo lugar, os autores referem a previsão da volatilidade, que se refere ao nível de variação dos preços ao longo do tempo. A estimação da volatilidade permitiria estimar a faixa de preço da criptomoeda, no entanto, as mudanças constantes no meio envolvente causam maior risco e incerteza, promovendo o aumento da volatilidade. Em terceiro lugar, os autores indicam a negociação automatizada, na qual os sistemas, com base no histórico do mercado, calculam os indicadores e procedem à criação de estratégias a qualquer momento do dia, tendo como condicionamento os recursos e a capacidade dos mesmos. Posteriormente, é evidenciado o anonimato e a privacidade, que apresentam desafios, como a possibilidade de recorrer de ilegalidades e o branqueamento de capitais, afetando a estabilidade e a confiança nas criptomoedas (Sabry *et al*., 2020).

2.3 Crimes Cibernéticos no Mercado das Criptomoedas

O risco cibernético é uma grande ameaça a instituições públicas e privadas, provocando perdas de reputação, de confiança com os seus parceiros e clientes, bem como, financeiras (Arcuri *et al*., 2018). Quando uma empresa sofre uma violação de informação, acarretará de imediato um custo elevado, dado que o crime cibernético é uma das maiores ameaças para as organizações. O impacto dos ataques deve ser compreendido em relação aos retornos no mercado de ações, para que seja possível decidir os níveis de investimento em atividades de segurança. No entanto, o impacto é difícil de medir. Uma violação na

segurança pode reproduzir uma diminuição nas receitas e despesas mais elevadas, o que leva a uma diminuição dos lucros e futuros dividendos, bem como afetar a reputação da empresa e o seu valor de mercado. Por outro lado, a longo prazo, as consequências económicas devem ser ligeiras, caso os dados de clientes e os métodos de negócios das empresas não tenham sido comprometidos. Com base neste pensamento, as organizações devem atuar proactivamente na sua gestão contra ataques cibernéticos e melhorar ao nível da segurança e das suas ações (Arcuri *et al*., 2018).

As criptomoedas podem sofrer ataques e enganos no sistema, como o gasto duplo (Zaghloul *et al*., 2020). O gasto duplo consiste em enganar o sistema, utilizando o mesmo bitcoin em mais do que uma transação. Para combater este problema, o processo de validação da transação devolve um código. Esse código tornou mais difícil enganar o sistema, uma vez que a pessoa que o está a tentar defraudar terá de reverter uma transação que já foi armazenada na *blockchain*, sendo este um processo extremamente complicado, mas não impossível. O ataque de corrida consiste na aceitação de uma transação antes da sua confirmação, ou seja, o vendedor fornece ao comprador um produto ou serviço antes de obter a confirmação no *blockchain*. O *hacker* nestas situações realiza duas transações. A primeira consiste na transação que paga ao comerciante em troca do produto ou serviço e a segunda, é a transação fraudulenta, na qual paga a mesma quantia à sua carteira. O *hacker* realiza as duas transações em simultâneo na rede Bitcoin, sendo que é validada a transação até ao momento em que uma delas será armazenada no *blockchain*. A transação fraudulenta se for verificada primeiro e adicionada ao *blockchain* provoca que a transação ao vendedor seja invalidada e rejeitada, sendo por este motivo que os vendedores devem aguardar a confirmação. Um ataque bem sucedido de gasto duplo será lucrativo se a receita for superior ao custo da execução do ataque (Zaghloul *et al*., 2020).

Caporale *et al*. (2020) evidenciam que as criptomoedas são consideradas um alvo preferencial para crimes cibernéticos o que se deve à sua vulnerabilidade provocada pelo anonimato das negociações e da tecnologia *blockchain* que é criptografada. Neste sentido, realizaram uma análise aos ataques cibernéticos, por indústria alvo, na qual concluíram que os ataques causam elevadas perturbações no mercado, que por sua vez, provocam efeitos negativos nos retornos e na volatilidade, sendo a aposta na cibersegurança um fator imprescindível (Caporale *et al*., 2020). Todos os anos decorrem invasões que são confirmadas nas bolsas, na qual ocorre o roubo de centenas de milhões de euros em ativos

criptográficos e o branqueamento de capitais decorrente da falta de regulamentação (Lapuh Bele, 2021).

De modo a investigar o impacto nas violações de segurança nos retornos das ações, os autores Arcuri *et al*. (2018), realizaram um estudo que envolveu 226 ataques cibernéticos a 110 empresas, onde a maioria delas pertence à área de finanças e seguros. Os autores concluíram evidências de uma reação geral negativa no mercado de ações, sendo o setor financeiro o mais afetado. Ataques, como vírus informáticos e falhas nos sistemas, podem ser os mais perigosos. O cibercrime prejudica o comércio, a competitividade e inovação nas empresas afetadas. Assim sendo, os sistemas devem ser monitorizados, devem ser realizadas periodicamente verificações e os avisos não podem ser ignorados ou desvalorizados. A resposta após o ataque dever ser eficaz para minimizar os impactos, sendo essencial existir um plano de ação pré-definido, além da consciencialização sobre o problema e o investimento em formações contínuas (Arcuri *et al*., 2018).

A metodologia a aplicar neste estudo é uma metodologia qualitativa. Segundo Creswell (2010), a investigação qualitativa é composta pelas estratégias de investigação, métodos de recolha, análise e interpretação de dados. Os investigadores obtêm os dados através de documentos, observações de comportamentos e entrevistas. Neste estudo, os investigadores recolheram diversas fontes de dados, como documentos variados e entrevistas. O processo de pesquisa, inicialmente, não está completamente definido e restrito. Ou seja, durante as diferentes fases do processo, o planeamento pode ser ajustado após o início da recolha de dados no campo. A pesquisa qualitativa é também considerada como interpretativa, isto é, os investigadores fazem a sua interpretação tendo em conta o que ouvem nas entrevistas, identificando as diversas perspetivas e visões. Nos estudos qualitativos, os investigadores identificam as questões de pesquisa, compostas por uma questão central e subquestões associadas. A questão central é ampla e aborda o conceito do estudo, enquanto que as subquestões, na maioria das vezes, são aplicadas nas entrevistas (Creswell, 2010).

A estrutura dos resultados constitui uma compilação de relatórios realizados por diversas empresas com o objetivo de compreender a cibersegurança na atualidade e em que medida a IA beneficiará a cibersegurança. Tendo em conta este objetivo, foram definidas as seguintes questões:

1. A cibersegurança é um tema presente?
2. A cibersegurança constitui uma preocupação generalizada?
3. A IA consegue combater os problemas atuais?

Os objetivos secundários deste estudo assentam na verificação do estado atual da cibersegurança, nas consequências que os países estão a enfrentar com ataques cibernéticos, em averiguar de que forma os países se estão a proteger e as práticas que estão a utilizar, bem como validar se a IA está a conseguir combater os problemas e avaliar o estado do mercado criptográfico.

De modo a conseguir dar resposta às questões estipuladas foram analisados 15 relatórios das entidades Arkose Labs, Chainalysis, Deloitte, IBM, European Union Agency for Law Enforcement Cooperation (Europol), ESET, Mckinsey, Microsoft, PricewaterhouseCoopers (PwC), Traficom e U.S. Department of the Treasury. Os relatórios selecionados abordam entrevistas realizadas em Portugal e entrevistas espalhadas pelo mundo, abrangendo diversas áreas de atividade entre 2021 e 2024. Uma

vez que estamos perante um tema bastante atual, apenas faria sentido considerar abordagens recentes. Relativamente ao mercado das criptomoedas, serão analisados relatórios de 2017 a 2024.

Em primeiro lugar, será exposto o caso português, através dos relatórios da PwC e do Centro Nacional de Cibersegurança (CNCS). Em seguida, apresentar-se-ão os relatórios com entrevistas realizadas em todo o mundo. Em terceiro lugar, teremos os relatórios sobre as criptomoedas. Por fim, haverá um resumo dos resultados, com a interligação de informação entre alguns dados comuns nos relatórios.

Os dados selecionados foram os seguintes:

Tabela 1 – Relatórios Selecionados para a Investigação

Título Publicação	**Entidades**	**Ano**
2023 Global Future of Cyber Survey	Deloitte	2022
Applying artificial intelligence in Cybersecurity	Traficom	2024
Blockchain & Cyber Security	Deloitte	2017
Building and improving cyber resilience	Microsoft	2023
Compreender a cibersegurança num novo panorama social	PwC	2021
Cost of a data breach Report 2024	IBM	2024
Five common data security pitfalls to avoid	IBM	2023
Guide to Cryptocurrency Security	Arkose Labs	2024
Internet Organised Crime Threat Assessment	Europol	2024
Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services	U.S. Department of the Treasury	2024
Relatório Cibersegurança em Portugal: Riscos & Conflitos	CNCS	2024
Relatório Cibersegurança em Portugal: Sociedade	CNCS	2023
The 2024 Crypto Crime Report	Chainalysis	2024
The state of AI in 2023: Generative AI's breakout year	Mckinsey	2023
Threat Report H1 2024	ESET	2024

Fonte: Elaboração Própria

3.1 Relatórios de Segurança Cibernética e Inteligência Artificial

A presente secção evidencia os relatórios selecionados, elaborados entre 2021 e 2024, sobre a segurança cibernética e a IA. Esta inicia-se por relatórios baseados em entrevistas realizadas a entidades portuguesas, seguidos pelos relatórios baseados em entrevistas realizadas em todo o mundo.

3.1.1 Relatório da PwC de 2021

Em 2021 a PwC publica o seu relatório de pesquisa cibernética em Portugal, sobre a compreensão da cibersegurança. PwC (2021) realizou um inquérito a 56 organizações, de 12 setores de atividade, entre 8 de fevereiro e 5 de março de 2021. Este inquérito revelou que 15% das entidades inquiridas se preocupam com danos reputacionais, cerca de 13% temem perdas financeiras devido a incidentes ou roubo de informações e, uma em cada dez organizações está preocupada com a perda de dados pessoais. O valor aproximado que as entidades inquiridas estimam gastar no próximo ano e meio com cibersegurança é de 50 000€. No entanto, um terço das entidades refere não ser adequado perante as ameaças existentes e apenas 15% prioriza iniciativas de consciencialização em cibersegurança para 2024. O estudo realizado revela as maiores preocupações para as empresas inquiridas, nomeadamente, os danos à marca e a reputação das entidades, indisponibilidade dos sistemas, comprometimento de informações pessoais, perdas financeiras e de dados pessoais, perda de clientes, aumento dos processos contra as entidades, perda de propriedade, roubo de segredos comerciais, perda de parceiros e de fornecedores, e, por fim, danos às instalações físicas (PwC, 2021).

Em 2020, o contexto da pandemia promoveu alterações ao ambiente de trabalho, como o aumento do trabalho remoto, a expansão da oferta de produtos digitais e regimes mais flexíveis, que promoveram o aumento dos riscos e dos ciberataques. Existiu um aumento de 88% de incidentes com vulnerabilidade em 2020 comparativamente com 2019. Perante este problema, houve uma necessidade de repensar o negócio e incluir a cibersegurança na estratégia das empresas (PwC, 2021).

O caminho a seguir, evidenciado por PwC (2021), inicia-se pela redefinição da estratégia em cibersegurança, repensando o orçamento disponível, priorizando iniciativas de implementação de modelos de segurança, preparando medidas perante as crises e aumentando as competências, através de formação, para construir uma equipa preparada para os acontecimentos futuros. Além disso, para garantir o sucesso na estratégia sobre a

segurança, são necessários cinco pilares, sendo eles as pessoas, as capacidades, os processos, a tecnologia e a automação. No que concerne às pessoas, será necessário melhorar as competências de segurança e criar uma equipa formada e atualizada. Em relação às capacidades e aos processos, devem ser tomadas iniciativas de segurança e privacidade, quantificar os riscos cibernéticos, unificar os relatórios sobre os riscos e trabalhar a resiliência cibernética. No pilar da tecnologia, é crucial investir em sistemas avançados com capacidade de defesa e de identificações de segurança, bem como reduzir o custo das operações através da automação. A automação envolve o investimento nas tecnologias, a monitorização dos processos para obter a eficácia dos mesmos, a pesquisa e analise de dados, e a utilização da IA na defesa cibernética (PwC, 2021).

3.1.2 Relatório do CNCS de 2023

O Relatório do CNCS (2023), analisa o tema da cibersegurança em Portugal, em relação a 2022 comparativamente com 2021, e evidencia:

- Aumento de pessoas a utilizaram a *internet*;
- Aumento de artigos publicados nos media com a palavra cibersegurança;
- Aumento de empresas a definir a Política de Segurança das Tecnologias da Informação e Comunicação (TIC);
- A medida de segurança mais aplicada foi a autenticação das palavras-passe, no entanto, apenas um terço optou por aplicar a autenticação multifator;
- 54% das empresas refere ter documentado medidas e procedimentos de segurança;
- Aumento de sessões presenciais e remotas sobre a sensibilização da cibersegurança;
- Aumento de ações sobre a segurança nas TIC das empresas para com os seus colaboradores.

O número de artigos publicados nos media com o termo cibersegurança aumentou substancialmente de 2021 para 2022. Contávamos com 1344 artigos publicados em 2021 e em 2022 foram publicados 2187. No que diz respeito a políticas de segurança sobre as TIC, o inquérito da Eurostat e do Instituto Nacional de Estatística, revela que apenas 43% das empresas tem definidas as políticas e as medidas de segurança mais utilizadas, nomeadamente, o uso de palavras-passe seguras, os *backups* de proteção em local distinto,

o controlo de rede, o histórico para efetuarem análises após os incidentes, a utilização de *virtual private network* e o monitoramento para detetar ameaças suspeitas e emissão de alertas para a empresa (CNCS, 2023).

3.1.3 Relatório do CNCS de 2024

De acordo com o relatório de riscos e conflitos em Portugal do CNCS (2024), os profissionais de cibersegurança identificam um aumento do risco das empresas em sofrer incidentes de segurança em 2023 e 2024. Identificam como tendências, a curto prazo, a potencialização do cibercrime, devido ao aumento da compra e venda de criptomoedas, um crescimento do risco de sabotagens e ataques às vulnerabilidades, desinformação da IA e a persistência de ameaças sobre os fatores humanos. Existem diversas ameaças eminentes, como burlas online, comprometimento das contas, ciberespionagem, comprometimento de sistemas, desinformação, e aproveitamento da IA para atividades maliciosas (CNCS, 2024).

CNCS (2024), através do *computer emergency response team* (CERT), revela o número de incidentes registados em Portugal por ano. O CERT é um serviço que coordena incidentes da administração pública, operadores de infraestruturas e serviços, e prestadores de serviços. Através do CERT, em 2016, foram registados 413 incidentes, enquanto em 2019 foram, o número subiu para 754 incidentes. Em 2020, temos o *boom*, subindo para 1418, que continua nos anos seguintes, com 1781, seguido de 2023 e 2025 incidentes. É importante destacar, que a partir de 2020, as vulnerabilidades também passam a ser consideradas e contabilizadas como incidentes, embora o seu impacto total não seja significativo. Ao nível dos setores, as áreas mais atacadas são os prestadores de serviço da *internet*, os bancos, a saúde, a educação e o ensino, seguido pelas infraestruturas digitais, os transportes e os serviços em nuvem. A principal forma de ataque foi através do *phishing*, que corresponde a crimes através dos correios eletrónicos, chamadas telefónicas ou mensagens de texto. Seguido pelos crimes de *ransomware*, na qual são bloqueados dispositivos, retiradas informações confidenciais e há ameaças de manter o bloqueio até que seja efetuado um pagamento ao invasor. Estes pagamentos rondam a casa dos sete ou oito dígitos, sendo um abalo para as entidades (CNCS, 2024).

A Direção Geral da Política de Justiça produz informação estatística na área da justiça e disponibiliza relatórios sobre a criminalidade. No relatório do CNCS (2024), são

mencionados o número de crimes relacionadas com a informática e os crimes informáticos, tendo ocorrido 2 868 crimes em 2009, com um aumento ao longo dos anos seguintes. Em 2015, já contavam com 9 534 crimes registados, em 2018 eram 12 087, sendo que o *boom* ocorreu em 2019 com 19 477, um aumento de mais de 7 000 crimes em relação ao ano anterior. Em 2020 ultrapassou-se 23 000 crimes, tendo ocorrido em 2023 cerca de 25 733 registos. Os crimes são essencialmente a burla informática e nas comunicações, seguido pelos acessos ilegítimos e a falsidade informática. A Procuradoria-Geral da República (PGR) contém um gabinete de cibercrime que recebe denúncias de cibercrimes. Segundo a PGR, existe um aumento elevado de denúncias, em 2016 apenas foram registadas 108 denúncias, em 2020 já contavam com 544 e em 2022 foram registadas 2125 denúncias. A criminalidade destas denúncias advém essencialmente do *phishing*, seguido pelas burlas online, no mercado imobiliário, burlas com criptomoedas e outros produtos financeiros, redes falsas, falsas convocatórias, telefonemas e mensagens falsas (CNCS, 2024).

Em relação às recomendações sobre o risco de ameaças, o CNCS (2024) subdivide pelas ciberameaças que considera principais. Em primeiro o lugar, o *ransomware*, destacando a salvaguarda de cópias de segurança fora da rede, atualização dos sistemas e das aplicações, evitar sites que não sejam seguros, formar os colaboradores sobre o *phishing*, segmentar as redes e monitorizar as ações com base nas políticas de segurança definidas. De seguida, o *phishing*, recomendando não abrir links de *emails* ou mensagens suspeitas, validar as origens dos *emails* recebidos e não partilhar conteúdos confidenciais por *email*, validar as fontes dos pedidos sobre transferências bancárias e realizar simulações de ações de *phishing* com os colaboradores. Em terceiro lugar, as burlas online, devendo os indivíduos desconfiar de ofertas de produtos demasiado apelativos, verificar as fontes de transferências e utilizar carteiras virtuais. Para finalizar, o compromisso das contas na qual é evidenciado as modificações das palavras-chave sempre que se verifiquem suspeitas, utilização de palavras-passes fortes e diferentes dos dados pessoais, aplicar o multifator, monitorizar e bloquear os ataques, registar e analisar os eventos (CNCS, 2024).

3.1.4 Relatório da Deloitte de 2023

A Deloitte (2023) criou um relatório com base no inquérito realizado sobre o Futuro Global da Investigação Cibernética, na qual afirma que o mundo está cada vez mais interligado e, juntamente com as oportunidades e o crescimento, também existem mais riscos. O inquérito foi realizado a mais de 1000 executivos e outros líderes seniores das Tecnologias de Informação, segurança e risco, em 20 países. O inquérito abordou diversos setores e foram limitadas a organizações com pelo menos 1 000 colaboradores e 500 milhões de dólares. Tem como objetivo partilhar as suas opiniões sobre as ameaças cibernéticas e as perspetivas futuras. Sobre os locais dos inquiridos, 35% concentra-se na América do Norte e do Sul, 40% na Europa, Médio Oriente e África e, 25% na Ásia. Neste inquérito, 70% dos inquiridos relatam que a cibersegurança está na sua agenda e, 55%, pretende aumentar o seu investimento nesta área. Para além disso, foi possível identificar organizações com um plano operacional e estratégico, com ações para melhoria contínua na segurança cibernética e com um programa de risco para monitorizar a segurança perante os seus parceiros e os seus fornecedores. Estas organizações afirmam o aumento de valor à sua estratégia de negócios e a sua eficiência, após a aposta na segurança cibernética (Deloitte, 2023).

Deloitte (2023) revela as prioridades de transformação digital dos seus inquiridos, estando em primeiro lugar a nuvem, seguido pela análise de dados, as operações com tecnologia e os sistemas de controlo, a IA, e por último o 5G. Em relação aos incidentes, 91% das entidades inquiridas, referiu já ter sofrido pelo menos um incidente. As consequências negativas resultantes dos incidentes, prende-se com as interrupções operacionais, a perda de receita, a perda de confiança por parte do cliente, a perda de reputação, o financiamento necessário para conseguir uma iniciativa estratégica, a perda de confiança e dificuldade em retenção de talento, o roubo de propriedades, a queda dos preços nas ações, as multas e, em casos mais extremos, a mudança de liderança (Deloitte, 2023).

As estratégias de planeamento cibernético são identificadas como a análise e atualização dos planos anualmente, constituir uma gestão de líderes seniores com excelentes capacidades de compreensão dos programas cibernéticos, quantificar o risco e avaliar o retorno dos investimentos com cibersegurança, criação de respostas a incidentes, validar com fontes externas as iniciativas aplicadas e a aplicar. No que diz respeito às atividades a aplicar, as organizações devem realizar formações aos colaboradores sobre a área,

executar testes sobre o plano de resposta, atualizar e validar a proteção dos seus dados e processamentos (Deloitte, 2023).

Com o seu estudo, a Deloitte (2023) subdividiu as entidades e a sua análise de resultados, com base na maturidade cibernética das entidades. Na definição da maturidade, avaliaram o planeamento robusto pelos planos estratégicos e operacionais a atuar nas defesas e respostas sobre as ameaças. Para além disso, avaliaram as atividades cibernéticas sobre a avaliação de risco e planeamento, e respostas a incidentes. Por fim, o envolvimento da direção sobre as questões cibernéticas e o período temporal entre as análises. Com base nesta maturidade verificaram que 35% não aderem a nenhuma das subdivisões, 41% apresenta maturidade média, pois está presente em pelo menos uma subdivisão, e 21% adere entre duas a três subdivisões, sendo considerada como alta maturidade. As organizações com alta maturidade têm melhores resultados e conseguem que o investimento proporcione valor estratégico para o seu negócio. Estas organizações têm uma melhor gestão dos seus líderes na área das tecnologia da informação, criam cenários e realizam testes sobre incidentes, para avaliar a sua capacidade de resposta, agilizar os seus métodos operacionais e utilizar os benefícios da IA (Deloitte, 2023).

3.1.5 Relatório da Microsoft de 2023

A Microsoft representa uma empresa com um compromisso de criar um mundo mais seguro, contendo um abundante investimento em investigação na segurança, inovação e na comunidade de segurança global. Em 2023, no seu estudo, revelaram a deteção de cerca de 65 triliões de sinais sintetizados por dia para combater as ameaças digitais e a ciberatividade criminosa (Microsoft, 2023). Convertendo em segundos, representa mais de 750 milhões de sinais através da sua análise de dados e algoritmos de IA e, evidenciam o bloqueio de cerca de 4 000 ataques por segundo. Contam com mais de 10 000 engenheiros, investigadores, analistas, especialistas em cibersegurança e também mais de 15 000 parceiros em soluções especializadas de segurança para aumentar a proteção dos seus clientes (Microsoft, 2023).

A Microsoft (2023) evidencia de que forma as empresas devem proteger-se contra os ataques. Em primeiro lugar, a utilização do *multi-factor authentication* (MFA). O MFA representa uma verificação de dois passos, que provam ao serviço se o indivíduo é efetivamente quem diz ser, protegendo os utilizadores com as palavras-passe

comprometidas e reforça as suas identidades. De seguida, refere os Princípios *Zero Trust*, que assentam na verificação explicita, validação dos utilizadores e dos dispositivos antes de dar acesso aos recursos. O acesso fornecido deverá ser o que contém menos privilégios, restringindo os acessos aos recursos e o assumir a violação e o comprometimento dos sistemas de modo a realizar a monitorização contante dos ambientes e dos possíveis ataques. Em terceiro lugar, a utilização de softwares de deteção e bloqueio contra os ataques em tempo útil. Para finalizar, as atualizações e os conhecimentos sobre os seus dados, localizações, bem como, a validação das defesas eficazes (Microsoft, 2023).

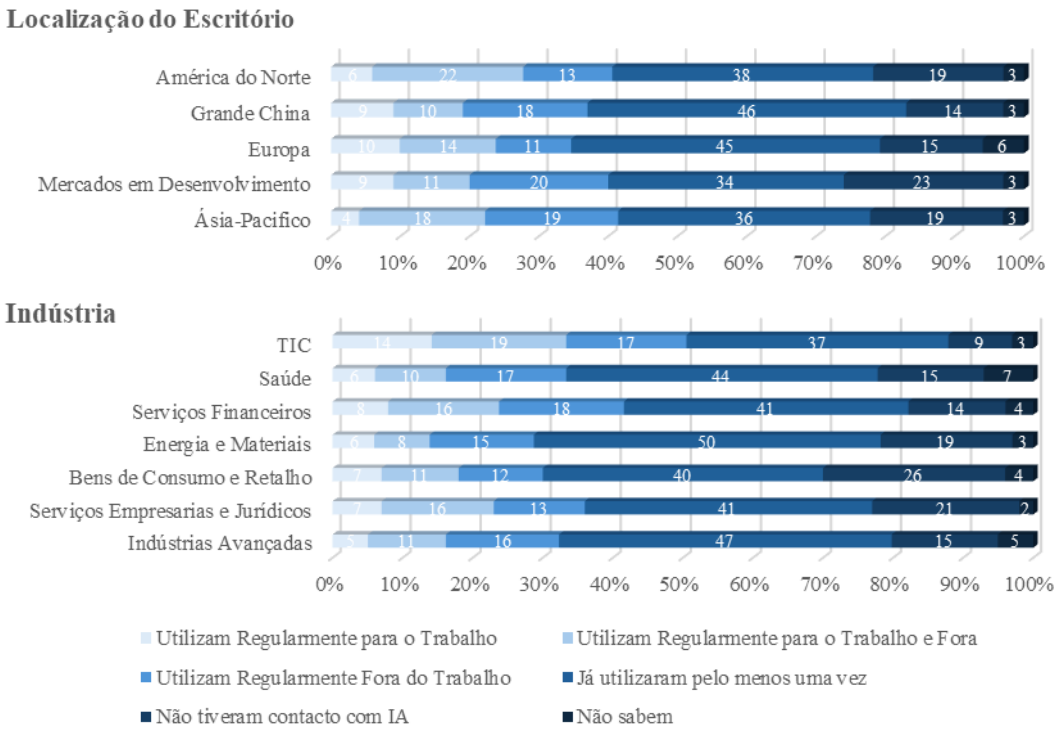
No relatório da Microsoft (2023) prevê-se um custo com o cibercrime de 10,5 biliões de dólares anuais até 2025. Para fazer face a este problema, os profissionais devem retirar partido das mais recentes tecnologias e inovações com o apoio da IA. Os *large language model* (LLM), modelos de linguagem de grande escala, são programas de IA que reconhecem e geram textos sobre grandes conjuntos de dados complexos. A Microsoft acredita no potencial dos LLM para melhorar significativamente a ciberdefesa. Neste sentido, ao nível da análise, os LLM recolhem e analisam dados para a formação de padrões e tendências sobre as ameaças, que, por sua vez, fornecerão recomendações e alertas sobre as mesmas. Em relação à resposta e recuperação de incidentes, os LLM ajudarão no tratamento de prioridades, geração de *scripts* de automatização nas respostas, coordenação de equipa e documentação detalhada sobre o incidente e as ações realizadas. Além disso, também contribuem para a aprendizagem sobre os incidentes, bem como nas sugestões de melhorias para prevenção e redução dos impactos no futuro. No que diz respeito à validação, os LLM podem automatizar as atividades em ambientes de testes, criar validações de segurança, avaliar os resultados e intervir com melhorias, desenvolver ferramentas específicas, automatizar tarefas repetitivas e tratar de tarefas ocasionais que dependam da intervenção humana. Contudo, são necessários ajustes contínuos, de modo a aumentar os módulos de análise e a fonte de dados, para que os LLM consigam obter as ameaças e os dados atualizados (Microsoft, 2023).

3.1.6 Relatório da McKinsey de 2023

McKinsey é uma empresa de consultoria empresarial americana que tem como propósito ajudar os seus clientes a alcançar melhorias diferenciadas a longo prazo. Todos os anos, a entidade realiza a sua pesquisa global, entrevistando 1684 indivíduos de 11 a 21 de abril

de 2023, de várias partes do mundo, e publica o seu relatório. No relatório sobre o estado da IA em 2023, confirmam o elevado crescimento das ferramentas de IA, que se tornou um tema de foco para os líderes das organizações. Para este relatório, foram entrevistados 164 indivíduos da Ásia-Pacífico, 515 indivíduos da Europa, 392 indivíduos da América do Norte, 337 indivíduos da Grande China (Hong Kong e Taiwan) e 276 indivíduos dos mercados em desenvolvimento (Índia, América Latina, Médio Oriente e Norte de África) (McKinsey, 2023).

Gráfico 1 – Utilização de IA Generativa por Localização do Escritório e por Indústria



Fonte: McKinsey (2023)

Segundo McKinsey (2023), a IA generativa consiste num tipo de IA que cria conteúdos e ideias com base em padrões identificados na aprendizagem. A IA generativa é treinada, por exemplo, para aprender os comportamentos humanos e as linguagens de programação. Pela análise do gráfico 1, verificamos que um terço das organizações entrevistadas já utilizam regularmente a IA generativa em pelo menos uma função, e 40% das organizações que utilizam esta tecnologia pretendem continuar a investir mais.

Através do gráfico por localizações, verifica-se que a Europa é a região que mais utiliza regularmente a IA generativa no trabalho, enquanto a Ásia-Pacífico utiliza pouco no

trabalho, mas em contrapartida, utiliza significativamente e regularmente fora do trabalho. A categoria com maior concentração na utilização de IA generativa de pelo menos uma vez, varia entre os 34% e os 46%. Quanto ao desconhecimento sobre esta ferramenta, a Europa contém 6% dos resultados e as restantes regiões apresentam resultados de 3%. Relativamente às indústrias, como seria expectável, as TIC são as que mais utilizam a IA generativa, com percentagens a concentrar-se entre os 41% e 50%, na utilização da ferramenta em pelo menos uma vez (McKinsey, 2023).

As empresas que mais utilizam a IA estão a obter bons resultados, relevando a intenção de investirem cada vez mais. Estas empresas têm maior probabilidade de utilizar a IA nas otimizações dos desenvolvimentos de produtos, na criação de funcionalidades para produtos existentes, na avaliação da gestão de desempenho e na otimização da carga de trabalho. Pelo lado negativo, as organizações revelam dificuldades em contratar para esta área, especialmente para funções como analistas de dados em IA, especialistas em dados, engenheiros de aprendizagem de máquina e supervisores de produtos de IA (McKinsey, 2023).

McKinsey (2023) em comparação com a sua entrevista no ano anterior, constatou que a adoção da IA se considera estável, uma vez que 50% dos indivíduos, afirmaram adotar esta ferramenta nos dois anos, assim como, os indivíduos que indicaram utilizar apenas numa função. Em 2023 os indivíduos entrevistados que utilizavam apenas uma função representam 55%, em duas funções 31%, em três funções 16%, em quatro funções 6% e, em 5 ou mais funções, 3%. As organizações obtêm benefícios com a adoção da IA e mencionam que a sua receita aumenta principalmente no fabrico, marketing, vendas, investigação e desenvolvimento e recursos humanos (McKinsey, 2023).

3.1.7 Relatório da Traficom de 2024

Segundo Traficom (2024), a utilização da IA proporciona diversos benefícios, tais como a velocidade e a automatização. Os ataques cibernéticos ocorrem em segundos e em qualquer momento do dia, neste sentido, é imprescindível ter uma resposta rápida para reduzir os impactos. Os analistas não têm capacidade suficiente para analisar a vasta gama de arquivos, objetos e alertas de segurança, sendo nesta fase que o poder da IA atua. A sua capacidade de processamento em escala e em tempo real é fascinante, conferindo um enorme poder para as organizações. A sua capacidade para resumir e extrair padrões

permitirá maximizar o tempo de pesquisa, e a sua automatização possibilitará a melhoria dos processos, as respostas e uma ação eficaz. Outro benefício consiste na escala e na complexidade. A IA processa uma vasta análise de dados em curtos períodos de tempo, promovendo a eficácia e a eficiência, independentemente da complexidade das amaças ou dos ataques. O apoio da IA nos processos torna célere a capacidade de resposta, além de garantir uma boa organização e compreensão dos comportamentos dos dispositivos e redes, o que facilita a deteção de anomalias ou padrões incomuns que sinalizam futuras ameaças. Além destes benefícios, a IA apresenta uma forte adaptabilidade em função dos diversos acontecimentos. Neste sentido, as defesas são reforçadas, as regras são adaptadas e os novos padrões são identificados para acompanhar as mudanças. A rapidez na perceção dos processos e na leitura dos dados promove ações rápidas e adaptabilidade à evolução dos padrões. Um fator também fundamental, consiste na utilização eficiente dos recursos. Os analistas são mais proativos quando podem analisar os padrões revelados pela IA, tornando a segurança que proporcionam mais estratégica e complexa. A priorização dos problemas é fundamental para reagir eficazmente e em tempo real, de acordo com a complexidade e urgência, reduzindo os riscos e os impactos nas organizações (Traficom, 2024).

A capacidade dos LLM em sintetizar dados complexos e criar resultados de fácil compreensão, fornecendo transparência e explicabilidade a diversos processos, facilita a tomada de decisão dos gestores e especialistas. Além disso, os LLM ajudam no aumento da automatização e na utilidade de ferramentas de IA na segurança cibernética, ao utilizar fontes de informação internas e externas, redefinindo as ameaças que afetam as entidades e que vulnerabilizam os sistemas. São considerados promissores na sugestão de respostas e ações para minimizar os impactos (Traficom, 2024).

Traficom (2024) afirma que a utilização da IA na segurança cibernética também apresenta particularidades e desafios. Os modelos de IA devem ser ágeis, robustos, conter capacidades de aprendizagem e adaptabilidade, o monitoramento deve ser contínuo, assim como, as atualizações perante as mudanças de cenários. A automatização deve ser o foco, sem comprometer a segurança. A otimização dos processos e a garantia de previsões precisas deve estar assegurada. Os invasores também utilizarão instrumentos com o apoio da IA e estão preparados para atacar o sistema, fragilizando o processo de IA utilizado para a defesa. Portanto, a resiliência, a defesa proativa, a vigilância e a capacidade de defesa sobre a identificação de falsos dados para enganar o sistema são

fundamentais. Um grande desafio para a IA consiste nos falsos positivos, que se referem à sinalização de comportamentos normais como maliciosos, provocando custos e erros nas respostas e nas ações futuras. Além disso, os modelos de IA também serão mais fracos se tiverem poucos dados na sua análise. A escassez de ataques e de informação sobre a resposta provoca dificuldades na identificação de ameaças e de anomalias. A compreensão por parte dos analistas sobre as decisões tomadas pela IA é essencial para garantir a confiança e a transparência sobre os métodos de ação e decisão. Os métodos que a IA utiliza devem ser interpretáveis de modo a identificar as causas dos problemas e a desenvolver contramedidas. O maior desafio pode consistir nas preocupações com a privacidade, uma vez que, diversas análises devem ser confidenciais, mas são essas análises que proporcionam os dados necessários nas avaliações (Traficom, 2024).

3.1.8 Relatório do U.S. Department of the Treasury de 2024

O U.S. Department of the Treasury (2024) escreveu um relatório sobre o estado da utilização da IA nos serviços financeiros para fins de segurança cibernética. Para este relatório, foram entrevistadas 42 instituições financeiras. Dos entrevistados, a maioria utiliza sistemas baseados em IA para apoiar os seus colaboradores em atividades de pesquisa e realização de relatórios. Relativamente às ferramentas de IA para deteção de fraudes, estas também são utilizadas por grande parte dos entrevistados para gestão de riscos. A adoção de IA pelos entrevistados, tem como propósito melhorar a qualidade e os custos das suas funções em segurança cibernética e antifraude, através da automatização de tarefas, processamento de dados mais amplos e profundos, e análises mais sofisticadas. Por outro lado, os sistemas de IA também podem ser considerados mais vulneráveis, uma vez que podem ocorrer enviesamentos de dados, exposição e roubo de informações, além de ataques à integridade. Neste sentido, a proteção dos dados de aprendizagem do sistema de IA deve ser prioridade (U.S. Department of the Treasury, 2024).

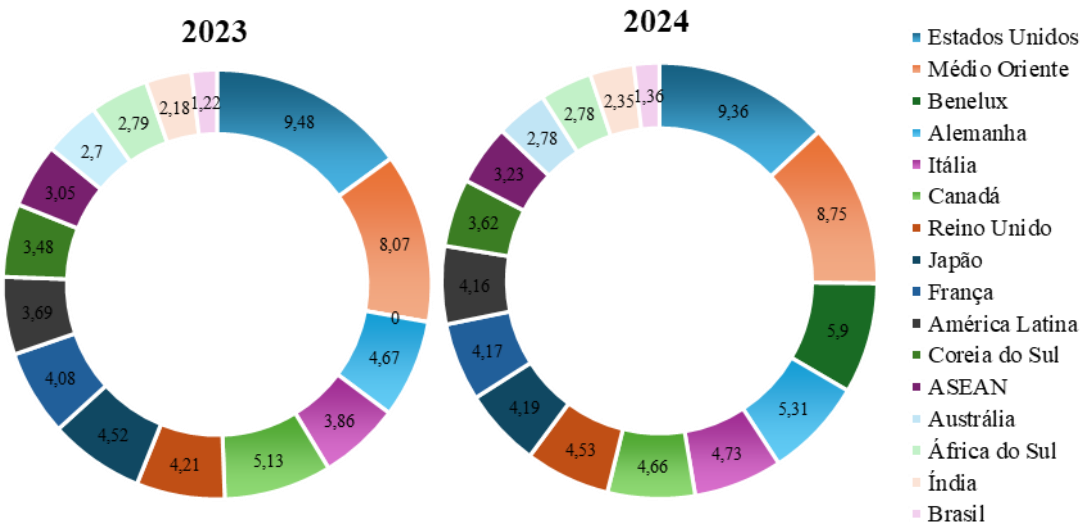
Os recursos avançados de IA estão cada vez mais disponíveis, o que torna as instituições financeiras mais vulneráveis para sofrer ataques que utilizem a IA (U.S. Department of the Treasury, 2024). Assim, teremos ataques baseados em IA e sistemas de defesa baseados em IA. Os entrevistados revelam já terem sofrido com ataques suportados com IA, mas que na sua grande maioria ainda são ataques tradicionais. Um dos ataques

comuns que utilizam IA são a falsificação de identidade sofisticada, onde o sistema se faz passar pelas pessoas, imitando a sua voz, bem como a criação de vídeos das pessoas. Um caso identificado no relatório, é a utilização de voz de um CEO para pedir a uma empresa subsidiária o pagamento avultado de um fornecedor. A primeira tentativa levou a uma perda de quase 250 000 dólares, mas as seguintes já não foram bem-sucedidas. Os entrevistados pelo Departamento do Tesouro revelam que estão a analisar como os sistemas suportados por IA melhoram a segurança cibernética, de modo a otimizar os fluxos, auxiliar os profissionais e identificar as tendências e padrões das ameaças, para conseguirem defender-se. Com este pensamento, percebem que a utilização da autenticação multifatorial melhora a segurança da empresa e protege-os contra fraudes (U.S. Department of the Treasury, 2024).

3.1.9 Relatório da IBM de 2024

A IBM elabora anualmente um relatório sobre os custos associados a violação de dados. O relatório baseia-se na análise de 604 organizações entre março de 2023 e fevereiro de 2024, abrangendo 16 países e grupos, tendo sido entrevistados 3 556 líderes empresariais de segurança e executivos, com conhecimento sobre os incidentes nas empresas (IBM, 2024). No seu estudo, indica o custo de violação de dados em milhões de dólares, entre países e regiões em 2023 e 2024. Pelo gráfico seguinte, conseguimos verificar que os Estados Unidos são quem apresentam um custo mais elevado, seguido pelo Médio Oriente e a Benelux, que representa a Bélgica, os Países Baixos e o Luxemburgo. De 2023 para 2024 é possível verificar um aumento significativo de custos na Itália, Médio Oriente e Alemanha. Pelo contrário, verificamos uma redução de custos significativa no Canadá e no Japão.

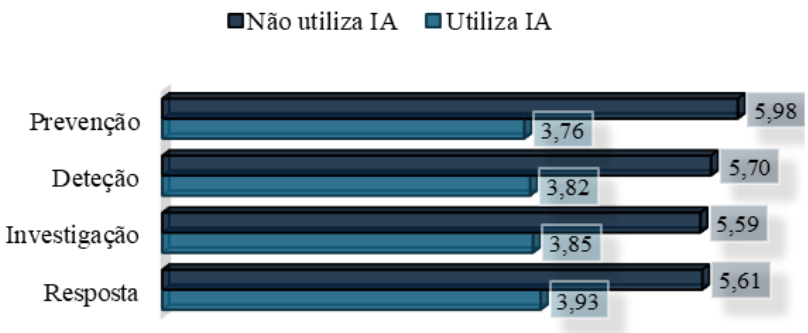
Gráfico 2 – Custo com Violação de Dados por Países e Grupos



Fonte: IBM (2024)

De acordo com IBM (2024), o número de empresas que utilizam IA de segurança cresceu em 31%, compratívamente com o ano anterior. Na sua perspetiva, os custos provocados pelo cibercrime e a utilização de IA, são duas variáveis correlacionadas. Ou seja, quanto mais as empresas utilizarem a IA na segurança cibernética, menores serão os custos associados aos ataques. Por outro lado, quanto menor partido tirarem das vantagens ofercidas pela IA, maiores serão os custos a enfrentrar. Segundo o seu estudo, as empresas conseguem uma redução significativa nos custos nas quatro áreas de segurança: prevenção, deteção, investigação e resposta. Essa dedução é evidenciada na gráfico seguinte, que apresenta os valores quantificados em milhões de dólares.

Gráfico 3 – Custo nos Ataques em Dados Com e Sem IA



Fonte: IBM (2024)

Relativamente aos problemas após os ataques, mais de 50% dos entrevistados revelam que os preços dos bens e serviços aumentam. Este aumento de preços é uma medida comum para lidar com as despesas elevadas resultantes dos ciberataques. Relativamente ao tempo que demoram a recuperar totalmente após o ataque, cerca de 35% demora mais de 150 dias, 24% entre 126 a 150 dias, 19% entre 101 a 125 dias, 14% entre 76 a 100 dias, 5% entre 51 a 75 dias e, apenas 3%, diz ter recuperado em menos de 50 dias (IBM, 2024).

3.2 Relatórios de Criptomoedas e Segurança Cibernética com o Apoio de IA

A presente secção evidencia os relatórios selecionados, elaborados entre 2017 e 2024, sobre as criptomoedas e a segurança cibernética com o apoio da IA.

3.2.1 Relatório da Deloitte de 2017

Relativamente às criptomoedas e a cibersegurança a Deloitte (2017) criou um relatório sobre o *blockchain* e a cibersegurança, na qual avalia a segurança da tecnologia *blockchain*, considerando diferentes perspetivas, incluindo sistema e dados, confidencialidade e integridade, nível de maturidade, autenticação, autorização e auditoria. Segundo o líder de risco cibernético da Deloitte nos Estados Unidos da América, ao ser questionado sobre a tecnologia *blockchain* ser considerada um obstáculo ou uma ajuda à cibersegurança, afirmou existir uma inovação promissora nesta tecnologia que ajudará as empresas a enfrentar os desafios dos riscos cibernéticos. A *blockchain* poderá prevenir ataques fraudulentos e detetar alterações de dados, tendo por base as suas características de transparência, auditabilidade e encriptação (Deloitte, 2017).

Se um indivíduo tentar atacar uma rede *blockchain*, existe uma forte possibilidade de conseguir aceder aos dados. De modo a reforçar as defesas para este problema, deverão existir controlos de acesso, fornecendo uma encriptação completa de dados em blocos. A encriptação garantirá que os dados apenas estarão acessíveis para as partes autorizadas. Assim, apesar de conseguirem aceder aos dados, os atacantes não conseguirão ler ou interpretá-los, protegendo, deste modo, a integridade e a privacidade da informação (Deloitte, 2017).

A tecnologia de *blockchain* também poderá fornecer controlos de segurança através de *public key infrastructure* (PKI), beneficiando processos de autenticação e autorização entre as partes envolvidas, e na encriptação das suas comunicações (Deloitte, 2017). A PKI contém um conjunto de funções, políticas, hardware, software e procedimentos com a finalidade de criar, gerir, utilizar, armazenar e revogar certificados digitais. Esta infraestrutura tem como objetivo facilitar as transferências eletrónicas em diversas atividades de rede com segurança. A combinação da encriptação com a PKI proporcionará às organizações um nível elevado de segurança (Deloitte, 2017).

Garantir a integridade durante todos os processos do sistema é crucial. Métodos como encriptação dos dados, comparação do *hash* e assinatura digital são essenciais para essa proteção. A impossibilidade de alterações e o rastreamento da *blockchain* beneficiam as organizações ao permitir a garantia da integridade (Deloitte, 2017). No entanto, incidentes anteriores, como o ataque à rede Bitcoin em 2014 devido a um *bug* nas transações pendentes, demonstram que a segurança de hoje pode não ser garantida amanhã. À medida que os cibercriminosos adquirem mais recursos e competências para entrar nos sistemas, é crucial que as organizações que utilizam *blockchain* na sua infraestrutura, implementem controlos rigorosos e sigam padrões de cibersegurança atualizados. Os profissionais cibernéticos da Deloitte sugerem uma abordagem cibernética segura, vigilante e resiliente para proteger a infraestrutura de *blockchain*. Segura na medida em que priorizam os riscos para se defender contra as ameaças. Vigilantes para conseguirem identificar com prontidão e rapidez os comportamentos que devem ser considerados prejudiciais. Resilientes para minimizar os impactos dos ataques e conseguir recuperar de forma célere (Deloitte, 2017).

3.2.2 Relatório do CNCS de 2024

Segundo CNCS (2024) as expetativas sobre o aumento de valor das criptomoedas impacta diretamente as atividades criminosas, criando uma correlação entre o aumento do valor das criptomoedas e o crescimento do cibercrime. Em 2023, com o crescimento do valor das criptomoedas, observou-se uma nova fase de atividade criminosa, prevendo-se que a tendência se mantenha em 2024. Essa correlação, será um forte potencializador para os aumentos do cibercrime, caminhando o cibercrime e a valorização de valor paralelamente, nas subidas e nas descidas.

3.2.3 Relatório da Chainalysis de 2024

O estudo da Chainalysis (2024) assenta as suas estatísticas em atividades de trasações ilícitas, na qual são considerados fundos enviados para endereços identificados como ilícitos e fundos roubados em *hacks* de criptografia. O branqueamento de capitais nas criptomoedas corresponde à transferência de fundos para serviços que, permitem a conversão em dinheiro e ocultam a origem dos fundos. Em 2024, os endereços ilícitos

enviaram cerca de 22,2 mil milhões de dólares em criptomoedas para serviços. Além disso, evidencia que o *hacking* de criptomoedas constitui uma ameaça generalizada, tendo provocado o roubo de milhares de milhões de dólares na criptografia e na exposição de vulnerabilidades (Chainalysis, 2024).

3.2.4 Relatório da Arkose Labs de 2024

Os problemas mais comuns com a segurança das criptomoedas são identificados por (Arkose Labs, 2024). Entre eles, destacam-se o *phishing* através de sites falsos e recebimento de *emails* de criptomoedas ilegítimas, a utilização de carteiras falsas para roubar fundos e/ou informações confidenciais dos utilizadores e, esquemas de Pump and Dump, onde os criminosos inflacionam o preço de uma criptomoeda com informações falsas. Adicionalmente, há os esquemas Ponzi, em que os cibercriminosos prometem retornos elevados e dependem dos fundos de novos investidores para pagar aos investidores antigos. Além dos problemas, Arkose Labs (2024) identifica as medidas para melhorar a segurança das criptomoedas. Inicia pela avaliação do risco de modo a identificar vulnerabilidades e ameaças no negócio. Proteção de chave privada, as chaves permitem aceder e controlar os ativos digitais e devem ser protegidas por criptografia e armazenamento seguro. Segurança da carteira e autenticação de dois fatores, a utilização de senhas fortes e adição de uma camada extra na proteção é fundamental para proteger as contas. Transações com segurança através da verificação dos endereços de carteira e assinatura. Proteção de rede pela utilização de algorítmos encriptados e monitorização recorrente. Outras práticas recomendadas incluem a criptografia de dados, controlo nos acessos dos utilizadores, formação aos utilizadores e planos de respostas a incidentes (Arkose Labs, 2024).

3.2.5 Relatório da ESET de 2024

No relatório da ESET (2024), foi evidenciado uma descoberta sobre uma família de *malware* que rouba dados de reconhecimento facial. Estes dados têm como propósito a criação de vídeos falsos através da utilização de IA. O *malware*, denominado GoldPickaxe, afeta dispositivos Android e de iPhone Operating System (iOS),

especialmente os de pessoas que possuem carteiras de criptomoedas e clientes de serviços financeiros.

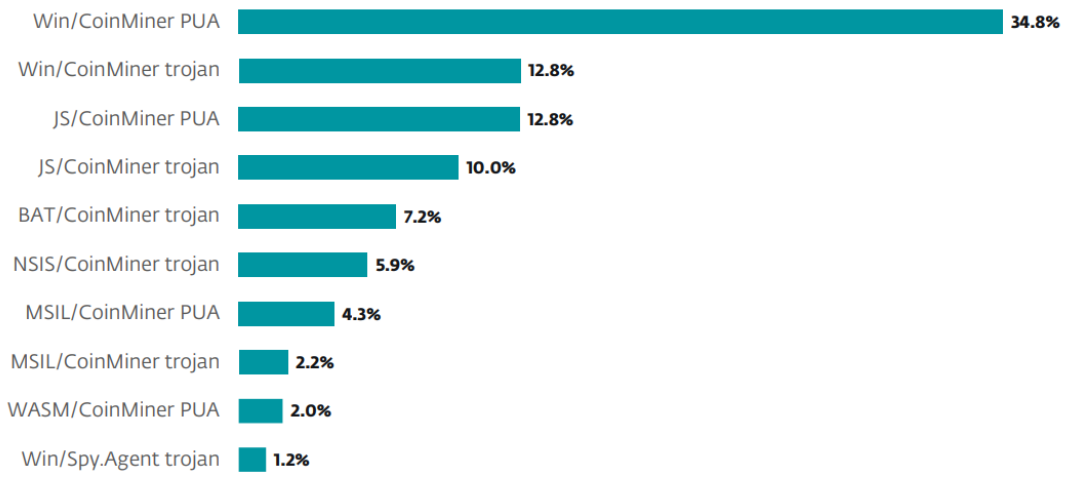
O processo de autenticação digital está sustentado, principalmente, pelos dados de reconhecimento facial e, foi criado com o objetivo de criar uma segurança extra e evitar fraudes (ESET, 2024). Contudo, o *malware* tira partido deste processo para roubar os dados. Este crime está a ser distribuido por sistemas que se fazem passar pela loja do Google Play. Em relação ao iOS, o *malware* foi colocado numa aplicação de testes que foi posteriormente removida da plataforma. Para combater esta remoção, os cibercriminosos utilizam atualmente um esquema de engenharia social, persuadindo as vítimas a instalar uma gestão de dispositivos que proporcionará aos cibercriminosos um acesso total sobre o dispositivo.

O GROUP-IB é uma empresa criadora de tecnologias de segurança cibernética para investigar, prevenir e combater crimes digitais. Segundo ESET (2024), o GROUP-IB acredita que esta ameaça é de um Grupo denominado GoldFactory. O GoldFactory é um grupo de crime organizado de língua chinesa, que se acredita conter também o GoldDigger e o GoldDiggerPlus. O GoldDigger atua apenas em Androids, e visa a extração de informações pessoais, o roubo de credenciais bancárias, a interceção de short message service (sms), entre outros problemas. O GoldDiggerPlus tem uma funcionalidade que permite aos criminosos fazer chamadas com as vítimas. Se a vítima atender a chamada dentro da aplicação maliciosa, o *malwa*re liga-se a um membro dos criminosos e cria a ilusão de que a chamada é de um centro de atendimento legítimo. O GoldDiggerPlus tem como alvo principal o Sudeste Asiático, mas já foi detetado na América Latina e na África do Sul. Este *malwa*re está presente em aplicações de bancos e apresenta uma falha que, aquando da colocação errada de credenciais, o sistema reproduz um erro em chinês (ESET, 2024).

A utilização indevida dos serviços dos Android permite aos criminosos aceder e registar eventos nos dispositivos das vítimas. Segundo o relatório da ESET, a Turquia foi o país que mais sofreu com ataques a Androids. As regiões selecionadas para os ataques são escolhidas prepositadamente, dado que se tratam de regiões em que grande parte da população não tem acesso a computadores, e por isso, utilizam o telemóvel pessoal para aceder aos bancos, aumentando o cibercrime nesta vertente (ESET, 2024).

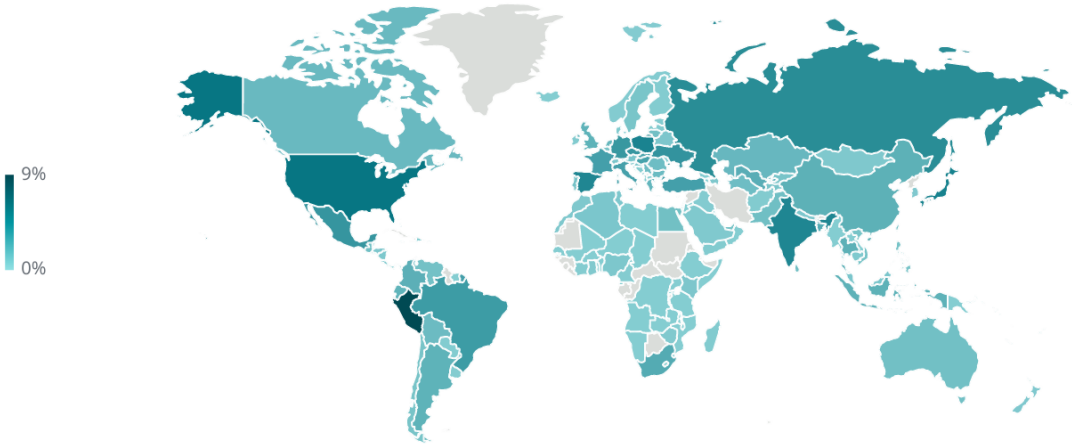
Os servidores Linus e Unix estão comprometidos pela família de *malwa*re Ebury (ESET, 2024). O Ebury rouba credenciais e é utilizado para redirecionamento da web. Atualmente, também rouba detalhes financeiros de sites transacionais, que têm como foco principal o roubo de dinheiro, atacando particularmente a criptomoeda e o roubo de cartões de crédito. No que diz respeito às criptomoedas, os operadores identificam os servidores valiosos, redirecionam o tráfego da rede para um sistema que tenham controlado, capturam as credenciais e executam *sripts* para extrair os dados da carteira de criptomoedas.

Figura 1 – As 10 Principais Deteções de Ameaças em Criptomoedas (1ºSemestre – 2024)



Fonte: (ESET, 2024)

Figura 2 – Distribuição Geográfica das Deteções de Ameaças em Criptomoedas (1ºSemestre – 2024)



Fonte: (ESET, 2024)

3.2.6 Relatório da Europol de 2024

Segundo o relatório da Europol (2024), denominado a "Avaliação da Ameaça do Crime Organizado na *Internet*", o número de ataques a criptomoedas aumentou significativamente em 2023, nomeadamente, em fraudes de investimentos e no branqueamento de capitais. Além disso, o aumento do valor das criptomoedas, aliado ao crescimento dos investimentos em criptomoedas anunciados pelos meios de comunicação, tem contribuído para o aumento das fraudes. Os criminosos de *ransomware*, nos seus resgates, exigem principalmente Bitcoin, e o uso criminoso de *altcoins* (qualquer criptomoeda que não seja Bitcoin) também está a aumentar. Similarmente, o branqueamento de criptoativos encontra-se em crescimento, através da utilização de soluções bancárias clandestinas e de canais criminosos. Atualmente, há um retorno da utilização dos cartões de débito com criptomoedas devido à facilidade de as converter em dinheiro nas caixas automáticas. Em 2023 foi registado um aumento de swaps para lavagem de criptomoedas (Europol, 2024).

Exploit, *XSS* e *BreachForums* foram os fóruns de cibercrime mais ativos em 2023 (Europol, 2024). No *Exploit*, eram partilhados conhecimentos de *hackers*, dados roubados, ferramentas e serviços de cibercrime, sendo predominantemente em língua russa e apresentando uma taxa de inscrição ou reputação verificada. O *XSS* oferece características de segurança que garantem o anonimato, enquanto o *BrachForums* é um fórum em inglês voltado para o mercado de cibercriminosos a nível global. O *BreachForums* facilitava o comércio de base de dados divulgadas, cartões bancários roubados e dados de empresas, mas foi encerrado em maio de 2023. Em agosto, outro grupo de *hackers* ressurgiu com o fórum, que foi novamente derrubado em maio de 2024 numa operação internacional. O *CryptBB* e o *Dread* são outros fóruns conhecidos, com maior atividade em 2023. *CryptBB* é um fórum fechado para cibercriminosos e programadores, reunindo tanto principiantes como especialistas. O *Dread*, criado em 2018, é um fórum que contém diversos conteúdos e que sofreu um ataque *de distributed denial-of-service* (DDoS), isto é, um ataque distribuído de negação de serviço, na qual um invasor sobrecarrega um website ou servidor com tráfego malicioso, que provocou o seu fecho em novembro de 2022. Contudo, voltou a estar ativo, em fevereiro de 2023, apresentando um serviço protegido para futuros ataques em DDoS. Existem diversos fóruns, sendo alguns gratuitos e outros pagos, que apresentam diversas informações roubadas, passagem de conhecimento entre os *hackers* e diversos crimes (Europol, 2024).

3.3 Análise dos Relatórios

Primeiramente, iniciou-se pela exposição dos relatórios referentes ao nosso país. Relativamente aos dados, é possível destacar que se trata de um problema que se começou a expandir recentemente, ainda não existindo uma preocupação generalizada entre as empresas. O *boom* dos ataques sucedeu-se em 2020, alavancado pela pandemia que proporcionou diversas alterações a nível laboral, proporcionando um aumento de vulnerabilidades aos indivíduos e, consequentemente, às empresas. As empresas que não consideravam a cibersegurança um tema na sua política de negócio, tiveram de repensar a sua estratégia, enquanto as empresas que já investiam na cibersegurança, reforçaram os seus investimentos e começaram a adotar novas medidas. No entanto, pelo inquérito da PwC, em 2021, verificamos que apenas 15% das empresas inquiridas se preocupa com os dados reputacionais após os ataques e, apenas 13% teme perdas financeiras. Com base nestes dados, num total de 56 empresas, apenas 8 se preocupam com os problemas e o esforço necessário com a cibersegurança. Pelo relatório do CNCS em 2023, podemos destacar um aumento sobre a pesquisa da cibersegurança em 2022 face aos resultados de 2021. Os media expõem cada vez mais este tema nos seus artigos, o que tem impulsionado diversas empresas a atualizar as suas políticas de segurança e, a contemplar este tema nas suas formações e eventos. Como resposta a estas exposições, as empresas têm adotado novas práticas, como o fortalecimento das palavras-passe, a implementação de autenticação multifatorial, repensam o orçamento disponível em cibersegurança, priorizam iniciativas de segurança, constroem equipas mais preparadas na prevenção, deteção, resposta e recuperação. Tendo em conta estas alterações em 2022, é possível afirmar que as empresas portuguesas começam a estar mais cientes dos problemas que estão a ocorrer nas redes e a sua preocupação com a defesa e a aprendizagem sobre este tema começa a crescer. O relatório de riscos e conflitos sublinha esta realidade ao mostrar o crescimento dos incidentes reportados. Enquanto até 2019 não chegavam aos 1000 casos, em apenas três anos, em 2023, já se registavam 2025 incidentes. A fonte principal deste problema ocorre devido aos problemas de *phishing*. Todas as pessoas já receberam ou conhecem alguém que recebeu mensagens a indicar ser um familiar que mudou o número de telemóvel e está a pedir dinheiro, ou casos em que recebemos chamadas falsas que roubam a identificação de empresas prestadores de serviços. Cada vez mais as pessoas estão cientes destes problemas e, no entanto, quando o caso se aplica a si, muitas vezes não acreditam que estão a ser burladas e cometem o erro de seguir os passos que os

criminosos indicam. Além disso, as burlas online também ganharam proporções elevadas, devendo os indivíduos desconfiar quando os preços são demasiado apelativos e utilizar as carteiras virtuais.

A nível mundial foram expostos vários relatórios de modo a ser possível verificar as respostas dos entrevistados, executivos e líderes no departamento de segurança de diversas organizações de setores diferentes e espalhadas pelo mundo. Os relatórios foram selecionados de modo a verificar a importância da cibersegurança, os crimes que correm e o apoio da IA para a ciberdefesa.

Pelos inquiridos conseguimos afirmar que a maioria das organizações em causa já sofreram pelo menos um incidente. Todos os incidentes causam consequências, nomeadamente, interrupções no negócio, perdas financeiras, perdas de confiança por parte dos seus clientes, fornecedores e parceiros, perda de reputação, dificuldade na retenção de talentos para combater os problemas, quedas nas ações e multas, aumento dos preços para combater a perda financeira.

De modo a combater estes problemas, e para evitar estes casos no futuro, os inquiridos definem as estratégias necessárias, nomeadamente, análise e atualização do plano de segurança, formação e contratação de experientes nos programas cibernéticos, quantificação do risco, avaliação do retorno no investimento em cibersegurança e validação das respostas aos incidentes. No que diz respeito à proteção contra os ataques, é destacada a utilização da autenticação por multifator, a validação dos acessos aos colaboradores e a limitação dos mesmos, tendo em conta as necessidades laborais, a utilização de softwares de deteção, bloqueios na eventualidade de ameaças, atualizações dos sistemas, conhecimento sobre os dados e aplicação de defesas eficazes.

Tendo em conta o estado atual e os problemas que as empresas enfrentam, os inquiridos afirmam que o investimento em cibersegurança faz aumentar o valor do seu negócio, bem como, a sua eficiência. Em prol desta afirmação, a maioria dos entrevistados reforça que a cibersegurança faz parte da sua agenda e pretendem continuar a aumentar os investimentos nesta área. Além disso, a aposta em IA apoiará a ciberdefesa. Os LLM facilitam a tomada de decisão dos executivos, pela sua sugestão e rapidez nas respostas e, pelas suas ações que permitem a minimização dos impactos. Os LLM recolhem e analisam um avultado conjunto de dados que por sua vez fornecerão padrões e tendências que serão analisados pelas máquinas e pelos analistas cibernéticos. Esta leitura facilita

uma grande parte do trabalho dos analistas, permitindo que se foquem no tratamento das ameaças e nas proteções contra os ataques.

A IA apresenta diversos benefícios, como o trabalho 24 horas por dia, respostas rápidas, automatização de processos, redução dos impactos, capacidade de processamento e de resumos, sinalização de futuras ameaças e a redução de custos. Relativamente a esses custos, um dos relatórios identifica uma correlação entre os custos e a IA. Quanto maior o investimento em IA, menores serão os custos de impacto, e vice-versa.

Contudo, a IA também contém as suas dificuldades, como a identificação de falsos positivos, bases de informação reduzidas, enviesamento de dados e roubo de dados. Além disso, assim como as empresas obtêm os proveitos da IA, os cibercriminosos também o fazem. Nesse sentido, os ataques com IA serão consecutivamente mais fortes, eficazes e com uma maior percentagem de sucesso. Alguns inquiridos reportaram que sofreram ataques com IA, sendo o caso mais comum, o das falsas identidades, onde são efetuadas chamadas telefónicas ou videochamadas por IA. Tendo por base este pressuposto, as empresas que não investirem em IA e forem atacadas por cibercriminosos que utilizem esta tecnologia, terão dificuldades acrescida na defesa, e podem demorar mais tempo a recuperar do ataque. Quanto mais tempo demorarem a recuperar, mais custos terão.

Relativamente às criptomoedas, o seu aumento de valor está a potencializar o aumento das atividades criminosas. A transferência de dinheiro sem registos e a preservação das entidades dos compradores e dos vendedores, permite o aumento dos ataques. No caso de ataques a *blockchain*, os dados devem estar encriptados, desta forma, os indivíduos que tentarem atacar a rede conseguem aceder aos dados, no entanto, não os conseguirão ler ou interpretar. Além disto, também devem estar salvaguardados com outras formas de segurança, nomeadamente, a proteção de chaves privadas, comparação do *hash* e da assinatura digital, autentificação de dois fatores, chaves de segurança fortes, encriptações, proteção da rede, monitorização recorrente e ter um plano de ação para responder aos incidentes.

Os ataques mais comuns a criptomoedas incluem o *phishing*, que é frequentemente realizado através de sites falsos ou envio de *emails* de criptomoedas ilegítimas. Além disso, os ataques de *malware* estão a causar o roubo de identificações facial das vítimas, com o intuito de criar vídeos utilizando a IA. Outros tipos de ataques identificados, incluem o roubo de credenciais bancárias, a interceção de sms, o furto de informações

pessoais, e chamadas fraudulentas aos clientes. A nível geográfico, foi possível observar que no primeiro semestre de 2024, praticamente todos os países detetaram ameaças relacionadas com criptomoedas.

É importante destacar que os criminosos exigem principalmente Bitcoin, e que tem havido um aumento no branqueamento de criptoativos, na utilização de cartões de débito com criptomoedas e nas operações de swap para lavagem de criptomoedas. Diversos fóruns estão presentes na *Dark Web*, funcionando como uma fonte de partilha de conhecimentos entre *hackers*, permitindo a identificação de dados e sistemas roubados, assim como a identificação das entidades atacadas, entre outros. Os fóruns contam com a inscrição de principiantes e especialistas, podendo exigir inscrições ou pagamentos. Além disso, o trabalho realizado pelas intervenções internacionais na luta contra o desmantelamento tem sido significativo, embora muitos desses fóruns se conseguiam reerguer. Considerando a vasta quantidade de fóruns existentes e a constante criação de novos, será desafiador combater este problema.

Em seguimento do objetivo principal do estudo, focado em "compreender a cibersegurança na atualidade e em que medida a IA beneficiará a cibersegurança" e através da metodologia qualitativa aplicada, comprova-se que a cibersegurança é um tema crucial para as entidades atualmente e que, o investimento em IA será uma mais-valia para as entidades. Dado o aumento do número de incidentes de cibercrime, as entidades começaram a reconhecer a necessidade de redirecionamento necessário a efetuar em prol da segurança. O desconhecimento sobre o tema, aliado à falta de investimento, começou a moldar-se desde 2020, tornando-se um foco nas agendas das empresas. A incapacidade de implementar a cibersegurança sem o apoio de diversas tecnologias existentes para combater os problemas, promoveu a procura de novas soluções. Neste contexto, o forte crescimento da IA beneficiará as entidades nos seus processos, especialmente no âmbito da capacidade de leitura de dados, a facilidade e rapidez na deteção de ameaças, na identificação de padrões e tendências, na possibilidade de automatismos de respostas e na redução do tempo de recuperação. Por outro lado, as empresas devem analisar se o custo com o investimento em IA será vantajoso para os seus processos e quais ações devem optar por privilegiar, tendo em conta a necessidade de restringir a IA, devido aos elevados custos que acarreta.

No que diz respeito ao restantes objetivos com o estudo, verificou-se que a cibersegurança já integra os planos estratégicos das empresas e é considerada fundamental para as entidades. Cada vez mais, é essencial implementar medidas em prol da segurança em todos os países e setores de atividade. Relativamente às consequências, estamos perante um caso acrescido de perdas, nomeadamente, ao nível financeiro, de confiança entre clientes, parceiros e fornecedores, danos à imagem, interrupção do negócio e queda de ações. Dependendo da reação das empresas aos ataques de que estão a ser alvo, os custos poderão ser mais elevados ou mais reduzidos. As práticas que os países estão a utilizar para se proteger incluem a autenticação por multifator, modificações de reforço nas palavras-passes, validação dos acessos aos colaboradores, redução dos recursos e limitação dos acessos, atualizações ao sistema, investimentos em novos sistemas de proteção, formação sobre o tema e apoio da IA para criar defesas mais eficazes.

No que se refere ao mercado das criptomoedas, o aumento do seu valor e do conhecimento por mais indivíduos do seu potencial, está a proporcionar um número crescente de ocorrências de cibercrimes. Este mercado tornou-se altamente atrativo para os criminosos cibernéticos, que, com o apoio das novas tecnologias, estão a produzir mais ataques com

uma elevada taxa de sucesso. Além disso, o anonimato dos compradores e vendedores cria vulnerabilidades adicionais e incentiva novos ataques. A cibersegurança atua fortemente neste mercado, havendo diversas empresas focadas no apoio à proteção, com várias soluções que, no entanto, carecem de investimentos avultados. As entidades de intervenção atuam no desmantelamento de fóruns de rede de *hackers* e procuram pelos superiores que criam estas organizações criminosas, contudo, com a crescente fonte desta rede criminosa, será praticamente impossível erradicar o problema por completo. As soluções para as empresas e indivíduos que operam com criptomoedas assentam na procura e seleção de empresas externas no apoio à sua segurança, na alteração dos procedimentos que utilizam, na adoção de uma postura vigilante relativamente a *emails*, sms, links e aplicações que utilizam, bem como a partilha de informações.

Tendo em conta as questões que o estudo pretendia responder, é possível afirmar que a cibersegurança está fortemente presente na atualidade e que se prevê o seu crescimento com o decorrer dos próximos anos. Atualmente, a cibersegurança é uma preocupação generalizada a nível mundial, e a IA consegue mitigar alguns dos problemas emergentes, apoiando fortemente os processos e reduzindo diversos ataques, devido à deteção de várias ameaças. No entanto, a IA não erradica totalmente os problemas dos ataques, embora seja fundamental no seu combate, sobretudo porque os ataques também se apoiam, cada vez mais, nas tecnologias da IA, tornando-se mais eficazes.

O tema em estudo apresenta diversas limitações, dado que aborda problemas atuais e com um historial reduzido. Muitas organizações ainda se encontram em fase de adaptação a estes temas e a aprender como devem proceder para proteger as suas empresas. Além disso, as contantes atualizações e modificações nos sistemas provocam desconhecimentos e exigem a realização de testes em ambientes de desenvolvimento, que não garantem apresentar o mesmo comportamento ou a exequibilidade no ambiente de produção. Fundamentalmente, a IA apresenta a limitação do elevado investimento necessário, bem como a elevada necessidade de informação em base de dados para evitar o enviesamento dos resultados. Sendo uma área recente, as empresas estão a aprender também com os seus erros e devem proteger os seus dados desde a fase inicial, uma vez que será nesta fase que a IA iniciará a sua análise. Caso os dados sejam comprometidos ou roubados pelos cibercriminosos, as conclusões obtidas serão enviesadas.

No que concerne a sugestões futuras, deve haver maior cooperação entre empresas de serviços, para melhorar o combate aos crimes, sendo que as atualizações e melhorias

devem ser compartilhadas. As ameaças identificadas devem ser divulgadas para enriquecer as fontes de dados dos sistemas, e as empresas devem continuar a investir nas tecnologias que carecem de diversas modificações para assegurar uma melhoria contínua. Ao nível dos estudos, é essencial avaliar com mais detalhe as tecnologias existentes e de que forma contribuem para cada área e setor de atividade. Além disso, é importante aprofundar o conhecimento sobre as empresas externas que auxiliam no combate a estes problemas e, comparar as soluções oferecidas por cada entidade. Seria útil realizar análises sobre as práticas adotadas por cada país, tendo em conta o número de crimes, de modo a avaliar quais os procedimentos mais eficientes e as táticas aplicadas.

O futuro será promissor nesta área, com as tecnologias cada vez mais presentes, o que trará consigo diversas vantagens, mas também problemas que devem ser analisados e corrigidos para evitar que se repitam. Não se devem negligenciar as vulnerabilidades existentes e o foco deverá ser combater essas vulnerabilidades para melhorar o negócio das empresas e garantir a sua segurança.

Abbas, R., Michael, K., Pitt, J., Vogel, K., & Zafeirakopoulos, M. (2023). *Artificial Intelligence (AI) in Cybersecurity: A Socio-Technical Research Roadmap*. The Alan Turing Institute. https://www.turing.ac.uk/news/publications/artificial-intelligence-ai-cybersecurity-socio-technical-research-roadmap

Adi, E., Baig, Z., & Zeadally, S. (2022). Artificial Intelligence for Cybersecurity: Offensive Tactics, Mitigation Techniques and Future Directions. *ACIG*, 1–23.

Arcuri, M. C., Brogi, M., & Gandolfi, G. (2018). The effect of cyber-attacks on stock returns. *Corporate Ownership and Control*, *15*(2), 70–83. https://doi.org/10.22495/cocv15i2art6

Arkose Labs. (2024). *Guide to Cryptocurrency Security*. Arkose Labs. https://www.arkoselabs.com/explained/guide-to-cryptocurrency-security/

Bagó, P. (2023). Cyber security and artificial intelligence. *Economy & finance*, *10*(2), 189–212. https://doi.org/10.33908/EF.2023.2.5

Barão, B. A. D. (2022). *Análise da relação entre criptomoedas e a incerteza da política económica* [masterThesis, Instituto Superior de Economia e Gestão]. https://www.repository.utl.pt/handle/10400.5/25238

Capgemini Research Institute. (2019). *Reinventing cybersecurity with artificial intelligence* (p. 28). https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf

Caporale, G. M., Kang, W.-Y., Spagnolo, F., & Spagnolo, N. (2020). *Cyber-Attacks and Cryptocurrencies* (Working Paper 8124). CESifo Working Paper. https://www.econstor.eu/handle/10419/216520

Chainalysis. (2024). *The 2024 Crypto Crime Report* (p. 114). https://go.chainalysis.com/crypto-crime-2024.html

Chakraborty, A., Biswas, A., & Khan, A. K. (2022). *Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation*. arXiv.Org. https://arxiv.org/abs/2209.13454v1

Chhatwani, M., & Parija, A. K. (2023). Who invests in cryptocurrency? The role of overconfidence among American investors. *Journal of Behavioral and Experimental Economics*, *107*, 102107. https://doi.org/10.1016/j.socec.2023.102107

Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., & Shah, M. (2024). A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking System. *Annals of Data Science, 11*(1), 103–135. https://doi.org/10.1007/s40745-022-00433-5

CNCS. (2023). *Relatório Sociedade 2023* (p. 79). https://www.cncs.gov.pt/docs/rel-sociedade2023-observ-cncs-dig.pdf

CNCS. (2024). *Relatório de Cibersegurança em Portugal 2024: Riscos e Conflitos* (p. 109). https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obcibercncs.pdf

Creswell, J. W. (2010). *Projeto De Pesquisa Métodos Qualitativo, Quantitativo Misto* (3ª). artmed. https://www.academia.edu/95271542/_Livro_Creswell_John_W_Projeto_de_Pesquisa_M%C3%89todos_Qualitativo_Quantitativo_Misto_2010_

Das, R., & Sandhane, R. (2021). Artificial Intelligence in Cyber Security. *Journal of Physics: Conference Series*, *1964*(4), 042072. https://doi.org/10.1088/1742-6596/1964/4/042072

Deloitte. (2017). *Blockchain and Cybersecurity* (p. 16). https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/Blockchain-and-Cyber.pdf

Deloitte. (2023). *Global Future of Cyber Survey 2023* (p. 28). https://www.deloitte.com/global/en/services/risk-advisory/content/future-of-cyber.html

ESET. (2024). *Threat Report H1 2024* (p. 39). https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-threat-report-h12024.pdf

Europol. (2024). *Internet Organised Crime Threat Assessment*. Publications Office of the European Union. https://data.europa.eu/doi/10.2813/442713

Grant Thornton. (2021). *The Economic Cost of Cybercrime* (p. 40). https://www.grantthornton.ie/insights/publications/cost-of-cyber/

IBM. (2023). *Five common data security pitfalls to avoid*. https://dach.tdsynnex.com/blog/ch/wp-content/uploads/sites/4/2024/08/five_common_pitfalls2_en_BP.pdf

IBM. (2024). *Cost of a data breach Report 2024* (p. 46). https://www.ibm.com/reports/data-breach

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Lapuh Bele, J. (2021). Cryptocurrencies as facilitators of cybercrime. *SHS Web of Conferences*, *111*, 01005. https://doi.org/10.1051/shsconf/202111101005

McKinsey. (2023). *The state of AI in 2023: Generative AI's breakout year | McKinsey* (p. 24). https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year#/download/%2F~%2Fmedia%2Fmckinsey%2Fbusiness%20functions%2Fquantumblack%2Four%20insights%2Fthe%20state%20of%20ai%20in%202023

%20generative%20ais%20breakout%20year%2Fthe-state-of-ai-in-2023-generative-ais-breakout-year-v3.pdf%3FshouldIndex%3Dfalse

Microsoft. (2023). *Microsoft Digital Defense Report: Building and improving cyber resilience* (p. 131). https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

Morovat, K., & Panda, B. (2020). A Survey of Artificial Intelligence in Cybersecurity. *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*, 109–115. https://doi.org/10.1109/CSCI51800.2020.00026

Narciso, M. de G. (2020). *Cryptocurrency Analysis based on User-Generated Social Media Content* [Instituto Universitário Lisboa]. http://hdl.handle.net/10071/22088

Nogueira, A. F. P. (2020). *O impacto da criptomoeda nas empresas de software em Portugal* [masterThesis, Faculdade Economia do Porto]. https://repositorio-aberto.up.pt/handle/10216/130406

Pernice, I. G. A., & Scott, B. (2021). Cryptocurrency. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1561

Pupillo, L., Fantin, S., Ferreira, A., & Polito, C. (2021). *Artificial Intelligence and Cybersecurity: Technology, Governance and Policy Challenges : Final Report of a CEPS Task Force*. Centre for European Policy Studies.

PwC. (2021). *Cyber Survey Portugal 2021: Compreender a cibersegurança num novo panorama social*. 26.

Rafi, M. F., Salma, R., & Kurniawan, A. E. (2017). *The Benefits and The Disadvantages of The Artificial Intelligence*. 14.

Sabry, F., Labda, W., Erbad, A., & Malluhi, Q. (2020). Cryptocurrencies and Artificial Intelligence: Challenges and Opportunities. *IEEE Access*, *8*, 175840–175858. IEEE Access. https://doi.org/10.1109/ACCESS.2020.3025211

Sadiku, M. N. O., Fagbohungbe, O., & Musa, S. M. (2020). Artificial Intelligence In Cybersecurity. *International Journal of Engineering Research and Advanced Technology*, *6*. https://doi.org/10.31695/IJERAT.2020.3612

Shanthi, R. R., Sasi, N. K., & Gouthaman, P. (2023). A New Era of Cybersecurity: The Influence of Artificial Intelligence. *2023 International Conference on Networking and Communications (ICNWC)*, 1–4. https://doi.org/10.1109/ICNWC57852.2023.10127453

Traficom. (2024). *Applying artificial intelligence in Cybersecurity* (p. 41). https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Applying%20AI%20in%20cybersecurity_EN.pdf

U.S. Department of the Treasury. (2024). *Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector*. 52.

Wilson, S. (2023). *Cybersecurity and Artificial Intelligence: Threats and Opportunities*.

Zaghloul, E., Li, T., Mutka, M. W., & Ren, J. (2020). Bitcoin and Blockchain: Security and Privacy. *IEEE Internet of Things Journal*, *7*(10), 10288–10313. IEEE *Internet of Things Journal*. https://doi.org/10.1109/JIOT.2020.3004273

Apêndice I – Resumo sobre os Relatórios de Segurança Cibernética e Inteligência Artificial

Tabela 2 – Relatório da PwC de 2021

Apenas 13% das entidades temem perdas financeiras devido a incidentes ou roubo de informações.
Uma em cada dez organizações está preocupada com a perda de dados pessoais.
Apenas 15% das entidades prioriza iniciativas de consciencialização.
O aumento dos crimes obrigou as empresas a repensar o negócio e incluir a cibersegurança na sua estratégia.
A redefinição da estratégia concentrou-se no repensar do orçamento disponível na área, na preparação de medidas para as crises e no aumento de competências através de formação.

Tabela 3 – Relatório do CNCS de 2024

43% das empresas têm definidas as políticas e as medidas de segurança.
Os profissionais de cibersegurança identificam um aumento do risco das empresas em sofrer incidentes de segurança em 2023 e 2024.
A principal forma de ataque foi através do *phishing*, que corresponde a crimes através dos correios eletrónicos, chamadas telefónicas ou mensagens de texto. Seguido pelos crimes de *ransomware*, na qual são bloqueados dispositivos, retiradas informações confidenciais e há ameaças de manter o bloqueio até que seja efetuado um pagamento ao invasor.

Tabela 4 – Relatório da Deloitte de 2023

As estratégias de planeamento referidas no relatório foram a análise e atualização dos planos anualmente, uma gestão de líderes seniores, a quantificação do risco e a avaliação do retorno dos investimentos com cibersegurança, a criação de respostas a incidentes e a validação com o meio externo das iniciativas aplicadas e a aplicar.
91% das entidades inquiridas sofreu pelo menos um incidente.
Os incidentes provocam interrupções operacionais, perda de receita, confiança e de reputação, dificuldade em retenção de talento, roubo de propriedades, queda dos preços nas ações, multas e, em casos mais extremos, a mudança de liderança.

Tabela 5 – Relatório da Microsoft de 2023

Detetam cerca de 65 triliões de sinais sintetizados por dia para combater as ameaças digitais e a ciberatividade criminosa.
Proteções contra os ataques: Utilização do MFA que representa uma verificação de dois passos, provando se o indivíduo é efetivamente quem diz ser. Princípios Zero Trust que constitui a validação dos utilizadores e dos dispositivos antes de dar acesso aos recursos. Utilização de softwares de deteção e bloqueio contra os ataques em tempo útil. Atualizações, conhecimentos sobre os seus dados, localizações e validação das defesas eficazes.

Tabela 6 – Relatório da Traficom de 2024

Os analistas não têm capacidade suficiente para analisar a vasta gama de arquivos, objetos e alertas de segurança.
É necessária uma resposta rápida para reduzir os impactos sendo nesta perspetiva que a IA deve atuar.

Os analistas são mais proativos quando podem analisar os padrões revelados pela IA, tornando a segurança que proporcionam mais estratégica e complexa.
Os modelos de IA devem ser ágeis, robustos, conter capacidades de aprendizagem e adaptabilidade, o monitoramento deve ser contínuo, e devem ser realizadas atualizações constantes.

Tabela 7 – Relatório do U.S. Department of the Treasury de 2024

A adoção de IA pelos entrevistados, tem como propósito melhorar a qualidade e os custos em segurança cibernética e antifraude. Utilizando automatização de tarefas, processamento de dados mais amplos e profundos, e análises mais sofisticadas.
Os ataques também são baseados em IA, sendo fundamental que os sistemas de defesa também sejam baseados em IA.
Um dos ataques comuns que utilizam IA são a falsificação de identidade sofisticada, onde o sistema se faz passar pelas pessoas, imitando a sua voz, bem como a criação de vídeos das pessoas.

Tabela 8 – Relatório da IBM de 2024

O número de empresas que utilizam IA de segurança cresceu em 31%.
Os custos provocados pelo cibercrime e a utilização de IA, são duas variáveis correlacionadas. Quanto mais as empresas utilizarem a IA na segurança cibernética, menores serão os custos associados aos ataques.

Apêndice II – Resumo sobre os Relatórios de Criptomoedas e Segurança Cibernética com o Apoio de IA

Tabela 9 – Relatório da Deloitte de 2017

A *blockchain* poderá prevenir ataques fraudulentos e detetar alterações de dados, tendo por base a transparência, auditabilidade e encriptação.
Uma encriptação completa de dados em blocos garantirá que os dados apenas estarão acessíveis para as partes autorizadas. Os atacantes conseguem aceder aos dados, mas não conseguirão ler ou interpretá-los.
Métodos para garantir a integridade podem ser a encriptação dos dados, a comparação do *hash* e a assinatura digital.

Tabela 10 – Relatório de Arkose Labs de 2024

Problemas mais comuns: *Phishing* através de sites falsos e recebimento de *emails* de criptomoedas ilegítimas; Utilização de carteiras falsas para roubar fundos e/ou informações confidenciais dos utilizadores; Esquemas de *Pump and Dump*, onde os criminosos inflacionam o preço de uma criptomoeda com informações falsas; Esquemas *Ponzi*, em que os cibercriminosos prometem retornos elevados e dependem dos fundos de novos investidores para pagar aos investidores antigos.

Tabela 11 – Relatório da Europol de 2024

Existem diversos fóruns de cibercrime: No Exploit, eram partilhados conhecimentos de *hackers*, dados roubados, ferramentas e serviços de cibercrime; O BreachForums é um fórum em inglês voltado para o mercado de cibercriminosos a nível global; O CryptBB é um fórum fechado para cibercriminosos e programadores, reunindo tanto principiantes como especialistas.
Os fóruns contam com a inscrição de principiantes e especialistas, podendo exigir inscrições ou pagamentos.
As intervenções internacionais lutam contra o desmantelamento, contudo, muitos desses fóruns conseguem se reerguer.