CENTRO UNIVERSITÁRIO PARA O DESENVOLVIMENTO DO ALTO VALE DO ITAJAÍ – UNIDAVI

GUSTAVO ERN GODOI

CRIMINALIDADE NO MEIO DIGITAL: A (IN) SUFICIÊNCIA DA LEGISLAÇÃO BRASILEIRA EM RELAÇÃO AOS CRIMES CIBERNÉTICOS NO BRASIL

RIO DO SUL

2022

CENTRO UNIVERSITÁRIO PARA O DESENVOLVIMENTO DO ALTO VALE DO ITAJAÍ – UNIDAVI

GUSTAVO ERN GODOI

CRIMINALIDADE NO MEIO DIGITAL: A (IN) SUFICIÊNCIA DA LEGISLAÇÃO BRASILEIRA EM RELAÇÃO AOS CRIMES CIBERNÉTICOS NO BRASIL.

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito, pelo Centro Universitário para o Desenvolvimento do Alto Vale do Itajaí - UNIDAVI

Orientador(a): Prof.Esp. Giovane Fernando Medeiros

RIO DO SUL

2022

CENTRO UNIVERSITÁRIO PARA O DESENVOLVIMENTO DO ALTO VALE DO ITAJAÍ – UNIDAVI

A monografia intitulada **"CRIMINALIDADE NO MEIO DIGITAL: A (IN) SUFICIÊNCIA DA LEGISLAÇÃO BRASILEIRA EM RELAÇÃO AOS CRIMES CIBERNÉTICOS NO BRASIL.."**, elaborada pelo(a) acadêmico(a) Gustavo Ern Godoi, foi considerada

( ) APROVADA

( ) REPROVADA

por todos os membros da banca examinadora para a obtenção do título de BACHAREL EM DIREITO, merecendo nota _____.

_____, _____ de _____ de _____.

_____

Profa. M.ª Vanessa Cristina Bauer

Coordenadora do Curso de Direito

Apresentação realizada na presença dos seguintes membros da banca:

Presidente: _____

Membro: _____

Membro: _____

TERMO DE ISENÇÃO DE RESPONSABILIDADE

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico conferido ao presente trabalho, isentando o Centro Universitário para o Desenvolvimento do Alto Vale do Itajaí, a Coordenação do Curso de Direito, a Banca Examinadora e o Orientador de toda e qualquer responsabilidade acerca do mesmo.

Rio do Sul , 04 de novembro de 2022.

Gustavo Ern Godoi
Acadêmico(a)

AGRADECIMENTOS

Agradeço à Deus pelas oportunidades que me foram dadas no decorrer da vida.

À minha mãe e aos meus irmãos por todo o apoio durante minha jornada acadêmica, em especial à minha irmã, a qual foi para mim uma inspiração na realização de um sonho.

Ao meu orientador Prof.Esp. Giovane Fernando Medeiros pelo incentivo e norteamento na elaboração deste projeto de pesquisa.

E em especial aos amigos Beatriz Lange Santos, Eduardo Thives de Miranda e por fim Helena Cristina Torinelli, não pelos exemplos que são, nem pelo grande apoio fornecido, mas acima de tudo, pela amizade.

A todos aqueles que contribuíram para a construção desse trabalho, em especial aos amigos que me acompanharam e incentivaram-me no estudo da matéria.

RESUMO

Neste trabalho serão abordados os aspectos históricos e conceituais dos crimes cibernéticos, bem como algumas noções gerais de cibercriminalidade e uma breve explanação das atuais leis brasileiras que tratam do referido tema. No mesmo sentido, o enfoque da presente pesquisa é um estudo mais aprofundado em relação à dinâmica da sociedade diante dos crimes cibernéticos, e também a fragilidade do enfoque brasileiro em relação à criminalidade digital. Assim, a priori, foi realizado um apanhado de conceitos relacionados aos crimes cibernéticos, bem como, a respeito da lacuna legislativa presente no ordenamento jurídico brasileiro a respeito desta temática. Posteriormente, desenvolveu-se uma análise acerca das atuais leis que tratam sobre o tema, como a Lei Azeredo e Lei Carolina Dickmann, bem como da Convenção de Budapeste. A metodologia utilizada para a construção do estudo foi em formato de pesquisa bibliográfica, respaldada por grandes doutrinadores do Direito Penal, jurisprudência e legislação, além de artigos renomados sobre o tema. Por fim, é essencial evidenciar que a falta de tipificação adequada para os delitos praticados no ambiente cibernético, promove insegurança tanto para a sociedade quanto para o âmbito jurídico brasileiro, assim, verifica-se a ausência tanto da legislação quanto da capacidade técnica para produzir a mesma, criando assim uma insegurança à sociedade e impunibilidade àqueles que se utilizam de meios escusos para provocar danos materiais e morais a terceiros.

Palavras-chave: Cibercrime, Convenção de Budapeste., Internet, Lei Azeredo, Lei Carolina Dickmann,

ABSTRACT

In this work, the historical and conceptual aspects of cyber crimes will be addressed, as well as some general notions of cybercrime and a brief explanation of the current Brazilian laws that deal with this topic. In the same sense, the focus of the present research is a more in-depth study in relation to the dynamics of society in the face of cyber crimes, and also the fragility of the Brazilian approach in relation to digital crime. Thus, a priori, a brief overview of concepts related to cyber crimes was carried out, as well as, regarding the legislative gap present in the Brazilian legal system regarding this theme. Subsequently, an analysis was developed about the current laws that deal with the subject, such as the Azeredo Law and Carolina Dickmann Law, as well as the Budapest Convention. The methodology used for the construction of the study was in the form of a bibliographic research, supported by great scholars of Criminal Law, jurisprudence and legislation, in addition to renowned articles on the subject. Finally, it is essential to highlight that the lack of adequate typification for crimes committed in the cyber environment promotes insecurity both for society and for the Brazilian legal scope, thus, there is a lack of both legislation and technical capacity to produce the itself, thus creating insecurity for society and impunity for those who use shady means to cause material and moral damages to third parties.

Palavras-chave: Azeredo Law, Budapest Convention., Carolina Dickmann Law., Cybercrime, Internet.

LISTA DE ABREVIATURAS E SIGLAS (SE HOUVER)

Elemento opcional. Listar somente se o trabalho tiver acima de 5 siglas e/ou abreviaturas.

MIT = Instituto de Tecnologia de Massachusetts
EUA = Estados Unidos da América
ARPA = Rede de Agência de Projetos de Pesquisa Avançada
ENIAC = Eletrical Numerical Integrator and Calculator
COVID-19 = Pandemia causada pelo vírus SARS-CoV-2 no ano de 2019
ONU = Organização das Nações Unidas
UIT = União Internacional de Telecomunicações
BBC = British Broadcasting Corporation
LNCC = Laboratório Nacional de Computação Científica

SUMÁRIO

INTRODUÇÃO

Primeiramente, analisa-se que com o advento da internet, surgiram novos meios de interação social, e como tal, também estes estão sujeitos a marginalização e criminalidade. Assim, procurou-se abordar acerca positivação dos crimes cibernéticos, contextualizando sobre o déficit em torno do sistema jurídico brasileiro e principalmente do Código Penal envolvendo a culpabilidade das condutas ilícitas praticadas no ambiente virtual, contextualizando em relação à eficácia ou não das leis referentes ao assunto, quais sejam, a lei 12.737/2012 e a lei 12.735/2012.

Não obstante, no presente estudo, utilizou-se jurisprudências, além de legislações nacionais e internacionais que regulamentam acerca da relação entre os crimes cibernéticos e a lacuna em torno da codificação dos referidos ilícitos virtuais dentro do ordenamento jurídico brasileiro. Do mesmo modo, procurou-se adotar um levantamento bibliográfico, com o uso de doutrinas renomadas pelo Direito Penal Brasileiro, como Guilherme de Souza Nucci, Rogério Grecco, Damásio de Jesus.

Em suma, o presente trabalho se propõem a uma abordagem dos fatos históricos pertinentes à evolução da internet, desde sua concepção até sua disseminação na sociedade atual, através de pesquisa bibliográfica de conceitos históricos e também de análise de gráficos elaborados com base na expansão da Internet e como essa está ligada ao cotidiano do ser humano.

Por fim, verifica-se que através do exposto, a internet cresce a cada dia, de forma que, atualmente, mais da população mundial possui acesso à rede, o que torna as medidas de restrição e conscientização ainda mais necessárias e urgentes. No mesmo sentido, a mesma não só facilitou o acesso ilegal a informações, como também criou uma espécie de realidade virtual, assim os usuários desenvolveram uma linguagem, um meio de interação social, próprios dessa realidade. Não obstante, analisa-se que através da atual legislação, falta de uma análise técnica por profissionais da área, tanto do Direito quanto de Sistemas de Informação, uma vez que a lacuna na lei gera insegurança e impunidade ao sistema jurídico brasileiro.

CAPÍTULO 1

1. ASPECTOS HISTÓRICOS E CONCEITUAIS DOS CRIMES CIBERNÉTICOS

1.1 CONCEITO DE INTERNET

Antes da abordagem histórica acerca do surgimento da Internet, precisamos entender o que é e como se conceitua nos dias atuais.Internet em poucas palavras é um conjunto de redes mundial, que teve origem inglesa , onde “inter” vem de internacional, e “*net*” significa rede, ou seja rede de computadores mundial.Assim, busca-se uma definição na doutrina de Luis Monteiro:

> A internet (ou a “Rede” como também é conhecida) é um sistema de redes de computadores interconectadas de proporções mundiais, atingindo mais de 150 países e reunindo cerca de 300 milhões de computadores (DIZARD, 2000) e mais de 400 milhões de usuários. Computadores pessoais ou redes locais (em um escritório, por exemplo) se conectam a provedores de acesso, que se ligam a redes regionais que, por sua vez, se unem à redes nacionais e internacionais. A informação pode viajar através de todas essas redes até chegar ao seu destino. Aparelhos chamados “roteadores”, instalados em diversos pontos da Rede, se encarregam de determinar qual a rota mais adequada. [1]

Em suma, a internet é um meio pelo qual se tem o acesso a informações de todos os tipos, além de obter uma grande variedade de recursos e serviços, como compartilhamento de arquivos, e-mails, serviços de comunicação ao vivo, redes sociais, entre outros.

---

[1] MONTEIRO, Luís. A INTERNET COMO MEIO DE COMUNICAÇÃO: POSSIBILIDADES E LIMITAÇÕES. Campo Grande/MS: INTERCOM, XXIV Congresso Brasileiro da Comunicação, set. – 2001. Disponível em :<http://www.jack.eti.br/www/arquivos/documentos/trabalhos/fae/Trabalho_Redes_Ainarte_26032008.pdf.> Acessado em 10/10/2022.

1.2 HISTÓRIA DA INTERNET E SEU ASPECTO EM ÂMBITO INTERNACIONAL

No atual capítulo serão indagados os aspectos históricos da internet, bem como sua relevância na presente sociedade, pois é igualmente importante explicar a conjuntura social que impeliu em seu advento, até ser transformada na poderosa ferramenta que é usada hoje, inclusive para fins citados como ilícitos. Ao fim, serão trazidos à pauta alguns conceitos iniciais de crimes cibernéticos, abordando como e quais são os crimes incisivos no âmbito virtual atualmente. Analisa-se que a Internet antes de ser nos moldes atuais, passou por muitas etapas para chegar em sua atual fase. Primeiramente, extrai-se que a mesma teve seu surgimento em uma pesquisa realizada pelo Instituto de Tecnologia de Massachusetts (MIT) na década de 1960, o qual tinha como objetivo buscar uma comunicação através da troca de informações entre computadores. Posteriormente, com base nesse estudo, desenvolveu-se a ARPANET, sendo gerenciada através do Departamento de Defesa dos Estado Unidos da América(EUA), sendo que apenas em 1969 começou sua operação de testes. O historiador Peter Knight, relata que:

> A ARPANET não foi projetada para uso militar, como normalmente se pensa,mas sim para compartilhar recursos de computação entre universidades de pesquisa apoiadas pelo Pentágono.[2]

Apesar de parecer ter surgido da simples conexão espontânea de computadores, a Internet não se desenvolveu do nada. Trata-se do fruto de um planejamento estratégico que remonta a década de 60. Ameaçado pelo véu da Guerra Fria, e temeroso de ataques militares oriundos do bloco soviético, o governo norte-americano, através do Departamento de Defesa, fomentou o projeto ARPANET, que foi criado e desenvolvido pela Advanced Research Projects Agency – Rede de Agência de Projetos de Pesquisa Avançada – (ARPA). Ocorre que não somente a transmissão de dados teve que ser estudada, mas sim um sistema que transmitisse essa informação para outro objeto, assim se criou o computador. Salienta-se que o computador tem sua história criada desde os tempos da Segunda Guerra Mundial, onde o governo britânico, desenvolveu um projeto a fim de

[2] Knight, Peter T.. A Internet No Brasil: Origens, Estratégia, Desenvolvimento E Governança. Estados Unidos: AuthorHouse, 2014. Acesso em 10 de outubro de 2022.

decodificar as mensagens criptografadas pela Alemanha Nazista, e assim, ter em suas mãos a informação de todos os ataques nazistas. Em relação ao estudo realizado pelo doutrinador Raul Wazlawick, diz que:

> Alan Turing foi contratado pelo governo britânico juntamente com outros cientistas para tentar decifrar as mensagens da Enigma em Bletchley Park. O problema era sério pois todos os dias, à meia-noite, os alemães trocavam as configurações dos plugues da máquina. Assim, se eles levassem mais de 24 horas para adivinhar a configuração atual, o trabalho se tornava inútil, pois neste momento outra disposição já estaria sendo usada.O ideal seria que conseguissem descobrir a nova configuração o mais rápido possível, pois assim poderiam decifrar um grande número de mensagens secretas nazistas durante o dia.[3]

Destaca Silva em relação a criptografia que:

> Conceitualmente, a criptografia se traduz em esconder ou mascarar informações através de linguagem codificada. Essa é uma prática quase tão antiga quanto a própria humanidade, pois já no período de conflitos entre a Grécia e a Pérsia emergia-se a necessidade de transmitir informações secretamente, ocultando-as, de maneira que somente o destinatário final da mensagem seria capaz de decifrá-la.[4]

Com a vitória sobre a Alemanha Nazista, Turing em colaboração com a Universidade da Pensilvânia, ajudou na construção do projeto ENIAC (*Eletrical Numerical Integrator and Calculator*), o qual estava em construção desde 1943, o projeto contava com 18000 válvulas, 15000 relés e emitia o equivalente a 200 quilowatts de calor.

> Em 1943 durante a II guerra mundial foi desenvolvido o ENIAC, que pesava 30 toneladas e tinha 5;5 metros de altura,25 metros de comprimento e 70 mil resistores e 17.468 válvulas.[5]

Assim, verifica-se que essa grande máquina acabou por ser concentrada em uma sala de 9m por 30m. Sendo que o desenvolvimento do computador prosperou, contudo apenas com a invenção do transistor de silício, no ano de 1947,

---

[3] Wazlawick, Raul. História da Computação. Disponível em: Minha Biblioteca, Grupo GEN, 2016.

[4] SILVA, Fernanda Tatiane da. PAPANI, Fabiana Garcia. Um pouco da história da criptografia. Publicado em Anais da XXII Semana Acadêmica de Matemática da Unioeste, 2016. Disponível em <http://projetos.unioeste.br/cursos/cascavel/matematica/xxiisam/artigos/16.pdf>. Acesso em 26 de setembro de 2022.

[5]Google, A História do Primeiro Computador. Disponível em: <https://sites.google.com/site/historiasobreossitesdebusca/Historia-da-tecnologia/historia-do-primeiro-computador> Acessado em 13 de setembro de 2022

possibilitou-se a demanda criada em relação com a velocidade das operações na computação, tendo em vista que a mesma era um obstáculo.

No mesmo sentido, em meados dos anos 60, os cientistas analisaram que um circuito eletrônico tinha um funcionamento de modo igualmente satisfatório se tivesse o tamanho menor, assim realizou-se experimentos a fim de colocar um projeto de circuito no chip. Não obstante, antes do fim da época supracitada, nasceu o "circuito integrado",acarretando em um grande passo para a computação. O desenvolvimento de um circuito em um único chip levou à construção de múltiplos circuitos em um só chip; e o resultado inevitável da colocação de vários chips juntos foi o começo do microprocessador.

Para os historiadores do *The Computer Society:*

> Na época, o ENIAC se destacou por realizar 5 mil operações por segundo, velocidade mil vezes superior à de seus antecessores. Hoje, se comparado com os computadores atuais, o poder de processamento do ENIAC seria menor do que o de uma simples calculadora de bolso. O computador começou a ser feito em 1943, durante a Segunda Guerra Mundial, para auxiliar o exército norte-americano a fazer cálculos de balística. O computador pesava 30 toneladas e ocupava 180 m² de área construída.[6]

Não obstante, destaca-se Paesani em sua fala:

> A década de 1950 teve maior relevância no contexto histórico da internet, pois foi nesse período em que se deu o auge da ocorrência de crimes informáticos, isso antes mesmo da percepção de cibercriminalidade sequer existir. Isso só foi possível com a criação do projeto militar ARPANET da Agência de Projetos de Pesquisa Avançada dos Estados Unidos. Esse projeto foi o precursor da internet, pois foi a primeira rede operacional de computadores interativa à base de comutação de dados.[7]

Assim, com a iminente ameaça que assolava o mundo com a Guerra Fria na década de 1960, o Estados Unidos com o estudo supracitada, o qual acabou por desenvolver o que hoje conhecemos como internet, uma vez que sua ideia consistia em não centralizar o conhecimento em apenas um lugar, o qual na nação supramencionada, estava direcionada apenas ao PENTÁGONO, onde se localiza seu departamento de defesa.

Segundo Marcelo Xavier Crespo em seu livro relata que:

---

[6]Google, A História do Primeiro Computador. Disponível em <https://sites.google.com/site/historiasobreossitesdebusca/Historia-da-tecnologia/historia-do-primeiro-computador> Acessado em 13 de setembro de 2022

[7]PAESANI, Liliana Minardi. Direito e Internet: liberdade de informação, privacidade e responsabilidade civil. 1ª ed. São Paulo, Atlas: 2000.

> Podemos dizer que ela surgiu na década de 60, mais precisamente no ano de 1966, quando algumas universidades se uniram para desenvolver a ARPANET (Advanced Research Projects Administration – Administração de Projetos e Pesquisas Avançados). Naquela oportunidade, seu uso era exclusivo das Forças Armadas norte-americanas. Seu propósito era prover um contínuo funcionamento daquela rede, mesmo em casos de calamidade como um ataque nuclear. Destarte, era de suma importância não haver um comando central que pudesse ser alvejado. Este é o típico retrato do medo causado pela Guerra Fria, que dominava o mundo naquela época.[8]

No mesmo sentido, em uma iminente guerra nuclear, o primeiro alvo para o ataque direto seria o seu próprio departamento de defesa, o qual não teria como ordenar as tropas remanescentes no campo de batalha, causando a disseminação do pânico e uma futura perda da guerra.

Não obstante, os historiadores Briggs e Burke corroboram com essa tese em seu livro:

> A visão do Pentágono era que a Arpanet seria um importante mecanismo de defesa: ainda que os computadores ou mesmo a infraestrutura de comunicação fossem destruídos em um ataque nuclear do rival soviético, a rede ainda seria mantida.[9]

Analisa-se que Baratta tem a mesma visão:

> Sabe-se que a internet teve início em plena guerra fria e foi utilizada como uma arma norte-americana de informação militar. E possuía como principal função interligar todas as centrais de computadores dos postos de comando estratégico, fazendo com que os americanos se prevenissem de uma suposta ofensiva russa. Porém se ocorresse algum imprevisto em um desses pontos estratégicos e os americanos fossem atacados, os demais pontos continuariam funcionando de forma autônoma, auxiliando e fortalecendo informações a outros centros militares.[10]

A junção de todas essas redes deu origem a chamada ARPA INTERNET que posteriormente passou a ser chamada de Internet, mas que continuava vinculada ao Departamento de Defesa Norte Americano, órgão responsável pelo seu financiamento, e à Fundação Nacional da Ciência, a quem cabia a sua operação.

Assim, o doutrinador Manuel Castells relata que:

> Nas origens da Internet está o trabalho de uma das instituições e pesquisa mais inovadoras do mundo: a Agência de Projetos de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos (DARPA). Quando, no final dos anos 50, o lançamento do primeiro Sputnik alarmou o establishment

---

[8] CRESPO, Marcelo Xavier de F. Crimes digitais, p.13: Editora Saraiva, 2011. E-book. ISBN 9788502136663. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502136663/. Acesso em: 29 set. 2022.

[9] BRIGGS e BURKE, Asa e Peter.Uma História Social da Mídia.Editora Zahar. Acesso em: 25 out. 2022.

[10] BARATTA, Alessandro. Criminologia Crítica e Crítica do Direito Penal – Introdução à Sociologia do Direito Penal. 3. Ed. Rio de Janeiro: Revan, 2002.

> militar norteamericano de alta tecnologia, a DARPA assumiu varias iniciativas ousadas, algumas das quais mudaram a história da tecnologia e estabeleceram a era da informação em grande escala. Uma dessas estratégias, que desenvolvia uma idéia concebida por Paul Baran da Rand Corporation, era projetar um sistema de comunicação invulnerável a ataque nuclear. Com base na tecnologia de comunicação por comutação de pacotes, o sistema tornou a rede independente de centros de comando e controle, de modo que as unidades de mensagens encontrariam suas rotas ao longo da rede, sendo remontadas com sentido coerente em qualquer ponto dela.[11]

Paesani ainda destaca que:

> A partir daí a internet começou a obter uma concepção mais próxima da atual, elevando o conceito de crimes informáticos a patamares mais elevados. De arma militar a produto lucrativo, a popularização somente começou em 1988. Com o fim da guerra e das tensões entre EUA e URSS, houve a abertura da rede para interesses comerciais, quando os Estados Unidos começaram a “comercializar” a internet [12]

Assim, em meados de 1990, o projeto ARPANET foi desativado. Todavia, a semente da Internet já tinha sido semeada. Ocorre que percebendo o enorme potencial oferecido por esse meio de comunicação, as universidades norte americanas aproveitaram a estrutura existente e interligaram-se, formando assim uma rede nacional de troca de informações científicas, uma vez que, os custos de uso da Internet para o envio de informações escritas eram muito menos onerosos do que os dos meios então existentes.

Do mesmo modo, CRESPO relata que:

> A ARPANET cresceu muito com a grande expansão da telefonia norte-americana. Porém, foi a implementação do TCP/IP25 (Protocolo de Controle de Transferência/Protocolo de Internet) que efetivamente possibilitou o surgimento da internet. Esse protocolo é responsável pela interligação dos diversos computadores, possibilitando que atuem em grupo. O tempo passou, mas o princípio básico da internet não desapareceu. Até hoje ela baseia-se na ideia de não se produzir comandos centrais, tornando todos os pontos equivalentes. Assim, não importa onde estejam os computadores, seja no Brasil ou em Burkina Fasso, na França ou em Togo.[13]

---

[11] CASTELLS, Manuel. Fim do Milênio. 4. ed. Tradução de Klauss Brandini Gerhardt e Roneide Venancio Majer. São Paulo: Paz e Terra, 2007. (A Era da Informação: economia, sociedade e cultura; v. 3).

[12]PAESANI, Liliana Minardi. Direito e Internet: liberdade de informação, privacidade e responsabilidade civil. 1ª ed. São Paulo, Atlas: 2000.

[13] CRESPO, Marcelo Xavier de F. Crimes digitais, p. 13: Editora Saraiva, 2011. E-book. ISBN 9788502136663. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502136663/. Acesso em: 29 set. 2022.

Não obstante, em face das facilidades e dos baixos custos, a rede que interligava as universidades americanas se expandiu para fora dos limites dos Estados Unidos e acabou tomando um caráter mundial, passando a servir de elo de comunicação entre meios acadêmicos de todo o mundo.

No mesmo sentido, Douglas Comer, especialista no assunto, alega que:

> O crescimento contínuo da Internet global é um dos fenômenos mais interessantes e empolgantes em redes. Em 1980, a Internet era um projeto de pesquisa que envolvia algumas dezenas de sites. Hoje, ela cresceu e se tornou um sistema de comunicação produtivo que alcança milhões de pessoas em todos os países povoados do mundo. Muitos usuários já têm acesso à Internet de alta velocidade por meio das conexões a cabo (cable modem), DSL, fibra óptica e tecnologias sem fio.[14]

Muito se evoluiu até à sua chegada ao Brasil em 1988, desde o seu nome até o seu objetivo, assim, de Arpanet foi para Internet, tendo seu uso no estado brasileiro apenas para fins acadêmicos, onde seu primeiro acesso se deu através do Laboratório Nacional de Computação Científica (LNCC).

A primeiro conexão precedida no Brasil ocorreu entre LNCC e FAPESP:

> A ligação da FAPESP não foi a primeira conexão de rede a chegar ao Brasil. Ela foi precedida pelo Laboratório Nacional de Computação Científica do CNPq que alugou uma linha da Embratel três meses antes da FAPESP, ligando-se à BITNET. Mas esta linha, embora muito importante, não teve a sorte de ter o mesmo impacto da iniciativa da FAPESP. A ligação do LNCC não evoluiu com o tempo e ela foi desativada com a mesma velocidade inicial de 9.600 bps, em 1996, quando da desativação da rede BITNET no Brasil.

Posteriormente, através de uma estruturação em âmbito nacional, vários estados começaram a ter internet em suas universidades, contudo, somente no ano de 1994, com a criação do World Wide Web (WWW-1990), possibilitou-se a implementação desse sistema para fins comerciais, sendo disponibilizada para o público em geral.

No mesmo sentido, extrai-se através do doutrinador Fernando Henrique Biolcati que:

> De modo geral, a Internet conceitua-se como uma rede mundial de computadores interligados entre si, que compartilham, para esse fim, um conjunto de protocolos denominado TCP/IP, a permitir a troca de dados entre aqueles. É a rede que conecta outras redes públicas, privadas, de pesquisa, do terceiro setor, por meio de uma infraestrutura global e local,

[14] Comer, Douglas E. Redes de computadores e internet [recurso eletrônico] / Douglas E. Comer ; tradução: José Valdeni de Lima, Valter Roesler. – 6. ed. – Porto Alegre : Bookman, 2016.

> sendo utilizada para os mais diversos fins, de natureza econômica ou não. Não se confunde com a “World Wide Web”, uma de suas ferramentas que possibilita o câmbio de documentos entre os usuários no ambiente da Internet.[15]

Sendo assim, a internet tornou-se um meio de comunicação que permite, pela primeira vez, a comunicação de grande massa, o uso dessa teve seu ápice no final de 1995, onde em seu primeiro ano, contou com cerca de 16 milhões de usuários de redes de comunicação por computador no mundo, assim, o governo estadunidense decidiu privatizar a internet, retirando do controle estatal, devido a sua alta demanda.

Segundo o relato de Luis Monteiro:

> Em 1995, devido ao grande aumento de usuários no início da década de 90 a internet foi transferida para a administração de instituições não-governamentais, que se encarregam, entre outras coisas,estabelecer padrões de infraestrutura, registrar domínios, etc.Exemplos dessas instituições são a Internet Society, situada nos Estados Unidos, mas atuando no mundo inteiro, e o Comitê Gestor da Internet que atua restritamente no Brasil. [16]

No mesmo sentido, após 6 anos do seu surgimento, havia mais de 400 milhões de pessoas conectadas e nessa expansão se segue até os dias atuais, sendo que em uma recente pesquisa realizada pelo Instituto de Ensino e Pesquisa(INSPER), estimulou que cerca há cerca de 5 bilhões de conexões ativas na rede mundial de computadores[17].

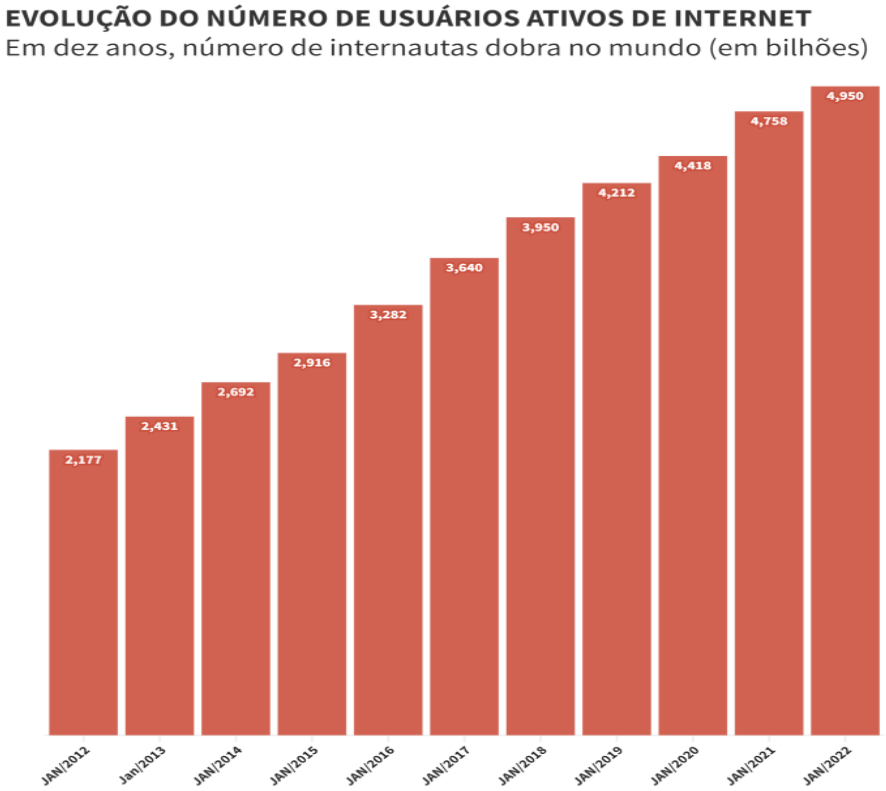
---

[15] Biolcati, Fernando Henrique de Oliveira. INTERNET, FAKE NEWS E RESPONSABILIDADE CIVIL DAS REDES SOCIAIS, Almedina, 2022.

[16] MONTEIRO, Luís. A INTERNET COMO MEIO DE COMUNICAÇÃO: POSSIBILIDADES E LIMITAÇÕES. Campo Grande/MS: INTERCOM, XXIV Congresso Brasileiro da Comunicação, set. – 2001. Disponível em :<http://www.jack.eti.br/www/arquivos/documentos/trabalhos/fae/Trabalho_Redes_Adinarte_26032008.pdf.> Acessado em 10/10/2022.

[17] Insper, Instituto de Ensino e Pesquisa, Mundo se aproxima da marca de 5 bilhões de usuários de Internet. Publicado em 2022. Disponível em: https://www.insper.edu.br/noticias/mundo-se-aproxima-da-marca-de-5-bilhoes-de-usuarios-de-internet-63-da-populacao/#:~:text=%E2%A0%80%E2%A0%80%E2%A0%80-,Mundo%20se%20aproxima%20da%20marca%20de%205%20bilh%C3%B5es,de%20internet%2C%2063%25%20da%20popula%C3%A7%C3%A3o&text=O%20n%C3%BAmero%20de%20usu%C3%A1rios%20ativos,Report%2C%20publicado%20pelo%20site%20Datareportal. Acesso em 26 de setembro de 2022.

Gráfico 01: Ranking de internautas ativos na internet até o ano de 2022



Fonte: Datareportal.com (Digital 2022: Global Overview Report)

Nos anos seguintes iniciou-se uma verdadeira revolução tecnológica, o que gerou um ciclo de mudanças frenético em toda a estrutura da internet, deixando de ser um sistema intricado de acesso restrito às minorias, para se tornar o meio de comunicação mais utilizado no mundo.

Do ponto de vista do Insper, relatórios apontam que:

> Outros dados do relatório mostram que há globalmente mais de 4,6 bilhões de usuários de mídia social. Esse número cresceu em média 12% ao ano na última década. Somente no ano passado, 424 milhões de pessoas passaram a acessar mídias sociais, o que representou uma média de mais de 1 milhão de novos usuários que aderiram às plataformas sociais a cada dia.O cibercrime também iniciou uma nova fase, já que a criptografia, utilizada para proteger dados digitais do mundo corporativo, se tornou objeto de atenção dos cibercriminosos.[18]

[18] Insper, Instituto de Ensino e Pesquisa, Mundo se aproxima da marca de 5 bilhões de usuários de Internet. Publicado em 2022. Disponível em: https://www.insper.edu.br/noticias/mundo-se-aproxima-da-marca-de-5-bilhoes-de-usuarios-de-internet-63-da-populacao/#:~:text=%E2%A0%80%E2%A0%80%E2%A0%80-,Mundo%20se%20aproxima%20da%20marca%20de%205%20bilh%C3%B5es,de%20internet%2C%2063%25%20da%20popula%C3%A7%C3%A3o&text=O%20n%C3%BAmero%20de%20usu%C3%A1rios%20ativos,Report%2C%20publicado%20pelo%20site%20Datareportal. Acesso em 26 de setembro de 2022.

Outrossim, através da mesma pesquisa, estipulou-se que o Brasil está entre os três países mais conectados do mundo, com uma média diária de 10h19min, ficando atrás somente da África do Sul e das Filipinas. Todavia, não há distinção entre usuários que desfrutam da mesma para fins pessoais ou a trabalho.

Do mesmo modo, não há como distinguir usuários que utilizam a internet como meio de ferramenta de usuários que fazem uso de forma social, através das mídias sociais, e além do mais, há uma mistura entre eles, os usuários que utilizam das redes sociais como forma de trabalhar, o qual só tende a crescer com o passar do tempo. Nota-se que a pandemia causada pelo COVID-19 em 2019 foi um grande impulsionador para alavancar os trabalhos realizados de maneira física para assim ser realizado através do trabalho remoto. Ainda assim, extrai-se um grande exemplo o Poder Judiciário no nosso país, onde praticamente todo o trabalho é realizado de maneira digitalizada atualmente, desde a audiência até a citação por meio do aplicativo “WhatsApp”.

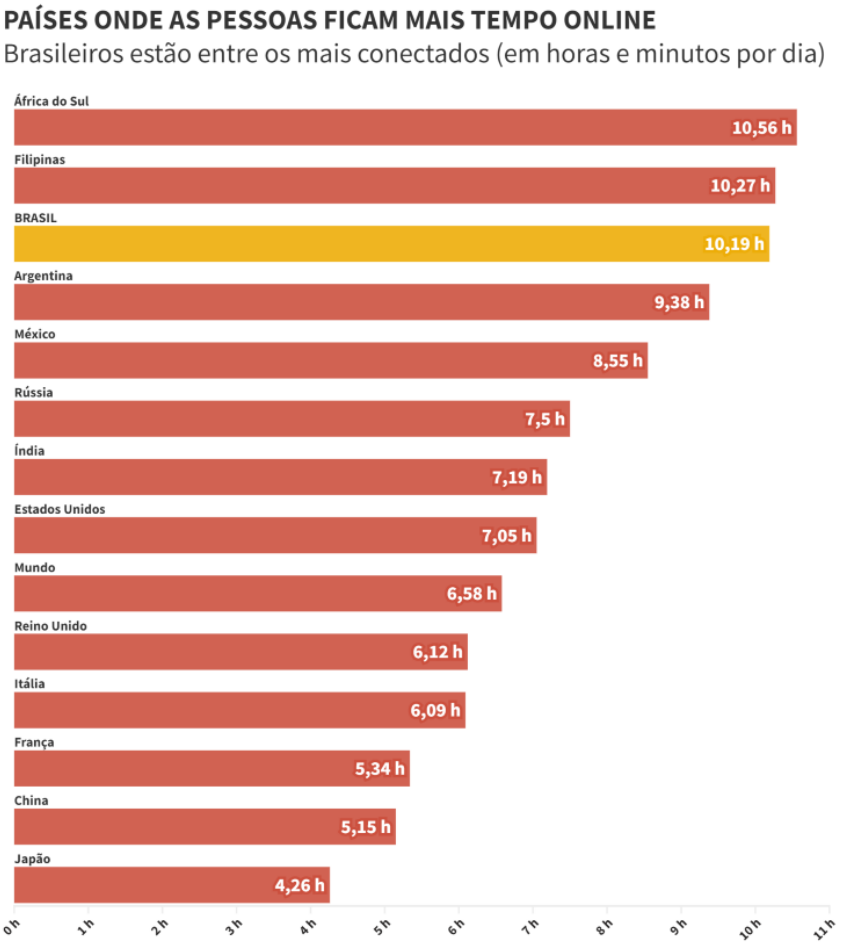
Assim, segundo a pesquisa realizada pela Associação de Empresas e Profissionais da Informação, diz que:

> O *e-commerce* brasileiro cresceu em média 74% frente a 2019. Um setor que vinha em constante crescimento, em média de 20% ao ano, em 2019 cresceu quase quatro vezes mais do que era comum para o setor. As pessoas terem ficado em casa, os shoppings terem fechado e a comoção das pessoas para ajudar os pequenos comércios foram algumas molas propulsoras desse crescimento – sem contar com a universalização das vendas pelo WhatsApp e redes sociais como o Instagram. O setor de supermercados cresceu quase 120% nas vendas online, o que fez com que a tendência das foodtechs tivesse um exponencial crescimento. Se no início de 2020, muitas empresas de porte grande ainda se davam ao luxo de sequer ter um site institucional, vemos um 2021 em que a disponibilidade de canais digitais se adequou exponencialmente à nova realidade de consumo e mercado.Os aplicativos de entrega e delivery cresceram quase 300%, muito porque as pessoas em casa precisaram desses serviços para itens básicos como o almoço de cada dia, uma vez que ,com medo, muita gente não colocou os pés na rua nem para ir à padaria na esquina de casa.[19]

[19] ABEINFO, Associação de Empresas e Profissionais da Informação. Disponível em: https://abeinfobrasil.com.br/a-digitalizacao-apos-1-ano-de-pandemia/. Acesso em 28 de setembro de 2022.

Vislumbra-se que em virtude do exposto, uma grande parte da população teve que trabalhar de forma remota, aumentando assim, a sua exposição frente a internet.

Gráfico 02: Ranking dos países mais conectados em horas no mundo.



Fonte: Datareportal.com (Digital 2022: Global Overview Report)

Assim, ano após ano, a tendência é cada vez mais de aumentar os usuários da internet, tendo em vista que seu uso está cada vez mais barato e operacional, além do mais, a tecnologia tende a evoluir e levar a conectividade para regiões extremas, o qual antes não era possível.

Deste modo, em seu relatório a Organização das Nações Unidas (ONU) afirma que:

> Seja em notebooks, tablets ou smartphones, a frequência com que as pessoas se mantém conectadas aumenta a cada dia, os aparelhos, especialmente o celular, tornarem-se essenciais e prevalentes na vida das pessoas. Muito se fala em dependência digital a nível global, embora ainda

> 10 reste 57% da população mundial sem acesso à rede, segundo relatório da ONU publicado em 2015. [20]

Do mesmo modo, conforme supracitado já existe tecnologia suficiente para levar a Internet para locais inóspitos, conforme se extrai, a empresa Starlink é responsável por difundir a tecnologia de conectividade via satélite, o qual não é nova nesse meio, contudo, a empresa busca operar com uma conexão rápida e de qualidade, onde anteriormente não era possível desse modo. No mesmo sentido, apesar de ser uma tecnologia cara pro atual cenário brasileiro, já se torna possível levar a conectividade para regiões como a Amazônia.

Segundo Elon Musk, o objetivo da *Starlink* é:

> Starlink é o nome de um projeto da SpaceX para oferecer acesso rápido à internet em qualquer lugar do mundo através de satélites. Ao contrário dos serviços atuais de Internet via satélite, que cobrem em regiões específicas, o objetivo da Starlink é oferecer cobertura global, saturando uma órbita baixa com satélites suficientes para servir a cada canto do planeta.[21]

Extrai-se segundo relatório da União Internacional de Telecomunicações (UIT), cerca de 2,9 bilhões de pessoas nunca acessaram a internet, o qual se ressalta que o mesmo tem ligação direta com a desigualdade social, tendo em vista que enquanto 90% da população europeia está conectada, a África por sua vez possui apenas 33% da população em contato com a internet.

Relatório realizado pela UIT e divulgado pela ONU:

> O número estimado de pessoas que se conectaram à internet aumentou para 4,9 bilhões em 2021, em parte devido às medidas de restrição, trabalho e estudo durante a pandemia. A descoberta faz parte do novo relatório da União Internacional de Telecomunicações (UIT), divulgado nesta semana.Entretanto, 2,9 bilhões de pessoas ficaram para trás, sem nunca terem usado a internet. Destas, 96% vivem em países em desenvolvimento.

---

[20]ONU, BR. No Brasil quase 60% das pessoas estão conectadas à internet, afirma novo relatório da ONU. Publicado em 2015. Disponível em: https://unicrio.org.br/no-brasil-quase-60-das-pessoas-estao-conectadas-a-internet-afirma-novo-relatorio-da-onu/. Acesso em 26 de setembro de 2022

[21]Olhar Digital, Saiba tudo sobre o projeto Starlink. Publicado em 2021. Disponível em: https://olhardigital.com.br/2021/04/07/ciencia-e-espaco/saiba-tudo-sobre-o-projeto-starlink/.Acesso em 26 de setembro de 2022

> Na África, apenas um terço da população possui acesso à internet. Em contrapartida, na Europa, 90% da população está conectada.[22]

Entretanto, apesar da internet em sua criação inicial ser usada para fins acadêmicos, conforme exposto, após à sua liberação para a população em geral, a comodidade que a mesma proporciona ao seus usuários com a entrega de serviços de forma instantânea de sites e aplicativos, desde a criação de empregos através das mídias sociais até a possibilidade de trabalhar remotamente da sua própria residência, acabou por possibilitar um universo o qual seria impossível se viver sem esse recurso atualmente. Todavia, apesar das comodidades que a internet entregou, com ela também surgem novos tipos de crime.

Conforme o doutrinador Raul Wazlawick explica que:

> O mundo atual é dominado pela tecnologia. Os smartphones são cada vez mais onipresentes e seus aplicativos têm mudado muito a forma como fazemos as coisas. Hoje, você não vai mais a videolocadoras nem assiste aos canais de TV, nem mesmo à TV por assinatura; hoje você assiste filmes diretamente na internet em alta qualidade. Hoje você não compra mais um PC; você coloca um dispositivo do tamanho de um pendrive na sua TV em alta definição e ela vira um computador instantaneamente.[23]

E com seu crescimento exponencial, a legislação brasileira não conseguiu acompanhar sua evolução, tendo em vista que o Código Penal teve sua criação em 1940, o qual até a presente data conta com déficit em legislação específica para a regulamentação. Assim, atualmente, qualquer pessoa com um simples celular consegue acessar a Internet de qualquer lugar do mundo, podendo utilizar desse meio para tudo, inclusive para fins considerados como ilícitos.

Wazlawick explica que a tecnologia acaba por:

> Os primeiros anos do século XXI viram surgir uma computação com a qual Babbage, von Neumann e mesmo Vannevar Bush possivelmente nem sonhavam: máquinas minúsculas, que cabem em um bolso, com mais capacidade de processamento do que um supercomputador Cray-2.
> A área de produção de software nesse período dá uma guinada na direção de métodos ágeis, afastando de muitos projetos o engessamento de estruturas rígidas de processos que são comuns em outras indústrias.

---

[22] ONU, Organização das Nações Unidas Brasil. 2,9 bilhões de pessoas nunca acessaram a internet .Disponível em:https://brasil.un.org/pt-br/161450-29-bilhoes-de-pessoas-nunca-acessaram-internet. Acesso em 10 de outubro de 2022

[23] Wazlawick, Raul. História da Computação, p.511.. Disponível em: Minha Biblioteca, Grupo GEN, 2016.

> Alguns produtos também mudaram paradigmas: a Wikipédia dominou as enciclopédias, o Skype mudou a telefonia, o YouTube acabou com as videolocadoras, o Facebook criou uma gigantesca comunidade global e o WhatsApp liquidou com as mensagens tarifadas de SMS.
> Foram muitas mudanças nessa época, mas o progresso continua. Talvez o leitor até se surpreenda por perceber que determinadas tecnologias que parecem estar por aí há tanto tempo são tão recentes quanto a década passada.[24]

Por fim, verifica-se através do capítulo em epígrafe que a humanidade acabou por criar uma tecnologia que cada vez torna-se mais dependente dela mesmo, uma vez que se necessita de internet para operar grande parte dos utensílios utilizados atualmente, a conexão se tornou algo indispensável à humanidade.

[24] Wazlawick, Raul. História da Computação, p.511.. Disponível em: Minha Biblioteca, Grupo GEN, 2016.

CAPÍTULO 2

2. CONCEITO DE CIBERNÉTICOS

Inicialmente, é de suma importância esclarecer que não existe uma única nomenclatura sobre crimes cibernéticos, e sim várias, sendo que não há um consenso sobre a melhor denominação que relaciona os delitos com a tecnologia. Contudo, neste trabalho científico será abordado o conceito abordado pelo Doutrinador Fabrizio Rosa:

> A conduta atenta contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar;. O „Crime de Informática‟ é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão;. Assim, o „Crime de Informática‟ pressupõe dos elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetuá-los. [25]

E nessa linha segue Fabrizio Rosa:

> A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão;. Nos 10 crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc.[26]

Em suma, crimes cibernéticos são todas as condutas típicas, antijurídicas e culpáveis contra ou praticadas com a utilização de instrumentos eletrônicos que podem entrar em rede, através da internet.

Assim, conceitua o doutrinador Sérgio Marcos Roque:

> Crimes cibernéticos nada mais são do que “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material.[27]

---

[25] ROSA, Fabrizio. Crimes de Informática. Campinas: Bookseller, 2002. Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimesciberneticos>. Acessado em: 10/10/2022.

[26] ROSA, Fabrizio. Crimes de Informática. Campinas: Bookseller, 2002. Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimesciberneticos>. Acessado em: 10/10/2022

[27] ROQUE, Sérgio Marcos. Criminalidade informática: crimes e criminosos do computador. São Paulo: ADPESP Cultural, 2007. P. 25

Assim, os crimes cibernéticos se dividem em dois, os crimes próprios e os impróprios, conforme se extrai da doutrinadora Patricia Peck Pinheiro em seu livro de Direito Penal.

> Os crimes virtuais têm modalidades distintas, dependendo do bem jurídico tutelado. Nesse sentido, podemos dar como exemplo o crime de interceptação de dados, que tem como bem jurídico tutelado os dados, ou seja, o que se quer é proteger a transmissão de dados e coibir o uso dessas informações para fins delituosos, como, por exemplo, captura de informações para envio de “e-mail bombing”, e o “e-mail com vírus”, o “spam”.Esse tipo penal protege também a questão da inviolabilidade das correspondências eletrônicas[28].

Por fim, verifica-se que o crime digital divide-se em duas esferas, onde primeiramente se tem o uso do bem digital como meio para se praticar a conduta delituosa, e a outra esfera, o bem digital é o fim para a conclusão da prática ilícita, conforme se verifica em epígrafe.

2.1 CRIMES CIBERNÉTICOS

No início do milênio, o mundo digital, embora extremamente fascinante, era ainda enigmático e obscuro para o homem comum, assim com a popularização e amplo uso da internet nas mais variadas atividades, conforme já exposto, ressurgiu também aquela familiar e genuína preocupação em relação à segurança das informações que eram compartilhadas online, não somente para os governos, mas a todos que faziam uso dela.

Assim, o especialista em cibercrime D’URSO relata que:

> A maior dificuldade com relação ao combate desses crimes está relacionada à dificuldade de se fazer prova e investigar a origem do delito, a materialidade e a autoria, bem como a falta de conhecimento técnico dos usuários, as supostas vítimas, tornando alvos fáceis do cibercriminoso e a variedade de delitos, que é quase ilimitada.[29]

Assim, com a evolução da tecnologia o mundo virtual cresce a cada dia. Impossível hoje em dia pensar em um mundo sem internet. São milhares de informações e dados informáticos transitando a todo momento na rede. Isso fez despertar em muitos criminosos uma nova possibilidade, novos espaços a serem tomados para a prática de crimes. Houve uma grande migração desses bandidos

---

[28] PECK PINHEIRO, Patrícia. Direito Digital, 2. Ed. rev., atual. E ampl. – São Paulo : Saraiva, 2007.
[29] D’URSO, Luiz Augusto Filizzola. Tudo sobre cibercrimes. 2019. Acesso em 25 de novembro de 2022.

com o objetivo de apoderar-se dessas informações para obter vantagem iniciando uma nova categoria de crimes: os crimes cibernéticos.

Assim relata, CRESPO:

> Entre os doutrinadores nacionais citamos duas classificações. A primeira, adotada por Vianna, que entende haver: a) Delitos em que o computador foi o instrumento para a execução do crime, mas que não provocou lesão ao bem jurídico "inviolabilidade da informação automatizada" (dados) são denominados Delitos Informáticos Impróprios; b) Delitos em que são afetados os dados são denominados Delitos Informáticos Próprios; c) Delitos complexos nos quais, além da inviolabilidade dos dados há outro bem jurídico lesado recebem a denominação de Delitos Informáticos Mistos; e d) Delitos informáticos próprios que atuem como crime-meio para a realização de crime-fim, são denominados Delitos Informáticos Mediatos ou Indiretos[30].

Assim, com o advento da internet em diversos lares e lugares, os crimes que já são tipificados pelo Código Penal passaram a ser praticados pelo meio virtual, sendo que o criminoso fica "escondido através da rede", dificultando a localização da autoria dos crimes, muda-se o meio, mas não se muda o crime.

Segundo o Delegado de Polícia Federal, Elmer Vicente responsável pelo Serviço de Repressão a Crimes Cibernéticos da PF, a dificuldade de rastreio pela internet se dá pelo seguinte motivo:

> (…)explicou que a investigação começa com a identificação do endereço IP do computador de onde partiu o crime, que é dado pelo provedor de serviço. O próximo passo é conseguir, com o provedor de internet, o nome do usuário do IP. Segundo Elmer, no entanto, há duas grandes dificuldades. A primeira é que, curiosamente, algumas empresas não aceitam a requisição de informações da polícia pela internet. Outra dificuldade é que, se antes algumas empresas concediam informações por meio de requisição policial, com o marco civil da internet, as empresas geralmente cedem os dados apenas por meio judicial.[31]

Não existe um consenso na literatura acerca do surgimento desses crimes. Entretanto existem muitos fatos datados a partir do século XX, nos anos 60. Casos de espionagem eletrônica em sistemas informáticos assim como de sabotagem destes sistemas foram levantados nesse período.

---

[30] CRESPO, Marcelo Xavier de F. Crimes digitais. [Digite o Local da Editora]: Editora Saraiva, 2011. E-book. ISBN 9788502136663. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502136663/. Acesso em: 05 out. 2022.

[31] CÂMARA, Agência Câmara Notícias. A CPI constata dificuldade em rastrear e punir crimes de internet. Disponível em: https://www.camara.leg.br/noticias/467819-cpi-constata-dificuldade-em-rastrear-e-punir-crimes-de-internet/. Acesso em 25 de novembro de 2022

Houve um desenvolvimento, por programadores, ainda nessa década, um jogo chamado "*Core Wars*", o qual se reproduzia todas as vezes que era ativado causando uma grande sobrecarga na memória do computador do outro jogador. Em contrapartida, os mesmos mentores desse jogo criaram um dispositivo que era capaz de destruir essas cópias de reprodução originadas do mesmo jogo, o que consideramos nos dias de hoje como um antivírus.

Consta na história que o primeiro sistema que conseguiu burlar um computador foi um jogo chamado "*Core Wars*"

Assim, através do artigo publicado pela *British Broadcasting Corporation* (BBC), se tem o início do "*Core Wars*"

> O início de tudo deu-se nos laboratórios da Bell Computers. Quatro programadores (H. Douglas Mellory, Robert Morris, Victor Vysottsky e Ken Thompson) desenvolveram um jogo chamado Core Wars, que consistia em ocupar toda a memória RAM da equipe contrária no menor tempo possível. No início da era da informática, não havia a pretensão de infectar ou roubar informações de usuários com esses aplicativos, mas apenas irritá-los com mensagens ou pequenas alterações no sistema.[32]

Assim, podemos fazer destaque também ao surgimento da figura do hacker que, na década de 70, já estava em evidência com a invasão feita em sistemas e furtos de *softwares* em computadores conectados à rede.

Em um artigo publicado pela CB Sistemas, relata que:

> A origem do termo hacker - hoje sinônimo de pessoas que anonimamente invadem sistemas de e-mails e websites - vem dos anos 50 e 60, quando um hack era apenas uma solução inspirada ou elegante para qualquer problema.[33]

Na década de 80 houve uma preocupação maior com as vulnerabilidades que apareceram no sistema, pois foi nesta época que os crimes cibernéticos se alastraram ainda mais, causando grandes problemas e prejuízos para o meio externo.

Assim, delitos como invasão de sistemas, pedofilia, pirataria começaram a despertando uma grande preocupação para com comunidade virtual exigindo assim uma postura mais firme no que diz respeito à punição dos responsáveis que podem

---

[32] BBC, British Broadcasting Corporation Brazil, **Saiba mais sobre a história dos hackers**. Disponível em: https://www.bbc.com/portuguese/noticias/2011/06/110623_historiahacking_is. Acesso em 05 de outubro de 2022.

[33] CB Sistemas, **A História do Primeiro Vírus**, Disponível em https://www.cbsistemas.com.br/historia-do-primeiro-virus-de-computador/. Acesso em 05 de outubro de 2022

estar espalhados em diversas partes do globo dificultando, desta forma, a captura do criminoso.

Primeiramente, tratando-se da história dos crimes cibernéticos, salienta-se que houve um caso da caça desesperada do governo norte americano em achar o paradeiro do hacker Kevin Mitnick, um dos hackers mais famosos dos Estados Unidos, se não o mais famoso do mundo, que após muitos anos de procura conseguir encontrar e puni-lo devidamente pelas invasões e crimes que ele havia cometido.

> Mas nem sempre o objetivo de Mitnick foi proteger sistemas de segurança. O especialista já esteve preso por invadir computadores e redes de corporações, além de desmantelar a segurança de alguns departamentos importantes do governo norte-americano. Seu histórico de invasões virtuais começou na década de 1970, quando burlou o sistema de cartão de ônibus, conseguindo passagens gratuitamente. Mitnick chegou a penetrar alguns dos sistemas mais bem guardados, incluindo, entre inúmeros outros, Sun Microsystems, Digital Equipment Corporation, Motorola, Netcom e Nokia.
> Sua última prisão ocorreu em 1995, com sentença de cinco anos e mais três em liberdade condicional, sendo negado a ele aproximar-se de um computador. A história de Mitnick e como o hacker foi preso foi transformada no filme “Caçada Virtual”, lançado no ano de 2000. A narrativa aborda a cooperação entre o também hacker Tsutomu Shimomura e o FBI na “caça” aos rastros deixados por Mitnick na rede, que culminou em sua captura.[34]

Atualmente, este trabalha para o governo americano na área de segurança de informação. No mesmo sentido, Kevin nos dias atuais é escritor de vários livros acerca do assunto supracitado.

Apesar de alguma discrepância doutrinária, são denominados de "crimes de informática" as condutas descritas em tipos penais realizadas através de computadores ou voltadas contra computadores, sistemas de informática ou os dados e as informações neles utilizados (armazenados ou processados).

Segundo Luiz Augusto Filizzola em seu livro sobre cibercrime, relata que:

> Embora o conceito seja antigo, o termo “cibercrime” surgiu somente no final da década de 90, em uma reunião do G-8 que se destinava à discussão do combate a práticas ilícitas na internet de forma punitiva e preventiva. Desde

[34]FECOMERCIO, Federação de Comércio de Bens, O hacker mais procurado do mundo ajuda empresas a melhorarem segurança virtual. Disponível em: www.fecomercio.com.br/noticia/hacker-mais-procurado-do-mundo-ajuda-empresas-a-melhorarem-seguranca-virtual. Acesso em 05 de outubro de 2022.

> então, o termo passou a ser usado para designar infrações penais praticadas online.[35]

Frisa-se que atualmente há diversos crimes envolvendo esse mundo, contudo, apenas alguns são voltados para a grande massa, tendo em vista que se espalham pelo próprio usuário afetado

> **E-mail *Bombing*** – é o envio de e-mails imensos ou vários e-mails, por isso *Bombing*, que se refere como "explosão, ou bomba" em inglês. De qualquer forma pode vir a causar atraso na recepção e gasto adicional com conta de internet, por exemplo. Nesses casos seria aplicável o art. 163 do Código Penal (crime de dano)[36]

No mesmo sentido, destaca-se um crime comum, como o :

> ***Spam*** – Propaganda maciça na Internet, feita em geral com software especialmente projetado para enviar solicitações aos usuários por meio de e-mail.[37]

Não obstante, também se tem uma prática tão comum quanto o *Spam*:

> **E-mail com vírus** – é quando a pessoa recebe um email, e vem anexado um vírus, é muito comum nos dias de hoje, e-mails com tentativas de vírus através de propostas bancárias, ou solicitação de dados por e-mail. Nesse sentido, a legislação prevê os artigos 151, § 1º, II e III, e 163 do Código Penal, com aplicação do artigo 65 da LCP, com pena de prisão simples de 15 dias a 2 meses, ou multa por perturbação da tranquilidade.[38]

No mesmo sentido, os crimes digitais estão em permanente transformação, o qual se deve ao aspecto dinâmico da tecnologia, ocorrendo assim, mudanças que a sociedade e as revelações sociais apresentam. Deste modo, a evolução de direitos e deveres do ser humano no meio virtual, surge com uma importância muito grande na garantia do respeito do ser e do respeito à dignidade humana.

2.2 CRIMES CIBERNÉTICOS PRÓPRIOS

Estes crimes são os quais só podem ser praticados na informática, ou seja, a execução do crime e a consumação ocorrem por este meio, tendo em vista que tipos novos dos quais o bem jurídico tutelado é o meio digital, visto que os crimes

---

[35] D'URSO, Luiz Augusto Filizzola. Cibercrime: perigo na internet. Publicado em 2017. Disponível em <http://politica.estadao.com.br/blogs/faustomacedo/cibercrime-perigo-na-internet/>. Acesso em 28 de Setembro de 2022.

[36]ZOLA, Andrew. What is a mail Bomb. Disponível em :https://www.techtarget.com/searchsecurity/definition/mail-bomb, Acesso em 30 de outubro de 2022

[37]VIAMONTE, Guilherme Avelino Viamonte.O que é SPAM?. Disponível em : https://www.gta.ufrj.br/grad/15_1/spam/. Acesso em 30 de out de 2022.

[38] AVAST. Avast Antivírus. Disponível em:https://www.avast.com/pt-br/c-phishing. Acesso em 30 de outubro de 2022

praticados contra os dados da vítima, o qual acaba por utilizar o computador, ou o celular.

Assim, Viana relata que:

> Os crimes digitais próprios são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados).[39]

As condutas supracitadas, geralmente são perpetuadas por "*crackers"*, tanto a invasão de sistemas, modificar, inserir dados ou informações falsas, ou seja, casos que acabam por atingir de maneira direta os softwares dos computadores, que geralmente invadem através de sistemas infectados, como pen drives, e-mails, ou outra forma de arquivo oriundo da internet, todos estes devem conter algum tipo de "*vírus*", a qual acaba por danificar ou corromper programas ou arquivos contidos no sistema operacional do computador ou celular.

Segundo o doutrinador Damásio de Jesus:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade de dados, da máquina e periféricos)é o objetivo do objeto jurídico tutelado[40]

Muito se engana em relação ao assunto, tendo em vista que há um enorme equívoco entre "*Crackers*" e "*Hackers*", assim os hackers utilizam o seu conhecimento para melhorar softwares de forma legal e não costumam invadir um sistema com o intuito de causar danos. Os crackers têm como prática a quebra da segurança de um software e usam seu conhecimento de forma ilegal, portanto, são vistos como criminosos.

Não obstante, é necessário analisar a diferença entre *Hackers* e *Crackers*, onde os conceitos em relação aos termos confundiram-se ao longo dos anos, levando a grande massa a trocar os termos corretos, também, frisa-se pelo conceito de Vírus.

Verifica-se que Cracker é:

---

[39] VIANA, Marco Túlio apud CARNEIRO, Adeneele Garcia. Fundamentos de direito penal informático. Do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003. Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acessado em: 10/10/2022.

[40] JESUS, Damásio de, e MILAGRE, José Antonio. Manual de crimes informáticos. São Paulo: Saraiva, 2016.

> **Cracker** - Perito em informática que usa seus conhecimentos para violar sistemas ou redes de computadores.[41]

Do mesmo modo define-se Hacker como:

> **Hackers** - são indivíduos com a capacidade de criar funcionalidades e aplicações para computadores, dispositivos móveis e internet. Eles modificam softwares, hardwares e aplicam seus conhecimentos para desenvolver soluções de segurança, criar ou adaptar novos sistemas.

Não obstante, Vírus digital seria:

> **Vírus** - Em termos mais técnicos, um vírus de computador é um tipo de programa ou código malicioso criado para alterar a forma como um computador funciona e desenvolvido para se propagar de um computador para outro. Um vírus atua inserindo ou se anexando a um programa ou documento legítimo, que tenha suporte para macros, a fim de executar o seu código. Durante esse processo, um vírus pode potencialmente causar efeitos inesperados ou prejudiciais, como danificar o software do sistema, corrompendo ou destruindo os dados.[42]

Por fim, extrai-se do exposto que os crimes cibernéticos próprios nada mais são do que a violação ou manipulação de dados, onde o bem jurídico tutelado é o meio digital.

3.3 CRIMES CIBERNÉTICOS IMPRÓPRIOS

Conforme já exposto, ao contrário dos próprios, os crimes cibernéticos impróprios são aqueles os quais já contam com alguma tipificação penal no ordenamento jurídico, mas são cometidos no âmbito virtual, tendo o dispositivo eletrônico para a prática de condutas consideradas como ilícitas. São crimes já tipificados que violam bens tutelados pela lei brasileira, sendo praticado de qualquer forma.

Do mesmo modo, corrobora DAMÁSIO:

> Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico o espaço real, ameaçando ou lesando outros bens não-computacionais ou diversos da informática.[43]

---

[41] Oxford. Dicionário. Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles/oxford. Acesso em 10 de out de 2022.

[42] Norton, O que é um vírus de computador? Disponível em https://br.norton.com/blog/malware/what-is-a-computer-virus. Acesso em 10/10/2022.

[43] JESUS, Damásio de, e MILAGRE, José Antonio. Manual de crimes informáticos. São Paulo: Saraiva, 2016.

Analisa-se que através do exposto, crimes considerados como impróprios são mais frequentes em nosso âmbito virtual, como calúnia, difamação, injúria, todos estipulados no Código Penal desde o artigo 138 até o artigo 140.

Assim relata Castro em seu livro:

> Nos crimes praticados através da informática, ou seja, tipos antigos, nos quais o agente utilizava a informática como meio de execução, como instrumento de sua empreitada, não há dificuldades. O crime é o mesmo previsto em sua origem, a forma de execução é que inovou, por exemplo, uma ameaça feita pessoalmente não se distingue na tipicidade de uma ameaça virtual. O problema surge em relação aos crimes cometidos contra o sistema de informática, atingindo os bens não tutelados pelo legislador, como dados, informações, sites, e-mails... São condutas novas que desenvolveram junto com a nossa sociedade razão pela qual o legislador de 1940, época do Código Penal, não pode prever tais tipos penais.[44]

Ocorre que os crimes contra a honra cometidos no meio virtual, acabam por prejudicar a reputação de alguém ou ofender à sua dignidade de uma maneira muito abrangente, tendo em vista que na internet há muito mais acessos e as informações circulam com muito mais velocidade, onde há casos irretratáveis.

Assim Bitencourt relata que:

> Contudo, para que haja configuração do crime contra a honra por meio das redes sociais, é preciso que estejam presentes todas elementares do tipo penal, bem como o elemento subjetivo do delito. No caso da calúnia, é necessária a imputação da prática de determinado fato, e que este seja qualificado como crime, sendo consumada quando a referida atribuição se torna conhecida por terceiro[45]

Por fim, tais crimes são compatíveis com o meio digital e podem ser facilmente praticados por meio da Internet, já que se trata de crimes de forma livre, que podem ser praticados por qualquer modo, seja por meio do correio eletrônico, aplicativos de mensagens instantâneas, blogs e redes sociais a fim de disseminar a ofensa. Cabendo ao legislador criar normas a fim de proteger os usuários de ataques a sua honra, intimidade e vida privada, com o devido aumento de pena, pelo uso da internet como meio de propagação.

---

[44] CASTRO, Carla Rodrigues Araújo de. Crimes de Informática e seus Aspectos Processuais. 2. Ed. Rio de Janeiro: Lumen Juris, 2003.

[45] BITENCOURT, Cezar Roberto. Tratado de direito penal: parte geral. 20 ed. São Paulo: Saraiva, 2014. v. 1.

CAPÍTULO 3

3. A ATUAL LEGISLAÇÃO BRASILEIRA EM RELAÇÃO AOS CRIMES CIBERNÉTICOS E SUA COMPARAÇÃO COM O RESTO DO MUNDO

Primeiramente, é importante lembrar-nos que a função do Direito Penal consiste em coibir condutas divergentes daquelas tipificadas, impondo sanção e protegendo bens jurídicos.

No mesmo sentido, uma estrutura normativa é gerada, criando uma lógica própria. Essa normatividade tem uma dupla função, já que ao tempo em que a pena, enquanto sanção normativa, é uma forma de garantir a eficácia do sistema penal, esta possui seu limite já imposto, servindo como uma garantia.

Assim, essas condutas são a base para a tipificação de crimes em uma sociedade, já que o Direito Penal retira os conceitos de condutas humanas a partir de condutas possíveis e já valoradas pela sociedade.

Extrai-se de toda a esfera penal brasileira, que através dos avanços tecnológicos, obrigou-se a criação de leis específicas para combater o crime virtual, a primeira lei específica e mais famosa na sociedade brasileira é a Lei Ana Carolina Dieckmann, o qual no ano de 2012, teve seu computador violado e seus dados expostos, onde não havia uma tipificação típica para este tipo de conduta até então.

3.1 LEI “CAROLINA DIECKMANN” - 12.737/2012

A Lei nº 12.737/2012 – Lei dos Crimes Cibernéticos, ou, também conhecida como, a Lei "Carolina Dieckmann", trouxe importantes alterações ao Decreto-Lei 2.848/40 – Código Penal brasileiro, ao passo que realizou a formalização e a tipificação de condutas delituosas no âmbito informático, constituindo os chamados “crimes cibernéticos”.

A tipificação dos crimes informáticos está prevista no primeiro artigo do referido diploma legal, mas, valendo-se da hermenêutica jurídica, onde se lê “crimes informáticos”, devem ser interpretados como “crimes cibernéticos”.

Destarte-se que a tipificação dos crimes cibernéticos criados com a lei supracitada, encontram-se amparadas atualmente no Código Penal Brasileiro, em seus artigos 154-A e 154-B.

Verifica-se no Código Penal que:

> 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:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, 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.
> § 2ºAumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

Não obstante, continua o dispositivo legal alegando que:

> § 3ºSe 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 6 (seis) meses a 2 (dois) anos, e multa, se conduta não constitui crime mais grave.
> § 4ºNa 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 obtidos.
> § 5ºAumenta-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.[46]

No mesmo sentido, verifica-se a parte B do artigo supracitado:

> 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. (Incluído pela Lei nº 12.737, de 2012)[47] Vigência

[46] BRASIL. Decreto Lei nº 2.848, de 7 de Dezembro de 1940. Institui o Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm Acesso em 30 de out de 2022.
[47] BRASIL. Decreto Lei nº 2.848, de 7 de Dezembro de 1940. Institui o Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm Acesso em 30 de out de 2022.

Assim, analisa-se através do exposto que, os novos artigos inseridos no Código Penal brasileiro pela Lei 12.737/2012 buscam combater a invasão de dispositivos informáticos alheios, conectados ou não à rede de computadores. É importante salientar que se entende por dispositivos informáticos: computador de mesa, notebook, laptop, ultrabook, tablete, ipad, smartphone etc.

Doutrinador Nucci relata em relação aos artigos supracitados que:

> O tipo penal indica, ainda, a necessidade de o dispositivo informático possuir algum mecanismo de segurança, sob pena de ser considerado desprotegido penalmente[48]

Assim, conclui-se que para cometer a conduta tipificada no referido artigo o sujeito ativo deverá invadir, ou seja, violar/transgredir o dispositivo alheio, sem precisar necessariamente estar conectado com a rede de computadores, e com a finalidade de obter, adulterar ou destruir dados ou informações.

Assim, analisa Capez:

> Em análise da lei, verifica-se a ineficácia em alguns pontos que possuem a função de atingir o seu objetivo primordial, seja quanto para obtenção de provas ou punição a ser aplicada. A ação central da conduta, se classifica no ato de invadir sem permissão a segurança de algum dispositivo eletrônico pessoal de alguém; (adulterando, modificando, prejudicando). Com objeto material [49]

Não obstante, quando a conduta seja praticada sem "violação indevida de mecanismo de segurança" ela será atípica. Isso porque tal elemento normativo se põe como necessário para adequação típica do comportamento. Assim, se o dispositivo informático invadido não possuir mecanismos de segurança, tais como senhas de acesso, firewalls, antivírus, entre outros, sua eventual invasão não será um fato típico.

Nucci classifica o artigo 154-A como:

> [...] crime comum (pode ser cometido por qualquer pessoa); formal (delito que não exige resultado naturalístico, consistente na efetiva lesão à intimidade ou vida privada da vítima, embora possa ocorrer); de forma livre (pode ser cometido por qualquer meio eleito 129 pelo agente); comissivo (as condutas implicam ações); instantâneo (o resultado se dá de maneira 47 determinada na linha do tempo), podendo assumir a forma de instantâneo de efeitos permanentes, quando a invasão ou a instalação de vulnerabilidade perpetua-se no tempo, como rastro da conduta;

---

[48] NUCCI, Guilherme de Souza. Manual de direito penal. 9.ed. São Paulo: Revista dos Tribunais, 2013.

[49] CAPEZ, Fernando; GARCIA, Maria Stela Prado. Código Penal comentado. Fernando Capez, Maria Stela Prado Garcia. 4. ed. São Paulo: Saraiva, 2013.

> unissubjetivo (pode ser cometido por uma só pessoa); plurissubsistente (cometido por vários atos); admite tentativa.[50]

Não obstante, relata Castro:

> " […]diante das circunstâncias analisadas da presente Lei, torna-se evidente a pressa do legislador em criar esse tipo penal, já que havia à época uma pressão midiática para a incriminação dessa conduta, por envolver uma atriz de grande prestígio em todo o país. "[51]

Desse modo, o tipo penal fora mal redigido e com o abuso de elementos normativos, contrariando a taxatividade, o qual dentre esses tipos penais elencados, o que se pode perceber é que todos possuem como elemento subjetivo a modalidade dolosa.

Não obstante conclui Ferreira:

> A ineficácia na normatização nos crimes virtuais, ainda não foi suprida para um combate efetivo contra estes delitos, por isso diante dessa dificuldade encontrada, ou até mesmo pela natureza taxativa do Código Penal, á uma grande impossibilidade da aplicação da analogia nos crimes virtuais. [52]

Sendo assim conclui o Doutrinador Castro:

> Não quis o legislador brasileiro incriminar a modalidade culposa. O legislador da referida codificação, possui pouca informação sobre o sistema informático, e isso é agravado pala falta de reflexão por parte da Dogmática Penal Brasileira, refletindo a lacuna normativa e a falta de debate em torno da moralidade das condutas cibernéticas, bem como as consequências e prejuízos causados por essas condutas[53]

Conclui-se então que a inexistência da culpabilidade é preocupante, pois a mesma consiste na condição regular necessária para fundamentar juridicamente uma responsabilidade, sendo constituída por livre arbítrio e juízos sobre a realidade, criando um sistema de subjetividade individual de aferição da culpabilidade do agente.

---

[50] NUCCI, Guilherme de Souza. Código penal comentado. 14. ed. Rio de Janeiro: Forense, 2014.
[51] CASTRO, Aldemario Araujo. A internet e os tipos penais que reclamam ação criminosa em público. 2018. Disponível em: https://egov.ufsc.br/portal/sites/default/files/anexos/13308-13309-1-PB.pdf. Acesso em 11 de novembro de 2022.
[52] FERREIRA, Érika Lourenço de Lima. Internet Macrocriminalidade e Competência Internacional. Érika Lourenço de Lima Ferreira. 1 edição (ano 2007), 1 reimpr. Curitiba: Juruá, 2010.
[53] CASTRO, Aldemario Araujo. A internet e os tipos penais que reclamam ação criminosa em público. 2018. Disponível em: https://egov.ufsc.br/portal/sites/default/files/anexos/13308-13309-1-PB.pdf. Acesso em 04 de novembro de 2022.

No mesmo sentido, não é apenas a percepção cultural, mas a percepção da realidade em si, o que alteraria a capacidade de entender o caráter ilícito da conduta e de se adequar perante tal entendimento.

3.2 LEI AZEREDO - Nº 12.735/2012

Preliminarmente, juntamente com o contexto histórico de criação da Lei 12.737/2012, criou-se também a Lei 12.735/2012, também intitulada de Lei Azeredo, o qual leva o nome do legislador que propôs a referida medida.

Não obstante, o projeto de lei do dispositivo acima informado, teve críticas desde seu início, devido aos seus pontos polêmicos, o qual também foi chamado também de “AI-5 Digital”, pelos motivos referentes à guarda dos logs de acesso dos usuários pelos provedores.

Assim, conclui CRESPO:

> Em resumo, o texto aprovado determina que os órgãos da polícia judiciária deverão criar delegacias especializadas no combate a crimes digitais (art. 4º). A medida é salutar, mas depende do Poder Público a ela prover a concretude necessária, investindo na especialização da Polícia com treinamentos e equipamentos. Ainda não se pode dizer que as delegacias que foram criadas estão plenamente aptas a prover o atendimento adequado às vítimas de crimes digitais.[54]

Do mesmo modo, em seu artigo 4º a referida lei esclarece:

> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.[55]

Além do mais, a lei nº 12.735 no art. 5º, determinou que a lei nº 7.716 passasse a conter o inciso II no § 3º do art. 20 para obrigar que a prática, a indução ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, praticados por intermédio dos meios de comunicação social

---

[54] CRESPO, Marcelo Xavier de F. Crimes digitais. [Digite o Local da Editora]: Editora Saraiva, 2011. E-book. ISBN 9788502136663. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502136663/. Acesso em: 05 out. 2022.

[55] BRASIL. Lei 12.735, de 30 de Novembro de 2012, Lei Azeredo. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em 30 de out de 2022.

ou publicação de qualquer natureza, tenham a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio.

Verifica-se que o art.20 da Lei 7.716 de 5 de janeiro de 1989 após a mudança restou assim:

> Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. (Redação dada pela Lei nº 9.459, de 15/05/97)
> Pena: reclusão de um a três anos e multa.(Redação dada pela Lei nº 9.459, de 15/05/97)
> § 1º Fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos ou propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo. (Redação dada pela Lei nº 9.459, de 15/05/97)
> Pena: reclusão de dois a cinco anos e multa.(Incluído pela Lei nº 9.459, de 15/05/97)
> § 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza: (Redação dada pela Lei nº 9.459, de 15/05/97)
> Pena: reclusão de dois a cinco anos e multa.(Incluído pela Lei nº 9.459, de 15/05/97)

Não obstante, continua a lei:

> § 3º No caso do parágrafo anterior, o juiz poderá determinar, ouvido o Ministério Público ou a pedido deste, ainda antes do inquérito policial, sob pena de desobediência: (Redação dada pela Lei nº 9.459, de 15/05/97)
> I - o recolhimento imediato ou a busca e apreensão dos exemplares do material respectivo;(Incluído pela Lei nº 9.459, de 15/05/97)
> II - a cessação das respectivas transmissões radiofônicas ou televisivas.(Incluído pela Lei nº 9.459, de 15/05/97)
> II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio; (Redação dada pela Lei nº 12.735, de 2012) (Vigência)
> III - a interdição das respectivas mensagens ou páginas de informação na rede mundial de computadores. (Incluído pela Lei nº 12.288, de 2010) (Vigência)
> § 4º Na hipótese do § 2º, constitui efeito da condenação, após o trânsito em julgado da decisão, a destruição do material apreendido. (Incluído pela Lei nº 9.459, de 15/05/97)[56]

Destarte-se que a referida lei possibilita a administração pública em criar delegacias especializadas a fim de apurar ilícitos digitais, contudo, desde à sua publicação, há mais de 10 anos, tem-se apenas 18 delegacias de repressão aos crimes digitais, localizados nos seguintes locais:

---

[56] BRASIL. Lei 7.716 de 5 de janeiro de 1989. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L7716.htm. Acesso em 30 de out de 2022.

57

Por fim, analisa-se que o projeto de lei é de 1999, tendo como nº 84 e o Relator Eduardo Azeredo, assim foram anos de tramitação para que o resultado se resumisse a essas duas normas, tecnicamente desejáveis, mas sem efetividade prática porque o poder geral de cautela dos juízes já poderia determinar a remoção dos ilícitos publicados e, especialmente porque a lei não cria as delegacias especializadas, dependendo da boa vontade da Administração Pública em fazê-lo.

3.3 CONVENÇÃO DE BUDAPESTE

O grande desafio para combater os crimes cibernéticos hoje é a sua internacionalização. Ou seja, o criminoso não tem fronteiras para atuar. Uma pessoa num país A pode realizar ato ilícito num país B.

Assim, esclarece Castells:

> O Estado não desaparece, porém. É apenas redimensionado na Era da Informação. Prolifera sob a forma de governos locais e regionais que se espalham pelo mundo com seus projetos, formam eleitorados e negociam com governos nacionais, empresas multinacionais e órgãos internacionais.O

57 Crimes na Web, Safernet. Delegacias Cibercrimes. Disponível em: https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em 30 de out de 2022.

> que os governos locais e regionais não têm em termos de poder e recursos é compensado pela flexibilidade e atuação em redes. [58]

Assim, se em algum deles não tivermos a tipificação jurídica não existe crime, logo, as autoridades daquele país não irão colaborar. No mesmo sentido, outra dificuldade na colaboração está no processo penal de cada entidade governamental. Como tratar a investigação, a coleta de evidências, cadeia de custódia entre outros fatores que possam ser usados de forma coerente numa investigação internacional.

Castells elucida sobre o fato:

> 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.[59]

No mesmo sentido Fernandes em relação ao exposto:

> Uma hipótese a favor da segurança jurídica do Direito Brasileiro em vista da tipificação dos crimes cibernéticos, configura-se no fato do Brasil adotar a Convenção de Budapeste, tendo em vista que, o conteúdo dos projetos de leis, que se encontram há anos sob o julgamento do Congresso Nacional, é similar aos tratados pela referida Convenção.[60]

Ocorre que em 2001, na capital da Hungria, Budapeste, houve uma convenção, no intuito de reunir os países membros do Conselho da Europa a fim de criar uma cooperação entre os países contra o crime cibernético. Atualmente 66 países já tinham aderido a referida convenção e estima-se que seus artigos sejam usados como orientação legal em mais de 158 países.

Assim a Agência do Senado anunciou:

> A Convenção foi elaborada pelo Comitê Europeu para os Problemas Criminais, com o apoio de uma comissão de especialistas. Foi o primeiro tratado internacional sobre os chamados cibercrimes. Até junho de 2021 tinha sido assinada por 66 países, além de usada por outros 158 como orientação para suas legislações nacionais.[61]

---

[58] CASTELLS, Manuel. Fim do Milênio. 4. ed. Tradução de Klauss Brandini Gerhardt e Roneide Venancio Majer. São Paulo: Paz e Terra, 2007. (A Era da Informação: economia, sociedade e cultura; v. 3).

[59] CASTELLS, Manuel. Fim do Milênio. 4. ed. Tradução de Klauss Brandini Gerhardt e Roneide Venancio Majer. São Paulo: Paz e Terra, 2007. (A Era da Informação: economia, sociedade e cultura; v. 3).

[60] FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. REVISTA DA FACULDADE DE DIREITO DA UFMG, 2013,

[61] SENADO, Agência Senado Notícias. Aprovada adesão do Brasil à Convenção sobre o Crime Cibernético Disponível em: https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico. Acesso em 04 de novembro de 2022

Do mesmo modo Fernandes continua:

> No Direito Internacional, existe o Direito Internacional Uniforme, utiliza por quase todos os países do mundo, que ocorre quando coincidem os direitos primários entre ordenamentos, seja porque têm a mesma origem, ou por sofrerem influências idênticas, ou, ainda, quando países adotam sistemas jurídicos clássicos total ou parcialmente, de outros Estados[62]

Entre as questões tratadas na Convenção de Budapeste estão a criminalização de condutas, normas para investigação e produção de provas eletrônicas e meios de cooperação internacional. Ainda assim, apesar da Convenção ter sido realizada em 2003, apenas em 2021 o Brasil adentrou na mesma.

3.4 LEI Nº 14.155 DE 27 DE MAIO DE 2021

Analisa-se que o referido dispositivo, tem como objetivo alterar o Código Penal para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet, além de alterar, também, o Código de Processo Penal para definir a competência em modalidades de estelionato, uma vez que estes são os crimes mais comuns retirando aqueles contra a honra.

Assim, ocorreu uma modificação consistente na criação da fraude eletrônica no crime de estelionato, segundo a qual, a pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo, bem como, teve-se o aumento de pena para aqueles que buscam invadir o dispositivo informático, crime previsto na Lei Carolina Dickmann conforme já exposto.

Relata assim Rogério Greco juntamente com Rogério Sanchez da Cunha:

> Rogério Sanches Cunha, com precisão, exemplificando cada uma dessas situações, nos esclarece:
> “a) por meio de redes sociais: atualmente são muito comuns os anúncios promovidos em redes sociais como Facebook e Instagram. Não raro, são anúncios fraudulentos, manobras ardilosas para atrair pessoas que forneçam seus dados;

[62] FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. REVISTA DA FACULDADE DE DIREITO DA UFMG, 2013,

> b) por contatos telefônicos: são também muito comuns as fraudes cometidas por meio telefônico. Um exemplo recorrente envolve os cartões de crédito. O fraudador telefona para alguém e afirma, por exemplo, que a instituição financeira detectou indícios de fraude com o cartão dessa pessoa. Pede a ela que confirme dados e digite a senha do cartão. Com a senha à disposição, o agente faz compras, efetua saques, toma empréstimos etc.;[63]

Não obstante ainda tenta esclarecer Greco:

> c) pelo envio de correio eletrônico fraudulento: neste caso, a vítima recebe um e-mail fraudulento, muitas vezes imitando os caracteres de empresas ou organizações conhecidas e, a partir do acesso por meio do link disponibilizado, o estelionatário pode obter os dados pessoais e bancários inseridos em formulários eletrônicos;
> d) por qualquer outro meio fraudulento análogo: nesta fórmula analógica se inserem quaisquer outras práticas fraudulentas cometidas por meios eletrônicos ou informáticos, como páginas na internet, por exemplo, em que a vítima não é diretamente abordada pelo estelionatário, como nas modalidades anteriores, mas é induzida em erro por fatores diversos (simulação de um estabelecimento comercial regularmente constituído; cópia de outra página conceituada etc.).[64]

Verifica-se através do ordenamento jurídico que:

> **Invasão de dispositivo informático** (Incluído pela Lei nº 12.737, de 2012) Vigência
> 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: (Redação dada pela Lei nº 14.155, de 2021)
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
> § 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) Vigência
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. (Redação dada pela Lei nº 14.155, de 2021)
> § 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 2 (dois) a 5 (cinco) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)[65]

No mesmo sentido, a referida lei busca:

---

[63] GRECO, Rogério. Curso de Direito Penal - Vol. 2. [Digite o Local da Editora]: Grupo GEN, 2022. E-book. ISBN 9786559771462. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559771462/. Acesso em: 04 nov. 2022.
[64] GRECO, Rogério. Curso de Direito Penal - Vol. 2. [Digite o Local da Editora]: Grupo GEN, 2022. E-book. ISBN 9786559771462. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559771462/. Acesso em: 04 nov. 2022.
[65] BRASIL. Decreto Lei nº 2.848, de 7 de Dezembro de 1940. Institui o Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm Acesso em 30 de out de 2022.

> § 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 obtidos. (Incluído pela Lei nº 12.737, de 2012) Vigência
> § 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra: (Incluído pela Lei nº 12.737, de 2012) Vigência
> I - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012) Vigência
> II - Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012) Vigência
> 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) Vigência
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Incluído pela Lei nº 12.737, de 2012) Vigência[66]

Não obstante, a referida lei também introduziu sensíveis modificações no artigo 155 do Código Penal, para inserir uma nova qualificadora no § 4º-B, determinando que a pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.

Conforme, extrai-se que o furto também teve a pena aumentava:

> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
> Pena - reclusão, de um a quatro anos, e multa.
> Furto qualificado
> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso: (Incluído pela Lei nº 14.155, de 2021)
> I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional; (Incluído pela Lei nº 14.155, de 2021)

Por sua vez, o crime de estelionato também sofreu acréscimo, § 2º-A, para prevê a fraude eletrônica, segundo a qual, a pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações

---

[66] BRASIL. Decreto Lei nº 2.848, de 7 de Dezembro de 1940. Institui o Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm Acesso em 30 de out de 2022.

fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

Deste modo, o doutrinador Rogério Greco aponta sobre o dispositivo informado:

> Aproveitando a vulnerabilidade de pessoas que utilizam uma rede pública de internet, um hacker intercepta a conexão e obtém dados de acesso a contas bancárias. Com esses dados à disposição, acessa as contas e transfere quantias em dinheiro para outra conta da qual efetua saques. É um caso típico de furto mediante fraude, no qual a manobra ardilosa (interceptar os dados transmitidos entre o usuário e o ponto de conexão) é utilizada para que as vítimas sejam despojadas de seus bens sem que nada percebam.[67]

Não obstante ainda continua:

> Pretendendo adquirir um televisor, um indivíduo faz uma pesquisa na internet e encontra a página de uma conhecida rede varejista na qual o produto está sendo anunciado por um preço muito abaixo das concorrentes. Insere seus dados pessoais e bancários sem saber que, na verdade, se trata de uma página clonada, que apenas copia os caracteres da famosa rede varejista, para induzir as pessoas em erro. Efetuado o pagamento, o dinheiro é creditado ao autor da fraude, que evidentemente não pretende entregar o produto anunciado. Nesse exemplo, ao contrário do anterior, a vítima tem participação direta, pois, induzida por um anúncio enganoso, fornece os dados para que o autor da fraude possa obter a vantagem. Trata-se, portanto, de estelionato[68]

Ainda assim, igualmente o furto, há previsão caso o criminoso faça uso do servidor mantido fora do território nacional, no intuito de ocultação dos agentes policiais responsáveis pelo seu rastreamento. Extrai-se o exposto no § 2º-A, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

Sendo assim relata Brito e Garcia:

> Desta forma, casos em que estes atos ilícitos informáticos sejam cometidos fora da fronteira nacional, é preciso que sejam avaliados a legislação e tratados estrangeiros, de forma consensual, para fazer da punição uma medida coerente e satisfatória. O instrumento internacional desses crimes cibernéticos é a Convenção de Budapeste que recomenda a adaptação das

---

[67] GRECO, Rogério. Curso de Direito Penal - Vol. 2. [Digite o Local da Editora]: Grupo GEN, 2022. E-book. ISBN 9786559771462. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559771462/. Acesso em: 04 nov. 2022.

[68] GRECO, Rogério. Curso de Direito Penal - Vol. 2. [Digite o Local da Editora]: Grupo GEN, 2022. E-book. ISBN 9786559771462. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559771462/. Acesso em: 04 nov. 2022.

> legislações penais e que as tornem una, por este motivo a legislação faz modificações pertinentes ao Código Penal e a legislação especial. [69]

Assim esclarece Greco:

> Já o § 2º-B diz que a pena prevista no mencionado § 2º-A do art. 171 do Código Penal, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.
> Aqui, a relevância do resultado gravoso fará com que o julgador aplique a causa especial de aumento de pena entre os patamares mínimo (um terço) e máximo (dois terços), desde que o crime seja praticado mediante a utilização de servidor mantido fora do território nacional, dificultando, assim, a investigação dos fatos ocorridos.[70]

Verifica-se o dispositivo:

> Fraude eletrônica
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. (Incluído pela Lei nº 14.155, de 2021)
> § 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.[71]

Por fim, verifica-se que o legislador aprovou o dispositivo supracitado em virtude na pandemia causada pelo COVID-19, uma vez que aumentou drasticamente toda forma de interação social no ambiente virtual. Assim, diversos criminosos, abusando do período frágil da humanidade, buscaram obter vantagem ilícita através do meio virtual, e por esse motivo, o legislador procurou aumentar drasticamente as penas para abusou dos delitos supracitados.

---

[69] GARCIA, Alline Tavares. O DIREITO A INTIMIDADE E A FRÁGIL PRIVACIDADE DA ERA DIGITAL: uma análise sobre os crimes cibernéticos e eficácia da lei Carolina Dieckmann. São Luiz – 2017- Disponível em : Acesso em: 04/11/2022.

[70] GRECO, Rogério. Curso de Direito Penal - Vol. 2. [Digite o Local da Editora]: Grupo GEN, 2022. E-book. ISBN 9786559771462. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559771462/. Acesso em: 04 nov. 2022.

[71] BRASIL. Decreto Lei nº 2.848, de 7 de Dezembro de 1940. Institui o Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm Acesso em 30 de out de 2022.

CONSIDERAÇÕES FINAIS

Por fim, buscou-se através do presente trabalho, apresentar alguns crimes virtuais, os quais se caracterizam como uma ameaça real, pois se trata de crimes desafiadores às autoridades, tendo em vista a dificuldade na punição destas práticas e o aumento em larga escala das mesmas nos últimos anos, em virtude do aumento do uso de tecnologias por parte da população.

Tendo em vista, que toda mudança tecnológica é também uma mudança cultural, o direito também é diretamente influenciado e cabe a este se adaptar à nova realidade, levando em consideração os riscos que as relações virtuais podem proporcionar, cabe ao legislador prever mecanismos que versem sobre a proteção desses indivíduos.

Assim, a internet se apresenta como ferramenta para a perpetração de delitos, potencializando seus efeitos em virtude de seu longo alcance, quebrando fronteiras e a própria legislação nacional.

No mesmo sentido com a internet, também acabou por surgir novos ilícitos, condutas voltadas para o próprio computador e informações nele armazenadas, em virtude do ambiente virtual ser atrativo para a prática da infração penal, pelo motivo do anonimato, a aparente ausência de vigilância proporcionada por esta e também pelo agente poder praticar a ação em qualquer lugar do mundo.

De certo modo, se tem o direito penal como o único meio de controle coercitivo contra a criminalidade no mundo virtual, punindo as conduções ilícitas, com as transformações trazidas pela globalização implicando assim, no aumento da criminalidade, especialmente, tendo em vista que a consumação de um crime praticado através da Internet se dá em todos os lugares de qualquer local do mundo.

Vislumbra-se que a falta de tipificação adequada para os delitos praticados no ambiente cibernético, promove insegurança tanto para a sociedade quanto para o âmbito jurídico brasileiro. As tentativas fracassadas de projetos de lei ou mesmo a publicação apressada de legislações, como é o caso da Lei nº 12.737/2012, geraram inúmeras consequências em desfavor da adequada classificação e regulamentação dos crimes em questão.

Verifica-se a necessidade de cautela na instauração de um ordenamento sob o referido tema, tendo em vista que o ambiente virtual está em constante evolução, devendo ser estudado de forma adequada.

Não obstante, em virtude da quebra de fronteiras que a internet proporciona ao usuário dessa, torna-se imprescindível ao pais, a adoção de medidas internacionais, em cooperação com outros países, como é o caso da Convenção de Budapeste, conforme já exposto.

Acarretando assim em mais tratados internacionais que disciplinam sobre o conteúdo em questão para adequação interna do país, não ferindo o princípio da legalidade ou da reserva legal.

Destarte-se também que cabe a cada um, portanto, assumir sua parcela de responsabilidade na internet, talvez até seja o momento adequado para a comunidade jurídica refletir se os crimes tradicionais, tais como a calúnia, a injúria, a difamação, a violação de privacidade, dentre outros, devem mesmo, manter-se com esta previsão quando ocorridos no espaço virtual

Sendo que, até onde se sabe, as pessoas que se sentem lesadas têm muito mais interesse em receber indenização pecuniária pela violação, pouco importando a punição do infrator, onde inúmeras vezes ocorre a desistência em virtude do esforço empregado do que pelo próprio crime em si.

Frisa-se que apesar da precária legislação brasileira em relação ao tema, evidencia-se também a falta de preparo técnico por parte da Polícia, Ministério Público e também da Magistratura no tratamento da criminalidade cibernética, uma vez que não há delegacias especializadas o suficiente, ficando a cargo das delegacias comuns, ocasionando atrasos e crimes sem soluções.

Por fim, o que se propõe é o uso da informática como forma de comunicação, indiscutivelmente é um fato social, assim, dessa forma, cabe ao ordenamento jurídico brasileiro acompanhar essa evolução, buscando regular, resguardar e proteger os bens jurídicos dos indivíduos de forma mais efetiva possível, tratando o assunto em questão com muito zelo e cuidado, tendo em vista que a vida humana e seu meio de sobrevivência cada vez mais depende da internet. No mais, evidencia-se que atualmente há um despreparo por parte do ordenamento jurídico e das instituições do estado a fim de coibir ilícitos penais.

REFERÊNCIAS

ABEINFO, Associação de Empresas e Profissionais da Informação. Disponível em: https://abeinfobrasil.com.br/a-digitalizacao-apos-1-ano-de-pandemia/. Acesso em 28 de setembro de 2022.

AVAST. Avast Antivírus. Disponível em:https://www.avast.com/pt-br/c-phishing. Acesso em 30 de outubro de 2022

BARATTA, Alessandro. Criminologia Crítica e Crítica do Direito Penal – Introdução à Sociologia do Direito Penal. 3. Ed. Rio de Janeiro: Revan, 2002.

BBC, British Broadcasting Corporation Brazil, Saiba mais sobre a história dos hackers. Disponível em: https://www.bbc.com/portuguese/noticias/2011/06/110623_historiahacking_is. Acesso em 05 de outubro de 2022.

Biolcati, Fernando Henrique de Oliveira. INTERNET, FAKE NEWS E RESPONSABILIDADE CIVIL DAS REDES SOCIAIS, Almedina, 2022.

BITENCOURT, Cezar Roberto. Tratado de direito penal: parte geral. 20 ed. São Paulo: Saraiva, 2014. v. 1.

BRASIL. Decreto Lei nº 2.848, de 7 de Dezembro de 1940. Institui o Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm Acesso em 30 de out de 2022.

BRASIL. Lei 12.735, de 30 de Novembro de 2012, Lei Azeredo. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em 30 de out de 2022.

BRIGGS e BURKE, Asa e Peter.Uma História Social da Mídia.Editora Zahar. Acesso em: 25 out. 2022.

CÂMARA, Agência Câmara Notícias. A CPI constata dificuldade em rastrear e punir crimes de internet. Disponível em: https://www.camara.leg.br/noticias/467819-cpi-constata-dificuldade-em-rastrear-e-punir-crimes-de-internet/. Acesso em 25 de novembro de 2022

CASTELLS, Manuel. Fim do Milênio. 4. ed. Tradução de Klauss Brandini Gerhardt e Roneide Venancio Majer. São Paulo: Paz e Terra, 2007. (A Era da Informação: economia, sociedade e cultura; v. 3).

CASTRO, Aldemario Araujo. A internet e os tipos penais que reclamam ação criminosa em público. 2018. Disponível em: https://egov.ufsc.br/portal/sites/default/files/anexos/13308-13309-1-PB.pdf. Acesso em 04 de novembro de 2022.

CASTRO, Carla Rodrigues Araújo de. Crimes de Informática e seus Aspectos Processuais. 2. Ed. Rio de Janeiro: Lumen Juris, 2003.

CB Sistemas, A História do Primeiro Vírus, Disponível em https://www.cbsistemas.com.br/historia-do-primeiro-virus-de-computador/. Acesso em 05 de outubro de 2022

Comer, Douglas E. Redes de computadores e internet [recurso eletrônico] / Douglas E. Comer ; tradução: José Valdeni de Lima, Valter Roesler. – 6. ed. – Porto Alegre : Bookman, 2016.

CRESPO, Marcelo Xavier de F. Crimes digitais. [Digite o Local da Editora]: Editora Saraiva, 2011. E-book. ISBN 9788502136663. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502136663/. Acesso em: 29 set. 2022.

D'URSO, Luiz Augusto Filizzola. Cibercrime: perigo na internet. Publicado em 2017. Disponível em <http://politica.estadao.com.br/blogs/faustomacedo/cibercrime-perigo-na-internet/>. Acesso em 28 de Setembro de 2022

FECOMERCIO, Federação de Comércio de Bens, O hacker mais procurado do mundo ajuda empresas a melhorarem segurança virtual. Disponível em:

www.fecomercio.com.br/noticia/hacker-mais-procurado-do-mundo-ajuda-empresas-a-melhorarem-seguranca-virtual. Acesso em 05 de outubro de 2022.

FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. REVISTA DA FACULDADE DE DIREITO DA UFMG, 2013.

GARCIA, Alline Tavares. O DIREITO A INTIMIDADE E A FRÁGIL PRIVACIDADE DA ERA DIGITAL: uma análise sobre os crimes cibernéticos e eficácia da lei Carolina Dieckmann. São Luiz – 2017- Disponível em : Acesso em: 04/11/2022.

GRECO, Rogério. Curso de Direito Penal - Vol. 2. [Digite o Local da Editora]: Grupo GEN, 2022. E-book. ISBN 9786559771462. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559771462/. Acesso em: 04 nov. 2022.

Google, A História do Primeiro Computador. Disponível em: <https://sites.google.com/site/historiasobreossitesdebusca/Historia-da-tecnologia/historia-do-primeiro-computador> Acessado em 13 de setembro de 2022

Insper, Instituto de Ensino e Pesquisa, Mundo se aproxima da marca de 5 bilhões de usuários de Internet. Publicado em 2022. Disponível em: https://www.insper.edu.br/noticias/mundo-se-aproxima-da-marca-de-5-bilhoes-de-usuarios-de-internet-63-da-populacao/#:~:text=%E2%A0%80%E2%A0%80%E2%A0%80-,Mundo%20se%20aproxima%20da%20marca%20de%205%20bilh%C3%B5es,de%20internet%2C%2063%25%20da%20popula%C3%A7%C3%A3o&text=O%20n%C3%BAmero%20de%20usu%C3%A1rios%20ativos,Report%2C%20publicado%20pelo%20site%20Datareportal. Acesso em 26 de setembro de 2022.

JESUS, Damásio de, e MILAGRE, José Antonio. Manual de crimes informáticos. São Paulo: Saraiva, 2016.

Knight, Peter T.. A Internet No Brasil: Origens, Estratégia, Desenvolvimento E Governança. Estados Unidos: AuthorHouse, 2014. Acesso em 10 de outubro de 2022.

MONTEIRO, Luís. A INTERNET COMO MEIO DE COMUNICAÇÃO: POSSIBILIDADES E LIMITAÇÕES. Campo Grande/MS: INTERCOM, XXIV Congresso Brasileiro da Comunicação, set. – 2001.

Norton, O que é um vírus de computador? Disponível em https://br.norton.com/blog/malware/what-is-a-computer-virus. Acesso em 10/10/2022.

NUCCI, Guilherme de Souza. Código penal comentado. 14. ed. Rio de Janeiro: Forense, 2014.

NUCCI, Guilherme de Souza. Manual de direito penal. 9.ed. São Paulo: Revista dos Tribunais, 2013.

Olhar Digital, Saiba tudo sobre o projeto Starlink. Publicado em 2021. Disponível em:https://olhardigital.com.br/2021/04/07/ciencia-e-espaco/saiba-tudo-sobre-o-projeto-starlink/.Acesso em 26 de setembro de 2022

ONU, BR. No Brasil quase 60% das pessoas estão conectadas à internet, afirma novo relatório da ONU. Publicado em 2015. Disponível em: https://unicrio.org.br/no-brasil-quase-60-das-pessoas-estao-conectadas-a-internet-afirma-novo-relatorio-da-onu/. Acesso em 26 de setembro de 2022.

Oxford. Dicionário. Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles/oxford. Acesso em 10 de out de 2022.

PAESANI, Liliana Minardi. Direito e Internet: liberdade de informação, privacidade e responsabilidade civil. 1ª ed. São Paulo, Atlas: 2000.

PECK PINHEIRO, Patrícia. Direito Digital, 2. Ed. rev., atual. E ampl. – São Paulo : Saraiva, 2007.

ROQUE, Sérgio Marcos. Criminalidade informática: crimes e criminosos do computador. São Paulo: ADPESP Cultural, 2007.

ROSA, Fabrizio. Crimes de Informática. Campinas: Bookseller, 2002. Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimesciberneticos>. Acessado em: 10/10/2022.

SENADO, Agência Senado Notícias. Aprovada adesão do Brasil à Convenção sobre o Crime Cibernético Disponível em: https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico. Acesso em 04 de novembro de 2022

SILVA, Fernanda Tatiane da. PAPANI, Fabiana Garcia. Um pouco da história da criptografia. Publicado em Anais da XXII Semana Acadêmica de Matemática da Unioeste, 2016. Disponível em <http://projetos.unioeste.br/cursos/cascavel/matematica/xxiisam/artigos/16.pdf>. Acesso em 26 de setembro de 2022.

VIAMONTE, Guilherme Avelino Viamonte.O que é SPAM?. Disponível em : https://www.gta.ufrj.br/grad/15_1/spam/. Acesso em 30 de out de 2022.

VIANA, Marco Túlio apud CARNEIRO, Adeneele Garcia. Fundamentos de direito penal informático. Do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003. Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acessado em: 10/10/2022.

Wazlawick, Raul. História da Computação. Disponível em: Minha Biblioteca, Grupo GEN, 2016

ZOLA, Andrew. What is a mail Bomb. Disponível em: https://www.techtarget.com/searchsecurity/definition/mail-bomb, Acesso em 30 de outubro de 2022