UNIVERSIDADE FEDERAL DE OURO PRETO

ESCOLA DE DIREITO, TURISMO E MUSEOLOGIA

DEPARTAMENTO DE DIREITO

Gabriel de Andrade Vicente

A TIPIFICAÇÃO DO CRIME DE *RANSOMWARE* NO DIREITO PENAL BRASILEIRO

Ouro Preto

2022

GABRIEL DE ANDRADE VICENTE

A TIPIFICAÇÃO DO CRIME DE *RANSOMWARE* NO DIREITO PENAL BRASILEIRO

Trabalho de Conclusão de Curso apresentado ao departamento de Direito da Universidade Federal de Ouro Preto - UFOP, como requisito parcial para a conclusão do curso de Direito. Orientadora: Juliana Evangelista de Almeida

Área de Concentração: Direito Penal e Direito Digital

Ouro Preto

2022

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
ESCOLA DE DIREITO, TURISMO E MUSEOLOGIA
DEPARTAMENTO DE DIREITO

FOLHA DE APROVAÇÃO

Gabriel de Andrade Vicente

A TIPIFICAÇÃO DO CRIME DE RANSOMWARE NO DIREITO PENAL BRASILEIRO

Monografia apresentada ao Curso de Direito da Universidade Federal
de Ouro Preto como requisito parcial para obtenção do título de Bacharel

Aprovada em 07 de Junho de 2022

Membros da banca

Doutora – Juliana Evangelista de Almeida - Orientador(a) Universidade Federal de Ouro Preto

Doutora – Beatriz Schettini- Universidade Federal de Ouro Preto

Mestranda – Kelly Christine Oliveira Mota de Andrade – Universidade Federal de Ouro Preto

Juliana Evangelista de Almeida, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 07/06/2022

Documento assinado eletronicamente por **Juliana Evangelista de Almeida**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 13/06/2022, às 10:59, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0343489** e o código CRC **E2D8A773**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35400-000
Telefone: (31)3559-1545 - www.ufop.br

AGRADECIMENTOS

Agradeço a Deus pela vida que Ele me concedeu.

Aos meus pais, pelo amor, incentivo e apoio incondicional.

Agradeço à minha mãe Ângela, heroína que me deu apoio, incentivo nas horas difíceis, de desânimo e cansaço.

Obrigado meus irmãos, que nos momentos de minha ausência dedicados ao estudo superior, sempre fizeram entender que o futuro é feito a partir da constante dedicação no presente!

Sou grato a minha companheira Ester que nunca me recusou amor, apoio e incentivo. Obrigado por compartilhar os inúmeros momentos de ansiedade e estresse. Sem você ao meu lado, o trabalho não seria concluído.

A todos os meus amigos, particularmente Gabriela e Douglas, meus sinceros agradecimentos. Vocês desempenharam um papel significativo no meu crescimento, e devem ser recompensados com minha eterna gratidão.

Por último, quero agradecer também à Universidade Federal de Ouro Preto e todo o seu corpo docente.

A todos que direta ou indiretamente fizeram parte de minha formação, o meu muito obrigado.

RESUMO

A presente monografia discute a tipificação do crime de *Ransomware* dentro da legislação brasileira, mostrando como o mundo se comporta perante aos crimes virtuais e como nossas normas vêm trabalhando para julgar e punir estes crimes, bem como o Direito vem se moldando a estes novos desafios sociais e claramente, judiciais. Por meio de uma pesquisa bibliográfica, histórica, documental e da legislação vigente, reunimos fontes para mostrar a necessidade de tipificar novas condutas realizadas através da internet para prática de crimes que já causam grandes prejuízos no mundo real e virtual e entender se as punições para alguns crimes já tipificados, depois que o Brasil aderiu a Convenção de Budapeste, são realmente proporcionais e eficazes e ajudam para que o meio virtual seja mais seguro.

Palavras-chave: Crimes cibernéticos; Tipificação de crime; *Ransomware*; Legislação.

ABSTRACT

This monograph discusses the Ransomware crime typification in the Brazilian legislation, showing how the world behaves in face of virtual crimes, how our legal standards have been working to judge and punish these crimes and how the Law has been adapting to these new social and clearly legal challenges. Through a bibliographical, historical, documental and the current legislation research, we gathered different sources to show the need to typify new behaviors carried out through the internet for the practice of crimes that already cause losses in the virtual and real world and to understand if the punishments for some already legally typified crimes, after Brazil joined the Budapest Convention, are really proportionate, effective and help in order to make the virtual environment safer.

Keywords: Cybercrimes; Crime *typification*; *Ransomware*; *Legislation.*

SUMÁRIO

1 INTRODUÇÃO

É de conhecimento popular que o primeiro crime cometido no mundo foi o assassinato de Abel por Caim[1]. Entende-se que onde existe interação humana, por um motivo ou outro, é necessário que haja normas que regulamentem as diversas situações corriqueiras ou não, da sociedade. Junto com cada avanço que nota-se na nossa evolução como *homo sapiens* surgiram novas habilidades, novos objetos e novas funções sociais e principalmente as disputas por poder, território e condições favoráveis à sobrevivência de um povo.

Sempre houve alguém disposto a obter vantagens sobre o outro e isso nos perpassa desde antes da invenção da roda, na internet não seria diferente. Quando algumas pessoas descobriram que era possível manipular informações e dados virtualmente, tiveram o surgimento de uma nova onda de crimes e golpes e junto disso, a sociedade teve a necessidade de criar normas que fiscalizasse essas atuações e punisse as ações consideradas criminosas e que trazem prejuízos para o ambiente virtual e para as pessoas que dele se utilizam.

A segurança é um dos pilares mais almejados da nossa sociedade contemporânea, e com novos desafios é necessário que até ela se remodele, que se entenda que novas situações surgem e que a justiça precisa estar preparada para prever novos riscos e novas ações e muitas das vezes sentimos que os crimes tendem a se desenvolverem muito mais rápido que a norma, fazendo com que a justiça às vezes apresente dificuldades em arbitrar certos casos.

Partindo dessas reflexões, sentimos a necessidade de estudar como a sociedade evoluiu com advento da internet e junto com esta transformação analisar as novas práticas criminosas cometidas em ambiente virtual. Será discutido como a legislação penal brasileira e a doutrina entende e classifica os crimes virtuais, se existe e é eficaz a tipificação destes crimes, como a justiça brasileira, julga e dá a sociedade uma resposta para os cibercrimes e por fim demonstrar a necessidade da tipificação específica do crime de Ransomware.

Esta pesquisa foi bibliográfica, histórica e documental, procurando reunir dados acerca deste assunto e trazer mais argumentos para a discussão da tipificação de crimes cibernéticos.

---

[1] Gênesis, capítulo 4.

2 DO DIREITO PENAL CIBERNÉTICO

Inicialmente, será abordado como surgiu a internet e o caminho que percorreu para chegar até como a conhecemos nos dias de hoje, também trataremos como a internet revolucionou as formas de interação social, e junto a esta contínua inovação, nasce também novos métodos para à prática de crimes com a intenção de obter vantagens indevidas.

2.1 CONTEXTUALIZAÇÃO

O Direito Penal Brasileiro tem como finalidade realizar a tutela dos bens jurídicos elencados na Constituição Federal de 1988, no art. 5º da constituição está previsto os direitos e garantias fundamentais da pessoa humana e dentre eles destaca-se o direito à privacidade e o direito a proteção dos dados pessoais, inclusive na forma digital, mencionados nos incisos XII e também o LXXIX (BRASIL, 1988), este último adicionado recentemente pela Emenda Constitucional nº 155 de 2022.

Bem antes da promulgação da nossa carta magna outros países já possuíam agências e normas voltadas ao meio tecnológico e ao avanço científico. Ilustra-se com a ARPA (*Advanced Research Projects Agency*, ou Agência de Projetos de Pesquisa Avançada de Defesa), agência federal que foi criada nos EUA em 1957, durante a Guerra Fria, após o lançamento do primeiro satélite espacial da história, o famoso Sputnik 1 criado pela já extinta URSS (ROZA, 2008). Cabe salientar que a Guerra Fria foi marcada pelo confronto histórico da União Soviética e os Estados Unidos pela disputa por aperfeiçoamento econômico, militar, político e tecnológico.

Diante dos conflitos da guerra fria, os EUA agindo de forma preventiva, cogitaram a possibilidade de sofrerem um ataque nuclear e com isso experimentar a perda de suas informações e estudos em seus centros de inteligência, bases militares e o acervo de suas universidades.

Neste contexto e frente a tais e ameaças de devastação sofridas, os estados unidos da américa através do seu departamento de defesa, investiram em pesquisas relacionadas à comunicação e redes como uma forma de garantir a transmissão de informações no caso de sofrerem um ataque nuclear (NAVARRO, 2011). Entretanto, pode-se dizer, fica claro que as tensões sofridas durante o período da guerra fria fizeram acelerar o processo de desenvolvimento de pesquisas relacionadas a criação da comunicação através das redes de computadores.

Cabe salientar que há época dos fatos, o uso dessas redes era de acesso restrito ao público, sendo utilizadas somente pelo governo, cientistas, engenheiros e profissionais indispensáveis para o aperfeiçoamento desta ferramenta que passou por inúmeras transformações para chegar no estado atual.

Após alguns avanços, em 1966 através do plano DARPA foi criado a primeira rede interligada de troca de pacote de dados que possibilitou que a conexão entre um computador da Universidade da Califórnia (UCLA) a outro computador da *Stanford Research Institute* (SRI). Com esse avanço, o que era considerado de extrema relevância naquele século, possibilitou em apenas 4 meses mais tarde a interconexão de quatro universidades americanas, assim inaugurando a era da ARPANET.

Um pouco mais tarde em 1974, com a implementação da tecnologia de Protocolo de Controle de Transmissão e do Protocolo Internet (TCP/IP) implementada por Vinton Cerf e Robert Kahn, considerado como um divisor entre o marco anterior, este avanço proporcionou a conexão e compatibilidade de mensagens e programas de se comunicarem entre si, o que não era possível anteriormente quando se usavam a tecnologia *File Transfer Protocol* (FTP) que só permitia a interconexão através do networks (rede de trabalho) caso houvesse compatibilidade dos sistemas informáticos.

Wendt e Jorge (2012), apontam que em 1986 foi implementada pela *National Science Foundation* a *National Science Foundation Network* (NSFNET) a transição do nome da ARPNET para *International Network* conhecida popularmente nos dias de hoje como Internet. Sob essa ótica, constata-se que na década de 80 a internet atingiu uma escala global de conexão de computadores, sendo considerada como a principal rede de comunicação do mundo com alcance de grande proporção.

No final dos anos 80, o cientista inglês Tim Berners-Lee que trabalhava na Organização Europeia para Pesquisa Nuclear (*European Organization for Nuclear Research*) foi o responsável pelo desenvolvimento de um sistema capaz de transmitir textos, imagens, sons e o outras mídias através da Internet, o popularmente conhecido como WWW ou 3W, cujo a expressão significa Rede de Alcance Mundial (*World Wide Web)* e o acesso se dá através de ligações (*links*) que nos direciona para determinada página na *web* conectada a Internet.

Neste ínterim, foi criado os famosos navegadores de internet (*browsers*) e demais programas e aplicativos com diversas finalidades sendo que a partir deste marco que a internet deixou de ser utilizada como ferramenta privada sob controle do governo norte-americano e se popularizou conectando pessoas de todas as partes do mundo inclusive inaugurando a era do comércio digital (*e-commerce*).

Diante das tensões geradas pela guerra fria, a internet revolucionou as formas de comunicação de todo mundo, inaugurando uma forma de levar informações livres e independentes e sua utilização nos possibilita levar informações a ao outro lado do planeta em frações de segundos.

Juntamente com a evolução social, os avanços da tecnologia e sobretudo o da informática, nasce também as novas formas de cometer antigos crimes, o que afetou rapidamente o Direito das pessoas, independentemente de quem aderiu ou não a esta nova ferramenta de transformação social.

A utilização da internet se tornou um meio para a realização de crimes cibernéticos, o que é explorada por pessoas má intencionadas a fim de obter vantagens indevidas. Assim, surgem lacunas no sistema jurídico-penal para a efetiva punição desses delitos, pelo fato do Direito não conseguir acompanhar na mesma velocidade as evoluções sociais, o que acaba gerando uma falsa sensação de impunidade e estimulando a prática de novos crimes em ambiente virtual.

2.2 DO CONCEITO DE CRIMES CIBERNÉTICOS

Na década de 1960 tiveram os registros dos primeiros casos de crimes virtuais, com manipulação de dados contidos nos computadores, resultando em sabotagem, espionagem e abuso ilegal dos sistemas de computadores, praticas difíceis de serem detectadas e punidas devido as tecnologias e condições técnicas disponíveis na época. Em 1980, surgiram mudanças mais categóricas sobre o tema, visto que foram identificados mais crimes cometidos virtualmente, de tal forma que diversos países buscaram criar legislações para regulamentar e punir os crimes.

Os Estados Unidos da América iniciaram essa importante mudança, quando em 1984 editaram a legislação "*Crime Control Act*" e na sequência o "*Computer Fraud and Abuse Act*", em 1986. A Alemanha, em 1986, editou a Lei "*Computer Kriminalitat*", seguida da França que em 1988 editou a Lei *Godfrain*. Anos depois, em 1995 a Espanha incluiu crimes de informática na reforma do seu Código Penal. Em 23/11/2001, o Conselho da Europa (*Council of Europe*), elaborou a Convenção Europeia sobre Crimes Cibernéticos, objetivando uniformizar a legislação europeia quanto à política criminal dos crimes cibernéticos, contudo, esta convenção será devidamente discutida logo adiante.

O entendimento é de que o conceito de crimes cibernéticos abrange amplamente qualquer ofensa criminal realizada por meio do acesso à internet. Com o governo, indústrias,

mercados e consumidores cada vez mais dependentes de conectividade, eles são propensos a uma série de ameaças (CABETTE, 2013). As práticas criminosas e seus resultados podem se enquadrar em uma conceituação de crimes virtuais como pornografia, furto de propriedade intelectual, investidas orquestradas a grandes redes de computadores e resultar em criminosos convencionais nos casos em que as provas se encontram em formato digital.

Rocha (2013) organiza os tipos criminais em grandes eixos, sendo eles: a interferência no uso legal de um computador; divulgação de materiais ofensivos; ameaça a comunicações; falsificação; fraude e outros crimes como interceptação ilegal de comunicações; comercial/corporativo espionagem; comunicações em promoção de conspirações criminosas; lavagem de dinheiro.

Todas essas ações parecem remeter ao que conhece tradicionalmente como crimes, em nossa esfera material, embora sejam executados com muito mais facilidade, rapidez e produzam um impacto por muita das vezes sem precedentes em todos os âmbitos jurídicos, sendo assim os meios de se responder a tais atos são dirigidos pelas novas disciplinas tecnológicas. Encontrar, identificar e penalizar cibercriminosos são enormes desafios à justiça em todo canto do mundo, exigindo cooperação de diversos órgãos e saberes oriundos das novas tecnologias.

Estudiosos em prevenção aos crimes contextualizados no comércio eletrônico ponderam que, virtualmente, o furto de informação e manipulação de identidade e confiança são os personagens principais e as armas mais utilizadas (PAESANI et al., 2009, p.79).

2.3 TIPOS DE CRIMES CIBERNÉTICOS

Antes de mais nada, salienta-se a diferença da figura do hacker da figura do *cracker*, o que é usualmente confundido no linguajar popular. Os *Hackers* são pessoas que se dedicam a encontrar falhas e vulnerabilidades em sistemas e programas de empresas privadas e de governos com o intuito de avisá-los e corrigir determinados defeitos de segurança e muitas das vezes são recompensados por isso, agindo de boa-fé e dentro da legalidade.

Todavia os *Crackers* buscam explorar as vulnerabilidades de segurança encontradas em sites, sistemas de segurança, perfis de redes sociais contra governos e suas autoridades, empresas privadas e pessoas naturais com o intuito de obterem vantagem, econômicas ou não, de forma ilícita, utilizando de seus conhecimentos para cometimento de delitos e causar determina agressão a algum bem jurídico tutelado de outrem, agindo de má-fé e na ilegalidade. Neste mesmo entendimento nos ensina Rogério Greco:

> Aquele que tem conhecimento e habilidade suficientes para violar mecanismos de segurança, invadindo dispositivo informático alheio, é chamado de hacker.

> Conforme lições de Sandro D'Amato Ogueira, "este indivíduo em geral domina a informática, é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade cometer crimes; costumam se desafiar entre si, para ver quem consegue invadir tal sistema ou página na internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual". Por outro lado, existe, também, a figura do cracker, que, ainda de acordo com os ensinamentos de Sandro D'Amato Ogueira, é aquele que usa a internet para cometer crimes, fraudes bancárias e eletrônicas, furto de dados, golpes e grandes estragos. São verdadeiras quadrilhas de jovens que não se contentam apenas em invadir um sistema, usam sua inteligência e domínio da informática para causar prejuízos de milhares de reais, tanto contra pessoas físicas, como jurídicas, órgãos públicos etc. Diversas são as técnicas, métodos, recursos e/ou ferramentas existentes e que são utilizadas pelos criminosos para o cometimento de delitos virtuais e/ou cometidos em ambientes virtuais, porém serão explanadas as tidas como mais relevantes relacionadas com a finalidade deste trabalho. No entanto, apesar de que muitas dessas técnicas, métodos, recursos e ferramentas existentes possuam propósito malicioso, nada impede que sejam utilizadas para outros fins diversos. Cabe observar também que algumas delas não possuem 15 finalidade maliciosa e sim determinadas pessoas as utilizam para o cometimento de crimes. (GRECO, 2013B, p. 1)

Na sequência, cumpre destacar que os crimes informáticos possuem diversas denominações, tais como: crimes cibernéticos, crimes virtuais, crimes digitais, dentre outros. Logo, para que seja configurado um cibercrime é necessário que haja uma violação a um bem jurídico devidamente tutelado pelo direito mediante conduta cometida ou facilitada através da internet.

Vale destacar que existem duas divisões a respeito dos cibercrimes, sendo eles são considerados como puros (ou próprios) ou impuros (ou impróprios) que serão explanados logo a seguir.

2.3.1 Crimes puros (ou próprios)

Os crimes puros ou também chamado de crimes próprios, são aqueles que buscam afrontar diretamente dispositivos informáticos tais como o sistema operacional[2], os *hardwares* [3]e ou os *softwares*[4] de um dispositivo contra uma ou várias vítimas, com o objetivo de causar

[2] Refere-se a um ou mais softwares que tem como papel central gerenciar e ainda administrar todos os recursos presentes em um sistema.
[3] Os hardwares são as peças físicas que compõem um computador, como as placas, o monitor, o teclado, a placa-mãe e o disco rígido.
[4] Um software é todo programa presente nos diversos dispositivos (computadores, celulares, televisores, entre outros)

um prejuízo que pode ser da esfera patrimonial, moral e/ou social. Neste mesmo diapasão nos ensina o estudioso Spencer Sydow:

> Delitos informáticos próprios são as condutas típicas antijurídicas e culpáveis que apenas podem utilizar-se de ferramenta informática. Podem visar atingir um sistema informático ou seus dados, precisamente violando sua confidencialidade, sua integridade ou sua disponibilidade (puros) e também podem visar atingir bens comuns através de estratégias informáticas (impuros, p. ex. patrimônio, via *Ransomware*). (SYDOW, 2022, p. 27).

Via de regra os crimes próprios são os crimes de invasão, modificação ou alteração em software ou hardware de computadores (Art. 154-A do Código Penal). Para melhor ilustrar os crimes puros, pode-se citar os seguintes exemplos de crimes: *Os Malwares* (programas maliciosos) são como um gênero e suas demais ramificações como espécie, uma vez que a palavra malware engloba vários tipos de programas que tem como objetivo comum causar algum prejuízo a vítima, neste mesmo raciocínio define Moisés Cassanti:

> O termo malware é a contração de "malicious software" programa malicioso e identifica qualquer programa desenvolvido com o propósito de causar dano a um computador, sistema ou redes de computadores. É um dos tipos de intrusos que podem invadir o seu computador (o outro é o próprio atacante). Os mais comuns são os vírus, worms e cavalos de Tróia. Geralmente se utilizam de ferramentas de comunicação conhecidas para se espalharem – como, por exemplo, worms enviados por e-mail e mensagens instantâneas, cavalos de Tróia provenientes de websites e arquivos infectados por vírus obtidos por downloads de conexões ponto-a-ponto. O malware também tenta explorar as vulnerabilidades existentes nos sistemas, tornando sua entrada discreta e fácil. (CASSANTI, 2014, p. 8).

O crime de *phishing* (pescaria) é um dos delitos informáticos mais antigos e conhecidos em ambiente virtual, ele tem como objetivo obter de forma fraudulenta quaisquer tipos de informação pessoal da vítima. Geralmente eles vêm através de: e-mails, links de redes sociais, compartilhamento de mensagens em massa, faturas bancárias, descontos exorbitantes, etc., fazendo com que a vítima clique em um link, ou faça download de determinado anexo e insira suas informações pessoais, assim entregando dados pessoais, dados de cartão de crédito, senhas dentre outros para os criminosos.

O *Ransomware*, objeto central desta pesquisa que melhor será explorado no próximo capítulo, também conhecido como sequestro de dados, é de um longe um dos crimes que mais surte efeitos danosos nas vítimas. Basicamente ele consiste na invasão de um sistema, realizando o bloqueio e criptografando seus dados e exigindo uma certa quantia financeira a título de resgate que na maioria das vezes são através de moeda virtual, assim dificultando sua rastreabilidade.

Entende-se que os crimes próprios são aqueles que tem por objetivo atacar o próprio sistema computacional da vítima, onde a execução e a consumação do delito se dão através do próprio meio digital, e que nos dias de hoje pode se dar por meio de dispositivos diversos ao computador, como smartphones, TV com conexão à internet, tablets, dentre outros dispositivos informáticos.

2.3.2 Crimes impuros (ou impróprios)

Por outro lado, os crimes impuros ou também chamado de crimes impróprios, são aqueles que se utilizam da internet como um instrumento para a prática de crimes que repercutem diretamente na vida real do ofendido, e assim como os delitos puros também tem como o objetivo de causar um prejuízo patrimonial, moral, e/ou psicológico em suas vítimas, com este mesmo entendimento Spencer Sydow preceitua:

> Delitos informáticos impróprios são delitos comuns, portanto condutas típicas, antijurídicas e culpáveis, que são perpetradas utilizando-se de mecanismos informáticos como ferramental, sendo que outros meios poderiam ter sido igualmente eleitos para a prática. São, pois, delitos de forma livre. (SYDOW, 2022, p. 27).

A título de exemplo, pode-se citar os seguintes crimes como impróprios: *Porn Revenge*: O Porn revenge (pornô de vingança) consiste na realização de ameaçada de divulgação de conteúdos de fotos e/ou vídeos íntimos de um casal, muita das vezes este crime for cometido pelo ex-companheiro(a) da vítima por não aceitar o fim de um relacionamento.

*Sextorsion***:** O delito de *sextorsion* (extorsão sexual) é cometido por um infrator através da exigência de cenas ou fotos de caráter íntimo de uma ou mais pessoa, ou qualquer outra vantagem libidinosa em troca de não divulgar determinado arquivo ou informação que possa vir a prejudicar a vida dessa pessoa.

Portanto, os delitos impróprios utilizam da internet como uma ferramenta para potencializar um resultado que prejudica algum bem juridicamente tutelado pela legislação penal brasileira. Por fim, nota-se que o que altera é o *modus operandi* na internet do criminoso, com o intuito de cometer antigos crimes, porém de novas formas.

2.4 ASPECTOS RELACIONADOS À ADESÃO DO BRASIL À CONVENÇÃO DE BUDAPESTE

A Convenção sobre o Crime Cibernético, popularmente conhecida como Convenção de Budapeste, foi celebrada em novembro de 2001 entrando em vigor em 01 de julho de 2004, na capital da Hungria. O Brasil aderiu à convenção em 15 de dezembro de 2021, com a aprovação do Senado. Esta organização visa criar uma maior cooperação dos países para combater os crimes virtuais, sendo elaborada pelo Comitê Europeu para os Problemas Criminais com abrangência no direito penal e no direito processual penal.

O documento elaborado elenca os crimes mais cometidos por meio da rede mundial e foi o primeiro tratado mundial sobre crimes virtualmente cometidos, discutindo a criminalização de condutas, as normas necessárias para investigar e produzir provas eletrônicas e os meios possíveis para que os países cooperem entre si e combatam os crimes por meio de um regime universal de normas:

> A prática do crime é tão antiga quanto a própria humanidade. Mas o crime global, a formação de redes entre poderosas organizações criminosas e seus associados, com atividades compartilhadas em todo o planeta, constitui um novo fenômeno que afeta profundamente a economia no âmbito internacional e nacional, a política, a segurança e, em última análise, as sociedades em geral. (CASTELLS, 2007, p. 203.)

Os tópicos de violações de direitos autorais, fraudes relacionadas ao acesso à internet pelo computador, pornografia infantil e violações de segurança de rede, são bem discutidos neste documento. Como posto em seu preâmbulo, a Convenção privilegia “uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional” como meio de reconhecer “a necessidade de uma cooperação entre os Estados e a indústria privada”. O Brasil não é signatário da Convenção de Budapeste, como foi criada por países Europeus, o Brasil só entrou como membro e teve sua participação efetivada anos depois.

3 DO CRIME DE *RANSOMWARE*

Neste capítulo será abordado a origem e de como funciona o crime de *Ransomware*, bem como seus impactos, aplicabilidade, previsões legislativas e ainda analisar a necessidade de sua tipificação no sistema jurídico penal brasileiro, e por fim de analisar como é tratado por outros ordenamentos jurídicos.

3.1 CONCEITUAÇÃO HISTÓRICA ACERCA DO *RANSOMWARE* (SEQUESTRO DE DADOS

A palavra *Ransomware* é uma conjugação da palavra "*ransom*" (resgate/valor pago a alguém) e do vocábulo "*malware*" (software malicioso) que originam a palavra *Ransomware*. O *Ransomware* é um vírus da classe do *malware* que age invadindo um dispositivo informático e criptografa os seus dados e tem como objetivo obter vantagem financeira, acesso a dados e informações privadas que supostamente será liberada mediante o pagamento de uma quantia financeira à título de resgate, e que normalmente se dá através da moeda virtual *bitcoin* ou outra criptomoeda, pelo fato de ser um mercado onde não existe rastreabilidade das transações facilitando o anonimato dos criminosos.

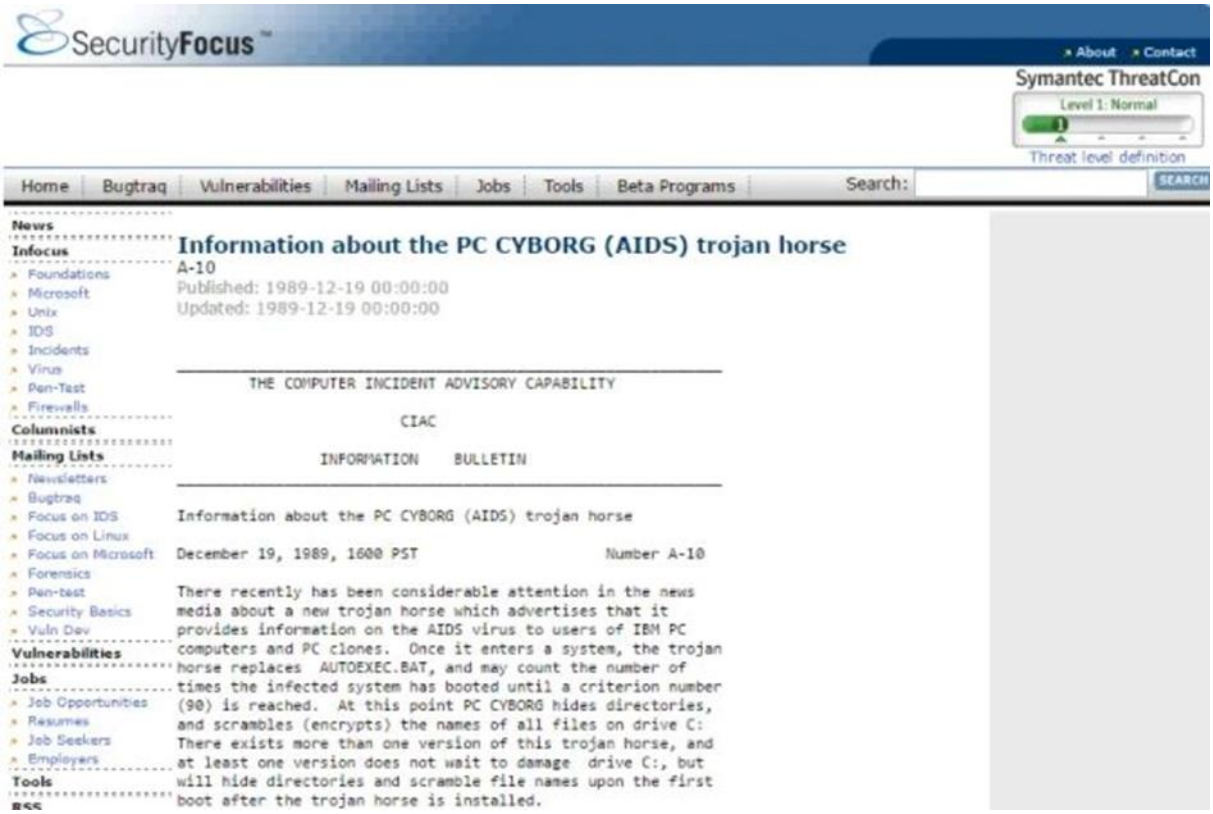
No ano de 1989 surgiu o primeiro registro de *Ransomware* na história, conhecido como *PC Cyborg* ou *Trojan* AIDS, este malware foi desenvolvido por Joseph Popp um cientista americano que distribuiu cerca de 20.000 disquetes ao redor do mundo para pesquisadores do vírus da AIDS, doença que era febre na época de sua aparição.

Joseph Popp enviou através dos disquetes distribuídos aos demais pesquisadores um questionário que alegava servir para analisar os riscos de um indivíduo de contrair o vírus, porém, além do suposto questionário, tinha também um malware que vinha camuflado no disco rígido e só era ativado após a nonagésima inicialização do computador. A partir daí o programa surgia exigindo o pagamento de um resgate no valor de $189,00 que deveria ser feito para uma caixa postal no Panamá, por utilização de um determinado software e impedindo a utilização de demais ferramentas do sistema.

A descoberta dos efeitos do programa foi feita por Eddy Willem, que trabalhava em uma seguradora médica e recebeu o disquete de seu chefe, que resolveu explorar o disco pelo fato do título do dispositivo ser "AIDS versão 2.0" o que parece misterioso e poderia ser explorado como fonte de dados. Assim, foi determinado a Eddy que o mesmo analisasse o conteúdo dos dados ali presente com foco em obter vantagens para a empresa. Após constatar que o golpe se

tratava de uma criptografia mal feita por alguém que não era um profissional da área de TI, rapidamente encontrou a solução para o problema descriptografando os dados do computador e restaurando o seu sistema.

Figura 1 - Imagem do primeiro *Ransomware* registrado



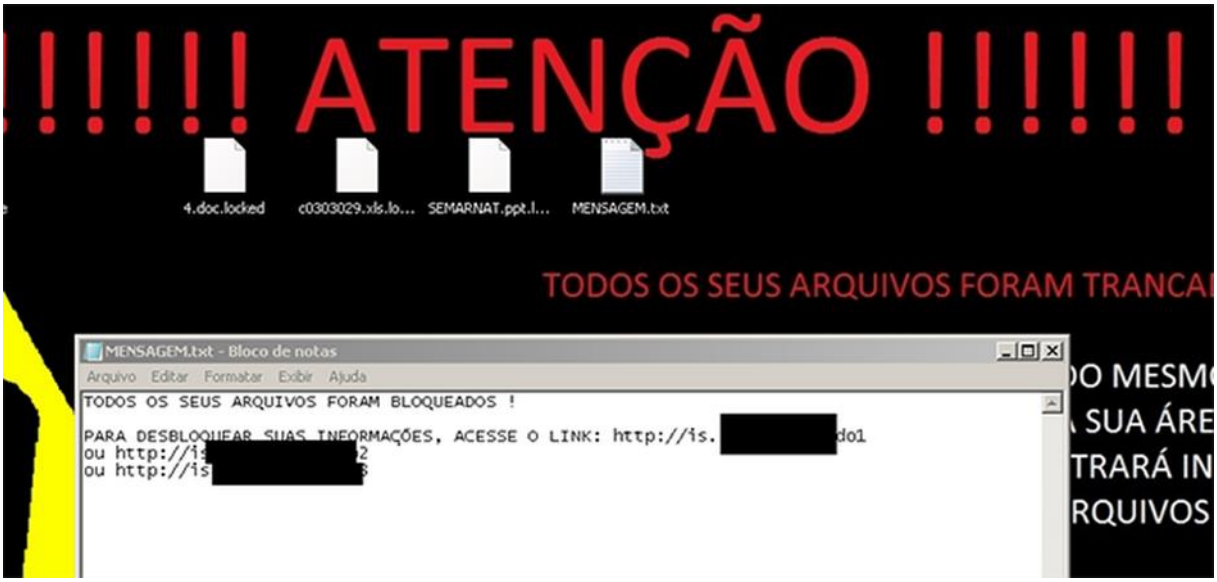
Fonte: 1989: O primeiro Ciberataque de Ransomware do Mundo. Dereco Tecnologia. 11 de fevereiro de 2022.

Apesar da rápida solução encontrada por Willems, os disquetes causaram um verdadeiro caos na época de sua aparição, tendo em vista que foi direcionada a um público alvo específico que era a comunidade científica que estava ligada a pesquisas médicas em busca da cura ao vírus da AIDS. Após ser descoberto, o autor dos fatos, Popp, foi preso pela polícia de *New Scotland Yard* por disseminar o vírus acusado de chantagem a diversas autoridades cumprindo pena na prisão de Brixton (SAISSE, 2017).

Em janeiro de 2016 foi divulgado pela empresa de segurança digital *Kapersky Lab* um *Ransomware* de origem brasileira onde induzia os usuários a acreditarem a realizar uma atualização do software *Adobe Flash Player*, famoso programa de uso cotidiano, onde após clicar em um link o computador era infectado pelo vírus criptografando seus dados e exigindo o pagamento de uma quantia de aproximada de R$ 2.000,00 (dois mil reais) através da moeda virtual *bitcoins*.

No Brasil, o caso de maior destaque foi em fevereiro de 2017 através do *Ransomware* conhecido *WannaCry* (Quero Chorar), sendo que este foi capaz de infectar mais de 200 mil computadores e atingir mais de 150 países ao redor de todo o planeta, atingindo grandes marcas como a Nissan, FedEx e a Renault. Durante o ataque foi "sequestrado" dados de diversas instituições públicas como o INSS, o STJ, TJ-RS e também o Ministério Público de São Paulo, onde este último decidiu desligar seus dispositivos da rede de energia na tentativa de frear e diminuir os prejuízos suportados, estima se que à época dos fatos o prejuízo causado ao redor do mundo chega a cerca de 4 bilhões de dólares.

Figura 2 - Registro do ataque do *WannaCry* no Brasil



Fonte: **Wannacry.** Ciberataque de Ransomware do Mundo.16 de maio de 2022.

Vale ressaltar que o golpe por trás deste crime demonstra ser altamente lucrativo para seus operadores, sendo que no ano de 2013 através do *Ransomware* mais temido de codinome *CryptoLocker*, foi arrecadado cerca de 42 mil *bitcoins* (o que equivalia a aproximadamente à 27 milhões de dólares em 2015) o que se torna extremamente expressivo até nos dias atuais. Portanto, conforme exemplificado acima, o cyber ataque através do *Ransomware*, tem como principal público alvo empresas privadas e órgãos da administração pública, sendo que estes, detém de maior poder econômico e geralmente têm armazenado em seus dispositivos informáticos, maiores dados e informações valiosas do que uma pessoa natural.

3.2 DA NECESSIDADE DE TIPIFICAÇÃO DO CRIME DE *RANSOMWARE*

Acima de tudo, é importante tecer como a legislação brasileira e a legislação penal pátria visa tipificar determinadas condutas como crimes cibernéticos ou cometidos ou através da rede

mundial de computadores, são diversas as leis que tratam sobre o tema no nosso ordenamento, porém será abordado aqui somente as que se demonstram de maior relevância no que tange aos crimes cibernéticos, sobretudo o *Ransomware*.

Considerada como a lei principal que visou tipificar diversos crimes cibernéticos, a Lei 12.737 de 2012 comumente conhecida como Lei Carolina Dieckmann, incluiu no Código Penal a punição de crimes cometidos em ambiente virtual, neste condão preceitua Damásio de Jesus:

> Apelidada de "Lei Carolina Dieckmann", a Lei n. 12.737/2012, que tipifica os crimes cibernéticos, adveio do projeto de Lei n. 2.793/20115, sendo agilizado no início de 2013 pelo "casuísmo em que fotos íntimas da atriz teriam sido supostamente copiadas de seu computador e divulgadas na internet". Na verdade, a legislação veio atender a uma demanda antiga do setor financeiro, duramente impactado com os golpes e fraudes eletrônicas, ainda que considerada uma lei absolutamente "circunscrita", em comparação aos projetos sobre crimes cibernéticos que tramitam no congresso nacional. Entendeu-se em aprovar uma lei menor, com pontos menos polêmicos, a não ter nada regulamentando crimes cibernéticos, eis que, diz o ditado, a lei é como remédio, deve ser ministrado em doses, pois se ministrarmos tudo de uma vez, podemos matar o paciente. (JESUS, 2016, p. 85)

Através da lei em questão, foi tipificado pelo Código Penal os crimes de Invasão de dispositivo informático (Art. 154-A); Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (Art. 266); Falsificação de documento particular, Falsificação de cartão (Art. 298), conforme descritos abaixo:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: (Incluído pela Lei nº 12.737, de 2012)
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (Incluído pela Lei nº 12.737, de 2012)
> §1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. (Incluído pela Lei nº 12.737, de 2012)
> §2º Aumenta-se a pena de um sexto a um terço se da invasão resultar prejuízo econômico. (Incluído pela Lei nº 12.737, de 2012)
> §3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012) Vigência Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (Incluído pela Lei nº 12.737, de 2012)
> §4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas. (Incluído pela Lei nº 12.737, de 2012)

> §5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: (Incluído pela Lei nº 12.737, de 2012)
> I - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012)
> II - Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012)
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou (Incluído pela Lei nº 12.737, de 2012)
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Incluído pela Lei nº 12.737, de 2012)
> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa.
> §1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. (Incluído pela Lei nº 12.737, de 2012)
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública. (Incluído pela Lei nº 12.737, de 2012)
> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro: Pena - reclusão, de um a cinco anos, e multa.
> Falsificação de cartão (Incluído pela Lei nº 12.737, de 2012)
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. (Incluído pela Lei nº 12.737, de 2012) (BRASIL, 1940)

Para tanto as penas impostas tinham o intuito de inibir a prática de determinadas condutas que inicialmente não eram expressamente previstas no Código Penal, e só era como ainda são trazidas à discussão pelo congresso após impactos sociais e econômicos de grande repercussão.

Recentemente no Brasil este tipo de ação recebeu uma atenção do legislador, que com a promulgação da lei 14.155/2021 sancionada em maio de 2021, em que alterou a Lei Carolina Dieckmann, tornou mais gravosos os crimes de violação de dispositivo informático, furto e estelionatos cometidos de forma eletrônica ou pela internet. Assim, prevendo penas mais severas no cometimento desses crimes em ambientes digitais.

Nos dias de hoje o art. 154-A do Código Penal (BRASIL, 1940), previsto na seção dos crimes contra a inviolabilidade dos segredos, prevê uma pena de reclusão de 1 (um) a 4 (quatro) anos, e dispõe em seu §2º o aumento de pena de 1/3 a 2/3 quando houver prejuízo econômico, que se dá no caso do pagamento do “resgate” dos dados sequestrados, e já no §3º este dispõe que, se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

A legislação penal brasileira que abarca os crimes digitais foi recentemente modificada com o intuito de prevenir e tornar mais gravosos os crimes de violação de dispositivo informático.

Entretanto, é importante frisar que além do delito de invasão de dispositivo informático previsto no art. 154-A do Código Penal, o crime de *Ransomware*, através do seu *modus operandi* se assemelha a outros crimes previstos na legislação penal, como o crime de extorsão mediante sequestro, estelionato e também o crime de falsidade ideológica, ambos previstos nos artigos 159, 171 e 299 do Código Penal, que segue:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
> Art. 159 - Sequestrar pessoa com o fim de obter, para si ou para outrem, qualquer vantagem, como condição ou preço do resgate:
> Pena - reclusão, de oito a quinze anos.";
> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.";
> Art. 299 - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante**:**
> Pena - reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, se o documento é particular.

> Parágrafo único - Se o agente é funcionário público, e comete o crime prevalecendo-se do cargo, ou se a falsificação ou alteração é de assentamento de registro civil, aumenta-se a pena de sexta parte. (BRASIL, 1940)

Nos crimes de extorsão mediante sequestro, estelionato e falsidade ideológica, a legislação penal nada diz a respeito sobre o modo a serem cometidos virtualmente, e nos reforça sobre o princípio da taxatividade que afirma que a lei penal deve ser clara e precisa e não pode ser analisada de forma extensiva, principalmente em casos que agrave a condição do réu.

A norma penal deixa certas lacunas a respeito da tipificação penal do *Ransomware*, bem como a possibilidade de existir obscuramente um possível concurso formal de crimes, o que reforça a tese da necessidade de sua tipificação em específico, o que poderia afetar diretamente a pena prevista para sua conduta, já que estamos diante de uma verossimilhança, e neste mesmo diapasão nos ensina Masseno e Wendet:

> [...] há que se ponderar que, dentre os dois últimos delitos citados, é muito mais comum e factível a ponderação e capitulação em relação ao delito de estelionato. Porém, é necessário ter em conta que, em nenhum dos casos, há previsão normativa especificamente orientada e dirigida para os aspectos tecnológico-digitais (MASSENO e WENDT, 2017).

Ademais, no crime de extorsão mediante sequestro os bens jurídicos devidamente tutelado pelo ordenamento jurídico são o de patrimônio e o da liberdade, já no crime de estelionato o bem protegido é a inviolabilidade do patrimônio, particularmente, em relação a atentados praticados mediante fraude, portanto percebe-se que ambas tutelas são análogas ao objetivo final do crime de *Ransomware*, atingir o patrimônio da vítima, o que evidência a necessidade de uma atenção especial a este delito.

Ressalta-se, que é importante frisar que o ataque cibernético através do *Ransomware* pode trazer inúmeros prejuízos, não só para as vítimas, mas também para toda a sociedade, tendo em vista que pode colocar em risco a segurança nacional de um país, o seu sistema de saúde, telecomunicação, economia e outros. A obtenção de informações sigilosas descritas no art. 154-A a nível governamental, pode desencadear graves problemas para uma nação perante todo o mundo.

Rogério Greco (2013B), importante jurista brasileiro, traz o conceito de informação sigilosa, informação e documento para a administração pública, dispostos no artigo 4º da Lei nº 12.527/11 (Lei de Acesso à Informação):

> Art. 4º Para os efeitos desta Lei, considera-se:
> I - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
> II - Documento: unidade de registro de informações, qualquer que seja o suporte ou formato;

> III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado. (BRASIL, 2011)

Contudo, a obtenção de informações através de espionagem governamental ou industrial, é uma realidade que não pode ser negada, e pode facilmente ser atacada por *Ransomware*. É sabido que as agências de inteligência estão em contínua melhoria de segurança, porém vulnerabilidades em sistemas informáticos governamentais, pode gerar uma onda de ataques motivados por crenças políticas, religiosas ou econômicas.

Para demonstrarmos melhor a situação fática narrada, cita-se o ataque ao metrô de São Francisco, que ocorreu nos Estados Unidos em 2016, onde criminosos invadiram o sistema de segurança, assim liberaram as catracas e houve relatos de furtos de dados. Também no ano de 2016, o alvo desta vez foi o hospital em Kansas (EUA), o mesmo sofreu dois ataques que impediram os funcionários de terem acesso aos arquivos, prontuários médicos e arquivos financeiros do hospital gerando um “estado de emergência interna”. Poucos meses depois, no início de 2017, um hotel na Áustria sofreu um ataque que invadiu o sistema de fechaduras eletrônicas, impedindo os clientes de entrarem ou saírem de seus quartos.

Nesta mesma esteira, o ataque por *Ransomware* conhecido como o *WannaCry* que atingiu o brasil em maio de 2017, surgiu após o vazamento por hackers de uma falha de segurança no sistema operacional *Windows* que já era de conhecimento do governo norte americano.

Em conformidade com o professor Damásio, percebe-se que inicialmente é necessário que haja uma onda de delitos informáticos, que geralmente envolvem artistas famosos, sendo na maioria das vezes através da exposição pornográfica, ou que gerem grandes prejuízos econômicos à influentes companhias para que a legislação penal informática possa ter a devida atenção e reagir pelo meio de um poder legislativo tardio para que assim se evite maiores prejuízos (SYDOW, p. 88 2022).

Desta forma, o crime previsto no art. 154-A do Código Penal (BRASIL, 1940), nos aparenta deixar implícito a tipificação do crime de *Ransomware*, bem como a pena estabelecida não apresenta compatibilidade com a gravidade do crime que se assemelha ao delito de extorsão mediante sequestro e estelionato, o que corrobora a necessidade de sua tipificação específica.

3.3 A TIPIFICAÇÃO DO *RANSOMWARE* EM OUTROS PAÍSES

Numa perspectiva antagônica, diante de uma ameaça global e a fim de evitar o caos institucional, o cenário internacional reconhece a importância da legislação penal informática e busca agir de forma preventiva no combate ao CyberCrime. Ademais, existem alguns países que saíram na frente do Brasil e inovaram seus ordenamentos jurídicos dando a atenção necessária no que tange aos delitos informáticos, em especial ao crime de *Ransomware*.

O país norte americano dos Estados do Unidos através do estado da Califórnia, tipificou o crime de *Ransomware* e este está previsto na (Section 523 (c) do Penal Code, que se encontra em vigor desde o início do ano de 2017):

> "Ransomware" significa um contaminante/vírus de computador, como definido na seção 502, ou como bloqueio de acesso ou introduzido sem autorização em um computador, sistema de computador ou rede de computadores que restringe o acesso por uma pessoa autorizada ao computador, sistema de computador ou rede de computadores, ou a qualquer dado dentro do computador sob circunstâncias em que a pessoa responsável pela colocação ou introdução do Ransomware exige pagamento em dinheiro ou outra consideração/compensação para remover o contaminante/vírus, restabelecer o acesso ao computador, sistema de computador, rede de computadores ou aos dados, ou caso contrário remediar o impacto do contaminante/vírus do computador ou bloqueio.(Tradução nossa)

Exemplificando com um país europeu, Portugal, após a promulgação da Lei n. 109/91, reconhecida como *Lei da Criminalidade Informática*, este passou a adotar e a interpretar a aplicação de regulamentos normativos da União Europeia, em especial a *Convenção do Conselho da Europa Sobre o Cibercrime*, popular Convenção de Budapeste que visa uma cooperação internacional de vários países ao combate à criminalidade virtual, conforme tratada no sub capítulo 2.4 desta monografia, corroborando esta análise:

> Assim, no que se refere a Portugal, temos à disposição o *Código Penal* (de 1995, com múltiplas atualizações), a *Lei do Cibercrime* (Lei n. 109/2009, de 15 de setembro) e, também, a *Lei da Proteção de Dados Pessoais* (Lei n. 67/98, de 26 de outubro). A este propósito, é necessário ter em atenção que, desde a *Lei da Criminalidade Informática* (Lei n. 109/91, de 17 de agosto), o conteúdo do Direito português resulta essencialmente da aplicação ou transposição de Instrumentos Normativos de origem europeia, os quais revelam também para a interpretação das Leis nacionais. Nomeadamente, nos importam a *Convenção do Conselho da Europa Sobre o Cibercrime*, adotada em Budapeste, a 23 de novembro de 2001, e a Diretiva 2013/40/UE, do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativamente aos ataques contra os sistemas de informação. (MASSENO; WENDT, 2017)

Em sentido oposto, o Brasil, que se tornou signatário da convenção de Budapeste somente no fim de 2021, mostra que vem evoluindo a passos lentos no que diz respeito a

legislação penal cibernética, tendo em vista que conforme demonstrado ao longo deste trabalho, o processo legislativo, em especial o penal, só sofre modificações após influências externas de grande repercussão ou que envolvem grandes prejuízos econômicos, assim como ocorreu com a promulgação da Lei Carolina Dieckmann (Lei 12.737/2012, de 30 de novembro), recentemente alterada pela Lei 14.155/2021 para tornar mais gravosos os crimes cometidos em ambiente virtual.

Visualiza-se que alguns países solidificaram e inovaram em seus regulamentos e deram a atenção devida à legislação penal e segurança cibernética, com o objetivo de punir adequadamente os criminosos que utilizam dessa indispensável ferramenta de comunicação para a prática de delitos virtuais.

4 CONCLUSÃO

Após realizar esta pesquisa entende-se que a Justiça não caminha de mãos dadas com a evolução social, muitos fatos ocorridos socialmente demoram a ser refletidos nas normas. Deve-se sempre raciocinar de que a internet é um espelho e álter ego da sociedade, o que acontece em meio a rede mundial de computadores é uma explanação do que vemos no mundo real, e se não buscarmos agir com uma justiça que solucione problemas em todos os âmbitos não terá uma justiça concreta, pois em alguns aspectos, em alguns lugares a justiça não estará protegendo seus cidadãos.

Conforme tratado ao longo desta pesquisa, a falta de regulamentação específica e a verossimilhança do delito previsto no artigo 154-A com outros crimes já tipificados no Código Penal (BRASIL, 1940), deixa dúvidas acerca de sua aplicação bem como a efetiva punição deste crime, o que nos demonstra que o poder legislativo brasileiro, em matéria penal informática, só funciona mediante pressão social e econômica, demonstrando que age de forma corretiva ao invés de preventiva.

Essa situação exposta implica na falta da devida discussão com especialistas no assunto, o que reflete em diversas leis que nem sempre são eficazes para combater e punir adequadamente os delitos comentos em ambiente virtual, sendo que e atingem diretamente a sociedade e a economia do país por falta da atenção necessária, dificultando o poder judiciário de julgar e punir apropriadamente os criminosos digitas.

Logo, a punição prevista no art. 154-A do Código Penal (BRASIL, 1940) não se justifica ao passo que geralmente o objetivo do criminoso se consuma do mesmo modo que se fosse realizado de maneira tradicional, porém na internet, tem-se o agravante da facilidade do anonimato e a exclusão dos rastros digitais, o que dificulta na identificação dos autores dos delitos, que muitas das vezes ultrapassam fronteiras e são cometidos do estrangeiro.

Deve-se conscientizar o poder legislativo e a segurança nacional brasileira sobre a potencial devastação social que este CyberCrime pode causar, tendo em vista que por não ser de fácil rastreabilidade, principalmente quando iniciado no estrangeiro como geralmente ocorre no crime de *Ransomware*, este ilícito pode servir como um meio de financiamento de organizações criminosas, quadrilhas armadas, lavagem de dinheiro, tráfico humano, manipulação de pleitos políticos, terrorismo, dentre outros crimes no ciberespaço. Após a recente adesão do brasil a convenção de Budapeste, que visa a cooperação mútua entre os países signatários no combate aos crimes virtuais, conta-se com a satisfatória utilização deste tratado internacional no que diz respeito ao combate destes crimes em nosso país.

O Brasil pode se espelhar em países que já tipificam o crime de *Ransomware* para que tente inibir a prática deste crime, uma vez que o Brasil é o quarto país a mais sofrer ataques de *Ransomware* no mundo, segundo o relatório *SonicWall* de Ameaças Cibernéticas, divulgado em fevereiro de 2022, o mundo tende a caminhar cada vez mais rápido para a virtualização das coisas, exemplifica-se com a criação da tecnologia do blockchain, do metaverso e das também das criptomoedas.

Essa evolução tecnológica que cresce de forma exponencial, traz novas formas e modos para a prática de antigos crimes em ambiente virtual, e como vimos que a justiça não enxerga e caminha na mesma velocidade, a burocratização do processo legislativo e a não atenção e discussão devida com os especialistas sobre a legislação penal cibernética, tende a dificultar e punir adequadamente os ataques de *Ransomware*.

Por fim, aponta-se que na legislação penal brasileira foi observada, até o momento, a falta de uma tipificação concreta e efetiva do crime de *Ransomware*, entende-se que para o surgimento de uma norma é necessário se percorrer um caminho burocrático longo e cheio de entraves.

Tipificar o crime de *Ransomware* se torna imprescindível ao passo que existe a necessidade de punir adequadamente condutas criminosas ocorridas no meio virtual, o que pode se tornar um problema cada vez mais grave, dado a constante revolução social que o mundo experimenta.

REFERÊNCIAS BIBLIOGRÁFICAS

1989: O primeiro Ciberataque de Ransomware do Mundo. *In:* DERECO Tecnologia. **DERECO Tecnologia.** *[S.l.]*. 11 fev. 2022. Disponível em: https://dereco.com.br/blog/f/1989-o-primeiro-ciberataque-de-ransomware-do-mundo. Acesso em: 21 mai. 2022.

ALMEIDA, Jéssica de Jesus *et al*. Crimes cibernéticos. **Ciências Humanas e Sociais Unit**, Aracajú, v. 2, p. 215-236, mar. 2015 2316-3143. Disponível em: https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217. Acesso em: 8 mai. 2022.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. Decreto-Lei nº 2.848, Código Penal. **Decreto-Lei nº 2848, de 07 de dezembro de 1940.** Brasília, 7 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 8 mai. 2022.

CABETTE, Eduardo Luiz Santos. **O novo crime de invasão de dispositivo informático**. Conjur, 2013, p.26- 30. Disponível em: http://www.conjur.com.br/2013-fev04/eduardo-cabette-crime-invasao-dispositivo-informatico. Acesso em: 15 mai. 2022.

CALIFORNIA. Penal Code. s.l, 1 jan. 2018. Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEN&sectionNum=523. Acesso em: 15 mai. 2022.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Editora Brasport. 2014.

CASTELLS, Manuel. **Fim de Milênio.** Tradução: Klauss Brandini Gerhardt; Roneide Venancio Majer; Thiago Ponce de Moraes. 4. ed. São Paulo: Paz & Terra, 2007. Título original: End of Millennium.

DAMÁSIO, Jesus de; MILAGRE, José Antonio. **Manual de crimes informáticos**. Editora Saraiva, 2016.

DEMARTINI, Marina. Hackers trancam quartos de hotel e exigem resgate em bitcoin. **Exame**, São Paulo: Exame, ano 2017, 1 fev. 2017. Disponível em: https://exame.com/tecnologia/hackers-trancam-hospedesem-hotel-e-exigem-resgate-em-bitcoin/. Acesso em: 7 mai. 2022.

DEZ fatos sobre o ransomware. *In:* Kaspersky Daily. **Kaspersky Daily.** s.l, 7 jan. 2015. Disponível em: https://www.kaspersky.com.br/blog/dez-fatos-sobre-o-ransomware/4614/. Acesso em: 19 mai. 2022.

GRECO, Rogério. **Código Penal Comentado**. 7ª ed. Niterói, RJ: Impetus, 2013A. p.447.

GRECO, Rogério. Invasão de dispositivo informático - art. 154-a do código penal. *In:* Jusbrasil. **Jusbrasil.** s.l, 8 jan. 2013B. Disponível em:

https://rogeriogreco.jusbrasil.com.br/artigos/121819872/invasao-de-dispositivo-informatico-art-154-a-do-codigo-penal. Acesso em: 15 mai. 2022.

HIGA, Paulo. Microsoft reclama de governos que "colecionam" falhas de segurança do Windows: WannaCry surgiu de uma vulnerabilidade descoberta pela agência de segurança dos EUA (e que foi vazada por hackers). *In:* Tecnoblog. **Tecnoblog.** *[S.l.]*. 15 mai. 2017. Disponível em: https://tecnoblog.net/noticias/2017/05/15/microsoft-nsa-cia-vulnerabilidades-windows-wannacry/. Acesso em: 17 mai. 2022.

HOSPITAL de Kansas atingido por Ransomware, extorquido duas vezes. *In*: Trend Micro. **Trend Micro.** *[S.l]*. 30 mai. 2016. Disponível em: http://blog.trendmicro.com.br/hospital-de-kansas-atingido-por-ransomware-extorquidoduas-vezes/. Acesso em: 07 mai. 2022.

JESUS, Damásio Evangelista de. **Manual de Crimes Informáticos**. 1 ed. São Paulo: Saraiva, 2016, p. 48.

MASSENO, Manuel David; WENDT, Emerson. O Ransomware na Lei: Apontamentos Breves de Direito Português e Brasileiro. Direito & TI, Porto Alegre: Direito & TI, 17 jul. 2017. Disponível em: https://direitoeti.emnuvens.com.br/direitoeti/article/view/80#:~:text=Este%20artigo%20visa%20enquadrar%20juridicamente,natureza%20penal%20a%20tais%20ataques. Acesso em: 10 mai. 2022.

PAESANI, Liliana Minardi. *et al.* **O Direito na sociedade da informação II.** 1 ed. São Paulo: Atlas, 2009.
ROCHA, Carolina Borges. **Evolução dos crimes cibernéticos**. Revista Jus Navigandi, Teresina, ano 18, n. 3706, p.56- 60.

ROHR, Altieres. Metrô de São Francisco libera catracas após ataque por vírus de resgate. *In:* G1. **G1**. [s.l]. 28 nov. 2016. Disponível em: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/metro-de-sao-franciscolibera-catracas-apos-ataque-por-virus-de-resgate.html. Acesso em: 10 mai. 2022.

SAISSE, Renan Cabral. Ransomware: Sequestro de Dados e Extorsão Digital. **Revista Eletrônica Direito & TI**, Porto Alegre: Direito & TI, ano 2016, 20 nov. 2016. Disponível em: https://direitoeti.com.br/direitoeti/article/view/44. Acesso em: 12 mai. 2022.

SYDOW, Spencer Toth. **Curso de direito penal informático:** partes geral e especial. 3. ed. São Paulo: JusPodivm, 2022, p. 27-88.

WENDT, Emerson; JORGE, Higor. Crimes Cibernéticos: Ameaças e Procedimentos de Investigação. 3. ed. Rio de Janeiro: Brasport, 2021.

WANNACRY: entenda o ciberataque que afetou mais de 200 mil PCs em 150 países. *In:* Olhar Digital. **Olhar Digital.** *[S.l.]*. s.d. Disponível em: https://olhardigital.com.br/especial/wannacry/. Acesso em: 16 mai. 2022.