PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRO-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

O USO DE CRIPTOMOEDAS EM ATAQUES DE *RANSOMWARE*:
UMA PERSPECTIVA DA SUA UTILIZAÇÃO EM ATAQUES CIBERNÉTICOS.

ORIENTANDA - CAMILA PEREIRA CAVALCANTI SOUZA

ORIENTADOR – PROF. DR. JOSÉ ANTONIO TIETZMANN E SILVA

GOIÂNIA - GO
2023

CAMILA PEREIRA CAVALCANTI SOUZA

O USO DE CRIPTOMOEDAS EM ATAQUES DE *RANSOMWARE*:

UMA PERSPECTIVA DA UTILIZAÇÃO DE LEIS VIGENTES CONTRA OS ATAQUES CIBERNÉTICOS.

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUCGOIÁS). Prof. Orientador – Dr. José Antônio Tietzmann e Silva.

GOIÂNIA – GO

2023

CAMILA PEREIRA CAVALCANTI SOUZA

O USO DE CRIPTOMOEDAS EM ATAQUES DE *RANSOMWARE*:
UMA PERSPECTIVA DA UTILIZAÇÃO DE LEIS VIGENTES
CONTRA OS ATAQUES CIBERNÉTICOS.

Data da Defesa: 22 de novembro de 2023

BANCA EXAMINADORA

_____

Orientador (a): Prof. (a): Dr. Jose Antônio Tietzmann e Silva Nota

_____

Examinadora Convidada: Prof. (a): Dra. Luciane Martins de Araújo Nota

DEDICATÓRIA

Dedico este trabalho, primeiramente a Deus, e a todos que estiveram ao meu lado durante esta jornada acadêmica. Em especial ao meu marido, Bruno de Oliveira Souza e nossos três filhos, Matheus, Louise e Marina que me deram amor e apoio incondicional. A minha mãe Vanisia Maria, a meu pai José Cavalcanti, meus sogros, minha amiga Maria Isabel que cuidou dos meus filhos enquanto estava correndo atrás de meus sonhos e meus professores da PUCGO, em particular, a meu orientador, Dr. José Antônio Tietzmann e Silva e meus eternos professores da Faculdade Três Marias, onde iniciei essa trajetória universitária especialmente a professora Rebeca Resende, Phillipe Martins e Renê Leite. E, finalmente a todos do escritório Ovídio Martins que me acolheram tão bem como estagiária e se tornaram parceiros, em especial Dr. Marco Túlio, que tanto me ensinou e a minha amiga Dra. Thawanny Marques. Agradeço também à instituição que tornou este sonho possível. Este TCC é dedicado a todos vocês com profundo agradecimento e carinho.

O USO DE CRIPTOMOEDAS EM ATAQUES DE *RANSOMWARE*:
UMA PERSPECTIVA DA UTILIZAÇÃO DE LEIS VIGENTES CONTRA OS ATAQUES CIBERNÉTICOS.

Camila Pereira Cavalcanti Souza[1]

Ao longo dos séculos, as formas de negociações evoluíram, levando ao surgimento de moedas e bancos para facilitar as transações. As criptomoedas, como o Bitcoin, representam uma evolução mais recente, criada como uma alternativa descentralizada e livre de controle governamental ou institucional. Eles operam utilizando a tecnologia blockchain, que garante segurança e transparência nas transações, eliminando a necessidade de intermediários. Apesar de seu potencial, as criptomoedas são vistas ou como uma forma de liberdade financeira ou como uma ameaça à estabilidade econômica e segurança nacional. No Brasil, uma ameaça crescente de ataques cibernéticos destaca a necessidade de medidas de segurança, treinamento e monitoramento, bem como o cumprimento das leis de proteção de dados. O objetivo geral deste artigo é investigar o uso de criptomoedas para pagamentos de ataques *ransomware* e o comportamento das leis para prevenção desses tipos de ações. As metodologias utilizadas foram a abordagem dedutiva, o procedimento histórico, bem como o monográfico e a técnica de pesquisa foi a documental indireta e a pesquisa exploratória. A conclusão aponta para a necessidade de medidas eficazes de prevenção e combate aos ataques de *ransomware*, uma parceria entre países, além da utilização das leis existentes de forma mais punitiva para que sejam enfrentados esses tipos de ataques.

Palavras-chave: Criptomoedas. Ransomware. LGPD. Leis criminais. Cibercriminalidade.

THE USE OF CRYPTOCURRENCIES IN RANSOMWARE ATTACKS:

A PERSPECTIVE OF THEIR USE IN CYBER ATTACKS.

[1] Graduanda em Direito pela Pontifícia Universidade Católica de Goiás (PUCGOIÁS). camilapereira1@gmail.com

Camila Pereira Cavalcanti Souza[2]

Over the centuries, forms of trading have evolved, leading to the emergence of currencies and banks to facilitate transactions. Cryptocurrencies, such as Bitcoin, represent a more recent evolution, created as a decentralized alternative free from government or institutional control. They operate using blockchain technology, which guarantees security and transparency in transactions, eliminating the need for intermediaries. Despite their potential, cryptocurrencies are seen either as a form of financial freedom or as a threat to economic stability and national security. In Brazil, a growing threat of cyber attacks highlights the need for security measures, training and monitoring, as well as compliance with data protection laws. The general objective of this article is to investigate the use of cryptocurrencies to pay for ransomware attacks and the behavior of laws to prevent these types of actions. The methodologies used were the deductive approach, the historical procedure, as well as the monographic and the research technique was indirect documentary and exploratory research. The conclusion points to the need for effective measures to prevent and combat ransomware attacks, a partnership between countries, in addition to the use of existing laws in a more punitive way to combat these types of attacks.

Keywords: Cryptocurrencies. Ransomware. GDPR. Criminal laws. Cybercriminality.

SUMÁRIO

[2] Law student at the Pontifical Catholic University of Goiás (PUCGOIÁS)

1. INTRODUÇÃO

Ao longo dos séculos, com a necessidade de maior conforto e com a evolução das formas de comércio, surgiram as primeiras moedas por volta do século VII AC, levando ao surgimento de bancos para guardar e gerenciar o

dinheiro. O desempenho do comércio foi um papel fundamental no avanço da sociedade, e a moeda se tornou o meio de facilitar as transações.

Com o avanço das tecnologias, surgiram novas formas de pagamento, incluindo as criptomoedas, cuja origem remonta ao final da década de 1990. O Bitcoin, criado em 2009 por Satoshi Nakamoto, foi motivado pela insatisfação com o sistema bancário tradicional e a busca por maior privacidade nas transações financeiras.

O impacto das criptomoedas na tecnologia financeira tem crescido globalmente, embora seu uso ainda seja alvo de controvérsias. Algumas pessoas veem como uma forma de liberdade financeira e privacidade, enquanto outras consideram uma ameaça à estabilidade econômica e segurança nacional.

Independentemente das opiniões, as criptomoedas desempenham um papel importante no futuro das finanças e do comércio global, com a possibilidade de inovações que as tornem mais acessíveis e úteis à medida que mais pessoas as adotam e compreendem sua funcionalidade.

Em 2008, uma grande crise econômica ocorreu nos Estados Unidos devido a uma bolha imobiliária, causada pela expansão desenfreada do crédito imobiliário, com juros baixos e disponível mesmo para pessoas sem comprovação de renda. Isso levou a uma demanda massiva, resultando na elevação dos preços imobiliários para níveis insustentáveis.

Com a explosão da bolha, houve uma queda abrupta nos preços, levando ao inadimplemento das prestações dos consumidores e a falta de recursos para os bancos financiadores. A crise levou os bancos à beira da falência a receber injeções massivas de dinheiro dos contribuintes, causando falências de pessoas e empresas sem contrapartidas para a população afetada e foi nesse contexto que surgiram as moedas digitais.

As moedas digitais são baseadas em criptografia, projetadas para serem descentralizadas e livres de controle governamental ou institucional. Eles operam usando a tecnologia blockchain, que registra transações de forma segura e transparente sem intermediários, na qual as criptomoedas são conhecidas por sua privacidade, anonimato e volatilidade, mas também pela sua vulnerabilidade a ataques cibernéticos.

Casos de ataques de *ransomware* que bloqueiam o acesso a informações importantes para que sejam feitos pagamentos em criptomoedas para assim permitir o desbloqueio dos arquivos é um exemplo de ataques. Destaca-se também a importância de medidas de segurança, treinamento de pessoal e monitoramento para prevenção e combate aos ataques cibernéticos.

Em geral, a natureza jurídica das criptomoedas é considerada dinâmica e pode variar de acordo com seu uso e especificações. As abordagens regulatórias variam de país para país, com algumas jurisdições optando por uma abordagem mais restritiva e outras por uma abordagem mais flexível. No entanto, a falta de consenso internacional tem dificultado a elaboração de uma regulamentação global para as criptomoedas abrindo espaço para ilegalidades.

De acordo com a empresa de segurança digital Fortinet (on-line, 2023[3]), em entrevista à revista exame, o Brasil já sofreu 23 bilhões de ataques cibernéticos nos meses de janeiro a junho deste ano, onde foi considerado o país com maior acometimento do mundo.

Existem vários tipos de *ransomware* que são responsáveis por muitos ataques cibernéticos em todo o mundo, causando prejuízos financeiros e danos à reputação de empresas e organizações e à confiança do público em relação às empresas afetadas. Por isso, a importância de informar a sociedade sobre a segurança cibernética que podem ter consequências graves, incluindo perda de dados e privacidade é uma temática muito importante a ser observada perante o governo, pois com a disseminação dessas informações torna mais fácil a análise desses tipos de ataques e sua prevenção.

Portanto, além das prevenções citadas, temos leis que ajudam a combater esses tipos de ataques como a Lei Geral de Proteção de Dados, as leis penais e acordos feitos entre países que contribuem na efetiva eficácia ao enfrentamento de ataques cibernéticos.

2. AS CRIPTOMOEDAS

Ao longo dos séculos, com o desenvolvimento do intelecto humano, o homem primitivo sentiu a necessidade de possuir maior conforto, surgindo as necessidades individuais e as trocas diretas. Com esse sistema de troca,

[3]Disponível em: https://exame.com/future-of-money/inteligencia-artificial-golpes-eficientes-fortinet/ Acesso em: 27 set. 2023.

surgiram vocábulos como o salário, o pagamento feito através de certa quantidade de sal e a pecúnia.

Segundo o livro Casa da Moeda do Brasil: 290 anos de História, 1694/1984, as primeiras moedas surgiram no século VII A.C. feitas de metais e com isso viu-se a necessidade de guardar as moedas em locais seguros e assim ocorreu o surgimento dos bancos, onde passaram a ser responsáveis de cuidar do dinheiro e a dar recibos pelos valores guardados. Esses documentos eram conhecidos como *goldsmith´s notes* e com o tempo se tornaram uma forma de pagamento, surgindo assim as primeiras cédulas de papel moeda, ou cédulas de banco.

O comércio foi um aspecto importante para o avanço da sociedade e a moeda foi o meio encontrado para que as transações fossem realizadas. Com a evolução das tecnologias, novas formas de pagamento vieram surgindo, e as criptomoedas são um exemplo disso.

A origem das criptomoedas remonta ao final da década de 1990, quando a ideia de uma moeda digital começou a ser discutida. No entanto, foi em 2009 que a primeira criptomoeda, o Bitcoin, foi criada por uma pessoa ou grupo de pessoas sob o pseudônimo de Satoshi Nakamoto. (DE ANDRADE, 2017).

A criação do Bitcoin foi motivada por uma série de fatores, incluindo a insatisfação com o sistema bancário tradicional e a busca por maior privacidade nas transações financeiras. Algumas foram criadas para serem mais rápidas ou mais privadas do que o Bitcoin, enquanto outras foram projetadas para serem usadas em setores específicos, como a indústria musical ou o comércio eletrônico.

De acordo com João Otávio Massari Chervinski e Diego Kreutz, em seu livro: “Introdução às tecnologias dos *blockchains* e das criptomoedas”, o surgimento das criptomoedas foi um evento importante na história da tecnologia financeira, e seu impacto tem sido cada vez mais sentido em todo o mundo.

Como a popularidade das criptomoedas tem crescido rapidamente, muitos acreditam que elas têm o potencial de revolucionar o comércio e as finanças globais. Apesar disso, as criptomoedas ainda são uma novidade para muitas pessoas, e seu uso ainda é alvo de controvérsias e debates. Algumas pessoas veem as criptomoedas como uma forma de liberdade financeira e privacidade, enquanto outras as veem como uma ameaça à estabilidade econômica e a segurança nacional.

Independentemente das opiniões, é inegável que as criptomoedas têm um papel importante a desempenhar no futuro das finanças e do comércio global. A medida que mais pessoas começam a usá-las e a entender sua funcionalidade, é possível que mais inovações surjam para torná-las ainda mais úteis e acessíveis a todos.

2.1 SUA ORIGEM

Em meados de 2008, ocorreu uma grande crise econômica devido a uma bolha imobiliária nos Estados Unidos, ocasionada pelo aumento desenfreado nos valores imobiliários, na qual não estava proporcional ao rendimento da população, mas o que seria essa bolha imobiliária?

A bolha imobiliária ocorreu com a expansão de crédito imobiliário que os bancos passaram a oferecer à população com baixos juros, até para aqueles que não tinham comprovação de renda, ocasionando uma procura massiva, resultando na diminuição dos preços imobiliários.

Entretanto, os preços dos imóveis foram subindo cada vez mais, ultrapassando muitas vezes o seu valor real (bolha imobiliária), sucedendo uma explosão na bolha e uma queda drástica nos preços dos imóveis ocasionando o inadimplemento das prestações dos consumidores junto as instituições financeiras, resultando na falta de pecúnia para os bancos financiadores realizarem suas operações.

Portanto, a bolha imobiliária é um fato econômico em que os preços dos imóveis aumentam rapidamente de forma insustentável, seguidos por uma queda significativa no mercado imobiliário.

Com esta crise econômica de 2008, os bancos à beira da falência tentam salvar-se fazendo injeções massivas de dinheiro dos contribuintes, levando assim pessoas e empresas a falência sem qualquer contrapartida do banco para a população afetada e foi neste contexto que surgiu as moedas digitais.

2.2 O QUE SÃO CRIPTOMOEDAS?

As criptomoedas são uma forma de moeda digital que usam criptografia para garantir segurança em transações financeiras e controlar a criação de novas unidades. Elas foram criadas para serem descentralizadas e livres de controle governamental ou de instituições financeiras tradicionais. (FOLLADOR,

2017).

Segundo Luiz Gustavo Doles Silva (2018, p.37), criptomoeda é

> um bem digital gerado com base na tecnologia Blockchain, baseada em criptografia, algoritmos distribuídos e uma rede descentralizada de usuários, independentemente de qualquer país soberano, divisível, com conteúdo personalizável, tendo o seu valor definido não por lastro como outras moedas, mas sim pelo interesse do mercado na sua utilização.

A funcionalidade das criptomoedas se baseia em uma tecnologia conhecida como *blockchain*, que permite registrar transações em um livro-razão distribuído e imutável. Essa tecnologia possibilita que as transações sejam seguras e transparentes, sem a necessidade de intermediários para validar as transações.

Umas das características das criptomoedas é a sua privacidade, anonimidade e sua natureza descentralizada, na qual não são emitidas ou controladas por um governo ou instituição financeira central e sim por meio de um processo conhecido como mineração, onde computadores solucionam problemáticas verificando e registrando transações na Blockchain sem que seja identificados as pessoas, evitando assim a intervenção estatal em suas finanças.

As criptomoedas também são conhecidas por sua volatilidade, o que significa que seus preços podem flutuar significativamente em curtos períodos. Isso se deve em parte à falta de regulamentação governamental e à natureza especulativa do mercado de criptomoedas.

Embora as criptomoedas tenham sido criadas para serem seguras, elas também são vulneráveis a ataques cibernéticos. Os hackers podem explorar vulnerabilidades em carteiras digitais e *Exchange* de criptomoedas para roubar moedas digitais.

Embora as criptomoedas tenham sido criticadas por sua falta de regulamentação e possíveis implicações legais, muitos acreditam que elas têm o potencial de transformar a forma como as transações financeiras são realizadas e desafiar o *status quo* das instituições financeiras tradicionais.

Um exemplo de moeda digital é o *bitcoin,* o qual funciona como uma combinação de criptografias de redes descentralizadas ainda não regulamentadas, diferente dos bancos do sistema tradicional, em que o Banco Central regulamenta e traz inúmeras normas para mostrar passo a passo como cada banco deve funcionar.

De acordo com Thiago Augusto Bueno em seu livro: *Bitcoin* e crimes de lavagem de dinheiro (p.19, 2020), o *bitcoin* funciona como um livro-caixa que registra toda operação entre computadores ao qual são interligados em um sistema distribuído, ou seja, existe uma combinação de criptografias feita por uma dessas máquinas que tem a função de realizar, registrar e conferir a autenticidade das operações de forma imutável, onde são conectadas com as informações anteriores, formando uma cadeia de blocos, garantindo assim a segurança e legitimidade de todo processo.

Em razão dessa adoção de um sistema em que distribui informações, só existe uma forma de ataque, os individualizados ao titular da carteira, quando estão de posse da chave de acesso privada. A prevenção é feita, como dito anteriormente, devido a existência de vários livros-caixa distribuídos entre os mineradores e em casos de tentativas de fraudes, todos os outros mineradores não reconhecerão a legitimidade da transação e não acrescentará a *Blockchain*, excluindo a informação dos blocos subsequentes. Lembrando que todos os registros são imutáveis e todos os registros são transmitidos apenas entre as chaves públicas transacionadas, sem qualquer indicação da identificação civil dos titulares da carteira, ajudando assim no bloqueio de falsas transações.

Com a configuração que foi composta a programação do *bitcoin* não se pode afirmar que as transferências sejam anônimas, mas que sua identificação é mais dificultosa para chegar ao usuário em questão. Porém, segundo Thiago Augusto Bueno (2020, p. 44), “foram lançadas outros criptoativos que tendo sua própria *Blockchain*, nos moldes do *bitcoin*, se preocuparam em garantir o anonimato de seus usuários. Monero, Zcash e Dash são exemplos das chamadas *privacy coins* (moedas privadas, em tradução livre)”.

Tendo em vista que existe uma limitação na quantidade de unidades do *bitcoin*, há um mecanismo chamado de *halving*, que é um procedimento que ocorre a cada 4 anos onde reduz pela metade o valor do pagamento da atividade de mineração e com isso fica o questionamento: Como serão remunerados quando essa forma de recompensa chegar a ser extinta?

Outro fator que pode ser levantado é o fato da crescente utilização desse novo meio de moeda, que aumenta a forma de tentativas para desfalcar moedas digitais das vítimas sem que os autores do crime sejam rastreados, onde nesse tipo de ataque cibernético é feito o bloqueio dos dados importantes de pessoas e/ou empresas em que a restrição no acesso por parte do utilizador força-o a

pagar um valor pecuniário em troca da chave de desencriptação que desbloqueia os seus documentos, daí o nome *ransomware* (*ransom* = resgate). Com a chegada das criptomoedas, os *hackers* exigem que esses valores sejam pagos em moedas digitais, pois torna quase impossível as autoridades detectarem para onde o dinheiro está sendo enviado.

De acordo com a CERT.br[4], as razões que determinam a prática dos crimes cibernéticos, surgem por meio da diversão, para se obter: a) Poder, por demonstrar que se consegue invadir sistemas alheios; b) Prestígio, para se ostentar perante outros cibercriminosos; c) Motivações financeiras, pela necessidade de obtenção de dinheiro; d) Motivações ideológicas, para impedir que conteúdos conflitantes a uma crença, por exemplo, sejam difundidos; e) Motivações comerciais, para tentar afetar a reputação da empresa/ vítima.

Quando se trata das criptomoedas, em que não existe um conceito formalmente formulado em nosso ordenamento, devemos utilizar uma interpretação sistemática das leis e adequar ao entendimento do sistema jurídico para atender aos interesses sociais. Percebe-se que as moedas digitais possuem uma natureza jurídica dinâmica, ao qual varia de acordo com seu uso e as especificações em como são empregadas. Uma possível definição de sua natureza jurídica está definida no artigo 4º da Lei de Introdução às Normas do Direito Brasileiro: “Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais do direito”.

Segundo a Fortinet (on-line, 2021[5]), cerca de 16,2 bilhões de tentativas de ataques cibernéticos ocorreram no primeiro semestre de 2021 no Brasil, número praticamente dobrado em relação ao ano de 2020, que teve a marca de 8,4 bilhões de tentativas e indica que o principal alvo dos criminosos são as empresas de capital aberto.

Em junho de 2021, a Forbes destacou que a unidade da empresa JBS nos Estados Unidos da América teve que resgatar o valor de US$ 11 milhões em *bitcoins* em um ataque de *ransomware*, ao qual foi interrompido temporariamente as fábricas para que informassem os preços das carnes bovinas e suínas no atacado. Ainda no mesmo artigo, traz a informação que o CSO (*Chief Security Officer*), da empresa de tecnologia Ativy, Bruno Giordano, explica que o uso das

[4] Disponível em https://cert.br/ Acesso em: 14 fev. 2023.
[5] Disponível em: https://exame.com/future-of-money/inteligencia-artificial-golpes-eficientes-fortinet/ Acesso em: 27 set. 2023.

criptos como pagamento decorre da proteção de dados pessoais que não torna obrigatória sua divulgação enquanto realizam transações e com isso dificulta a investigação da polícia e complementa que:

> o cibercrime reverte todo o retorno financeiro em tecnologia para desenvolver, automatizar e direcionar ataques com ameaças cada vez mais complexas, onde a falta de capacitação técnica especializada e investimentos direcionados para a camada de segurança cibernética no ambiente corporativo atual, possibilita a exploração das vulnerabilidades, comprometendo diretamente a integridade dos dados. (Forbes, 2021)

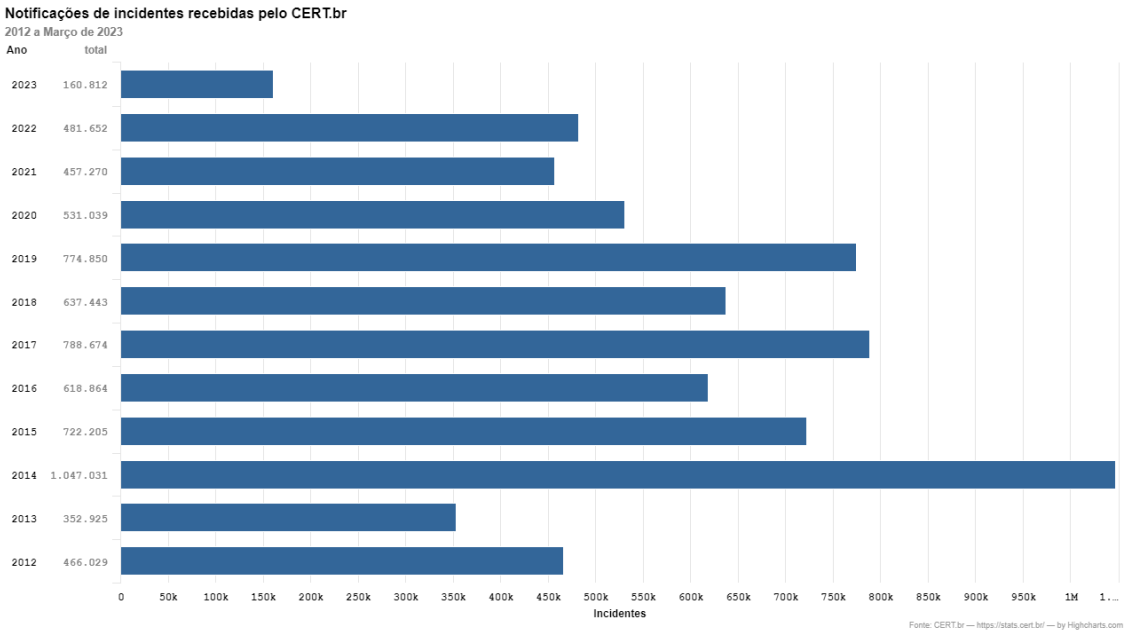
Com a obrigatoriedade de transparência que as empresas possuem com os stakeholders, afirma Giordano que “essas regulamentações obrigam as companhias a tornarem público qualquer incidente de segurança, refletindo diretamente em sua reputação e desvalorização no preço das ações.” Onde, segundo ele, logo após os ataques e a sua divulgação, os títulos das empresas chegam a depreciar aproximadamente 8,6% e em casos mais gravosos podem chegar a 15,6% de desvalorização.

Um outro caso de ataque do tipo *ransomware* foi cometido contra as lojas Renner em agosto de 2021, onde foi utilizado o tipo RansomEXX para invadir o sistema. Por essa razão percebe-se a relevância de se informar a sociedade sobre a temática, ajudando, assim, a combater ou ao menos diminuir os casos de ataques cibernéticos. Além de que, os ataques cibernéticos estão cada vez mais atuantes e representam uma ameaça crescente para as empresas e organizações.

Estes ataques podem ter consequências graves, desde a perda de dados confidenciais até a interrupção de serviços críticos, bem como à violação de direitos autorais, a violação de privacidade, a destruição de dados e a interrupção de operações. Além disso, os ataques cibernéticos podem levar as empresas a perda de credibilidade e receita, oferecendo aos criminosos anonimato e facilidade de transferência de fundos.

Segundo dados da CERT.br, as notificações de incidentes recebidas em 2021 foram de 457.270 notificações enviadas, sendo 15,91% de ataques DoS, 6,5% em fraudes, 0,36% em acometimentos de invasões a computadores ou redes, 72,99% em bombardeios *Scan*, 2,28% em ataques Web, comprometendo os servidores ou desconfigurando páginas, e, 1,97% de outros tipos de acometimentos.

Em 2022, foram de 481.652 notificações enviadas, sendo 14,64% de ataque DoS, 7,25% de fraudes, 0,41% de invasões, 72,57% de ataques Scan, 2,35% de ataques Web e 2,79% de outros tipos; Já em 2023 os dados já estão na casa de 160.812 notificações enviadas, sendo 17,16% de ataque DoS, 5,19% de fraudes, 0,16% de invasões, 74,01% de ataques Scan, 1,54% de ataques Web e 1,95% de outros tipos de ataques. Segue abaixo o gráfico dos dados[6] desde 2012.



Fonte: CERT.br - https://stats.cert.br/incidentes/ Acesso em: 17 fev. 2023.

[6] Disponível em: CERT.br - https://stats.cert.br/incidentes/. Acesso em: 14 fev. 2023.

Totais mensais e anual classificados por categoria de incidente -- Janeiro a Dezembro de 2021

Mês	Total	DoS (%)		Fraude (%)		Invasão (%)		Scan (%)		Web (%)		Outros (%)	
jan	44.775	5.559	12,42	1.852	4,14	378	0,84	35.594	79,50	846	1,89	546	1,22
fev	38.893	2.851	7,33	1.389	3,57	139	0,36	32.986	84,81	770	1,98	758	1,95
mar	49.561	7.963	16,07	1.547	3,12	130	0,26	38.270	77,22	803	1,62	848	1,71
abr	33.320	2.234	6,70	1.703	5,11	146	0,44	28.134	84,44	850	2,55	253	0,76
mai	36.507	3.947	10,81	2.215	6,07	100	0,27	28.936	79,26	1.022	2,80	287	0,79
jun	41.557	9.517	22,90	4.507	10,85	135	0,32	25.937	62,41	1.052	2,53	409	0,98
jul	40.870	8.906	21,79	5.591	13,68	74	0,18	25.238	61,75	754	1,84	307	0,75
ago	53.632	8.934	16,66	2.013	3,75	150	0,28	38.731	72,22	895	1,67	2.909	5,42
set	32.012	4.534	14,16	1.875	5,86	76	0,24	23.954	74,83	757	2,36	816	2,55
out	28.465	7.538	26,48	2.420	8,50	121	0,43	17.548	61,65	475	1,67	363	1,28
nov	31.329	7.540	24,07	2.053	6,55	95	0,30	19.893	63,50	1.225	3,91	523	1,67
dez	26.349	3.207	12,17	2.546	9,66	80	0,30	18.533	70,34	999	3,79	984	3,73
Total	457.270	72.730	15,91	29.711	6,50	1.624	0,36	333.754	72,99	10.448	2,28	9.003	1,97

Fonte: CERT.br - https://stats.cert.br/incidentes/ Acesso em: 17 fev. 2023.

Totais mensais e anual classificados por categoria de incidente -- Janeiro a Dezembro de 2022

Mês	Total	DoS (%)		Fraude (%)		Invasão (%)		Scan (%)		Web (%)		Outros (%)	
jan	33.477	3.305	9,87	2.440	7,29	73	0,22	26.118	78,02	729	2,18	812	2,43
fev	27.472	3.694	13,45	2.387	8,69	76	0,28	19.601	71,35	958	3,49	756	2,75
mar	37.553	5.704	15,19	2.961	7,88	85	0,23	26.694	71,08	935	2,49	1.174	3,13
abr	28.351	5.811	20,50	2.520	8,89	91	0,32	18.519	65,32	977	3,45	433	1,53
mai	50.437	6.795	13,47	2.805	5,56	203	0,40	38.819	76,97	1.276	2,53	539	1,07
jun	35.706	9.724	27,23	3.059	8,57	100	0,28	20.945	58,66	1.087	3,04	791	2,22
jul	34.098	7.225	21,19	3.049	8,94	71	0,21	22.054	64,68	1.403	4,11	296	0,87
ago	62.695	11.398	18,18	3.659	5,84	55	0,09	42.470	67,74	837	1,34	4.276	6,82
set	45.396	4.925	10,85	3.238	7,13	93	0,20	35.861	79,00	918	2,02	361	0,80
out	48.178	7.232	15,01	2.612	5,42	75	0,16	36.956	76,71	651	1,35	652	1,35
nov	26.809	2.772	10,34	3.099	11,56	964	3,60	17.509	65,31	728	2,72	1.737	6,48
dez	51.403	1.932	3,76	3.070	5,97	69	0,13	43.984	85,57	802	1,56	1.546	3,01
Total	481.652	70.517	14,64	34.899	7,25	1.955	0,41	349.530	72,57	11.301	2,35	13.450	2,79

Fonte: CERT.br - https://stats.cert.br/incidentes/ Acesso em: 17 fev. 2023.

Totais mensais e anual classificados por categoria de incidente -- Janeiro a Março de 2023

Mês	Total	DoS (%)		Fraude (%)		Invasão (%)		Scan (%)		Web (%)		Outros (%)	
jan	59.030	11.827	20,04	2.843	4,82	63	0,11	41.691	70,63	605	1,02	2.001	3,39
fev	47.990	7.503	15,63	2.510	5,23	82	0,17	37.037	77,18	643	1,34	215	0,45
mar	53.792	8.258	15,35	2.987	5,55	105	0,20	40.289	74,90	1.230	2,29	923	1,72
Total	160.812	27.588	17,16	8.340	5,19	250	0,16	119.017	74,01	2.478	1,54	3.139	1,95

Fonte: CERT.br - https://stats.cert.br/incidentes/ Acesso em: 17 fev. 2023.

O *ransomware* é um tipo de *malware* que bloqueia o acesso aos arquivos de um computador ou servidor, exigindo um pagamento para liberar os dados. O

pagamento é geralmente solicitado em criptomoedas, como Bitcoin, Ethereum ou Monero. [7]No entanto, o uso de criptomoedas também tem seus riscos, pois podem ser usadas para financiar atividades ilegais, como terrorismo, lavagem de dinheiro e outras atividades criminosas.

Existem várias soluções para prevenir e combater os ataques cibernéticos. Primeiro, as empresas, organizações e a sociedade em geral devem implementar medidas de segurança adequadas, como *firewalls*, antivírus, criptografia e autenticação de usuários.

Além disso, as empresas e organizações devem treinar seus funcionários para que eles possam identificar e responder aos ataques cibernéticos e devem monitorar constantemente seus sistemas para detectar e responder rapidamente a qualquer ataque cibernético. Já as pessoas físicas, além da prevenção mencionada, em casos de ocorrência de ataques, devem procurar especialistas na área para que assim consigam atuar positivamente e ao menos consigam diminuir a perda de dados.

2.3 COMO SE DEU O SEU DESENVOLVIMENTO?

Desde o surgimento do Bitcoin, em 2009, as criptomoedas têm sido um assunto recorrente nas discussões sobre tecnologia e economia. Ao longo do tempo, as criptomoedas têm se desenvolvido e se popularizado, atraindo a atenção de investidores, empresas e governos. (FOLLADOR, 2017).

O desenvolvimento das criptomoedas tem sido caracterizado por uma série de inovações tecnológicas e financeiras, que foi iniciada pela criação do Bitcoin gerando uma nova forma de transação financeira sem a necessidade de intermediários. Desde então, outras criptomoedas vêm surgindo com características distintas, com maior privacidade, velocidade de processamento e escalabilidade.

[7] O Bitcoin, Ethereum e Monero são três criptomoedas diferentes, cada uma com suas próprias características e funcionalidades, por exemplo, o **Bitcoin (BTC)**, é baseado em uma tecnologia chamada blockchain, que é um registro público de todas as transações, ele é frequentemente usado como uma forma de armazenar valores e como um meio de pagamento on-line; O **Ethereum (ETH)** é outra criptomoeda, mas também é uma plataforma que permite a criação de contratos inteligentes e aplicativos descentralizados. Ela é usada principalmente para pagar taxas de transação e recursos de computação na plataforma; Já o **Monero (XMR)** é uma criptomoeda focada na privacidade, ao contrário do Bitcoin, onde todas as transações podem ser rastreadas em um livro público, o Monero usa tecnologias avançadas para ofuscar a origem, o valor e o destino das transações. Isso torna o Monero popular entre aqueles que desejam transações financeiras privadas e seguras.

A popularização das criptomoedas tem sido impulsionada por um conjunto de fatores, incluindo a crescente aceitação por empresas e governos, a especulação financeira, a busca por privacidade e a facilidade de uso. Atualmente, além desses fatores existe a possibilidade de comprar bens e serviços utilizando criptomoedas, além de poder negociá-las em corretoras especializadas.

No entanto, com essa crescente popularização também tem atraído a atenção de criminosos e hackers e a falta de regulamentação e o anonimato garantido pelas criptomoedas tornam-nas atraentes para atividades ilegais, como lavagem de dinheiro e financiamento do terrorismo.

Apesar dos riscos associados ao uso das criptomoedas, elas têm atraído cada vez mais a atenção de investidores e de empresas. Tais como a Tesla, PayPal, BTG Pactual, Reserva, a construtora Brasileira Even, dentre outros, na qual anunciaram que passarão a aceitar Bitcoin como forma de pagamento, o que pode gerar impulso na popularização das criptomoedas.

O desenvolvimento das criptomoedas tem sido acompanhado de perto pelos governos e reguladores financeiros, porém seu futuro é incerto. Vários países têm adotado medidas para regulamentar as criptomoedas e evitar o seu uso para atividades ilegais, evitando incertezas, riscos para investidores e usuários de criptomoedas e prejuízos na inovação ou disrupção dessa crescente forma de transação. No entanto, a falta de consenso internacional tem dificultado a elaboração de uma regulamentação global para as criptomoedas abrindo espaço para ilegalidades.

2.4 NATUREZA JURÍDICA DA CRIPTOMOEDA

As criptomoedas são um fenômeno relativamente novo no mundo financeiro e, como tal, ainda não possuem uma definição jurídica uniforme em todos os países. A natureza jurídica das criptomoedas tem sido objeto de debate e divergência, uma vez que elas não são emitidas ou regulamentadas por governos centrais ou entidades financeiras tradicionais. (DE ANDRADE, 2017).

Embora algumas jurisdições tenham adotado regulamentações específicas para criptomoedas, muitos países ainda estão em processo de elaboração de leis e regulamentações para lidar com o seu uso e impacto na economia. Em outros casos, as criptomoedas são totalmente proibidas ou não reconhecidas como moedas legais.

No entanto, algumas jurisdições têm optado por adotar uma abordagem mais flexível em relação às criptomoedas, reconhecendo o seu potencial para inovação e desenvolvimento econômico. Essas jurisdições podem permitir o uso de criptomoedas por empresas e indivíduos, desde que cumpram com certas condições e requisitos, como registro e controle de identidade. (DE ANDRADE, 2017).

Outra questão importante na natureza jurídica das criptomoedas é a sua classificação como ativos ou incorpóreos. Algumas jurisdições as consideram como ativos, sujeitas a impostos sobre ganho de capital, enquanto outras as consideram um bem incorpóreo cujo maior objetivo é render frutos para o proprietário, sendo este o enquadramento mais utilizado atualmente.

Em geral, a natureza jurídica das criptomoedas ainda é um tema em evolução, com muitas perguntas e desafios a serem resolvidos. As abordagens regulatórias variam de país para país, com algumas jurisdições optando por uma abordagem mais restritiva e outras por uma abordagem mais flexível.

O portal Legislação & Mercados (on-line, 2023) elencou sobre a normatização das criptomoedas como nos Estados Unidos da América, onde as moedas virtuais são tratadas como propriedade, onde todas as transações que envolvam criptomoedas, deverá ser levantado o lucro para tributá-lo conforme a sistemática geral da venda de outros ativos. Já na União Europeia, o Tribunal de Justiça (Quinta Secção) julgou, em 2015, um caso (C-264/143[8]) na qual ficou determinado que a troca de bitcoins por moedas tradicionais configura serviço de pagamento, em que são isentos de Impostos sobre o Valor Acrescentado (IVA).

Embora a regulamentação das criptomoedas possa ser vista como um meio de mitigar riscos e incertezas, a falta de regulamentação também pode abrir espaço para a inovação e o desenvolvimento de novos sistemas financeiros e econômicos.

É importante que os governos e as entidades reguladoras continuem a monitorar o desenvolvimento das criptomoedas e avaliar a necessidade de regulamentação adequada para lidar com os seus impactos na economia e na sociedade.

[8] Disponível em: https://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=uriserv%3AOJ.C_.2015.414.01.0006.01.POR . Acesso: 27 set. 2023.

3. A UTILIZAÇÃO DE *RANSOMWARE* PARA RESGATE COM CRIPTOMOEDAS

O *ransomware* é uma forma de ataque cibernético que tem se tornado cada vez mais comum nos últimos anos, que segundo Wakka (on-line, 2019[9]) o Brasil é um dos países com mais ataques de *ransomware*, onde no ano de 2019 houve um aumento de 109,95% nas denúncias que se referem a crimes cibernéticos, dentre eles o chamado “sequestro de dados”. Esse tipo de ataque consiste em bloquear o acesso a sistemas ou dados de uma vítima, exigindo o pagamento de um resgate para que o acesso possa ser restaurado. O uso de criptomoedas como meio de resgate tem sido uma das principais características desses ataques.

De acordo com a empresa de segurança digital Fortinet (on-line, 2023[10]), em entrevista à revista exame, o Brasil já sofreu 23 bilhões de ataques cibernéticos nos meses de janeiro a junho deste ano, onde foi considerado o país com maior acometimento do mundo, ficando a uma distância bem superior aos outros países, como o México (14 bilhões) e a Venezuela (10 bilhões).

O *ransomware* pode ser propagado de várias formas, sendo uma das mais comuns por meio de e-mails de *phishing*, que consiste em tentativas de fraude para obter ilegalmente informações como número da identidade, senhas bancárias, número de cartão de crédito, entre outros. Uma vez que um sistema é infectado, o *ransomware* criptografa os arquivos da vítima, tornando-os inacessíveis até que o resgate seja pago. A forma de pagamento atualmente utilizada é por moedas digitais, pois torna difícil para as autoridades rastrearem os criminosos, o que tem sido uma das principais razões para o aumento desses ataques.

Existem vários tipos de *ransomware*, que possuem características próprias. O *ransomware* de bloqueio, por exemplo, impede completamente o acesso ao sistema ou arquivos da vítima, exigindo um pagamento para restaurar o acesso. Já o *ransomware* criptográfico, criptografa os arquivos da vítima usando algoritmos avançados de criptografia, tornando-os inacessíveis até que

[9] Disponível em: https://canaltech.com.br/seguranca/brasil-e-o-2o-pais-com-mais-ameacas-de-ransomware-no-mundo-aponta-estudo-134683/ . Acesso em: 16 jun. 2023.

[10] Disponível em: https://exame.com/future-of-money/inteligencia-artificial-golpes-eficientes-fortinet/ Acesso em: 27 set. 2023.

um resgate seja pago. Além desses, existem o *ransomware* de resgate virtual utiliza táticas de intimidação e ameaças falsas forçando a vítima a acreditar que seu sistema foi comprometido ou que cometeu uma infração. Já, o *ransomware* móvel que visa dispositivos móveis, como smartphones e tablets, bloqueando o acesso ou criptografando dados do dispositivo até que um pagamento seja feito. E, por fim o *ransomware* híbrido que combina características de diferentes tipos de *ransomware*, visando maximizar o impacto e a eficácia do ataque.

Todos esses tipos de *ransomware* têm sido responsáveis por muitos ataques cibernéticos em todo o mundo, causando prejuízos financeiros e danos à reputação de empresas e organizações e à confiança do público em relação às empresas afetadas. Por isso, é importante que as empresas adotem medidas de segurança eficazes para proteger seus sistemas e dados contra esse tipo de ataque.

A Lei Geral de Proteção de Dados (LGPD) pode ser uma das ferramentas mais importantes, uma vez que estabelece diretrizes claras para a proteção de dados pessoais e exige medidas de segurança eficazes. No entanto, ainda é necessário um esforço conjunto das empresas, das autoridades e da sociedade em geral para combater efetivamente os ataques de *ransomware* e o uso de criptomoedas em transações ilegais.

3.1 AFINAL, O QUE É O *RANSOMWARE*?

O *ransomware* é uma forma de ataque cibernético que sequestra dados ou sistemas de computadores e exige um resgate para sua liberação. Esse tipo de malware é usado por criminosos para obter lucro e pode ser devastador para empresas e indivíduos que são vítimas. O *ransomware* pode assumir diferentes modalidades e formas de propagação, tornando-se cada vez mais sofisticado. (GOMES; NUNES; WILMERS, 2020).

A disseminação dos *ransomwares* ocorre por meio dos mesmos mecanismos utilizados para propagar vírus e outros tipos de *malwares* utilizando a engenharia social, que nada mais é que a manipulação de pessoas para obtenção de informações confidenciais utilizando a confiança, curiosidade, medo e falta de cuidado, a fim de obter acesso a informações sensíveis para persuadir alguém a realizar determinada ação ou comprometer a segurança de sistemas. Esses métodos incluem o uso de redes sociais, serviços de mensagens instantâneas, sites fraudulentos dentre outros.

> Por ter uma estrutura de propagação com ares pandêmicos, o *ransomware* pode se propagar irrestritamente, contando com o benefício de não ter limites territoriais, representando uma grave ameaça para a sociedade. A interdependência da estrutura dos Estados com o uso e manutenção de dados e segurança de rede é um fator intrínseco à manutenção da organização social apresentada em uma perspectiva global, podendo-se assim visualizar um grande aumento de crimes digitais, sendo necessário um duro combate para que tais práticas sejam coibidas de forma usual (ATAPOUR - ABARGHOUEI; BONNER; MCGOUGH, 2019).

Na maioria dos casos, utilizam mensagens que mencionem uma dívida não paga, uma pendência judicial, uma suposta atualização de segurança do banco ou até mesmo um convite para visualizar fotos íntimas de uma personalidade famosa. Esses textos exploram o medo ou a curiosidade do usuário, visando reduzir sua cautela e levando-o a clicar no link ou anexo e uma vez que o *malware* infecta o sistema, ele se espalha rapidamente, criptografando ou bloqueando todos os arquivos encontrados.

3.2 TIPOS DE *RANSOMWARE*

Os *ransomwares* são programas maliciosos que têm como objetivo bloquear o acesso de usuários a seus dispositivos ou sistemas, solicitando um resgate para restauração o seu acesso aos arquivos encriptados. Existem diferentes tipos de *ransomware*, como *lockers, cryptors, scarewares*, móveis e híbridos, que se destacam nesse cenário.

Uma das modalidades mais comuns de *ransomware* é o bloqueio de arquivos, também conhecido como *locker*. Nesse tipo de ataque, o invasor impede totalmente o acesso aos arquivos do usuário, exigindo um pagamento para liberar o sistema. Eles podem ser particularmente devastadores para empresas ou organizações, que podem ser impedidas de acessar seus próprios sistemas e arquivos que dependem desses dados para operar.

Outra forma de *ransomware* é o criptográfico, também conhecido como *cryptor*. Nesse caso, o malware encripta arquivos utilizando algoritmos avançados tornando-os inatingíveis até que seja efetivado o pagamento para o resgate dos dados, que muitas vezes possuem um valor bem elevado e quando os usuários não efetuam tal liquidação, os dados podem ser totalmente perdidos.

O *scareware* é uma forma de *malware* que tem como objetivo infectar o computador de usuários que tentam baixar determinados programas ou clicam em algo específico. Esse tipo de ataque utiliza táticas de intimidação e medo para forçar as vítimas a pagarem o resgate, com o aparecimento de telas que

indicam que seu computador está infectado com algum vírus, ou até propagandas de *softwares* que irá banir tais infecções. O *ransomware* de resgate virtual é uma outra forma comum de *scareware*.

Recentemente, o *ransomware* móvel tem se tornado mais comum, visando dispositivos móveis, como smartphones e tablets. Esse tipo de *ransomware* pode bloquear o acesso ou criptografar dados do dispositivo até que um pagamento seja feito. O *ransomware* móvel pode ser especialmente perigoso, pois muitos usuários não estão cientes das ameaças cibernéticas em dispositivos móveis além de armazenarem informações confidenciais em seus dispositivos móveis.

Os *ransomwares* híbridos combinam características de diferentes tipos de *ransomware*, visando maximizar o impacto e a eficácia do ataque. Eles podem, por exemplo, combinar a capacidade de criptografar arquivos com táticas de intimidação para forçar o pagamento do resgate.

Embora os *ransomwares* sejam uma ameaça significativa para empresas e indivíduos, existem medidas que podem ser tomadas para proteger-se contra esses ataques. É importante manter backups regulares de seus dados, manter softwares de segurança atualizados e nunca pagar o resgate exigido pelos criminosos.

Os *ransomwares* têm sido cada vez mais utilizados por cibercriminosos em todo o mundo. Eles são particularmente eficazes porque podem gerar grandes lucros em um curto espaço de tempo. O uso de criptomoedas como meio de resgate tem se tornado cada vez mais comum, dada a sua facilidade de uso e anonimato.

A natureza jurídica dos *ransomwares* e seu status legal em diferentes países ainda é objeto de debate. Embora muitos países tenham leis que criminalizam os ataques de *ransomware*, a aplicação dessas leis pode ser complicada devido à natureza transnacional dos ataques.

Esses tipos de ataques cibernéticos estão tipificados em leis, como no Código Penal do Texas[11], que desde 2017 trata sobre a temática. Já no Brasil, a Lei Geral de Proteção de Dados (LGPD) é uma ferramenta útil no combate aos ataques de *ransomware*, uma vez que ela estabelece regras claras para a proteção de dados pessoais, evitando que informações importantes sejam

[11] Disponível em: https://statutes.capitol.texas.gov/docs/PE/htm/PE.33.htm. Acesso em: 27 set. 23

comprometidas, reduzindo ataques de *ransomware*, além da Lei nº 12.737, de 30 de novembro de 2012, conhecida Lei Carolina Dieckmann ao qual foi criada para combater crimes cibernéticos, especialmente os relacionados à divulgação não autorizada de imagens e dados pessoais na internet, além da invasão de dispositivos eletrônicos. Essa lei prevê penalidades para quem pratica tais ações, tornando-as crime passíveis de punição, como multas e prisão.

3.3 A CIBERCRIMINALIDADE COM O USO DE CRIPTOMOEDAS: O *RANSOMWARE*

No atual contexto social, a internet está cada vez mais presente em vários aspectos da vida em sociedade, desde relações pessoais, passando por relações negociais, de aquisição de adquirir conhecimento, lazer, etc. Em outras palavras, praticamente toda comunicação social pode usar a Internet como substrato, conectado por fio ou não (PRASAD; ROHOKALE, 2020).

A maioria dos usuários de internet acreditam que não estão sendo vítimas de ataques, que todas as leis de proteção estão sendo respeitadas e não utilizam proteções para esses possíveis ataques, o que pode gerar um grande problema principalmente para aqueles que utilizam dados sensíveis.

Visto isso, compreende os autores AKHILESH e MÖLLER (2020, p. 1-16), que:

> a tecnologia surge como uma das principais forças motrizes da sociedade, pois é capaz de expandir, adaptar e atualizar, modificando comportamentos e ambientes, utilizando sensores inteligentes que podem fornecer dados para serem processados e a partir disso serem praticamente infinitas as possibilidades as quais os seres humanos terão de lidar com o advento das novas tecnologias.

Por tais motivos se faz importante uma regulação para impor limites e regramentos em um espaço tão vasto e inimaginável, evitando que pessoas mal-intencionadas interfiram em dados privados.

A natureza descentralizada das criptomoedas torna mais difícil a identificação dos criminosos, porém não significa que as autoridades não possam rastrear as transações suspeitas, apenas torna dificultosa a identificação de quem está por trás dos ataques. Diferente das transações em dinheiro ou cartões de crédito, que podem ser rastreadas até um indivíduo.

No entanto, a aplicação efetiva da lei nesse contexto enfrenta desafios significativos. Uma das principais questões é a jurisdição transnacional. Como

as transações em criptomoedas ocorrem em todo o mundo, as autoridades precisam cooperar internacionalmente para rastrear os criminosos e levar à justiça.

Outro desafio é a dificuldade em identificar os perpetradores. Os criminosos que usam criptomoedas para receber resgate podem permanecer anônimos, dificultando a identificação de quem está por trás do ataque. Além disso, a adaptação da legislação para lidar com as inovações tecnológicas é um desafio constantemente enfrentado pelas autoridades, pois precisam empregar técnicas forenses avançadas para rastrear transações suspeitas e identificar os criminosos por trás dos ataques. (SANTOS; STEIN, 2022).

A relação entre criptomoedas e cibercriminalidade é um campo em constante evolução, com novas ameaças surgindo regularmente. As autoridades precisam permanecer vigilantes e atualizadas sobre as últimas tendências em cibercriminalidade para proteger empresas e indivíduos dos ataques.

3.4 CASOS PRÁTICOS

A utilização de criptomoedas em ataques de *ransomware* se tornou uma prática comum no mundo cibernético. Diversos casos demonstram a eficácia dessas moedas na realização de resgates, uma vez que, por sua natureza de transações descentralizadas, torna difícil rastrear o pagamento realizado pelos criminosos.

Um dos casos mais conhecidos é o do *WannaCry*, um *ransomware* que atingiu mais de 230 mil computadores em 150 países em maio de 2017. O ataque exigia o pagamento de resgate em *Bitcoin*, e acredita-se que os criminosos conseguiram arrecadar mais de US$ 140 mil em criptomoedas. O *WannaCry* foi responsável por diversos prejuízos, incluindo afetar o sistema de saúde britânico. (MOREIRA et al., 2017).

Outro caso que chamou atenção foi o ataque ao Colonial Pipeline nos Estados Unidos em 2021. Os criminosos exigiram um resgate em Bitcoin para liberar sistemas críticos da empresa, o que resultou em interrupções no abastecimento de combustível em diversos estados americanos. O resgate exigido foi de cerca de US$ 4,4 milhões, que posteriormente foi recuperado pelo governo americano. (VAZ-FERREIRA; RODRIGUES, 2021).

O ataque ao CD Projekt RED, uma empresa polonesa de jogos eletrônicos, em fevereiro de 2021, também foi um exemplo de uso de

criptomoedas em *ransomware*. Os hackers utilizaram o *ransomware HelloKitty* para criptografar arquivos importantes da empresa, exigindo um resgate em Bitcoin para liberá-los. Embora a empresa afirmasse que não pagaria o resgate, informações vazadas posteriormente indicaram que os criminosos conseguiram arrecadar cerca de US$ 7 milhões em criptomoedas. (DA SILVA FILHO, 2016).

Um caso ocorrido no Brasil foi o ataque ao STJ em novembro de 2020, onde os criminosos exigiram um resgate em criptomoedas para liberar o acesso aos sistemas da Corte. O STJ afirmou que não pagaria o resgate, mas a investigação sobre o caso ainda está em andamento. (PHILOT, 2021).

O uso de criptomoedas em ataques de *ransomware* levanta diversas questões legais e éticas. Muitos países ainda não possuem uma regulamentação específica para lidar com a utilização dessas moedas em crimes cibernéticos. Além disso, há o debate sobre a responsabilidade das empresas em relação à segurança de suas redes e sistemas, bem como sobre a adequação das medidas de segurança adotadas. (PHILOT, 2021).

Além desses casos, com o surgimento das casas inteligentes que são conectadas a internet, abre as portas para outros tipos de ameaças a privacidade, pois tendo acesso a esses dados como senhas do aplicativo que abrem e fecham portas, janelas, dentre outros acessos, existe a possibilidade de conseguir violar além dos ambientes tecnológicos, os residenciais, sem que sejam descobertos, pois com tais atalhos, é provável que sejam desligados todos os aparelhos de monitoramento antes da efetiva invasão residencial. Esses casos evidenciam a real necessidade de medidas efetivas de prevenção e combate a esses crimes cibernéticos.

4. DEBATE SOBRE A LGPD

4.1 O QUE É A LGPD?

A Lei nº 13.709/2018, mais conhecida como a Lei Geral de Proteção de Dados (LGPD), entrou em vigor em setembro de 2020, com objetivo de proteger a privacidade e os dados pessoais dos cidadãos, estabelecendo regras para o tratamento dessas informações por empresas públicas e privadas. No contexto da cibercriminalidade, a LGPD tem um papel crucial no combate aos ataques de *ransomware*. Isso porque muitos desses ataques envolvem o roubo ou a exploração de dados pessoais das vítimas, que são utilizados como moeda de

troca para o resgate. (DE TEFFÉ, 2020).

Os ataques de *ransomware* têm impactos significativos, resultando na perda de dados, arquivos e informações, devido à criptografia e podem ter consequências ainda mais gravosas, como por exemplo, em setores hospitalares as implicações vão além da simples perda de dados, e têm um impacto direto na saúde e segurança das pessoas afetadas, pois esses ataques podem resultar na perda ou corrupção de dados de pacientes, bem como no desligamento de equipamentos médicos vitais para a vida, o que potencialmente coloca em risco a vida dos pacientes, podendo levar ao óbito.

Pesquisadores na área de segurança e tecnologia estão dedicados a encontrar soluções efetivas para combater e prevenir esses ataques, visando aumentar a segurança dos usuários e garantir uma solução duradoura. É importante destacar que a tecnologia está em constante evolução, o que demanda um esforço contínuo para acompanhar e enfrentar os desafios impostos pelos *ransomwares* e outras ameaças cibernéticas.

Portanto, ao estabelecer regras claras sobre o tratamento de dados pessoais, a LGPD cria um ambiente mais seguro para os usuários da internet. Isso significa que, ao atacar uma empresa ou indivíduo, os criminosos não terão acesso a informações sensíveis que poderiam ser utilizadas para extorsão. Além disso, a LGPD também prevê punições rigorosas para empresas que não cumprem as regras de proteção de dados, como multas e outras sanções, o que pode desencorajar ações de cibercriminalidade.

No entanto, a efetividade da LGPD no combate aos ataques de *ransomware* depende da sua aplicação correta e eficiente pelas autoridades competentes. Isso significa que é preciso haver investimento em recursos e tecnologia para garantir que a lei seja cumprida e os criminosos sejam punidos. (BOTELHO, 2020). Além disso, é importante lembrar que a LGPD não é uma solução mágica para os problemas de cibercriminalidade. Embora seja uma ferramenta importante no combate aos ataques de *ransomware*, ela não pode resolver todos os problemas relacionados à segurança cibernética. (DE TEFFÉ, 2020).

Por isso, como dito anteriormente, é necessário que empresas e indivíduos também invistam em medidas de segurança cibernética, como backups regulares de dados, uso de softwares de segurança e treinamento de funcionários para evitar ataques de *phishing* e outras formas de exploração.

4.2 COMO ELA PODE AJUDAR PARA O COMBATE DA CIBERCRIMINALIDADE?

A Lei Geral de Proteção de Dados (LGPD) é uma legislação recente no Brasil que tem como objetivo regularizar o tratamento de dados pessoais em todo o território nacional trazendo importantes medidas de proteção para os cidadãos e empresas brasileiras. Essas medidas incluem o uso de criptografia, a implementação de políticas de segurança da informação e a realização de *backups* periódicos dos dados que servem para prevenir ataques de *ransomware* e garantir a segurança dos dados dos usuários.

Uma das principais medidas de proteção de dados previstas na LGPD é o consentimento do titular dos dados. Isso significa que as empresas precisam obter o consentimento expresso e específico dos usuários antes de coletar, armazenar ou compartilhar seus dados pessoais. Essa medida é importante para garantir que as informações dos usuários estejam seguras e protegidas contra ataques de *ransomware*. (RIBEIRO, 2022).

Outra medida importante prevista na LGPD é a obrigatoriedade de comunicação de incidentes de segurança. Se uma empresa sofrer uma invasão virtual, ela precisa notificar os usuários afetados sobre o incidente e as medidas tomadas para resolver a situação. Essa medida é importante para garantir a transparência e a confiança dos usuários nas empresas.

A LGPD também estabelece a figura do controlador de proteção de dados, que tem como função garantir o cumprimento da legislação de proteção de dados pelas empresas. Essa figura é importante para garantir que as empresas sigam as medidas de proteção de dados previstas na LGPD e evitem propagações de *ransomware*.

Além disso, prevê penalidades para as empresas que não cumprem as medidas de proteção previstas na legislação. Essas penalidades podem incluir multas e sanções administrativas, o que incentiva as empresas a adotarem medidas de segurança adequadas para evitar invasões cibernéticas. (RIBEIRO, 2022).

Por fim, a Lei Geral de Proteção de Dados antecipa a possibilidade de ações judiciais para os indivíduos que tiverem seus dados pessoais violados. Essa medida é importante para garantir que os usuários tenham seus direitos

respeitados e protegidos contra ataques de *ransomware*.

5. LEIS PENAIS E SUAS APLICAÇÕES NOS ATAQUES DE *RANSOMWARE*

As leis penais desempenham um importante papel na sociedade tecnológica, pois combatem ataques como a dos *ransomware*. Embora as leis e regulamentações específicas possam variar de acordo com o país, muitas jurisdições possuem legislações que tratam de crimes cibernéticos.

Nas propagações de *ransomware*, os criminosos que se envolvem nesse tipo de atividade buscam obter lucro financeiro por meio de extorsão, exigindo pagamentos em criptomoedas para liberar o acesso a sistemas e dados bloqueados. Tais leis abordam várias questões relacionada as disseminações de *ransomware*, como a criminalização de atividades, na qual estabelecem que a execução de um ataque é criminoso quando o seu acesso as informações pessoais ou empresariais não foram autorizados ou exista a disseminação de *malware* ou extorsão de vítimas.

A aplicação das leis penais a esses ataques é um desafio complexo, pois muitos desses crimes são cometidos por indivíduos ou grupos que operam em diferentes países e jurisdições. Para lidar com isso, existem acordos internacionais de cooperação e assistência judicial mútua que permitem a troca de informações e ações conjuntas para a aplicação da lei.

No Brasil, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), estabelece regras para o tratamento de dados pessoais e prevê penalidades para aqueles que violam suas disposições e exijam resgate para evitar a divulgação dessas informações.

As penalidades para os perpetradores desses tipos de propagações variam de acordo com a legislação de cada país e a gravidade do crime. Em alguns casos, os criminosos podem ser condenados a penas de prisão, multas e outras sanções. Em outros casos, as autoridades podem confiscar os ativos em criptomoedas utilizados para o pagamento do resgate. (MASSENO, 2017).

No entanto, a aplicação da lei nos casos de *ransomware* pode ser desafiadora, porque os ataques são frequentemente realizados por meio de redes anônimas e outras técnicas de ocultação da identidade. Para enfrentar esses desafios, as autoridades policiais e judiciais precisam adotar uma

abordagem multidisciplinar e cooperativa para combater as disseminações, como o uso de técnicas de investigação avançadas, a colaboração com empresas de segurança cibernética e outras partes interessadas, e a implementação de leis e regulamentos atualizados e eficazes, além da atualização de softwares para que todos os tipos de vírus encontrados sejam efetivamente combatidos por esses aplicativos, ajudando assim o não vazamento de dados e oferecendo proteção adequada.

Além disso, a legislação também deve ser acompanhada por medidas de segurança eficazes que possam prevenir a proliferação cibernética negativa minimizando seus impactos. Essas medidas incluem políticas para garantir a proteção adequada de dados, treinamento de funcionários em segurança cibernética e implementação de sistemas de backup de dados para garantir a recuperação rápida em caso de ataque.

A cooperação internacional é fundamental no combate aos ataques de *ransomware*, como a troca de informações entre os países que pode ajudar na identificação dos criminosos e na sua investigação. No entanto, a colaboração nem sempre é fácil de alcançar, pois cada país possui diversas leis que regulamenta cada tipificação legal.

A dificuldade em identificar e punir os perpetradores de ataques de *ransomware* também é agravada pela falta de recursos para investigações e de pessoas qualificadas para lidar com a grande quantidade de ataques a empresas, organizações e da população em geral, o que pode afetar a eficácia no combate direto aos crimes informáticos.

Por todos os motivos elencados, muitas pessoas, empresas e organizações ainda não se conscientizaram dos riscos ao navegar na Internet sem uma mínima proteção e como lidar com dados sensíveis.

De igual forma, segundo FORNASIER; SPINATO; RIBEIRO (p. 208-236, 2020), “observa-se que a falta de cooperação entre as empresas também apresenta um grande desafio no combate a disseminação de *ransomware*, pois ficam relutantes em compartilhar informações sobre seus sistemas e vulnerabilidades de segurança”, para não afetar seus valores de mercado.

CONCLUSÃO

Ao longo desta pesquisa, foi analisado o uso de criptomoedas em ataques de *ransomware* e sua relação com a cibercriminalidade. Exploramos as características das criptomoedas e sua origem, bem como o desenvolvimento das moedas digitais e sua popularização. Também discutimos a natureza jurídica das criptomoedas e seu status legal em diferentes países.

Além disso, investigamos o *ransomware* como uma forma de ataque cibernético e sua utilização de criptomoedas como meio de resgate. Abordamos os diferentes tipos de *ransomware*, como *ransomware* de bloqueio, *ransomware* criptográfico, *ransomware* de resgate virtual e *ransomware* móvel. Também exploramos o *ransomware* híbrido e sua combinação de características de diferentes tipos de *ransomware*.

Ao avaliar a relação entre criptomoedas e cibercriminalidade, estudamos casos reais de ataques de *ransomware* que envolvem o uso de criptomoedas. Discutimos a importância da Lei Geral de Proteção de Dados (LGPD) no combate à cibercriminalidade e as medidas de proteção de dados previstas na legislação.

Analisamos as leis penais aplicáveis aos ataques de *ransomware* e as consequências legais para os criminosos. Avaliamos os desafios jurídicos enfrentados no combate aos ataques de *ransomware*, como a jurisdição transnacional, a dificuldade na identificação e punição dos perpetradores e a necessidade de cooperação internacional.

Em termos de contribuições, esta pesquisa destaca a necessidade de medidas eficazes de prevenção e combate aos ataques de *ransomware*. É vital que as empresas e organizações implementem medidas de segurança cibernética robustas para proteger seus dados e sistemas. Além disso, é importante que os governos trabalhem juntos para combater a cibercriminalidade e garantir que os perpetradores sejam responsabilizados.

Essa pesquisa também destaca a necessidade de mais estudos sobre a relação entre criptomoedas e cibercriminalidade. É importante que as pesquisas futuras se concentrem em soluções eficazes para prevenir e combater os ataques de *ransomware*, incluindo mudanças na legislação e medidas de segurança cibernética mais eficazes.

Outra contribuição desta pesquisa é a análise de como as criptomoedas

estão mudando a natureza da cibercriminalidade. À medida que as criptomoedas se tornam mais populares, é provável que mais criminosos as utilizem em seus ataques. É vital que os governos e empresas estejam atentos a essa mudança e trabalhem juntos para garantir a segurança cibernética de suas organizações.

REFERÊNCIAS

AKHILESH, K. B. Smart Technologies—Scope and Applications. In: AKHILESH, K. B; MÖLLER, Dietmar P. F. (eds.). **Smart Technologies**. Singapore: Springer, 2020, p. 1-16.

ATAPOUR-ABARGHOUEI, Amir; BONNER, Stephen; MCGOUGH, Andrew Stephen. Volenti non fit injuria: *Ransomware* and its Victims. arXi.org, p.1 - 7, 2019. Disponível em: https://arxiv.org/abs/1911.08364. Acesso em: 18 jun 2023.

BOTELHO, Marcos César. **A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes**. Revista Direitos Sociais e Políticas Públicas–Unifafibe, v. 8, n. 2, p. 18, 2020.

BRASIL. **CPI constata dificuldades em rastrear e punir crimes de internet**. Disponível em: https://www.camara.leg.br/internet/Jornal/JC20150824.pdf. Acesso em: 17 fev. 2023.

BRASIL, **Constituição Federal**, promulgada em 5 de outubro de 1988.

BRASIL. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança. **Cartilha de Segurança para Internet**. Disponível em: https://cartilha.cert.br/. Acesso em: 17 fev. 2023.

BRASIL. **Decreto-Lei nº 2.848**, de 7 de dezembro de 1940, "Código Penal". *DOU* de 3.1.1941.

BRASIL. **Safer Internet Center do**: Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. Disponível em: https://indicadores.safernet.org.br/. Acesso em: 17 fev. 2023.

BUENO, Thiago Augusto. ***Bitcoin* e crimes de lavagem de dinheiro**. Contemplar, 2020.

CANUTO, Luiz Claudio. **CPI constata dificuldades em rastrear e punir crimes de internet**. Disponível em: https://www.camara.leg.br/noticias/467819-cpi-constata-dificuldade-em-rastrear-e-punir-crimes-de-internet/. Acesso em: 17 fev. 2023.

CHERVINSKI, João Otávio Massari; KREUTZ, Diego. **Introdução às tecnologias dos *blockchains* e das criptomoedas**. Revista Brasileira de Computação Aplicada, v. 11, n. 3, p. 12-27, 2019.

CUNHA, Rogério Sanches, **Manual de direito Penal**: parte especial, Salvador. JusPODIVM, 2016.

DA SILVA FILHO, Wilson Leite. **Crimes Cibernéticos e Computação Forense**. Sociedade Brasileira de Computação, 2016.

DE ANDRADE, Mariana Dionísio. **Tratamento jurídico das criptomoedas**: a dinâmica dos bitcoins e o crime de lavagem de dinheiro. Revista Brasileira de Políticas Públicas, v. 7, n. 3, p. 43-59, 2017.

DE OLIVEIRA FORNASIER, Mateus; SPINATO, Tiago Protti; RIBEIRO, Fernanda Lencina. ***Ransomware* e cibersegurança**: a informação ameaçada por ataques a dados. Revista Thesis Juris, v. 9, n. 1, p. 208-236, 2020.

DE TEFFÉ, Chiara Spadaccini; VIOLA, Mario. **Tratamento de dados pessoais na LGPD**: estudo sobre as bases legais. Civilistica. com, v. 9, n. 1, p. 1-38, 2020.

FOLLADOR, Guilherme Broto. **Criptomoedas e competência tributária**. Revista brasileira de políticas públicas, v. 7, n. 3, p. 79-104, 2017.

GOMES, Luiz Eduardo dos Santos Pereira; NUNES, Luana Esteche; WILMERS, Michael Felipe. **Natureza Jurídica do crime de *ransomware* e a utilização da criptomoeda como meio de impunidade**. Revista Acadêmica Escola Superior do Ministério Público do Ceará, v. 12, n. 2, p. 213-234, 2020.

GONÇALVES, Cleber Baptista. **Casa da Moeda do Brasil**: 290 anos de História, 1694/1984. Imprinta Gráfica e Editora, 1984.

MALAR, João Pedro. **Inteligência artificial está tornando golpes mais eficientes, diz CEO da Fortinet**. Revista Exame, 2023. Disponível em: https://exame.com/future-of-money/inteligencia-artificial-golpes-eficientes-fortinet/. Acesso em: 27 set. 2023.

MASSENO, Manuel David; WENDT, Emerson. **O *ransomware* na Lei**: apontamentos breves de Direito português e Brasileiro. Revista Eletrônica Direito & TI, v. 1, n. 8, p. 13-13, 2017.

MOREIRA, Fernando. **Cibercriminalidade e Cibersegurança**. 2019.

MOREIRA, Guilherme Baesso et al. **A era dos *crypto ransomwares***: um estudo de caso sobre o *wannacry*. In: Anais do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. SBC, 2017. p. 509-516.

NICOCELI, Artur. **6 ataques de cibersegurança com resgate em criptomoedas**. Revista Forbes, São Paulo, 2021. Disponível em: https://forbes.com.br/forbes-money/2021/06/6-ataques-de-ciberseguranca-com-resgate-em-criptomoedas/. Acesso em: 27 set. 2023.

PHILOT, Daniel Rocha. Segurança da informação: ataques *ransomware* e proteção de dados. 2021.

PRASAD, Ramjee; ROHOKALE, Vandana. **Cyber Security:** The Lifeline of Information and Communication Technology. Springer, 2020.

RIBEIRO, Giovanna Saturnino. **LGPD e segurança da informação em empresas**: aspectos jurídicos da prevenção dos ataques de *ransomware*. 2022.

SAISSE, Renan Cabral. ***Ransomware*:** "sequestro" de dados e extorsão digital. Disponível em: http://direitoeti.com.br/artigos/ransomware-sequestro-de-dados-e-extorsao-digital/#_edn4. Acesso em: 17 fev. 2023.

SANTOS, Renato Ferreira Jácomo dos; STEIN, Staell dos Santos. **Considerações sobre o uso de criptomoedas no financiamento ao terrorismo e seus impactos para a Segurança e Defesa nacionais**. 2022.

SILVA, Luiz Gustavo Doles et al. **A regulação do uso de criptomoedas no Brasil**. 2017.

SIMÃO, Pedro; BARRETO, Júlia; PARTIKA, Sarah. **Tributação de criptoativos:** o desafio da natureza jurídica. Portal on-line Legislação & Mercados, 2023. Disponível em: https://legislacaoemercados.capitalaberto.com.br/tributacao-de-criptoativos-o-desafio-da-natureza-juridica/#_ftn5. Acesso em: 27 set. 2023.

TOGNATO, Paulo Gustavo. ***Ransomware* em IoT**. 2020.

VAZ-FERREIRA, Luciano; RODRIGUES, Filipe Bach. **O *Ransomware* como ameaça à cibersegurança da gestão pública de dados no Brasil**: *Ransomware as a threat to cybersecurity in public data management in Brazil.* Revista Intellector-ISSN 1807-1260-[CENEGRI], v. 18, n. 35, p. 34-44, 2021.

VOLPI, Matheus Tauan; VOLPI, Murilo Alan. ***Ransomware* no ordenamento jurídico brasileiro**. Joatan Marcos de Carvalho, p. 79, 2021.

WAKKA, Wagner. **Brasil é o 2º país com mais ameaças de *ransomware* no mundo, aponta estudo**. In.: Canaltech. Publicado em 13 de março de 2019. Disponível em: https://canaltech.com.br/seguranca/brasil-e-o-2o-pais-com-mais-ameacas-de-ransomware-no-mundo-aponta-estudo-134683/. Acesso em: 16 jun. 2023.