Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

MARCOS VINICIUS VALICELLI GONÇALVES

CIBERCRIMES:

LEGISLAÇÃO BRASILEIRA EM UM CENÁRIO DE EVOLUÇÃO TECNOLÓGICA

Assis/SP
2024

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

MARCOS VINICIUS VALICELLI GONÇALVES

CIBERCRIMES:

LEGISLAÇÃO BRASILEIRA EM UM CENÁRIO DE EVOLUÇÃO TECNOLÓGICA

Projeto de pesquisa apresentado ao curso de Direito do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando(a): Marcos Vinicius Valicelli Gonçalves
Orientador(a): Claudio José Palma Sanchez

Assis/SP
2024

FICHA CATALOGRÁFICA

Gonçalves, Marcos Vinicius Valicelli

G635c Cibercrimes: legislação brasileira em um cenário de evolução tecnológica / Marcos Vinicius Valicelli Gonçalves.

Assis, 2024. -- 46p.

Trabalho de Conclusão de Curso (Graduação em Direito) -- Fundação Educacional do Município de Assis (FEMA), Instituto Municipal de Ensino Superior de Assis (IMESA), 2024.

Orientador: Prof. Me. Cláudio José Palma Sanchez.

1. Crime por computador. 2. Ciberespaço. 3. Direito penal informático. I Sanchez, Cláudio José Palma. II Título.

CDD: 341.59

Biblioteca da FEMA

Elaborada por Anna Carolina Antunes de Moraes – Bibliotecária – CRB-8/10982

CIBERCRIMES:

LEGISLAÇÃO BRASILEIRA EM UM CENÁRIO DE EVOLUÇÃO TECNOLÓGICA

MARCOS VINICIUS VALICELLI GONÇALVES

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: _____
Claudio José Palma Sanchez

Examinador: _____

ASSIS/SP

2024

DEDICATÓRIA

Dedico este trabalho aos meus pais, Marco Antônio Teixeira Gonçalves e Simone Akiko Seki, por sempre me apoiarem em todos os meus sonhos, sem vocês nada disso seria possível.

Vocês são responsáveis pelo meu desenvolvimento até aqui e o que vier adiante.

Amo muito vocês!

RESUMO

O presente trabalho discorre desde a história até inserção da internet e dos sistemas informáticos na sociedade atual, ponderando os seus benefícios e malefícios, trazendo o surgimento da criminalidade digital na denominada ‘’era da informação’’ e como os cibercriminosos se utilizam deste meio para a prática de delitos no ciberespaço. Além disto, apresentando o posicionamento de doutrinadores a respeito das especificidades desta modalidade de condutas ilícitas e, verificando como a legislação vigente brasileira está combatendo os cibercrimes, a fim de entender o processo de evolução e as lacunas a serem preenchidas pelo ordenamento jurídico.

Palavras-chave: Cibercrimes, Legislação, Internet, Sistemas informáticos, Ciberespaço, Cibercriminosos, Direito digital, Era da informação.

ABSTRACT

This work goes from history to the insertion of the internet and computer systems in today's society, considering its benefits and harms, bringing the emergence of digital crime in the so-called "information age" and how cybercriminals use this means to the commission of crimes in cyberspace. Furthermore, presenting the position of scholars regarding the specificities of this type of illicit conduct and verifying how current Brazilian legislation is combating cybercrimes, in order to understand the process of evolution and the gaps to be filled by the legal system.

Keywords: Cybercrime, Legislation, Internet, Computer systems, Cyberspace, Cybercriminals, Digital law, Information age.

SUMÁRIO

INTRODUÇÃO

O Brasil nos últimos anos com o avanço da tecnologia e inclusão digital demonstrou uma relevância no uso da internet, a revista G1[1], compilou dados sobre o aumento do uso da internet no Brasil. Diante disto, foi relatada uma taxa de que 84% dos Brasileiros possuem acesso à internet, contabilizando um total de 156 Milhões de pessoas, na faixa etária de 10 anos ou mais. Assim, os dados relatam o quanto a população brasileira está inserida no mundo virtual.

No entanto, o avanço na tecnologia e o seu uso pelos brasileiros está sendo alvo de diversos crimes cibernéticos. A revista CNN publicou um levantamento realizado pelo ‘’laboratório de inteligência e ameaças, FortiGuard Labs, uma empresa de soluções em segurança cibernética’’ que, demostra que o Brasil registrou no primeiro semestre de 2023, 31,5 bilhões de tentativas de ataques cibernéticos a empresas. Isso demonstra que ninguém está seguro ao usar a maior rede de informação do mundo.

Nessa perspectiva, diante do enorme número de atentados as redes, percebe-se a necessidade de entender como o sistema jurídico necessita adaptar-se a esta evolução tecnológica para garantir a proteção dos direitos individuais e fundamentais.

Sendo Assim, o intuito da pesquisa é avaliar os meios jurídicos para determinada proteção dos dados e punição para os transgressores. Devendo levar em consideração as dificuldades em relação aos meios investigativos.

Portanto, indaga-se: Se o sistema jurídico é frutífero quando se trata de garantir a proteção dos direitos individuais dos cidadãos e a segurança cibernética e, se os meios investigativos são aptos para localizarem tais transgressores.

---

[1] Disponível em: https://g1.globo.com/tecnologia/noticia/2023/11/16/acesso-a-internet-cresce-no-brasil-e-chega-a-84percent-da-populacao-em-2023-diz-pesquisa.ghtml. Acesso em: maio. 2024.

No cenário atual, o sistema jurídico já possui legislação em relação ao tema da pesquisa, por exemplo; O crime de invasão de dispositivo informático, a lei 12.737/2012, também conhecida como ‘’Lei Carolina Dieckmann’’. Além disto, a lei 13.709/2028, conhecida como ‘’Lei geral de proteção de Dados Pessoais (LGPD).

Parte-se da hipótese de que somente a criação de normas não é o necessário para impedir a transgressão, pois, sem a devida investigação no âmbito policial torna-se dificultoso a aplicação das devidas responsabilidades punitivas. Assim, havendo necessidade de expansão de profissionais e delegacias capacitadas nestes tipos de ações delituosas.

O desenvolvimento deste trabalho será realizado através de dados estatísticos de pesquisas relacionadas ao tema, tipificação Brasileira, Estrangeira, Doutrinas e Jurisprudência.

Diante da escassa doutrina em relação ao tema, possuem alguns posicionamentos norteadores, como Marcelo Xavier de Freitas Crespo (2017, p. 11), entende que é justificável novas propostas de delitos no ordenamento jurídico, pois, a criminalidade informática não é apenas um ‘’meio’’ para a prática de condutas já tipificadas, levando em considerando que existe lesão de bens jurídicos específicos.

Além disto, José Antônio Milagre e Damásio de jesus, (2017, p. 7) discorrem a

Respeito de não vigorar a lei de talião, autotutela ou a lei mais forte, pois, o direito deverá prevalecer frente aos crimes virtuais, fazendo assim valer a justiça, tendo controle daqueles que realizarem condutas criminosas cibernéticas.

A pesquisa divide-se em três capítulos. O primeiro trata-se da Internet e avanços tecnológicos, sendo discorrido desde a história até os impactos sociais causados por ela. O segundo será retratado uma análise dos principais crimes virtuais,

O trabalho possui como objetivo esclarecer as lacunas que podem serem preenchidas no sistema jurídico brasileiro em consonância com a necessidade de evolução dos meios investigativos, para que assim, as pessoas tenham maior seguridade quanto aos crimes cibernéticos e, tirando o paradigma de que a internet é uma terra sem lei.

1. INTERNET E AVANÇOS TECNOLÓGICOS

1.1 ORIGEM E EVOLUÇÃO DA ‘’ERA DA INFORMAÇÃO’’

A palavra tecnologia tem origem no grego "*tekhne*" que significa "técnica, arte, ofício" juntamente com o sufixo "*logia"* que significa "estudo". Desta forma, é uma arte de estudo que busca desenvolver meios de resolução de problemas ou facilitar a vida das pessoas. Atualmente, a palavra tecnologia remete aos meios atuais, como; Internet, computadores, celulares, robôs. Nesse sentido, os autores Damásio Evangelista de Jesus e José Antônio milagre de Oliveira, no livro *Manual de crimes informáticos*, discorrem a respeito da evolução da sociedade:

> É preciso que se diga que a sociedade não é uma pedra, estática, mas um organismo de mudanças, em constante transformação. A tecnologia é um dos fatores que motivam as principais mutações sociais nesta era, chegando a ditar comportamentos e a criar costumes. (JESUS E MILAGRE, 2016, p.7).

Contudo, as invenções consideradas tecnológicas estão inseridas na sociedade muito antes da criação dos sistemas informáticos, redes ou banco de dados. As primeiras invenções são de centenárias. Dessa forma, o mundo está em constante evolução, sendo sempre presente um ser com descobertas inovadoras. Diante disto, para entender como se formou a atual sociedade, necessita-se conhecer um pouco do passado, para que assim seja possível visualizar a atualidade.

O mundo passou por diversas eras, até a chegada da denominada sociedade ou era da informação. Nesse viés, sua base está na revolução industrial, um período conhecido pelo grande desenvolvimento tecnológico. Este momento pode ser considerado o ponto de partida para a criação de tudo que conhecemos e utilizamos do mundo virtual atualmente.

Marcelo Xavier de Freitas Crespo, discorre a respeito do que é conhecido como era da informação:

> Comumente se conhece a “Era da Informação” como o período após a Era Industrial, principalmente após a década de 1980, apesar de suas bases fundarem-se no início do século XX, especialmente na década de 1970, com as invenções do microprocessador, das redes de computadores, da fibra ótica e do computador pessoal. (CRESPO, 2017, p.12)

Sendo assim, para que chegássemos a este patamar de tecnologia, a sociedade passou por uma série de processos evolutivos. O início de criações tecnológicas foi muito antes do primeiro sistema informático construído ou de uma rede computadores.

De acordo com a revista UOL, a revolução industrial[2] (1760 – 1840) foi um processo com origem na Inglaterra, iniciado na metade do século XVIII, responsável introdução de maquinários na cadeia de produção, como; máquina de fiação, máquina de tear e o motor a vapor. Crespo, em seu livro *Crimes Digitais*, disserta a respeito do impacto da revolução industrial no surgimento da ‘’Era da informação’’:

> O impacto da Revolução Industrial se verificou pela substituição da força humana pelas máquinas, tendo a era agrícola perdido espaço, impondo-se novas relações entre o capital e o trabalho, estabelecendo novas relações entre as nações. Disso também se deu a disseminação do uso da eletricidade, bem como o desenvolvimento da física e da química, o que foi providencial para o surgimento dos computadores. (CRESPO, 2017, p.14)

Nesse sentido, a internet é uma tecnologia criada capaz de interligar sistemas informáticos do mundo inteiro, ela é responsável por romper as fronteiras entre países. Atualmente é considerada a principal fonte de informação, comunicação, interação. Sendo assim, segundo dados da União Internacional de Telecomunicações (UIT) no ano de 2023, 67% da população mundial, 5,4 bilhões de pessoas utilizando a internet.

---

[2] Disponível em: https://brasilescola.uol.com.br/geografia/terceira-revolucao-industrial.htm. Acesso em: maio.2024.

1.2 INTERNET

De acordo com Guitarrara, em uma matéria publicada no site Brasil Escola, ‘’Globalização é o fenômeno de integração econômica, social e cultural do espaço geográfico em escala mundial’’.[3] Nesse viés, é a internet é um dos meios que mais proporciona tal fenômeno, ou seja, possui uma importância em escala mundial, sendo utilizado em todo o mundo. Assim, na sociedade atual, a internet está ligada intimamente com o conceito de globalização.

Além disto, a revista G1, publicou em uma matéria ‘’ O acesso à internet no Brasil aumentou em 2023: 84% da população brasileira com 10 anos ou mais se conectou à internet**,** o que representa 156 milhões de pessoas. Em 2022, este índice era de 81%’’. . Portanto, é inegável que ela é um fator responsável por um mundo globalizado. Contudo, para que tal fenômeno fosse possível e que a internet pudesse se popularizar desta forma, ocorreu diversos acontecimento que permitirem a evolução.

De acordo com Marcelo Xavier de Freitas a primeira rede construída foi a ‘’ARPAnet’’ (*Advanced Research Projects Administration)*[4]*,* no ano de 1966. No entanto, era de domínio das forças militares dos Estados Unidos da América (EUA), com o intuito de transmitir dados sigilosos, assim como, interligar os departamentos de pesquisas. Insta ressaltar que, na época que foi desenvolvida estava em meio ao conflito denominado como ‘’Guerra Fria’’, entre o EUA (Estados Unidos da América e a URSS (União Soviética). (CRESPO, 2017, p.13)

Nesse viés, a revista a revista *National Geographic*, explicou brevemente como funciona o sistema ‘’Apartnet’’:

> Foi assim que ARPAnet se tornou uma das primeiras redes a desenvolver e implementar a ideia de “comutação de pacotes”, que é

[3] Disponível em: https://brasilescola.uol.com.br/geografia/globalizacao.htm#:~:text=Globaliza%C3%A7%C3%A3o%20%C3%A9%20o%20fen%C3%B4meno%20de,na%20comunica%C3%A7%C3%A3o%20e%20nos%20transportes. Acesso em: jun. 2024.

[4] Disponível em: https://developer.mozilla.org/pt-BR/docs/Glossary/Arpanet. Acesso em: jun. 2024.

> uma tecnologia fundamental para a comunicação com uma linguagem própria e única para a Internet. Ela consiste na técnica que envia uma mensagem de dados dividida em pequenas unidades, como explica um artigo da revista National Geographic da Espanha intitulado “Quem é o dono da Internet? Quando e quem a inventou?”. (REDAÇÃO NATIONAL GEOGRAPHIC BRASIL, 2024, Online)[5]

Um dos seus criadores, chamado Vinton Cerf foi intitulado por muitos de ‘’Pai da Internet’’. Entretanto, houve outros sistemas criados que foram essenciais para que a Internet fosse criada. Nesse viés, um dos principais marcos para sua criação foi o TCP/IP25 (Protocolo de Controle de Transferência/Protocolo de Internet).

O TCP/IP25 foi desenvolvido por Robert Kahn, que permitiu a efetiva interligação de computadores, tornando-se realmente uma rede de computadores, não existindo um ponto fixo, mas cada computador um equivalente.

De acordo com o a Fortinet, uma empresa renomada e destinada a segurança cibernética, em um artigo publicado em seu site, o TCP/IP25 tem como definição:

> O TCP organiza os dados para que possam ser transmitidos entre um servidor e um cliente. Ele garante a integridade dos dados que são comunicados em uma rede. Antes de transmitir os dados, o TCP estabelece uma conexão entre uma origem e seu destino, que ele garante que permaneça ativa até que a comunicação comece. Então, ele divide grandes quantidades de dados em pacotes menores, garantindo que a integridade dos dados estejam em vigor durante todo o processo.

O ‘’APARtnet’’ foi dissolvido, mas foi criada uma rede denominada de ‘’NSFNET’’. No entanto, a expansão da Internet foi novamente revolucionária com a chegada do ‘’www’’ (a *World Wide Web*), desenvolvido pelos engenheiros do CERN (*Centre Européen pour la Recherche Nucléaire*). Assim, sua criação permitiu que fosse criado páginas e navegadores, assim como os que temos hoje; Google, Microsoft Edge, Firefox, entre outros. Diante disto, a internet foi crescendo exponencialmente e continua em um processo de evolução. A chegada da linguagem em HTML

[5] Disponível em: https://www.nationalgeographicbrasil.com/historia/2024/05/qual-e-a-origem-da-internet. Acesso em: mai. 2024.

(*HyperText Markup Language*), utilizada para criar páginas de web, que são utilizados para interpretação dos navegadores. Portanto, houve um grande e longo processo até a sua popularização, presente em todo o planeta[6].

Ademais, a revista UOL pontuou a chegada da internet no Brasil somente no ano de 1988, um pouco tarde comparada com o início da criação de sistemas de redes. Seu surgimento se deu através da FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo), UFRJ (Universidade Federal do Rio de Janeiro) e LNCC (Laboratório Nacional de Computação Cientifica).

1.3 OS IMPACTOS CAUSADOS DA ERA DA INFORMAÇÃO E DO SURGIMENTO DA INTERNET:

A internet pode ser considerada atualmente o principal meio para a globalização, levando em consideração os dados expostos anteriormente a respeito de seu uso no mundo. Desta forma, assim como a vida em sociedade, em seu espaço físico e real, ações e omissões geram consequências, boas ou ruins. Diante disto, é necessário pontuar até onde ela é benéfica para as pessoas e, onde inicia-se suas problemáticas, para que assim seja possível pontuar estratégias de melhorias.

No dia 19 de julho de 2024 (Sexta-Feira) ocorreu oque chamam de ‘’apagão cibernético’’, uma falha em um sistema de segurança fez com que sistemas informáticos no mundo inteiro não funcionassem corretamente. Segundo a revista G1 ‘’A falha em um dos sistemas de segurança da empresa norte-americana CrowdStrike tirou computadores do ar e causou atraso de voos, prejudicou serviços bancários e de comunicação ao redor do mundo.’’ (G1, 2024, Online)[7]. Assim, é crível que os sistemas informáticos possuem impactos volumosos no mundo, onde uma falha tecnológica acarretou diversos danos, em múltiplas esferas de uma sociedade.

---

[6] Disponível em: https://exame.com/tecnologia/as-5-linguagens-de-programacao-mais-usadas-no-mundo-segundo-o-github/. Acesso em: jun. 2024.

[7] Disponível em: https://g1.globo.com/tecnologia/noticia/2024/07/20/apagao-global-cibernetico-afetou-85-milhoes-de-aparelhos-com-o-windows-diz-a-microsoft.ghtml. Acesso em: jun. 2024.

Desta forma, a sociedade é diretamente impactada com a tecnologia ou com sua ausência, pois, tornamos dependentes dela como mecanismo de vida. Estar presente no mundo digital não é apenas uma escolha por luxo, mas se tornou uma necessidade, pois, inúmeras situações realizadas no cotidiano se tornaram virtuais.

Diante disto, este meio que deixou de ser uma ferramenta e, tornou-se um espaço com valor para a era da informação. Assim como, o espaço real, ou seja, fora do mundo virtual existe pessoas que se utilizam de meios e artefatos para tirarem vantagem e cometer delitos, na internet não poderia ser diferente. Segundo Damásio Evangelista de Jesus e José Antônio Milagre de Oliveira (2016, p.7), ‘‘A Internet é rica, e onde há riqueza, existe crime.’’

Sendo assim, as novas tecnologias presentes, que acarretam a formação da era da informação transformou diversos setores das sociedades, sendo um deles o meio jurídico. Delitos que eram cometidos em um meio físico passaram a serem realizados em um ambiente virtual, onde torna-se mais dificultoso em questões processuais.

De acordo com Haidar (2023, Online), em uma matéria publicada na revista Terra, apresentou dados sobre as investigações de crimes cibernéticos no Brasil:

> A Polícia Federal enfrenta um recorde de investigações de crimes cibernéticos. Levantamento obtido pela coluna mostra que só no ano passado a PF abriu 845 inquéritos para investigar ataques cibernéticos em todo o país. Foi o período anual com a maior quantidade de inquéritos abertos contra esse tipo de crime. (HAIDAR, 2023)

Diante disto, é crível que as pessoas inseridas na era da informação estão correndo riscos, pois, está ocorrendo um aumento de ataques cibernéticos. Sendo assim, a insegurança no uso das redes se torna uma emoção presente na era da informação. Discorre Damásio Evangelista de Jesus e José Antônio Milagre de Oliveira, a respeito dos riscos inerentes da sociedade da informação:

> E a sociedade da informação (ou para muitos, pós-industrial) tem, sim, seus riscos. Pode ser chamada de sociedade dos riscos. Riscos que podem ser aceitos e riscos que devem ser mitigados. E um deles está associado à criminalidade digital. Ao considerarmos que nem todo o cidadão decidiu ingressar, mas lançado foi no universo digital, constitui-se presa fácil nas mãos de especialistas em crimes cibernéticos (JESUS E MILAGRE, 2016, p.7)

2 ANÁLISE DOS CIBERCRIMES

2.1 ASPECTOS CONCEITUAIS

A dissertação dos aspectos conceituais envolvendo a criminalidade digital é um ponto que possui controvérsias, levando em consideração a agilidade que possui a evolução tecnológica, todos os dias surgem novos softwares, termos e, modus operandi no meio cibernético. Neste viés, disserta Crespo, com uma tese justificando está o porquê desta diversidade:

> Por conta das inovações tecnológicas, é comum nos depararmos com termos ou expressões que, à primeira vista, soam-nos estranhos. Cremos que isso se dá por dois motivos: (a) a constante evolução tecnológica faz com que muito frequentemente haja novos mecanismos, aparelhos e técnicas disponíveis, sendo intuitivo que isso interfere no vocabulário; (b) no mais das vezes, os termos são cunhados na língua inglesa e, depois, introduzidos em nosso vocabulário ou "nacionalizados", havendo forte presença de neologismos. (CRESPO, 2017, p.20).

De acordo com Alexandre Júnior (2019, p.3), em uma publicação na Revista Eletrônica da Faculdade de Direito de Franca, entende que um cibercrime pode ser definido como "todo ato em que o computador ou meios de tecnologia da informação serve para atingir um ato criminoso ou em que um computador ou meios de tecnologia da informação é objeto de um crime.''

> Diversas são as ações delituosas no meio da criminalidade digital, como; cyberstalking, cyberbullying, invasão de sistemas informáticos (hacking), disseminação de vírus e malware, crimes contra a honra. Desta forma, os sistemas informáticos e meios da TIC (Tecnologia da informação e comunicação) são meios que atingem bens jurídicos já tutelados e delitos tipificados, mas também podem ser o bem ofendido. Nesse contexto, corroboram com este entendimento, ''O crime virtual pode ser um crime-meio, mas vem se desenvolvendo como crime-fim, o que demandou, aliás, a tipificação de alguns crimes informáticos próprios, com a edição das Leis n. 12.735/2012 e n. 12.737/2012.'' (JESUS E MILAGRE, 2017, p.21)

Entretanto, há de se mencionar a existência teses esparsas na conceituação dos cibercrimes, pois, alguns doutrinadores entendem o ciberespaço como um meio para a prática de delitos já tipificados no ordenamento jurídico, considerando exceção aqueles que atingem outras condutas não tipificadas. Nesse sentido, disserta Patrícia Peck Pinheiro

> ’O crime virtual, em tese, era considerado um crime-meio, em que se utiliza um meio virtual. Assim reforçava Patrícia Peck Pinheiro (2007, p. 250; 2014, p. 307): “Não é crime-fim por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por hackers, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros”.

Ademais, existem inúmeros posicionamentos de doutrinadores acerca da conceituação das condutas ilícitas praticadas em ambientes virtuais, sendo possível citar diversas teses.

Entretanto, é possível visualizar um alinhamento a respeito da não concordância da tecnologia somente com mero meio para a prática de delitos já tipificados. Sendo assim, a prática de alguns delitos denominados de ‘’crimes cibernéticos próprios’’ ocorrem através de meios virtuais e, o bem jurídico prejudicado são os sistemas informáticos e meios da TIC, sendo possível considerar os cibercrimes como um crime-fim.

2.1.1 NOMECLATURA

> É possível visualizar uma multiplicidade de nomenclatura utilizadas por doutrinadores e em legislações vigentes, o que pode vir a causar dúvidas pertinente de qual nomen juris seria o correto para se utilizar. Contudo, não existe um consenso a respeito do termo correto ao citar tais delitos. Desta forma, compreende-se no mesmo viés, “não há uma nomenclatura sedimentada pelos doutrinadores acerca do conceito de crime cibernético. que muda é só o nome atribuído a esses crimes, posto que devem ser observados o uso de dispositivos informáticos.” (DA SILVA, 2015, p.39)

Desta forma, a própria legislação brasileira não definiu um termo único para se referir aos delitos cibernéticos, a Lei Nº 12.737/12, utiliza-se da nomenclatura

‘’delitos informáticos’’, no entanto, o termo ‘’cibercrime’’ é utilizado no Acordo Internacional do Conselho da Europa, conhecido como ‘’convenção de Budapeste’’, que foi aprovado através Decreto Legislativo nº 37, de 16 de dezembro de 2021.[8]

Neste sentido, Vladimir Aras, relata acerca das nomenclaturas utilizadas para definir estas condutas ilícitas:

> Delitos computacionais, crimes de informática, crimes de computador, crimes eletrônicos, crimes telemáticos, crimes informacionais, ciberdelitos, cibercrimes... Não há um consenso quanto ao nomen juris genérico dos delitos que ofendem interesses relativos ao uso, à propriedade, à segurança ou à funcionalidade de computadores e equipamentos periféricos (hardwares), redes de computadores e programas de computador (estes denominados softwares) (ARAS,2001, p.01)

Insta ressaltar que:

> Em algumas nomenclaturas como; crimes de computador, crime informático, crimes eletrônicos, podem transmitir uma ideia esparsa dos conceitos doutrinários, pois, referenciam-se a computadores ou sistemas informáticos. No entanto, os cibercrimes também são definidos por delitos cometidos através da telecomunicação, telemática (internet). (CRESPO, 2017)

Portanto, não há o uso de uma nomenclatura sólida em face da denominação utilizada ao discorrer acerca da criminalidade digital. Sendo assim, para fins desta pesquisa a nomenclatura ‘’cibercrime’’ foi a escolhida em observância com a convenção de Budapeste, mas todas as outras denominações utilizadas são consideradas sinônimos.

2.2 DO CIBERCRIMINOSO:

É perceptível um paradigma da sociedade ao se tratar dos criminosos do mundo virtual, onde por muita das vezes são considerados *experts* da tecnologia, pessoas

[8] Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: jun. 2024.

com alto nível de conhecimento informático, capazes de romperem barreiras de proteção de aparelhos informáticos, aplicativos, telemáticas. No que tange a este modelo de cibercriminoso é correto este viés de pensamento, contudo, ser um denominador do assunto não é mais uma qualidade necessária.

Em uma matéria publicada por Mauro Marcelo de Lima e Silva (2000), afirmavam que a polícia teria revelado o perfil do criminoso na internet, sendo assim, narram como:

> Geralmente, os criminosos são de oportunidade e os delitos praticados por agentes que, na maioria das vezes, têm a sua ocupação profissional ligada à área de informática.O perfil do criminoso, baseado em pesquisa empírica, indica jovens, inteligentes, educados, com idade entre 16 e 32 anos, do sexo masculino, magros, caucasianos, audaciosos e aventureiros, com inteligência bem acima da média e movidos pelo desafio da superação do conhecimento, além do sentimento de anonimato, que bloqueia seus parâmetros de entendimento para avaliar sua conduta como ilegal, sempre alegando ignorância do crime e, simplesmente, "uma brincadeira".Mais: preferem ficção científica, música, xadrez, jogos de guerra e não gostam de esportes, sendo que suas condutas geralmente passam por três estágios: o desafio, o dinheiro extra, e, por fim, os altos gastos e o comércio ilegal. (LIMA E SILVA, 2000, Online)

Entretanto, o estereótipo de criminoso virtual como *nerd* é desmistificado por alguns doutrinadores. Levando em consideração que o conhecimento tecnológico se tornou trivial, estando nas mãos de milhares de pessoas através da própria *internet,* plataformas de vídeos, blogs, comunidades, disponibilizando ensinamentos de técnicas para a prática de delitos virtuais.

Corroboram com este entendimento Jesus e Milagre:

> Este cenário foi modificado. A realidade, hoje, é que grande parte dos crimes digitais se deve à ignorância dos usuários, despreparo das autoridades investigativas e, principalmente, à banalização e difusão das técnicas e ferramentas para aplicação de golpes. (JESUS E MILAGRE, 2016, p.23)

Através das classificações dos tipos de cibercrimes apontados anteriormente é possível extrair a diferença de crimes impróprios e próprios. O primeiro seria o tipo de delito que se utiliza de aparatos informáticos ou das telemáticas para atingir bens jurídicos já protegidos, ou seja, qualquer pessoa está apta a cometê-los.

No entanto, o segundo seria aqueles em que o bem jurídico ofendido são os meios informáticos e meios da tecnologia da informação, sendo assim, necessita-se de um conhecimento mais técnico informático.

O termo *hacker* por sua vez é visto diversas vezes quando o assunto é se referir aos agentes responsáveis pelas condutas ilícitas digitais, contudo, existe uma negativa quanto ao seu uso de uma forma pejorativa. Ademais, existem diversas nomenclaturas com conceituações distintas ao se tratar do cibercriminoso, mas as mais conhecidas são *hacker* e *cracker*, logo abaixo será discorrido as definições dos principais termos utilizados no meio digital, no que diz respeito ao perfil do criminoso virtual.

2.2.1 HACKER

O termo hacker muita das vezes é utilizado para definir os agentes responsáveis por realizar condutas ilícitas no âmbito digital. Entretanto, não são eles os verdadeiros responsáveis por tais ilícitos, pois, o real significado desta palavra não condiz com atos danosos. Em contrapartida a este preconceito, estes são considerados pessoas boas para o ciberespaço e o para o desenvolvimento dele.

> Apesar da fama de “criminosos virtuais”, nem todo hacker deseja o prejuízo alheio. Há aqueles que se dizem “hackers do bem”, pois invadem os computadores e deixam mensagens informando a vítima do risco existente, aconselhando-a a providenciar uma proteção mais efetiva. Outros passam a trabalhar em empresas a fim de desenvolver programas que sejam capazes de frear as invasões. (CRESPO, 2017, p.26)

Nesse sentido, os hackers são considerados especialistas da tecnologia, pessoas que detém grande conhecimento sobre a tecnologia da informação, mas diferente do preconceito que carrega esta nomenclatura não se utilizam do seu intelecto para a prática de atos ilícitos. Carlos Morimoto (2004) conceitua no site Hardware.com.br o termo *hacker* como:

> Alguém que estuda sistemas ou qualquer tipo de conhecimento humano pelo simples desafio de dominá-los. No sentido original da palavra, o Hacker é alguém que usa seus conhecimentos para ajudar outros, direta ou indiretamente. Hackers foram os principais responsáveis pelo desenvolvimento da Internet, criaram o Linux, o MP3 e a filosofia do software livre. (MORIMOTO, 2004, Online)

Portanto, a visualização destes agentes vinculados as condutas criminosas são equivocadas, tendo em vista que, são estudiosos do mundo informático e das redes telemáticas e, na maioria das vezes trabalham desenvolvendo sistemas e contribuindo com a sociedade no que tange a cibersegurança.

2.2.2 CRACKER

Por outro lado, o *cracker* pode ser considerado um termo relevante no quesito cibercrimes, pois, possuem o intuito de prejudicar sistemas informáticos e telemáticos.

Sua motivação na maioria das vezes é pecuniária, com o roubo de dados e informações. De acordo com Morimoto (2004), o sujeito intitulado com este termo é:

> O cracker é um vândalo virtual, alguém que usa seus conhecimentos para invadir sistemas, quebrar travas e senhas, roubar dados etc. Alguns tentam ganhar dinheiro vendendo as informações roubadas, outros buscam apenas fama ou divertimento.Uma segunda definição, mais branda, é alguém que quebra travas de segurança de programas e algoritmos de encriptação, seja para poder rodar jogos sem o CD-ROM, ou gerar uma chave de registro falsa para um determinado programa, quebrar as travas anti-cópias usadas em alguns softwares. (MORIMOTO, 2004, Online)

Marcelo Xavier de Freitas Crespo corrobora com este entendimento, afirmando:

> Esses podem ser considerados os verdadeiros criminosos da rede. Eles se divertem com destruições de sites e sua repercussão na imprensa. São também ladrões, valendo-se da internet para roubar dinheiro e informações. O cracker é aquele que, basicamente, “quebra” um sistema de segurança, invadindo-o. Fanáticos pelo vandalismo, também adoram “pichar” páginas da web deixando, na maioria das vezes, mensagens de conteúdo ofensivo e racista. (CRESPO, 2017, p.26)

Portanto, é necessária esta distinção entre os dois termos para não tomar conclusões precipitadas quando ao sujeito ativo de condutas ilícitas. Ademais, o termo *cracker* também é utilizado quando se possui o intuito de *crackear* algo, por exemplo: para utilizar-se do sistema operacional Windows é necessário adquirir este programa, assim, o usuário que adquirir vai ter acesso a ele, através de uma *key,* contudo, existe a possibilidade de realizar este procedimento para possuir o sistema sem precisar pagar.

2.2.3 LAMMER

Este termo é relacionado a sujeitos que dizem serem *hackers,* entretanto, não possuem o conhecimento de um, sendo assim, são considerados iniciantes técnicos. De acordo com Crespo os experts utilizam-se deste termo para insultar este tipo de pessoa que se acham os *experts.* ‘’Na hierarquia o Cracker está acima do Lammer (que sabe muito pouco) mas abaixo do Hacker, que é alguém de mais maturidade.’’ (MORIMOTO, 2004).

2.2.4 WANNABES:

Estes na escala de conhecimento técnico informático estão acima de um *lammer,* entretanto, possuem menos conhecimento do que um hacker ou um cracker, mas ainda assim buscam aprimorar suas habilidades, mas não considerados sujeitos danosos a o mundo virtual.

> São assim chamados porque querem ser especialistas, mas não são. São pessoas que já aprenderam um pouco sobre hacking e não estão aptos a praticar grandes feitos. Apesar disso, já fazem o que aprenderam com competência. Diferenciam-se dos lammers por terem mais consciência do que são capazes de fazer. (CRESPO, 2017, p.26)

2.2.5 PHREAKERS

Esta nomenclatura difere sendo diversa dos outros termos, pois, o meio utilizado não é o informático em si, mas sim da telemática, pois, utilizam-se indevidamente os meios telefônicos. Diante disto, estes sujeitos possuem a destreza de interceptar linhas telefônicas, entre outras técnicas que exploram a vulnerabilidade, como; obter acesso a serviços pagos, manipular chamadas, etc.

> Mas os phreackers não se limitam a escutar conversas alheias. Eles são capazes de fazer ligações sem pagar a conta. O que ocorre é o seguinte: através de computadores, eles fazem com que as operadoras de telefonia confundam-se quanto à origem de uma ligação. Assim, quem paga a conta é qualquer outra pessoa que tenha telefone daquela operadora. (CRESPO, 2017, p.26)

2.2.6 WHITE E BLACK HATS:

Inicialmente, *Hats* significa chapéu, sendo assim, a nomenclatura varia entre chapéu branco e chapéu preto. Estas distinções de cores são utilizadas para referirem ao caráter do sujeito, nesse viés, os *White Hats* são os *hackers*, como exposto anteriormente, são aqueles que utilizam de seu vasto conhecimento para um lado positivo da informática.

Por outro lado, os *Black Hats* são os *crackers*, pessoas com intuitos maliciosos, aproveitando-se de suas habilidades e falhas tecnológicas para tirarem vantagens, principalmente pecuniária.

> Black Hats são os crackers, pessoas com elevados conhecimentos de tecnologia que os utilizam para atividades criminosas. White Hats seriam os hackers, ou ainda “Hackers” éticos, especialistas que usam suas habilidades para o bem e para o fortalecimento da segurança dos sistemas. (JESUS E MILAGRE, 2016, p.24)

2.3 DO CIBERESPAÇO E A COMPETÊNCIA JURISDICIONAL

A era da informação trouxe consigo o rompimento de fronteiras através do que denominamos de meios tecnológicos. Nesse contexto, surgem quesitos a respeito do local do crime referente aos cibercrimes que devem ser esclarecidos, para que assim consiga-se definir o juiz competente para julgar tais delitos.

Os crimes cometidos no espaço virtual possuem diferenças dos realizados em um físico, a principal é a questão é multilocalidade, ou seja, o criminoso está em um local e a vítima em outro, não se limitando ao território brasileiro.

> Assim, os crimes digitais podem ser praticados parcialmente em diversos países, fragmentando-se o iter criminis. Questões sobre a presença física para a prática delitiva, bem como fronteiras territoriais ganham novas perspectivas, de modo que algumas características se mostram frequentes: a velocidade com a qual o delito é praticado, a distância a partir da qual se cometem os crimes, o volume de dados envolvido. Consequentemente, questões relativas à prova processual também ganham destaque. (CRESPO, 2017, p.29)

Crespo complementa que:

> Em primeiro plano, quanto ao lugar do crime existem três teorias que regem tal matéria, sendo elas; teoria da atividade, teoria do resultado e teoria da ubiquidade. A primeira considera o lugar do crime onde foi praticada a conduta de ação ou omissão. Na segunda, não importa o local da conduta, mas sim, o lugar onde se produziu ou deveria produzir o resultado. Já na terceira, é uma mistura das duas teorias, considerando o lugar do crime onde se produziu ou deveria se produzir o resultado e onde foi praticado a conduta (ação ou omissão). (CRESPO, 2017)

O código penal brasileiro adotou a teoria da ubiquidade, ‘’Art. 6º - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.’’ Por outro lado, o artigo 70º do código de processo penal trouxe consigo a teoria do resultado, pois, prevê, ‘’Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução’’

Desta forma, é possível visualizar um empasse quanto a aplicação da lei penal no espaço. Neste contexto, se faz necessário entender ainda que brevemente a respeito dos crimes plurilocais e dos crimes a distância, cuja especificidade é que a ação e o resultado são em locais distintos.

No primeiro tipo se verifica a diversidade de locais, entre a execução e o resultado, mas se limitam ao território nacional, ou seja, existe uma diferença de comarcas. Contudo, no segundo, o *iter criminis* transcende o território nacional.

Desta forma, entende Masson que:

> Crimes à distância: também conhecidos como “crimes de espaço máximo”, são aqueles cuja conduta e resultado ocorrem em países diversos. Como analisado na parte relativa ao lugar do crime, o art. 6.º do Código Penal acolheu a teoria mista ou da ubiquidade.Crimes plurilocais: são aqueles cuja conduta e resultado se desenvolvem em comarcas diversas, sediadas no mesmo país. No tocante às regras de competência, o art. 70 do Código de Processo Penal dispõe que, nesse caso, será competente para o processo e julgamento do crime o juízo do local em que se operou a consumação. (MASSON, 2024, p.186)

Diante deste entendimento, nos crimes a distância, se o agente ativo estiver localizado em foz do Iguaçu e a vítima na cidade Del Leste (Paraguai), o juízo competente pode ser tanto o local onde ocorreu a ação ou omissão, inteira ou em parte, bem como onde se produziu o resultado ou deveria produzir-se.

Por outro lado, em crimes plurilocais, um crime informático realizado em território brasileiro, mas em comarcas diferentes, por exemplo, o agente ativo que está sediado em São Paulo e realiza uma invasão a um computador de uma vítima que mora na Bahia, o juízo competente será considerado o do dispositivo invadido, conforme a teoria do resultado.

Entende desta mesma forma os autores Alesandro Gonçalves Barreto e Beatriz Silveira Brasil, do livro *Manual de Investigação Cibernética: Á luz do Marco Civil da Internet* que:

> O lugar do crime é definido nos termos do art. 70, do CPP, que adota a Teoria do Resultado, ou seja, a competência será, em regra, determinada pelo lugar em que se consumar o delito, ou, no caso de tentativa, pelo lugar que for praticado o último ato executório. Caso a conduta criminosa seja praticada em um país e o resultado venha a ser produzido em outro, aplica-se o Art. 6 do Código Penal Brasileiro, que trata dos chamados crimes a distância, inspirado pela Teoria da Ubiquidade, ou seja, considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado. (BARRETO E BRASIL, 2016, p.49)

Contudo, alguns doutrinadores divergem deste entendimento, visto que, no que tange ao juízo competente consideram os artigos 6 e 7 do código penal corretos para definirem a competência jurisdicional, ou seja, a teoria da ubiquidade seria tanto para crimes em âmbito nacional e internacional.

> Quanto ao Direito brasileiro, adotou-se a teoria da ubiquidade, segundo dispõe o art. 6° do CP, o que, em tese, soluciona problemas de Direito Penal Internacional, o que pode ser auxiliado, ainda, pela aplicação da lei brasileira a crimes cometidos fora do território nacional, conforme dispõe o art. 7° (extraterritorialidade). Dessa forma, os delitos praticados por brasileiro, tanto no país quanto fora, ainda que transnacionais, serão alvo da lei brasileira. (CRESPO, 2017, p.29)

Corrobora com este entendimento os autores Jesus e Milagre:

> No que tange ao lugar do crime, o Código Penal adotou, em seu art. 6º, a teoria da ubiquidade, sendo considerado o lugar do crime o local onde ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria se produzir o resultado. Deste modo, ao se considerar alguém, no Estado do Rio de Janeiro, que invade o computador de outrem, localizado em São Paulo, teríamos o juízo onde está o dispositivo invadido como competente para processar e julgar o delito informático. (JESUS E MILAGRE, 2016, p.25)

Entretanto, estes autores tratam a questão de crimes informáticos praticados no estrangeiro de forma distinta, pois, levam em consideração a soberania do país, onde não poderia ser aplicado a legislação brasileira, exceto se for alvo de acordo de extradição ou o agente for brasileiro e adentrar em território nacional.

No entanto, este não exatamente oque nosso sistema jurídico prevê, pois, o artigo 7 do Código Penal prevê os crimes em que será aplicado a lei penal brasileira, mesmo que praticado no estrangeiro e o artigo 70 do Código de Processo Penal, paragrafo

1, diz que ‘’1º Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução.’’

Insta ressalta que, a aplicação da competência por prevenção, prevista no artigo 83 do Código de Processo Penal, que prevê casos em que a competência recairá sobre o juízo que praticar primeiro algum ato do processo, antes de qualquer outro que também seja competente, pois, necessita-se que ambos os juízos sejam competentes, em todos os critérios estabelecidos pelas normas de processo penal.

Ademais, esta antecipação trata-se de nulidade relativa, não absoluta, conforme entendimento do STF: ‘’Nos termos da Súmula 706/STF, é relativa a nulidade decorrente da inobservância da competência penal por prevenção, a qual deve ser arguida oportuna e tempestivamente, sob pena de preclusão.’’[9]

2.4 CLASSIFICAÇÃO DOS CIBERCRIMES:

A classificação dos cibercrimes se faz necessária quando visualizado pela ótica de um tratamento jurídico adequado, bem como o bem jurídico o qual se deve ser protegido e condutas especificas a serem combatidas. Diversos doutrinadores buscaram classificar os crimes digitais, de formas distintas e outras semelhantes, alguns até mesmo pela nomenclatura.

Diante disto, Crespo discorre a respeito da importância de classificar a condutas ilícitas no mundo digital, ‘’Embora se diga que classificações não são corretas ou equivocadas, mas úteis ou inúteis, cumpre classificarmos os crimes digitais, pois a

[9] Disponível em: https://portal.stf.jus.br/jurisprudencia/sumariosumulas.asp?base=30&sumula=2433#:~:text=Nos%20termos%20da%20S%C3%BAmula%20706,tempestivamente%2C%20sob%20pena%20de%20preclus%C3%A3o. Acesso em: jun. 2024.

partir disso é que se fará exposição sobre condutas específicas.'' (CRESPO, 2017, p.24)

A classificação mais asseverada pelos doutrinadores brasileiros é a que separa os crimes informáticos puros ou próprios dos impuros ou impróprios. O primeiro são aqueles em que os sistemas informáticos são o alvo dos ataques. Em contrapartida, os impuros ou impróprios são os que os meios tecnológicos são utilizados como veículo para a prática de delitos já tipificados. Insta ressaltar que, quando referido sistemas tecnológicos ou sistemas informáticos, também é considerado o uso das telecomunicações.

Nesse viés, Aras (2001) anuncia a classificação de Croze e Bismuth, que corrobora com a classificação exposta acima:

> Não há consenso na classificação dos delitos de informática. Existem várias maneiras de conceituar tais condutas in genere. Todavia, a taxionomia mais aceita é a propugnada por HERVÉ CROZE e YVES BISMUTH(15), que distinguem duas categorias de crimes informáticos:a) os crimes cometidos contra um sistema de informática, seja qual for a motivação do agente; b) os crimes cometidos contra outros bens jurídicos, por meio de um sistema de informática. (ARAS, 2001, p.1)

A título exemplificativo, de crime impróprio, uma pessoa que postar ofensas a um terceiro, através de redes sociais ofendendo sua honra subjetiva estaria realizando a conduta já tipificada no Art. 139 do Código Penal, crime de difamação, utilizando-se apenas de um meio tecnológico para realizar tal delito, sendo assim, trata-se de um crime impróprio.

No que tange ao crime próprio temos, por exemplo, o crime de invasão de dispositivo informático, conforme o art, 154-A, do código penal, sendo assim, um crime cujo sistema da informática é o objeto atingido, ou seja, um crime-fim. Diante disto, Crespo corrobora com esta classificação quando disserta que:

> Assim, entendemos que a melhor classificação, porque mais objetiva e passível de enquadrar as condutas ilícitas mais modernas é aquela adotada por Ferreira e também por Greco, assim representada: (a) condutas perpetradas contra um sistema informático; (b) condutas perpetradas contra outros bens jurídicos. As condutas praticadas contra um sistema informático ou dado são o que se pode chamar de delito de risco informático, ao passo que as demais podem ser denominadas delitos vinculados à informática.

> Nesse sentido, podemos dizer que todas as condutas praticadas contra bens jurídicos informáticos (sistemas, dados) são delitos de risco informático ou próprios, ao passo que aquelas outras condutas que se dirigirem contra bens jurídicos tradicionais (não relativos à tecnologia) são crimes digitais impróprio (CRESPO, 2017, p.24)

Neste viés, merece nota a classificação de Jesus e Milagre classificando os cibercrimes na mesma vertente, possuindo a figura dos crimes próprios e impróprios,

> Assim, classificamos os crimes informáticos em: a) crimes informáticos próprios: em que o bem jurídico ofendido é a tecnologia da informação em si. Para estes delitos, a legislação penal era lacunosa, sendo que, diante do princípio da reserva penal, muitas práticas não poderiam ser enquadradas criminalmente; b) crimes informáticos impróprios: em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Para estes delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais; c) crimes informáticos mistos: são crimes complexos em que, além da proteção do bem jurídico informático (inviolabilidade dos dados), a legislação protege outro bem jurídico. Ocorre a existência de dois tipos penais distintos, cada qual protegendo um bem jurídico; d) crime informático mediato ou indireto: trata-se do delito informático praticado para a ocorrência de um delito não informático consumado ao final. (JESUS E MILAGRE, 2016, p.22)

Baseado nesta classificação, Jesus e Milagre enunciaram outras duas classificações, sendo elas; crime informático mistos e/ou crime informático mediato ou indireto. A primeira, possui como elemento essencial o uso da internet para a efetiva conduta, contudo, o bem jurídico visado é outro, ou seja, o objeto atingido não será informático. Na segunda, trata-se da realização de um delito informático para a consumação de um delito não informático.

Já a convenção de Budapeste classifica da seguinte forma:

> Título 1 – Infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos: acesso ilegítimo; interceptação ilegítima; interferência em dados; interferência em sistemas; uso abusivo de dispositivos.
> Título 2 – Infrações relacionadas com computadores: falsidade informática; burla informática.
> Título 3 – Infrações relacionadas com o conteúdo: infrações relacionadas com pornografia infantil.

> Título 4 – Infrações relacionadas com a violação do direito de autor e direitos conexos.[10]

Assim, por mais que existam rios de classificações, é visível que o Brasil está seguindo de certa forma uma sincronização na regulação dos cibercrimes. Esta relação de semelhança é importante, visto que, o país é membro da convenção de Budapeste, um acordo internacional de combate aos cibercrimes que, em seu preâmbulo possui como objetivo união e cooperação dos membros signatários para uma política criminal comum e, harmoniosa no que tange ao ordenamento jurídico mundial.

2.5 TÉCNICAS MALICIOSAS:

Nesta parte da pesquisa será destinado para dissertar a respeito dos métodos utilizados por cracker para o alcance de seus objetivos. Consiste em uma principal problemática, pois, estes meios estão em constante transformação e evolução, juntamente por conta do avanço da tecnologia. Nesta parte da pesquisa será apresentado as principais formas conhecidas que os cibercriminosos usam, mas sem a pretensão de esgotamento, visto que, existem múltiplas formas que ainda nem se quer foram descobertas. A maioria dos ataques exploram vulnerabilidade de sistemas, sites, configuração de aplicativos e programas e/ou sistemas informáticos conectados ou não a rede de internet.

> Um ataque de exploração de vulnerabilidades ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível (CERT.BR, 2012, p.18)

Ademais, os cibercriminosos utilizam códigos maliciosos, também conhecidos pela nomenclatura *‘’malware’’,* este é considerado gênero e os códigos espécies que são

---

[10] Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: jul. 2024.

programas destinados a causarem danos a sistemas informáticos, possuindo diversas formas para infectar e comprometê-los, neste viés, os mais comuns são; vírus, trojan, spyware, backdoor, rootkits.

Os ataques possuem diversas motivações, desde interesse em valores pecuniários até simples questões de ego por parte dos criminosos. Desta forma, qualquer pessoa conectada a uma rede, está vulnerável aos cibercriminosos.

O Centro de estudos, resposta e tratamento de incidentes de segurança no Brasil (CERT), publicou uma cartilha de segurança para internet, onde estabelece algumas das principais motivações para a realização dos ataques, sendo elas:

> Demonstração de poder: mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente. Prestígio: vangloriar-se, perante outros atacantes, por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar sites considerados visados ou difíceis de serem atacados; disputar com outros atacantes ou grupos de atacantes para revelar quem consegue realizar o maior número de ataques ou ser o primeiro a conseguir atingir um determinado alvo. Motivações financeiras: coletar e utilizar informações confidenciais de usuários para aplicar golpes (mais detalhes no Capítulo Golpes na Internet). Motivações ideológicas: tornar inacessível ou invadir sites que divulguem conteúdo contrário a opinião do atacante; divulgar mensagens de apoio ou contrarias a uma determinada ideologia Motivações comerciais: tornar inacessível ou invadir sites e computadores de empresas concorrentes, para tentar impedir o acesso dos clientes ou comprometer a reputação destas empresas. (CERT.BR, 2012, p.17)

2.5.1 FALSIFICAÇÃO DE E-MAIL

A falsificação de e-mail se tornou uma técnica comum pelos cibercriminosos, atrelada as falhas no protocolo, utilizam este meio de comunicação para a prática de diversos golpes, como; spam, propagação de malware, phishing, falso pagamento.

> Esta técnica é possível devido a características de protocolo SMTP (Simple Mail Transfer Protocol) que permitem que campos do cabeçalho, como ‘’From:’’ (endereço de quem enviou a mensagem, ‘’Reply-To’’ (endereço de resposta da mensagem) e ‘’Returno-Path’’ (endereço para onde possíveis erros no envio da mensagem são reportados), sejam falsificados. Exemplos de e-mails com campos falsificados são aqueles recebidos como sendo:
> • de alguém conhecido, solicitando que você clique em um link ou execute um arquivo anexo;

> • do seu banco, solicitando que você siga um link fornecido na própria mensagem e informe dados da sua conta bancária;
> • do administrador do serviço de e-mail que você utiliza, solicitando informações pessoais e ameaçando bloquear a sua conta caso você não as envie. (CERT.BR, 2012, p.35)

De acordo com uma matéria publicada por Guilherme Tagiaroli, na revista Uol, acerca do golpe do falso pagamento:

> O golpe do falso pagamento foi o mais comum nas transações online no ano de 2023. Ele representa 30,5% dos golpes em plataformas de venda entre consumidores. Na sequência, vêm invasão da conta (25,6%) e coleta de dados (17,8%).Brasileiros tomaram um prejuízo estimado de R$ 1,1 bilhão no ano passado em golpes digitais ligados a compras online. Houve um crescimento de 12%, na comparação com o ano de 2022, diz a pesquisa.[11]

Desta forma, o golpe de falso pagamento vem sendo utilizada principalmente em *marketplaces online*. Os cibercriminosos entram em contato com a vítima (anunciante) querendo ‘’comprar’’ o produto anunciado, mas dizem que a plataforma está solicitando o e-mail do vendedor e/ou número de telefone, assim, enviam uma cópia da comprovação de ‘’pagamento’’ em nome do próprio marketplace, com detalhes semelhantes ao verdadeiro, fazendo-se presumir que a compra foi realmente realizada.

2.5.2 FORÇA BRUTA

A técnica de força bruta (*Brute Force*) advém de uma falha ou tentativa de acesso não autorizado, através de adivinhar o usuário e senha, de sites, redes sociais e/ou outros serviços, possibilitando o invasor de ter os mesmos benefícios do dono da conta. Insta ressaltar, que existem aplicativos que permitem este tipo de acesso para o cibercriminoso, realizando combinações automáticas.

---

[11] Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2024/02/08/golpe-falso-pagamento-brasil.htm. Acesso em: jun. 2024.

Este tipo de ataque vem se tornando comum em invasões de redes sociais, como; *Instagram*, *Facebook*. O ministério Público do Estado de Minas Gerais publicou uma nota, alertando este tipo de crime cibernético:

> Um crime cibernético tem chamado a atenção do Ministério Público do Estado de Minas Gerais (MPMG) neste início de ano: a invasão de perfis na rede social Instagram. De acordo com levantamento bruto de dados realizado pela Coordenadoria Estadual de Combate aos Crimes Cibernéticos do MPMG (Coeciber), somente em janeiro de 2022 foram registradas 388 ocorrências de acessos indevidos seguidos de golpes para obtenção de valores no estado de Minas Gerais. Esse número é quase 4 vezes maior do que a média do segundo semestre de 2021, que foi de 104 casos por mês. “Este é um dos golpes cibernéticos de maior incidência neste início de ano”, diz o coordenador da Coeciber, promotor de Justiça Mauro Ellovitch. (MPMG, 2022, Online)

Contudo, esta não é o único meio que estes criminosos utilizam para ter acesso, a técnica de “phishing” é uma forma comum para este crime. Neste viés, este tipo de invasão pode vir a causar diversos danos aos proprietários das contas. O Cert.br, em sua cartilha de segurança para internet, discorreu a respeito dos danos causados:

> Se um atacante tiver conhecimento do seu nome de usuário e da sua senha ele pode efetuar ações maliciosas em seu nomo, como, por exemplo:
> • trocar a sua senha, dificultando que você acesse novamente o site ou computador invadido;
> • invadir o serviço de e-mail que você utiliza e ter acesso ao conteúdo das suas mensagens e à sua lista de contatos, além de poder enviar mensagens em seu nome;
> • acessar sua rede social e enviar mensagens aos seus seguidores contendo códigos maliciosos ou alterar as suas opções de privacidade;
> • invadir o seu computador e, de acordo com as permissões do seu usuário, executar ações, como apagar arquivos, obter informações confidenciais e instalar códigos maliciosos.[12]

[12] https://www.cnnbrasil.com.br/tecnologia/phishing/

Disponível em: https://www.cnnbrasil.com.br/tecnologia/phishing/. Acesso em: mai. 2024.

2.5.3 ATAQUE DOS E DDOS

Os ataques DoS e DDoS também denominados como ‘’ataques de negação de serviços’’ é um meio utilizado para causar inacessibilidade de recursos informáticos e das telecomunicações.

> O aplicativo de mensagens Telegram disse que sofreu, nesta quarta-feira (12), um "poderoso ataque de negação de serviço", conhecido como "DDoS Attack" (sigla para "Distributed Denial of Service"). Trata-se da tentativa de tornar os serviços indisponíveis para os usuários. (G1, 2019, Online)

Os cibercriminosos realizam este tipo de ataque a servidores de *internet,* sistemas de empresas, aplicativos de comunicação, deixando os fora do ar, assim, solicitam o pagamento para cessar o ataque. Contudo, existem cibercriminosos que realizam esta conduta somente por mero prazer e *status*.

2.5.4 PHISHING

Esta técnica o objetivo dos cibercriminosos possuem é roubar informações confidenciais, como senhas, dados pessoais, dados de cartão de crédito. Na maior parte das vezes, se passam por instituições, empresas, aplicativos induzindo a vítima a acreditar ser algo legitimo, através de e-mail, links, mensagens de WhatsApp.

> O termo “phishing” tem origem na palavra em inglês “fishing” (pesca), devido à semelhança entre as táticas utilizadas pelos criminosos cibernéticos e a prática de pescar. Os golpistas empregam essa estratégia para obter ilegalmente as informações das vítimas que caem na armadilha criada pelo phisher (ou “pescador”), termo utilizado para descrever aqueles que realizam ataques de phishing. (CNN, 2023, Online)

Diante disto, com as informações em seu domínio estes criminosos podem realizar diversas condutas, como ameaça de exposição de informações, venda de dados de

cartão de crédito, realização de compras. Ademais, esta técnica, assim como outras, também possuem variações na forma de serem realizadas.

2.5.5 TROJAN

Conhecido como ‘’cavalo de troia’’ é uma espécie de malware consiste em um programa, normalmente de uso malicioso, capaz de tornar ou utilizar-se de vulnerabilidades de sistemas informáticos. São altamente perigosos, pois, através dele é possível ter acesso ao sistema também poderá possuir todas as funções do administrador legitimo, executando ações como; cópia de dados, alterar configurações do usuário, corromper arquivos. Este tipo de código malicioso pode ser contraído de diversas maneiras, como por exemplo, clicar em um link ou executar um programa cuja origem é duvidosa

> Exemplos de trojans são programas que você recebe ou obtém de sites na Internet e que parecem ser apenas cartões virtuais animados, álbuns de fotos, jogos e protetores de tela, entre outros. Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador. (CERT.BR, 2012, p. 28)

Insta ressaltar que, existem diversos tipos de códigos, de acordo com o dano que se pretende causar e, uma das suas características é que o invasor na maioria das vezes fica em anonimato, mas o antivírus é possível detectar este tipo de ameaça.

2.5.6 VÍRUS

Esta nomenclatura de código normalmente é utilizada indevidamente como gênero, entretanto trata-se de uma espécie de código malicioso. É dependente da execução de um programa ou arquivo hospedeiro, que se propaga no sistema informático (Como um vírus no corpo humano), assim, conseguindo ter acesso a dados e/ou ao sistema central de um sistema informático possibilitando alterar, destruir, copiar. Propaga-se através de cópias de si mesmo, por isso, denominado como um ‘’vírus’’.

> Há diferentes tipos de vírus. Alguns procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Há outros que permanecem inativos durante certos períodos, entrando em atividade apenas em datas específicas. (CERT.BR, 2012, p.40)

Contudo, o avanço da tecnologia possibilitou sua inserção através de outros meios, mais fáceis para os cibercriminosos, através de e-mail, download de aplicativos cujo a fonte não é confiável, execução de aplicativos, acesso a páginas de web.

2.5.7 SPYWARE

Este tipo de programa atua como uma ‘’central de monitoramento’’, visto que, através dele é possível monitorar as atividades de um sistema e coletar estas informações, sendo uma exceção o controle de um sistema informático através dele. É utilizado tanto de forma legitima, como de forma maliciosa.

> Código ou programa malicioso instalado ou injetado normalmente em aplicativos baixados de fontes duvidosas, que tem a função de coletar informações do usuário de um computador e enviá-las ao destinatário. Informações comumente coletadas são hábitos de consumo, informações de navegação, dentre outros. (JESUS E MILAGRE, 2016, p.15)

O acesso legitimo é aquele em que o proprietário do sistema instala para possuir um controle das informações, sejam elas de navegação, pesquisas e/ou se possuem invasores utilizando seu sistema. Por outro lado, o legitimo é aquele em que um cibercriminoso ‘’invade’’ a privacidade do usuário legitimo, a fim de capturar suas informações e segurança, como por exemplo, senhas e usuários. Além disto, para este tipo de código possuem diversos programas que são utilizados para este tipo de conduta, como; Keylogger, Screenlogger, Adware.

2.5.8 WORM

Esta espécie de *malware* pode ser equiparada ao *vírus,* visto que, também se replicam no computador da vítima. Entretanto, possui uma maneira de propagação distinta. Sua disseminação ocorre através da execução

> Diferente do vírus, o worm não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores. (CERT.BR, 2012, p.25)

Seu objetivo é semelhante aos outros *malware*, pois, visam o acesso aos dispositivos informáticos, roubo de informações confidenciais, corromper arquivos, copiar e/ou alterador dados. Neste viés, é possível contrair este tipo de código através de e-mail, internet, compartilhamento de aplicativos.

3 LEGISLAÇÃO BRASILEIRA

3.1 DESAFIOS ENFRENTADOS PELAS LEIS DE COMBATE AOS CIBERCRIMES

A legislação Brasileira ainda é considerada escassa em relação a tipificação dos cibercrimes, visto que, nosso Código Penal Brasileiro é do ano de 1940, cenário que ainda não era presente os ilícitos digitais ou o ciberespaço. Diante disto, a Constituição Federal de 1988 prevê o princípio da legalidade em seu artigo 5, inciso 2, ‘’ ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei;’’, sendo assim, a ausência da norma penal não permite o Estado de realizar seu direito *Jus Puniendi* (direito de punir). Assim, decorre desta problemática a sensação de insegurança jurídica no que tange a criminalidade digital.

> Sempre foi um desafio tratar de crimes informáticos com um Código Penal da era do Rádio. Nosso Decreto-Lei n. 2.848/40, embora tutele a maioria dos delitos informáticos, é omisso em questões onde a informática deveria ser o bem protegido pelo Direito Penal. (JESUS E MILAGRE, 2016, p.20)

Neste viés, a legislação brasileira já possui alguns dispositivos legais para o combate aos cibercrimes e, vem se desenvolvendo no que tange a área tecnológica, mas com a ágil expansão da tecnologia e condutas ilícitas sofisticadas ainda pegam o ordenamento jurídico de surpresa, trazendo assim, uma reflexão quanto a necessidade de legislações especificas para um combate eficaz das novas formas de realização de condutas ilícitas no ciberespaço, para que assim seja possível uma efetiva proteção de um direito constitucional e fundamental, a segurança e privacidade dos usuários.

> Em tempos onde tudo se torna alvo de leis incriminadoras é preciso ter bom senso e cuidado ao se pretender criar novos crimes. Todos estão exauridos de verificar a enxurrada de tipos penais em nosso ordenamento sem que tragam efetiva contribuição para o convívio em harmonia, para que haja paz social. Isso se dá pela incriminação indistinta de condutas que, no mais das vezes, deveriam ser objeto de políticas sociais mais cuidadosas e de áreas

> Civil e Administrativa, deixando o ramo Penal como a ultima ratio, sempre tão discutida cientificamente, mas que, na prática, não é observada. Em suma, frequentemente não se verifica a ponderação de política criminal ao legislar sobre Direito Penal. (CRESPO, 2017, p.34)

Diante disto, possuem debates a cerca de legislações específicas, visto que, existe uma corrente doutrinária acerca do direito penal mínimo, ou seja, o direito penal só deveria ser acionado em casos de risco social concreto, casos de delitos graves.

> Entretanto, os cibercrimes demonstram uma grande relevância em uma sociedade altamente dependente de sistemas informáticos, telemáticas, redes sociais, aplicativos. Neste viés, ‘’Uma corrente que defendia o “direito penal mínimo” justificava a não necessidade de legislação, afirmando que 95% dos crimes eletrônicos já eram previstos no Código Penal brasileiro.’’ (JESUS E MILAGRE, 2016, p.25)

Ademais, diante do exposto anteriormente existem os crimes próprios e impróprios, os impróprios não causam tanta preocupação, pois, o objeto jurídico já é tutelado pelo código penal, somente sendo um instrumento o meio informático. Entretanto, é necessária uma ênfase na ótica dos crimes próprios, visto que, ainda não são todas as condutas que são devidamente tipificas e todos os objetos jurídicos devidamente protegidos.

> Ao que parece, no Brasil, o legislador criminal pátrio caminha no sentido das alterações do Código Penal e do Código de Processo Penal, ao invés de leis específicas. Tal premissa se justifica com o Projeto de Lei n. 933/99, de autoria do Poder Executivo, que criou a Lei n. 9.983, de 14 de julho de 2000, nascida a princípio para proteger os sistemas da previdência social, e que posteriormente abrangeu toda a Administração Pública, alterando o Código Penal. (JESUS E MILAGRE, 2016, p.25)

3.2 LEIS N.º 12.737/2012 E 12.735/2012

A lei N. 12.735/2012, também conhecida como “Lei Carolina Dieckmann” adveio de um projeto de Lei n. 2.793/2011 que foi acelerado pelo caso da atriz, pois, ela foi alvo de um acesso indevido de seus dados e vazamento de suas fotos intimas após

criminosos invadirem seu computador, além disto, tentaram obter valor pecuniário através de chantagem para que não divulgassem.

Diante disto, discorre Jesus e Milagre a respeito da criação desta legislação:

> 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 tramitavam 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 E MILGARE, 2016, p.35)

Sendo assim, este instrumento penal estabelece princípios, garantias e deveres para o uso da internet no Brasil e criminaliza condutas ilícitas no meio cibernético. É considerado um marco em combate aos cibercrimes, visto que, trouxe novas tipificações penais e alterou o código penal brasileiro, inserindo os artigos 154-A e 154-B. Anteriormente a esta legislação o acesso e cópia indevida de dados era tratado sob outra perspectiva, entretanto, ocorria controvérsias acerca da associação deste tipo de conduta.

> A cópia indevida de dados ou informações no Brasil era conduta sem tipo associado. Muitos promotores, em tais casos, ofereciam denúncias em face do crime de furto, previsto no art. 155 do Código Penal (subtrair, para si ou para outrem, coisa alheia móvel). Na doutrina, muitos asseveravam ser impossível a aplicação do tipo, considerando que a coisa “dados” não saía da esfera de disponibilidade da vítima, mas tão somente era “copiada”. Um “ctrl+c” não poderia ser considerado furto. Estes ajustes na legislação criminal são supridos com a Lei n. 12.737/2012, pelo art. 154-A do Código Penal. (JESUS E MILAGRE, 2016, p.35)

Diante disto, a referida lei possui o viés da proteção dos direitos de segurança, privacidade, intimidade e proteção das informações dos usuários, encerrando as controvérsias acerca da associação de qual seria a conduta correta atrelada a este tipo de delito.

Neste viés, os artigos 154-A e 154-B descrevem como conduta ilícita:

> 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:
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos

Sendo assim, aquele que realizar o tipo objetivo ‘’invadir’’ dispositivo informático alheio, protegido por mecanismo de segurança (legislador não foi taxativo quanto a isso), com a finalidade de obter, adulterar ou destruir dados ou informações, sem a devida autorização incorre no crime do art. 154-A.

Outra legislação de suma importância é a Lei 12.735/2012, denominada “Lei Azeredo”, adveio do Projeto de Lei n. 84/99 (89/2003), realizando alterações no Código Penal e Código Penal Militar e, não trouxe novos tipos penais, apenas alterou aqueles já existentes.

Diante disto, trouxe a figura de equipes especializas no combate ao cibercrime, conforme seu artigo 4, diante disto, a polícia judiciária já possui delegacias em conformidade com este artigo.

3.3 DECRETO Nº 11.491/2023

O Brasil tornou-se signatário da conhecida como convenção de Budapeste, um acordo internacional contra os cibercrimes, firmada em 2001.

Este instrumento é considerado relevante no que tange a um combate eficiente e harmônico entre países, visto que, o *inter criminis* neste tipo de delito ocorre de forma fragmentada e as ações e resultados podem ser realizadas em multilocais.

> Reconhecendo a importância de fomentar a cooperação com as outras Partes desta Convenção; Convencidos da necessidade de buscar prioritariamente uma política criminal comum destinada à proteção da sociedade contra o crime cibernético, nomeadamente pela adoção de legislação apropriada e pela promoção da cooperação internacional, entre outras medidas; Conscientes das profundas mudanças desencadeadas pela digitalização, interconexão e contínua globalização das redes informáticas; Preocupados com os riscos de as redes informáticas e as informações eletrônicas também poderem ser utilizadas para a prática de crimes e de as provas dessas infrações poderem ser armazenadas e transferidas por meio dessas redes;

Neste contexto, é um acordo crucial para uma cooperação internacional, devendo o Brasil seguir seus objetivos para que assim ocorra uma frente unida em outros países que fazem parte deste acordo. Além disto, é responsável por trazer classificações dos cibercrimes, medidas a serem tomadas, definições terminológicas, que em conjunto auxiliam em uma compreensão mais detalhada e tornando o sistema jurídico brasileiro mais abrangente no que tange as estas condutas ilícitas praticadas no ciberespaço.

4. CONSIDERAÇÕES FINAIS

A presente pesquisa abrangeu a respeito dos cibercrimes, sua conceituação, nomenclaturas, diferença de crimes próprios para os impróprios, questões referentes ao ciberespaço, bem como as formas de realização destes delitos por parte dos cibercriminosos. Diante disto, se tornou possível entender o nível de complexidade inerente a esta nova ‘’modalidade’’ de crimes e/ou forma de *modus operandi*, levando em consideração a constante evolução do meio tecnológico no Brasil e no mundo.

Neste viés, esta complexidade influencia no contexto jurídico tornando desafiador questões envolvidas na adaptação e eficácia de legislações brasileiras acerca dos cibercrimes na denominada ‘’era da informação’’. Ademais, nosso código penal é anterior ao surgimento deste tipo de delito, visto que, é de 1940 e uma das primeiras redes de ‘’internet’’ é de 1966, ou seja, não tinha como o legislador prever este tipo de cenário.

Contudo, este cenário chegou, os riscos e danos causados por esta evolução se mostraram preocupantes, pois, a sociedade atual está vivendo um mundo tecnológico e ainda mais globalizado. Sendo assim, o direito penal Brasileiro não pode ser ainda considerado um instrumento apto contra os cibercrimes, fundamentado pela falta de tipificação de condutas específicas. Além disto, se faz necessário uma harmonia quanto as tipificações, pois, as controvérsias acerca da necessidade de uma tipificação especificam ainda se fazem presente.

Muito temos a caminhar no ordenamento jurídico brasileiro, até mesmo quando se trata da criação de legislações embasada nos princípios adotados pelo direito penal, possibilitando lacunas a serem preenchidas de forma recorrente, pois, as condutas ilícitas vão se modificando dia após dia e, a necessidade da aproximação da cooperação internacional, no que tange a isso, o Brasil está caminhado em um bom sentido, pois, já se tornou signatário da convenção de Budapeste.

5. REFERÊNCIAS

ARAS, VLADIMIR. Crimes de informática. Disponível em: https://jus.com.br/artigos/2250/crimes-de-informatica. Acesso em: jun. 2024.

BARBAGALO, Fernando Brandini Barbagalo. O novo crime de fraude eletrônica e o princípio da legalidade. Portal TJDFT. 2022. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2022/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade#:~:text=%22A%20pena%20%C3%A9%20de%20reclus%C3%A3o,qualquer%20outro%20meio%20fraudulento%20an%C3%A1logo%22. Acesso em: jun. 2024.

BRACO, Anselmo Lázaro. Revoluções industriais - Primeira, segunda e terceira revoluções. 2021. Disponível em: https://educacao.uol.com.br/disciplinas/geografia/revolucoes-industriais-primeira-segunda-e-terceira-revolucoes.htm. Acesso em: jun. 2024.

BRASIL. Decreto n. 11.491, de 12 de abril de 2023. Convenção sobre o Crime Cibernético.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

BRASIL. Lei 14.155. de 27 março de 2021.

DA SILVA, Patrícia Santos. Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015.

HAIDER, Daniel. PF tem recorde de investigações sobre crimes cibernéticos. 2023. Disponível em: https://www.terra.com.br/noticias/daniel-haidar/pf-tem-recorde-de-investigacoes-sobre-crimes-ciberneticos,5775122ec61ae1eec7ec852a883239fb42e9xt21.html#:~:text=Policiais%20federais%20abriram%20845%20inqu%C3%A9ritos%20para%20investigar%20ataques%20virtuais%20em%202022&text=A%20Pol%C3%ADcia%20Federal%20enfrenta%20um,cibern%C3%A9ticos%20em%20todo%20o%20pa%C3%ADs.Acesso em: maio. 2024.

HELDER, Darlan. Entenda O Que É Um 'Hacker' E A Diferença Para 'Cracker'. Portal G1. Disponível em: https://g1.globo.com/tecnologia/noticia/2023/08/18/entenda-o-que-e-um-hacker-e-a-diferenca-para-cracker.ghtml. Acesso Em: Jun. 2024.

SANTOS, Milton. Por uma outra globalização: do pensamento único à consciência universal. Rio de Janeiro: Record, 2011. 20ª ed. 174p.

SANTOS, Milton. Técnica, Espaço, Tempo: Globalização e Meio Técnico-científico-informacional. São Paulo: Editora da Universidade de São Paulo, 2013. 5 ed., 1 reimp. 176p."

SILVA, Daniel Neves. História da Internet. Portal UOL. 2015. Disponível em: https://brasilescola.uol.com.br/informatica/internet.htm. Acesso em: maio. 2024.