FACULDADE MINAS GERAIS

ALISSON AFONSO DE SOUZA
JOÃO VITOR MILAGRES DE PAULA CARVALHO
WEDER RODRIGUES DA SILVA

A FRAGILIDADE NA LEGISLAÇÃO QUANTO AOS CRIMES CIBERNÉTICOS NO DIREITO PENAL BRASILEIRO

Belo Horizonte, 23 de junho de 2023

ALISSON AFONSO DE SOUZA
JOÃO VITOR MILAGRES DE PAULA CARVALHO
WEDER RODRIGUES DA SILVA

A FRAGILIDADE NA LEGISLAÇÃO QUANTO AOS CRIMES CIBERNÉTICOS NO DIREITO PENAL BRASILEIRO

Monografia apresentada à Faculdade Minas Gerais – FAMIG, curso de Direito, como pré-requisito para conclusão da graduação e obtenção do título de Bacharel em Direito.

Orientadora: Professora Jaqueline Cardoso

Belo Horizonte

2023

A FRAGILIDADE NA LEGISLAÇÃO QUANTO AOS CRIMES CIBERNÉTICOS NO DIREITO PENAL BRASILEIRO

Monografia apresentada à Faculdade Minas Gerais – FAMIG, curso de Direito, como pré-requisito para conclusão da graduação e obtenção do título de Bacharel em Direito.

BANCA EXAMINADORA

_____

Orientadora: Profa. Jaqueline Cardoso

_____

Prof.(a) Avaliador(a)

_____

Prof.(a) Avaliador(a)

Belo Horizonte, 23 de junho de 2023

RESUMO

A presente monografia tem por objetivo trazer à tona o viés dos conceitos inerentes à judicialização de atos praticados no ambiente virtual da internet, que, especificamente no âmbito do território nacional brasileiro, face a fragilidade de legislação para que seja julgado corretamente o crime, pois a classificação existente para o crime cibernético não é eficaz devido a dinâmica dos computadores e da internet. Além de esclarecer os conceitos inerentes ao tema, apresentar-se-ão também as definições e formas jurídicas que fazem abordagem e alusão da titpificação dos então denominados Crimes Cibernéticos contemplados no Direito Penal Brasileiro, assim como também, face a ausência legislação específica para as relações de consumo no ambiente virtual da internet, a fragilidade do apregoado pela Lei Nº8078/90, assim como também, as consequências do mais contemporâneo advento da Lei nº 12.737/2012. Prioritariamente, desenvolveu-se-uma coletânea dos conceitos relacionados ao cerne do presente trabalho, assim como, e concomitantemente. Posteriormente, se apresenta análise sobre as praticadas interpretações da legislação penal a partir da abordagem do constitucional princípio da Legalidade, e também, e por consequência, da eficiência da Lei n°12.015 de 2009, bem como da Convenção de Budapeste. Adotou-se como metodologia para desenvolvimento deste a pesquisa bibliográfica, respaldada por grandes doutrinadores do Direito Penal, naturalmente, legislações que perpassam por mudança de pena para os crimes cibernéticos, vindo da lei Lei nº 14.155/2021, além de renomados artigos que discorrem sobre o tema. Conclusivamente, apresentar-se-ão as impressões dos autores, embassados pelo material consultado e apresentado no discorrer do presente, a cerca do ambiente conjuntural ocasionado pelo crescente advento de ocorrência dos denominados Crimes Cibernéticos, em contra partida da ausência de específica e ampla titpificação destes pela legislação brasileira, incorrendo, inevitavelmente, na promoção de notória insegurança tanto jurídica, quanto social no território brasileiro, tanto físico, quanto virtual.

PALAVRAS-CHAVE: fragilidade; crimes cibernéticos; tipicidade.

ABSTRACT

This monograph aims to bring light the bias of the concepts inherent to the judicialization of acts practiced in the virtual environment of the internet, which, specifically within the scope of the Brazilian national territory, given the fragility of legislation for the crime to be judged correctly, since the Existing classification for cybercrime is not effective due to the dynamics of computers and the internet. In addition to clarifying the concepts inherent to the subject, the definitions and legal forms that approach and allude to typification of the so-called Cyber Crimes contemplated in Brazilian Criminal Law will also be presented, as well as, in the face of the absence of specific legislation for the relations of consumption in the virtual environment of the internet, the fragility of what is proclaimed by Law nº 8078/90, as well as the consequences of the more contemporary advent of Law nº 12.737/2012. As a priority, a collection of concepts related to the core of the present work was developed, as well as, and concomitantly. Subsequently, an analysis is presented on the interpretations of criminal law based on the approach of the constitutional principle of Legality, and also, and consequently, the efficiency of Law No. 12.015 of 2009, as well as the Budapest Convention. Bibliographical research is adopted as a methodology for developing this, supported by great scholars of Criminal Law, naturally, legislation that permeates by changing the sentence for cyber crimes, coming from Law nº 14.155/2021, in addition to renowned articles that discuss the theme. Conclusively, the impressions of the authors will be presented, based on the material consulted and presented in the course of the present, about the conjunctural environment caused by the increasing advent of the so-called Cyber Crimes, in contrast to the absence of specific and broad typification of these by Brazilian legislation, inevitably incurring in the promotion of notorious legal and social insecurity in the Brazilian territory, both physical and virtual.

Keywords: fragility; cybercrimes; typicality.

SUMÁRIO

1 INTRODUÇÃO

O tema proposto, diz respeito ao crescimento dos contingentes populacionais, e com eles, dos sistemas de comunicação e interatividade, tornando cada vez mais acelerados nas últimas décadas, principalmente em relação a rede mundial de computadores, popularmente conhecida como Internet.

Com a difusão e disposição em tempo real de toda ordem de dados e informações promovida pelo exagerado avanço tecnológico, associado à popularização de acesso ao denominado ciberespaço, pode-se observar que em um ambiente tão amplo de interatividade humana promover-se-ia também o surgimento de conflitos entre os elementos humanos, conflitos esses que o ordenamento juridico em alguns casos se encontra fragil.

Essa liberdade de expressão e cada vez maior possibilidade e viabilidade de acesso ao ciberespaço vem ocasionar, naturalmente, em atos que, embora embuídos de liberdade de quem os pratica, são repreensíveis e danosos à coletividade, figurando, em incontáveis vertentes, abordagens e culturas, como crimes, já que ocasionam na desarmonia social, ainda que no ambiente virtual, sem que os elementos envolvidos tenham qualquer tipo de contato presencialmente no ambiente físico, ou comummente chamado, mundo real.

Como também faz parte do processo evolucionário humano, o processo de regularização das relações humanas em prol da sua harmonização e equilíbrio, por instrumentos legais, também se fazem presentes em diversas culturas, especificamente sobre as práticas no ambiente virtual/ciberespaço, com a criação de leis que visam doutrinar e reduzir os conflitos e transtornos sócio económicos promovidos nesse ambiente, claro, também é uma vertente conjuntural.

Especificamente sobre este aspecto é que versa o presente trabalho, pois, a partir de uma breve e objetiva análise, deparar-se-á com a de difícil aceitação, conjuntura de que na realidade, a legislação brasileira não possui componentes que contemplem de forma expressiva, ampla e determinada, a regulamentação e proteção jurídica dos brasileiros no ambiente virtual, tornando a sua abordagem o que imbuída de extrema fragilidade, salvo raras exceções, como será demonstrado no decorrer do presente.

Assim sendo, o presente trabalho visa apresentar e esclarecer em seu teor,

além do caráter da fragilidade das leis vigentes em relação as praticas ilícitas na internet, também apresentar o esforço dos operadores do Direito, tanto por parte dos legisladores, quando dos atores envolvidos no judiciário, em dirrimir os conflitos decorrentes dos crimes, mas que ainda assim, prejudica de forma significativa as relações sociais.

Naturalmente, também compor-se-á o presente, de algumas abordagens jurídicas que discorrem sobre o vácuo legislativo presente no ordenamento jurídico brasileiro inerente ao tema, que serão apresentados em 5 capítulos:

O trabalho começa a tratar do tema a partir do 2º capítulo que apresenta o conceito e as classificações dos crimes cibernéticos, no 3º capítulo vai tratar dos dados atuais sobre a expansão do acesso a internet e consequentemente o aumento dos crimes no Brasil, no 4º capítulo, o trabalho vai trazer as leis atuais no Brasil que tratam sobre o tema, e no 5º capítulo vai tratar da fragilidade das leis referentes a algumas condutas criminais vigentes que precisam ser interpretadas para sua possível condenação.

Enfim no 6º e ultimo capítulo o trabalho vai trazer a conclusão, onde os autores vão expor um relatório do seus pontos de vista particular sobre o tema, onde tras possíveis soluções para a fragilidade dessas leis referentes ao tema.

A perspectiva do resultado do presente estudo é, além de contribuir para futuras consultas sobre o tema, também ocasionar em um referencial sobre o transcurso da operacionalidade jurisdicional face a fragilidade da legislação existente, decorrente, naturalmente, da diversidade específica e ampla titpificação destes atos repreensíveis, ou mesmo crimes cometidos no ciberspaço, quando se, encontrada na legislação brasileira, que promove assim, inevitável insegurança jurídica, tanto no ambiente físico, quanto no virtual.

2 DOS CRIMES CIBERNÉTICOS

O computador e a internet além dos inúmeros benefícios que trouxeram para a sociedade moderna, também se tornaram meio pelo qual se pratica crimes, gerando o que se denomina de macro criminalidade, visto que o meio virtual permite que os criminosos tenham acesso a muitas vítimas.

Quando se fala em macro criminalidade, o Brasil destaca-se como alvo dos *crackers* em ataques cibernéticos, tais como phishing (pescaria de senhas). São bilhões de prejuízo com ataques de *crackers*, roubos de senhas, clonagens de cartões, pirataria virtual, espionagem governamental e industrial, entre outros crimes cibernéticos.

O acelerado desenvolvimento dos sistemas de comunicação e interatividade humana promovem, também, a geração e expansão de um ambiente de difícil controle e fiscalização, uma vez que a difusão e disposição em tempo real de toda ordem de dados e informações decorrente da também popularização e crescimento da acessibilidade ao denominado ciberespaço, essa, por premissa da natureza humana, ocasiona natural e incondicionalmente, conflitos, posto que a quase ilimitada oportunidade de difundir qualquer coisa que se tem condição de produzir, tanto no mudo real, quanto no, e para o, ambiente virtual, viabiliza tal negativa conduta.

Nesse contexto, com o surgimento e aumento de prática de crimes ligados à tecnologia tem demandado um estudo também por parte da ciência do direito.

2.1 Conceito e Classificação dos Crimes Cibernéticos e Digitais

Partindo da questão da grafia do termo cibernético, também encontrado amplamente sobre a apresentação de “cybernético”, “cybercrime” ou “cyber espaço”, de acordo com Went e Jorge (2012), apud Assunção (2021, p. 8), “os crimes cibernéticos consistem no cometimento de atividades ilícitas por meio do computador ou rede de internet e classificam-se de acordo com a sua forma de cometimento”.

Sobre a conceituação desses delitos Augusto Eduardo de Souza dispõe:

> Conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa/culposa, praticado por pessoa física/jurídica, com uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade (ROSSINI, 2004, p. 8)

Não obstante essa pontual e objetiva definição, há também uma corrente doutrinária que aponta que os crimes cibernéticos podem ser estudados se levando em consideração o papel desempenhado pelo computador no contexto da prática do ato ilícito, abordagem essa que nos é esclarecida por Pinheiro (2013, *apud* FERREIRA, 2001), que afirma

> [...] 1) quando o computador é o alvo – p. Ex.: crime de invasão, contaminação por vírus, sabotagem do sistema, destruição ou modificação de conteúdo do banco de dados, furto de informação, furto de propriedade intelectual, vandalismo cibernético, acesso abusivo por funcionário, acesso abusivo por terceirizados, acesso abusivo por fora da empresa; 2) quando computador é o instrumento para o crime – ex.: crime de fraude em conta corrente e/ou cartões de crédito, transferência de valores ou alterações de saldos e fraude de telecomunicações, divulgação ou exploração de pornografia; 3) quando o computador é incidental para outro crime – ex.: crimes contra honra, jogo ilegal, lavagem de dinheiro, fraudes contábeis, registro de atividades do crime organizado; 4) quando o crime está associado com computador – p. Ex.: pirataria de software, falsificações de programas, divulgação, utilização ou reprodução ilícita de dados e programas de comércio ilegal de equipamentos e programas.

Por um outro viés, a Academia Braslieria de Letras difunde como **cybercrime** “A atividade ou prática ilícita perpetrada no espaço digital (como invasão de sistemas, disseminação de vírus, roubo de dados pessoais, falsidade ideológica, acesso as informações confidenciaos, fraude, chantagem, além da propagação de conteúdo que incite ódio, xenofobia, racismo e outros tipos de discriminação)”.

Já outra corrente doutrinária aponta que os crimes cibernéticos podem ser estudados levando-se em consideração o papel desempenhado pelo computador no contexto da prática do ato ilícito, e neste sentido, conforme esclarece Pinheiro (2013, *apud* FERREIRA, 2001), pode ser conceituado em duas diferentes abordagens, pois vejamos:

> [...] 1) quando o computador é o alvo – p. Ex.: crime de invasão, contaminação por vírus, sabotagem do sistema, destruição ou modificação de conteúdo do banco de dados, furto de informação, furto de propriedade intelectual, vandalismo cibernético, acesso abusivo por funcionário, acesso abusivo por terceirizados, acesso abusivo por fora da empresa; 2) quando computador é o instrumento para o crime – ex.: crime de fraude em conta corrente e/ou cartões de crédito, transferência de valores ou alterações de saldos e fraude de telecomunicações, divulgação ou exploração de pornografia; 3) quando o computador é incidental para outro crime – ex.: crimes contra honra, jogo ilegal, lavagem de dinheiro, fraudes contábeis,

> registro de atividades do crime organizado; 4) quando o crime está associado com computador – p. Ex.: pirataria de software, falsificações de programas, divulgação, utilização ou reprodução ilícita de dados e programas de comércio ilegal de equipamentos e programas.

De forma mais sintética e objetiva, Higor Vinicius Nogueira Jorge (2012) e Emerson Wendt (2012), afirmam que “os “crimes exclusivamente cibernéticos” são aqueles que necessariamente precisam do meio da informática para cometer tal crime”, abordagem que notoriamente abrange de forma significativa as práticas lesivas à sociedade dentro do ambiente virtual.

Aliás, sobre os crimes digitais Crespo (2022) os classifica como próprios e impróprios a saber:

> São todas as condutas previstas em lei que sejam punidas com pena criminal e cuja prática envolva aparatos tecnológicos, seja porque a conduta destina-se contra os sistemas informatizados e contra dados, seja porque o meio utilizado é tecnológico, embora o crime pudesse ser praticado de outra forma. Há, portanto, basicamente dois tipos de crimes digitais, a saber:
>
> 1. crimes digitais próprios ou puros (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático. São exemplos de crimes digitais próprios o acesso não autorizado (hacking), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas.
> 2. crimes digitais impróprios ou mistos (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc). São exemplos de crimes digitais impróprios os contra a honra praticados na Internet, as condutas que envolvam trocas ou armazenamento de imagens com conteúdo de pornografia infantil, o estelionato e até mesmo o homicídio. (crespo, 2022, p6.)

Essa sub classificação de crimes digitais também é defendida e classificada por outros autores, como TATEOKI (2015), que em seu artigo de título Clasificação dos Crimes Digitais, esses são divididos em classificações diferenciadas, fazendo então, uso do proferido por Tulio Viana e Felipe Machado (2013), que afirmam existir quatro tipos de classificações de **crimes digitais**,

> na qual segundo os autores o principal bem jurídico a ser protegido pela lei penal nesses casos é a inviolabilidade da informação automatizada (dados), assim os crimes informáticos próprios, são aqueles que o computador é usado como meio para executar o crime, mas não existe a inviolabilidade da informação automatizada (exemplos: ameaça, incitação ao crime e etc), os crimes informáticos próprios são aqueles em que o bem jurídico protegido pela lei penal é inviolabilidade de dados (Como é o caso do crime de invasão de dispositivo informático do art 154-A e 154-B do CP, inserção de dados falsos em sistema de informações do art 313-A do CP e modificação e alteração não autorizada de sistema de informações do art 313-B do CP), os crimes mistos são aqueles que além de proteger a inviolabilidade de dados, a legislação visa proteger bem jurídico de natureza diversa (crime

> eleitoral do artigo 72, da Lei nº 9504/1997), e por fim o crime informático mediato ou direto é aquele considerado o delito fim não informático que herdou a característica do meio para consumar o crime. (Tateoki, 2015, p3.)

Nesse caso, percebe-se uma convergência de termos, para não afirmar categoricamente , transformação, pois ao falar de crimes digitais, o autor, fazendo uso inclusive das palavras de outros autores, faz uso dos termos “crimes informáticos”, e crimes mistos”, dentre outros, para explicar a operacionalidade jurídica da utilização/definição do que pode ser considerado como crime digital.

Ainda, importante trazer o que significa **crimes eletrônicos,** que tem, por definição, o mesmo entendimento dos crimes cibernéticos e informáticos, e por este motivo, esta é uma das definições e termos mais comuns e encontrados no ambiente jurídico, e justamente por sua amplitude de interpretação e diversidade de conceitos, se mostra um dos elementos que promove a insegurança jurídica aos usuários da internet.

Por outro lado, os **crimes da Informática,** os autores Jesus e Milagre (2016), trazem consigo a classificação mais precisa de delito informático, dividindo o delito em quatro tipos, a saber:

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

Não obstante essa pontual e objetiva definição e classificação, existe uma corrente doutrinária que aponta, embora em menor volume, convergentes tipos de classificações: os puros, mistos e comuns, conforme Teixeira (2014) expõe

> o primeiro são aqueles em que o sujeito visa especialmente o sistema de informática; as ações materializam, por exemplo, por atos de vandalismo contra a integridade do sistema ou pelo acesso desautorizado ao computador. Crime de informática misto se consubstancia nas ações em que o agente visa o bem juridicamente protegido diverso da informática,

> porém o sistema de informática é ferramenta imprescindível. E os crimes de informática comum são condutas em que agente utiliza o sistema de informática como mera ferramenta, não essencial à consumação do delito. (Teixeira, 2014, p1.)

Demonstra-se assim que, além dos denominados crimes cyberneticos, também que os chamados crimes de informática possuem ampla e diversificada conceituação e percepção de operacionalidade.

Por fim, há o que se denomina de **Fraude eletrônica** nos é apresentada pelo Douto Juiz Barbagalo, que em seu artigo intitulado “O novo crime de fraude eletrônica e o princípio da legalidade” esclarece que

> [...] finalmente, foram criados os crimes específicos de furto mediante fraude eletrônica (art. 155, § 4º-B do CP) e de fraude eletrônica (art. 171, § 2º-A do CP).

Complementando e de forma a dirimir dúvidas a respeito dessa alteração, expõe:

> [...] foi acrescentado no art. 171 do Código Penal, que define o crime de estelionato, o § 2º-A, uma modalidade de estelionato qualificado, a qual recebeu o *nomen iuris* de "fraude eletrônica", cuja definição legal é a seguinte:
> "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 eletrónico fraudulento, ou por qualquer outro meio fraudulento análogo".

E complementa o douto juiz, delimitando

> Conforme a definição legal, colacionada acima, ocorrerá o crime "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".(Barbagalo, 2022, p3).

Não obstante esclarecedora definição e informação apresentada pelo Douto Juiz, nítida é a percepção de que este se limita-se a apenas o segundo momento em que, nas definições dos termos inerentes aos Crimes Cibernéticos no Direito Penal Brasileiro, em que se faz surgir menção a dispositivo legal específico sobre o teor do termo amplamente utilizado, aspecto que também ser-se-á discorrido em momento oportuno do presente trabalho.

Sobre os delitos computacionais, de acordo com Pinheiro (2017),

> Os crimes computacionais são praticados mediante a utilização de um computador conectado ou não a uma rede, com a finalidade de manipular dados de instituições financeiras, fazendo cópias de programas de

> computador de forma ilegal, revelando segredos de informação computadorizada não autorizada, ou seja, provocando danos sociais por meio de um computador.

Há ainda, referenciado pela mesma autora, a definição apresentada por Costa (1997), que afirma que tomar-se-ia por delito computacional:

> conduta que 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.

Para Aras (2001), o delito informático é gênero e abrange crimes e contravenções penais praticados no âmbito da Internet, como quaisquer condutas relacionadas aos sistemas informáticos, para crimes de meio ou de fim.

A uma convergência desse conceito com os demais, o que demonstra, mais uma vez, a natureza da dificuldade de desenvolver um consenso que favoreça a atividade jurisdicional por parte, tanto dos operadores do direito, quanto também por parte dos legisladores.

3 DA EXPANSÃO DA INTERNET E O AUMENTO DO NÚMERO DE CRIMES CIBERNETICOS

A Internet surgiu no contexto da Guerra Fria, década de 1960, através da guerra tecnológica entre os EUA e Rússia, quando a Agência de Projetos de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos (a DARPA) projetou a rede para impedir a tomada ou destruição do sistema norte-americano de comunicações pelos soviéticos, isso num caso de guerra nuclear. Daí criou-se uma arquitetura de rede sem controle central, formada por milhares de redes de computadores autônomos, com inúmeras maneiras de conexão, contornando barreiras eletrônicas. (Barros, 2007).

No Brasil a Internet se iniciou em setembro de 1988 iniciando suas conexões no setor académico e somente, anos depois, foi destinada a usuários domésticos e empresas. Após o ano de 1995 a internet se expandiu por todo o mundo, assim como o número de usuários favorecendo assim que inúmeros vírus fossem criados e que esses se propagassem por todo mundo com uma velocidade assustadora. (autor, ano)

Naturalmente, conforme já exposto, uma vez que o acesso da internet se multiplicou, como também, os crimes cibernéticos cometidos, o que delimita então, a fragilidade da legislação aplicada no mundo real.

O poder público frente à tal conjuntura, organizações não governamentais aplicam-se as tentativas para diminuir as questões que surgiram sobre o tema e, nesse contexto, a Safernet[1] (https://www.safernet.org.br), através de pesquisa quantitativa junto a tribunais, fez e divulgou levantamento em que se identificou os principais crimes cibernéticos, de acordo com SANTOS; MARTINS;TYUSCHS (2017), sendo eles, à época do referenciado estudo, delimitados como pirataria, pornografia infantil, calunia, difamação, injúria, e estelionato, dentre outros.

A expansão da internet advinda da evolução dos sistemas comunicacionais, onde, atualmente se acessa a rede mundial de computadores através de um relógio de pulso, em contraponto com os vultuosos e extremamente dispendiosos e inacessíveis computadores que faziam muito menos, e em velocidade muito inferior,

[1] A SaferNet Brasil é uma associação civil de direito privado, com atuação nacional, sem fins lucrativos ou econômicos, sem vinculação político partidária, religiosa ou racial. Fundada em 20 de dezembro de 2005 por um grupo de cientistas da computação, professores, pesquisadores e bacharéis em Direito. Disponível em https://www.safernet.org.br/site/institucional. Acesso em 16/11/2022

quando do início da expansão da rede, também refletir-se-á sobre a desarmonização social, ou seja, na prática de crimes cibernéticos, que evoluem, e se alteram também em todas essas variáveis, concomitantemente com as mesmas.

Esse exponencial crescimento dos crimes cibernéticos no Brasil, seja em volume, seja em diversidade, nos é também relatado pela referida Safernet, que expõe que no primeiro semestre de 2022 as denúncias de crimes cibernéticos aumentaram 67,5% em relação ao mesmo período de 2021. Tal fato foi atribuído à incidência das eleições, destacando que a maioria dos crimes diversificaram para os de racismo, lgbtfobia, xenofobia, neonazismo, misoginia, apologia a crimes contra a vida e intolerância religiosa, demonstrando e comprovando o acima apregoado, que é a facilidade e velocidade com que os crimes cometidos alteram seu volume e formas de ocorrência, tanto no ambiente físico, quanto no virutal, cerne do presente.

3.1 – Principais Crimes Cibernéticos Praticados no Brasil

Tendo em vista o aumento dos crimes no ambiente virtual, popularmente denominado internet, e no teor do ciberepaço, FERNANDES (2013) esclarece sobre o papel do poder público em que “a internet atua como novo agente de organização de massas e também influencia as esferas de poder do Estado, pois este deixa de ter a hegemonia do controle sobre as pessoas”, e complementa, sobre a incapacidade do poder público em combater os crimes afirmando, a respeito do viés da inserção do ciberespaço no cotidiano social que

> Com esse desenvolvimento tecnológico, entra em cena uma nova modalidade criminosa. Infelizmente o Estado, tal como ocorre na mobilização popular, não tem a competência de antever a ação criminosa e, na maior parte das vezes, age reativamente após sua ocorrência (Fernandes, 2013, p2)

Tal pespectiva do Professor vem demonstrar de forma expressiva que também já mencionado, a ausência de legislação ampla e específica que discorra sobre os crimes cibernéticos advém, desse comportamento reativo do poder público.

Essa entendimento é amplamente adaptável quando, e somente após, a ocorrência de fatos que desarmonizam as relações sociais no ambiente virtual, equiparam-se às situações comumente encontradas no ambiente físico, sendo deste, extraídos as nomenclaturas e conceitos dos crimes cibernéticos.

Dá-se então a percepção de fragilidade da legislação, pois decorre do fato de que, quando nos referimos ao ambiente virtual, aplicando-se o praticado no

ambiente físico, se não há previsão legal, não há crime, porém, ele ocorrendo num ambiente (a internet), mesmo que não haja previsão legal, não deixa de ser crime.

Tendo em vista a dimensão de possibilidades da liberdade de expressão no mundo digital, como no mundo real, o elemento humano prever, elaborar, instituir, e principalmente, fazer cumprir, de forma globalizada, ou mesmo isolada, normas reguladoras do comportamento de forma a proteger os interesses coletivos e ainda, garantir a promoção do bem estar social, minimizando de forma significativa, o volume e os tipos criminais ocorrentes.

4 A LEGISLAÇÃO BRASILEIRA RELATIVA AOS CRIMES CIBERNÉTICOS

Uma vez que já se encontra concluído que a existente legislação brasileira que versa sobre os crimes cibernéticos se mostra limitada em quantidade, e fragilidade no que diz respeito à sua aplicabilidade e operacionalização, necessário se faz, esclarecer como se dá o que reconhecemos como hercúleo esforço, tanto dos legisladores, quanto dos operadores do direito brasileiro, e suas ações na tentativa de suprimir a cada vez mais acelerada e crescente, incidência dos cibercrimes.

A partir do conceito de crime, como crimes cibernéticos, as condutas consideradas “típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática”, o que sinteticamente se compreende como sendo os atos praticados no mundo real, que tem por objetivo lesar os sistemas de informática, e/ou seus usuários.

Valemo-nos do também apregoado pelo mesmo autor, como forma de reiterar o até então proferido no presente, assim como também enaltecer o porque de considerar o esforço dos legisladores e operadores do direito brasileiro como hercúleo, pois o mesmo afirma que “as classificações existentes para os crimes cibernéticos não são eficazes, devido à dinâmica dos computadores e da Internet. A evolução proporcionada por eles é muito grande, assim como as novas formas delitivas que vão surgindo”, o que esclarece e ilustra a imensurável complexidade e dinâmica que conota o tema, reiteramos, tanto para os legisladores, quanto para os operadores do direito brasileiro.

Importante ressaltar, que tal complexidade dos crimes cibernéticos e o desenvolvimento de uma legislação específica para estes é também, já expostas no decorrer deste, reiteradas pelo mesmo autor, que enfatiza o caráter de territorialidade, existente somente no ambiente físico, e a complexidade de aplicação da lei no meio virtual, já que afirma categoricamente que

> Como a Internet não possuí fronteiras, qualquer conteúdo pode ser acessado de qualquer lugar do mundo. O Brasil pode proibir, por exemplo, a pornografia na Internet, entretanto, somente poderá cumprir a proibição entre os provedores e usuários do território brasileiro.

E complementa sua percepção dizendo que:

> A partir daí, temos um conflito de competência entre o foro do local de onde

> partiu a ofensa, do domicílio do ofendido e do infrator e ainda, do local onde o ofendido tomar ciência da ofensa.

Fazendo ainda Shimidt (2014), uso das palavras de Marco Antônio de Barros, para enfatizar tal argumento e percepção (com a qual, face o até então exposto no presente, se coaduna), que exemplifica tal situação dizendo que

> Se um crime contra a honra de uma pessoa foi perpetrado em um estado da federação ou em outro país, sua transmissão virtual propagará efeitos para todo o mundo. Pode ser que a vítima se encontre em outra unidade da federação ou país, e ali venha a tomar conhecimento do crime.

A fragilidade da legislação, ante ausência de uma especificidade que abranja todas as vertentes e possibilidades de ocorrência de crimes cibernéticos, e mais ainda, também confirmado que a punibilidade já se apresenta de complexa implementação no ambiente físico, face todas as nuances operacionais e jurídicas existentes, e no ambiente virtual a dimensão da operacionalidade jurídica é massificada e ampliada na mesma dimensão que o próprio ambiente virtual, o que nos é reforçado por Garbossa (2010), que conclui a respeito do tema

> Realmente, diante do atual quadro é mais que necessária a criação de uma legislação penal adequada à prevenção e repressão de crimes praticados a partir de sistemas informáticos, com ou sem a utilização da internet, sob pena de ignorar-se a evolução tecnológica e deixar vítimas desprotegidas.

Não obstante nos pareça natural, face a dimensão do ambiente cibernético, já existem instrumentos, ou ao menos busca destes, que tentam coibir as práticas lesivas à harmonia social dos atos praticados na Internet, conforme demonstrar-se-á a seguir.

4.1 Convenção de Budapeste

Em trabalho, que discorre sobre crimes cibernéticos e o papel do Estado em seu combate, FERNANDES (2013) nos esclarece de forma pontual e completa, a denominada Convenção de Budapeste é um tratado internacional, cujo resultado advém

> (...) de um trabalho desenvolvido pelo Conselho da Europa, na qual estava sendo priorizada a proteção da sociedade contra a criminalidade no ciberespaço. Propunha-se a escolha de uma legislação comum que objetivasse uma maior cooperação entre os Estados da União Europeia, sendo que tal tarefa já vinha sendo desenvolvida desde a década de 1990.

Complementando a informação com a assertiva afirmativa de que “(...) ficou demonstrada a atualidade desta nova modalidade de crime e a necessidade de ele ser combatido por toda a sociedade mundial, visto que não só atinge a Europa, mas

todo o mundo", expandindo assim, uma proposta de legislação que trata especificamente dos considerados à época (já transcorrido o lapso temporal de mais de 30 anos), mais comuns crimes cometidos na internet, e que certamente, já havia ocasionado vítimas destes no território europeu, posto que fora de iniciativa de entes governamentais deste, a sua elaboração.

Compõe o relato do supra referenciado autor, o fato de que o documento em questão foi desenvolvido na Hungria, especificamente em 23 de novembro de 2001, tendo como signatários, na maioria de origem europeia, 43 países, que concordaram em ratificar em seus próprios ordenamentos jurídicos, com as disposições constantes no tratado, em que se tinha "o objetivo primário é a repressão dos crimes cibernéticos com a utilização de normas eficientes e práticas, (...)", que, apesar de ser fruto de árduo trabalho desde os anos 90, só entrou em vigor efetivamente em 2004, após cinco ratificações exigidas por grande parte dos signatários, sendo que dentre eles, até o ano de 2006, 15 Estados haviam assinado, ratificado ou aderido à Convenção, enquanto outros 28, embora signatários, não a ratificaram.

Ainda no trabalho do mesmo autor, deparamo-nos com a informação de que, sinteticamente, tipificou criminalmente as condutas de

> 1) Infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos:
> a) acesso doloso e ilegal a um sistema de informática;
> b) interceptação ilegal de dados ou comunicações telemáticas;
> c) atentado à integridade dos dados (conduta própria de um subgrupo hacker, conhecido como cracket);
> d) atentado à integridade de um sistema;
> e) produção, comercialização, obtenção ou posse de aplicativos ou códigos de acesso que permitam a prática dos crimes acima indicados.
> 2) Infrações informáticas:
> a) falsificação de dados;
> b) estelionatos eletrônicos;
> 3) Infrações relativas ao conteúdo:
> a) pornografia infantil (produção, oferta, procura, transmissão e posse de fotografias ou imagens realistas de menores ou de pessoas que aparecem como menores, em comportamento sexual explícito);
> b) racismo e xenofobia (difusão de imagens, ideias ou teorias que preconizem ou incentivem o ódio, a discriminação ou a violência contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica; injúria e ameaças qualificadas pela motivação racista ou xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade);
> 4) Atentado à propriedade intelectual e aos direitos que lhe são conexos.

Encontra-se então, irremediável convergência com o proferido no presente trabalho, mesmo que em ocorrência em lapsos temporais distintos, no que diz repeito aos principais crimes cibernéticos, pois a Convenção de Genebra, elaborada

há cerca de trinta anos antecedentes ao estudo desenvolvido pela Safernet, alguns dos crimes por ela relatados de ocorrência, já faziam parte do cotidiano da época de seu desenvolvimento, o que nos leva à percepção de que o nela proferido encontra eco no tema em desenvolvimento.

Assim sendo, se percebe um movimento globalizado no esforço da busca por mecanismos legais que venham a coibir tais práticas no amiente virtual.

Nesse contexto, reafirma Shimidt (2014) que:

> A inexistência da culpabilidade pelos crimes cibernéticos 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 dos crimes cibernéticos.

A realidade brasileira nos é apresentada por Albuquerque (2006), que afirma categoricamente que:

> O Direito Penal não está alinhado adequadamente para fazer frente à criminalidade informática, o que cria uma incerteza na sociedade sobre o que é e o que não é permitido. No entanto, o Direito Penal pode delimitar com clareza o que pode ou não fazer com a tecnologia da informação.

Essa conjuntura é ampliada no relato de Muggah (2015), que descreve de forma expressiva a situação brasileira frente a prática de crimes cibernéticos, que, dentre outras considerações, esclarece que

> O Brasil está no epicentro de uma onda global de crime cibernético, ou cibercrime. O país está em segundo lugar na classificação mundial de fraudes bancárias online e malware financeiro, e o problema continua a se agravar.

E ainda, apresenta alarmantes dados, ao relatar que:

> [...] Não há clareza sobre o custo do cibercrime para a economia brasileira. Um relatório alega que, em 2013, o furto de dados no Brasil gerou prejuízos entre 4,1 bilhões de dólares e 4,7 bilhões de dólares. Segundo outras fontes, desde 2012 cerca de 3,75 bilhões de dólares foram hackeados de boletos bancários – um método de pagamento administrado pela Federação Brasileira de Bancos. Isso representa aproximadamente 495.000 transações envolvendo 30 bancos e mais de 192.000 vítimas.

É de conhecimento público nos ambientes jurídicos, no caso de tentativa de penalização dos autores de crimes cibernéticos, há o elemento dificultador do sucesso face a necessidade de que, para acesso à informações privadas, se faz necessária a expedição de ordem judicial específica para tal, não podendo, no entanto, o provedor do sinal de internet, fornecer dados como o identificador do usuário, senha e login dos investigados, deixando o trabalho de investigação, e claro, o atingimento da punibilidade, moroso e ineficaz.

O advento de inserções de artigos que abranjam de forma significativa, na legislação brasileira, seja em existentes e tradicionais leis aplicáveis no ambiente físico (inclusive ultrapassadas, percepção massificada, porém que não diz respeito ao cerne do presente trabalho), seja em específicas leis criadas contemporaneamente, por mais válida e ampla que seja a tipificação de garantias e direitos previstos, tais instrumentos não abarcam por completo o campo de atividade dos cibercriminosos.

Esta conjuntura é que delimitou o desenvolvimento do presente trabalho, que a lembrar, versa justamente sobre a fragilidade legal, e decorrente desta, judicial, sobre os crimes cibernéticos no direito penal brasileiro, como demonstrar-se-á em seguida, assim como também, apresentar-se-á o resultado do já citado, embora considerado hercúleo, pontual esforço dos legisladores e operadores do direito brasileiro na tentativa de solucionar esse problema da exacerbada fragilidade.

4.2 CODIGO DEFESA DO CONSUMIDOR LEI Nº 8.078/90

Remanescente à inserção da internet no Brasil, a inovadora Lei nº 8.078/90, denominada Código de Defesa do Consumidor (CDC), foi considerada, à época de sua instituição, divisor de águas nas relações de consumo do Brasil, de acordo com o conteúdo do site da Associação Nacional das Defensoras e Defensores Públicos (ANADEP), que esclarece sobre a lei

> A Lei 8.078, de 11 de setembro de 1990, é considerada uma das leis mais completas do mundo na área, fruto da Constituição Cidadã de 1988, que assemelha os direitos dos consumidores como basilares na sociedade. Com o advento do CDC, abre-se caminho para a melhoria das relações sociais.[2]

E confirma o acima proferido com a afirmação de que:

> O CDC é anterior ao início da popularização da internet no Brasil e o comércio online explodiu durante a pandemia do novo coronavírus. As vendas pela internet no Brasil cresceram 71% nos 90 dias iniciais da pandemia no país, chegando a R$ 27,3 bilhões, (...).

Ainda, de acordo com os integrantes da ANADEP, o CDC veio a corroborar com relevantes transformações na relação de consumo, sendo então a partir do mesmo, instituída e formalmente reconhecida a consideração do consumidor como parte mais frágil da relação, alterando assim, definitivamente a percepção da figura

---

[2] ANADEP. CE: Código de Defesa do Consumidor completa 30 anos nesta sexta-feira, dia 11. O que avançou?. ASCOM/-CE. 10/09/2020. Disponível em https://www.anadep.org.br/wtk/pagina/materia?id=45808#:~:text=A%20Lei%208.078%2C%20de%2011,consumidores%20como%20basilares%20na%20sociedade. Acesso em 18/11/2022.

do consumidor perante o judiciário, que passou a encontrar maiores subsídios para impedir abusos nestas relações, tornando o mesmo de forma definitiva como elemento vulnerável.

Destaca também a matéria do referido site, algumas conquistas, que mesmo sendo consideradas básicas, não encontravam segurança jurídica no mercado de consumo, como a simples inserção nas embalagens de prazo de validade, composição do teor da própria embalagem, condições de troca ou substituição, prazos de manifestação de ambas as partes (consumidor e fornecedor), respeito aos valores anunciados e valores de aquisição, sobre cobranças, etc.

A relevância desta Lei para o teor do presente está no fato de que, além de ter sido remanescente à inserção da internet no Brasil, e antecedente à massificação de sua utilização, esta já devidamente explorada no teor deste, já em seu teor, previa regras para as relações de consumo virtuais, popularmente delimitadas e conceituadas como compras online

Dessa forma, não se pode olvidar que, apesar de fazer menção à um processo de relação virtual de consumo, o CDC não corresponde diretamente como uma legislação específica que penaliza os crimes cibernéticos, e assim sendo, ainda que consideradas brandas as punibilidades aplicadas aos infratores dos artigos nele previstos sobre os que trazem prejuízo aos consumidores, é tão notória quanto inegável então, o caráter da fragilidade da lei para os crimes cometidos em paralelo às infrações previstas no mesmo ambiente, como o de estelionato, ocasionado pelo recebimento de valores e não entrega do bem/produto, locupletando-se indevidamente o fornecedor, por ludibriar e enganar o consumidor.

Podemos concluir que no âmbito do comércio virtual, os crimes cibernéticos extrapolam as relações da Lei nº 8.078/90, pois demonstram a efetiva ocorrência de possível, se fragilizando assim, então a referida lei, frente o previsto no Código Penal Brasileiro[3], Decreto Lei 2.848/40, em seus arts. 171 e 175, que versa especificamente sobre o estelionato e fraude, respectivamente, deixando o CDC então, desprovido de uma punibilidade mais significativa e abrangente às relações de consumo, principalmente, no ambiente virtual.

Não obstante se chegue a tal consideração, se faz necessário destacar mais um esforço feito por parte dos legisladores brasileiros em busca de aprimoramento

---

[3] Decreto Lei nº 8.078. Código Penal. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 18/11/2022.

de regras que versem sobre a regulamentação dos crimes cibernéticos, pois se encontra em tramitação no Senado Federal Brasileiro, o projeto de Lei nº 76/00, que prevê alterações em vários Códigos, dentre eles, o de Defesa do Consumidor.

4.3 MARCO CIVIL DA INTERNET: LEI 12.965/14

Cronologicamente, o último avanço difundido e amplamente reconhecido no esforço dos entes jurídicos em buscar regulamentar os crimes cibernéticos, e assim, reduzir a fragilidade legislativa e jurisdicional, é proveniente do ano de 2014, quando foi sancionada a Lei nº 12.965, intitulada Marco Civil da Internet.

Com vistas a preencher as lacunas de nosso sistema jurídico no tocante aos crimes virtuais, traz em seu teor, na parte inicial, fundamentos e conceitos, elencando os direitos dos usuários da internet, e posteriormente, delimita a tipificação de alguns princípios, dentre outros, o da liberdade e privacidade, que se mostra, diante do até então exposto, ter maior relevância, pois no campo das garantias, é destacado o direito (a lembrar, constitucional, o que nos remonta à uma redundância jurídica), da não violação da intimidade e vida privada.

A respeito do advento desta lei, e a conjuntura sobre a qual se desenvolveu, temos o exposto por e Ângelo e Sanches (2018) a percepção com a qual coadunamos,

> Em nosso país, são inúmeros os casos de divulgação de conteúdo sem autorização, e que ocorrem meio de invasão computacional. Pesquisas apontam que as mulheres são vítimas recorrentes de tal conduta, segundo a Safernet Brasil, em 2016, 300 pessoas tiveram suas fotos íntimas vazadas. Destas, 202 eram mulheres.

E conclui, com o principal aspecto a respeito da configuração jurídica perante o ordenamento legal brasileiro sobre os crimes cibernéticos, percebendo que

> Apesar de haver tipificação para tal conduta, (...) as punições não são suficientes para coibir os criminosos. Um indivíduo espalha as fotos, ele comete o crime, porém quem sofre as maiores consequências é a pessoa exposta.

Dessa forma, podemos concluir que ainda que não tenha um efetivo resultado do hercúleo esforço dos operadores do direito brasileiro em buscar soluções para os crimes cibernéticos, a implementação do Marco Civil da internet não consubstancia suficiente solução, conforme exposição dos supramencionados autores, que afirmam:

> Com o avanço tecnológico e o crescente número de usuários, se torna indispensável a criação de uma lei que defina as condutas criminosas

> praticadas no meio virtual, com penas destinadas aos seus agentes proporcionais aos resultados danosos que estes produzem. (Muggah, 2015).

Não obstante o até então apresentado demonstre árduo trabalho por parte dos operadores do direito no Brasil, a fragilidade legislativa e judicial dos crimes cibernéticos no direito penal brasileiro se mostra uma realidade que não possui pespectivas de imposição de limite de aplicailidade, nem tampouco extensão ou duração.

4.4 LEI CAROLINA DIECKMANN: LEI Nº 12.737/12

Diferentemente do Código de Defesa do Consumidor, que foi uma ramificação e evolução do apregoado na Constituição de 1988, e foi reconhecido marco nas relações de consumo, a popularmente conhecida como “Lei Carolina Dieckmann” compõe o mencionado papel reativo do Estado na busca pela solução de problemas que acontecem e ganham repercussão popular.

No caso em tela, a Lei nº 12.737/12 recebeu essa conotação popular justamente pelo advento do exacerbado crescimento da internet, pois uma atriz, ao encaminhar seu computador para um prestador de serviços para manutenção, ela teve fotos íntimas suas dele extraídas e difundidas na internet, tendo então a mesma, divulgado na imprensa e redes sociais cibernéticas o ocorrido extravio, assim como também as judiciais providências que procurou para se resguardar, diga-se de passagem, tardiamente, já que as fotos foram amplamente difundidas e até a presente data são passíveis de se encontrar.

Essa configuração conjuntural de ser a referida lei uma ação reativa do Estado, conforme já afirmado no presente, nos é delimitada e confirmada por Machado e Viana (2013), que expõem e demonstram claramente essa percepção, afirmando:

> No Direito Penal brasileiro, antes do advento da Lei nº 12.737/2012, a conduta de invadir dispositivos informáticos não era considerada crime. Contudo, com a vigência da nova legislação, esta ação passou a ser tipificada no art. 154 A do Código Penal Brasileiro.

E complementam esclarecendo que:

> Conforme prevê o artigo 5º da Constituição Federal “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (Viana, 2013).

Em síntese, a inovadora Lei 12.737, de 30 de novembro de 2012, trouxe para o ordenamento jurídico penal brasileiro o novo crime de “Invasão de Dispositivo Informático”, e tal assertiva nos é consubstanciada por Assunção (2021), que elucida detalhadamente

> A referida Lei criou o artigo 154-A, que fora acrescido no Código Penal brasileiro, *in verbis*:
> 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.

Resta incontroverso então que realmente o Estado brasileiro, no que diz respeito à regulamentação, demonstra-se reativo, pois somente após elemento repercutório na mídia, e claro, ainda mais no ambiente cibernético, é que se promoveu a alteração de um dispositivo legal existente, inserindo no mesmo, aspectos inerentes ao ambiente virtual, ou conforme elucidado no presente, ao crime cibernético.

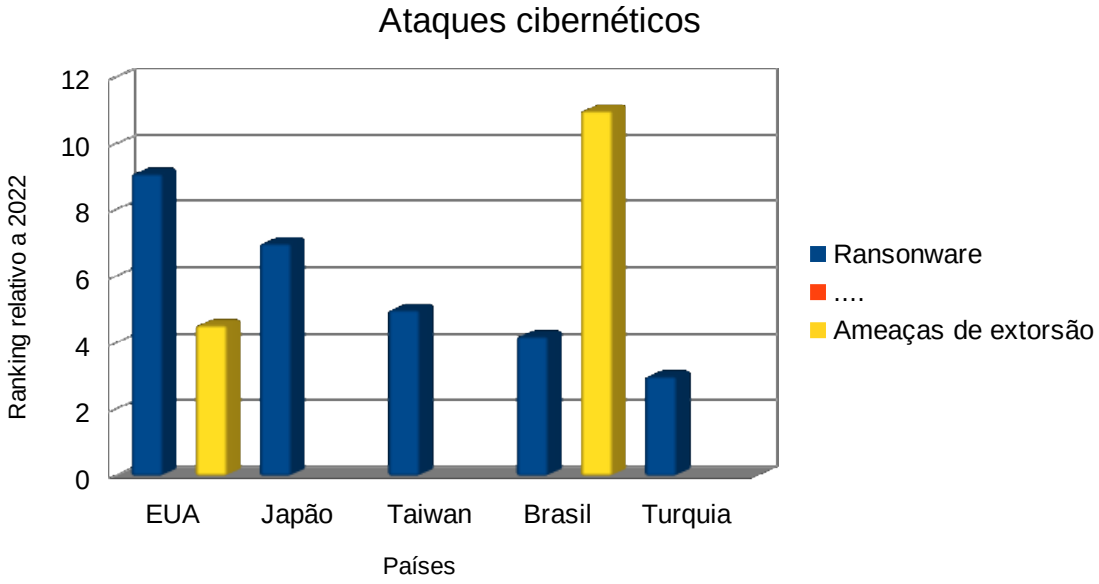
Relevante se faz lembrar que antes desta reativa ação por parte dos legisladores, motivada por ampla repercussão e desarmonização social, se fazia necessário fazer uso de frágeis dispositivos legais para coibir tais práticas, colocando as vítimas desses crimes, então encobertas pelo sentimento de desamparo legal e jurídico.

5 A FRAGILIDADE DA LEGISLAÇÃO FRENTE OS CRIMES CIBERNÉTICOS

O Brasil, de acordo com o site consumidor moderno, está entre os cinco países com maior ataque de ransonmaware do mundo. De acordo“Fast Facts” da Trend Micro, líder mundial em soluções de cibersegurança, ele é o quarto pais que mais sofre ataque de ransonmaware, que é o mesmo que é um software nocivo que é usado para bloquear dados de computadores e servidores através do uso de algum tipo de criptografia.

Veja o gráfico dos 5 países mais atacados:

Gráfico 1 – Ataques cibernéticos



Fonte: https://consumidormoderno.com.br/2022/09/06/

Uma vez que já está concluído de que a ocorrência de delitos através da internet é um fato inevitavel, e claro, que estes crimes acontecem em todo o mundo (até porque o advento da internet tem por premissa ser uma rede mundial de comunicação).

A percepção de que a legislação brasileira faz um enorme esforço, em tentar coibir as práticas dos crimes cibernéticos, é dotada de fragilidade, posto que a punibilidade e instrumentos de combate aos mesmos, se prova, se não ineficazes,

tênues em sua aplicabilidade.

Assim sendo, o dever de se estabelecer então, o reconhecimento de duas abordagens, a primeira que determina esta fragilidade, e a segunda que versa sobre o, embora reativo hercúleo esforço dos legisladores na tentativa de reduzir essa fragilidade.

Denominada cidadã, a Constituição da República Federativa do Brasil de 1988 é a lei fundamental e suprema do Brasil, servindo de parâmetro de validade a todas as demais espécies normativas, situando-se no topo do ordenamento jurídico, obteve essa denominação justamente por defender o cidadão brasileiro como maior bem jurídico a ser tutelado pelo Estado brasileiro, e sendo a lei maior do país, considera-se cumprir ao que se propôs.

Relevante esclarecer que, assim como as demais legislações brasileiras, à exceção das mencionadas no presente trabalho, e pontuais jurisprudências inerentes ao tema, a Constituição da República Federativa do Brasil é proveniente de uma época em que a internet, e naturalmente o ambiente virtual onde ocorrem os crimes cibernéticos, ainda não existia no Brasil, da forma como é atualmente, de aberto acesso à população, e cada vez mais amplo e acelerado.

À esta conjuntura, como demonstrar-se-á seguir, atribui-se o parâmetro de ser o maior elemento motivacional promovente da fragilidade da legislação no tocante aos crimes cibernéticos no direito penal brasileiro.

5.1 Código Penal Brasileiro: Decreto Lei Nº 2.848/1940

Integrantes e um grupo de propensos operadores do direito, natural nos é o entendimento de que desde que o elemento humano se agrupou, os conflitos de interesses se fizeram presentes, sendo resolvidos das mais diversas formas, até a natural evolução para a atual concepção de estabelecimento de regras que minimizem esses conflitos, em prol do estabelecimento de uma incansável busca pela harmonização social, o que concebemos como leis.

Fundamentado no direito Romano, a legislação penal brasileira, teve, naturalmente, origem na legislação dos descobridores e principais colonizadores do país, advindos de Portugal, logo, os colonizadores aplicavam no território descoberto, as regras/leis de seu país de origem, sendo que a primeira legislação penal brasileira teve origem somente em 1830, ou seja, mais de 300 anos apóps o

descobrimento do país, sendo considerado o então Código Criminal do Império do Brasil, o primeiro código penal brasileiro.

Perpassando por mais um longo lapso temporal, a saber, mais de um século após a instituição do Código Criminal do Império do Brasil, buscando atender às novas configurações sociais do país, então já não mais colônia de Portugal, e muito menos de regime monárquico, destacamos, por elementos reativos à várias nuances sociais, políticas e económicas da época, é que fora desenvolvido e instituído, em 1940, o Código Penal Brasileiro, vigente até a presente data.

Implementado pelo Decreto Lei nº 2.848/1940, naturalmente, é composto por um conglomerado de leis que tem por viés o caráter de punibilidade junto à elementos que transgredirem o nele apregoado, como elemento desmotivacional à praticas que ocasionem a desarmonia social.

O supra sucinto e objetivo histórico se fez necessário de apresentação para demonstrar que, em primeiro, que a legislação brasileira sempre advém de um processo reativo à nuances sociais, políticas e económicas. Em segundo, que no lapso temporal transcorrido desde sua criação, até a presente data, o código Penal Brasileiro, além de lento processo de criação, perpassou por poucas e pontuais alterações até a contemporaneidade, sendo sempre essas, também reativas à amplas movimentações sociais.

Natural nos é também, tanto a percepção, quanto conclusão, que o mesmo, face sua época de criação, não poder-se-ia ser dotado de abordagem que contemplasse os crimes cibernéticos, elemento que sequer a Carta Magna do país, advinda de quase meio século após a elaboração do Código Penal Brasileiro, também possui, por razão já exaustivamente mencionada, a lembrar, a inexistência da Internet no país.

Não obstante, conforme já exposto, se faz relevante também mencionar que, além das pontuais alterações já sofridas, o legislador ainda se esforça para adequar o mesmo à vertentes contemporâneas, o que, notoriamente, vem se demonstrando um pequeno fracasso, posto que o avanço tecnológico e as transformações sociais ocorrem em velocidade, frequência e diversidade muito superiores ao trabalho dos legisladores e juristas, corroborando assim, em ampliação do caráter da fragilidade da legislação brasileira frente aos crimes cibernéticos.

Conclusivamente sobre o Código Penal Brasileiro, se faz relevante mencionar que o mesmo encontra-se sobre ampla discussão com várias propostas

perpassando por longo e moroso processo de discussão de alterações diversas (PLS 236/2012, e outras), que abrangem questões que em breve, poder-se-ão se mostrar também ultrapassadas e inóquas, já que versam sobre elementos reativos a conjunturas sociais, com o viés de que considera-se lamentável, nenhuma proposta que contemple o ambiente virtual, ao menos, de que se tenha conhecimento.

6 CONCLUSÃO

Frente ao teor exposto no presente trabalho, em primeiro, podemos concluir que ainda que o legislador e poder judiciário se sacrifiquem para tipificar os atos no ambiente virtual, ainda existem lacunas para punição dos infratores no Brasil, tendo em vista o acelerado crescimento da rede social.

Em segundo, podemos concluir que a conjuntura sócio jurídica é decorrente de um natural e cada vez mais acelerado processo de evolução das relações sociais, promovido e decorrente inclusive, de irremediável avanço tecnológico, principalmente dos sistemas de comunicação e interatividade humana, que rompeu tradicionais paradigmas sociais, e claro, a começar com os jurídicos, pela destruição de limites territoriais, dantes, marcos divisores das relações humanas e culturais.

Dessa forma, se mostra categórico que a diversificada amplitude de surgimento de novos termos e práticas sociais, e claro, jurídicos atos, conceitos e percepções sobre, não só as relações sociais no ambiente virtual, mas também nas estruturas operacionais e suas formas de abordagem, promovem também a mesma conjuntura no que diz respeito às praticas lesivas à harmonia social, principalmente em função de uma ausência de proporcionalidade variedade de definições legais que assim os determine, mas que em contra partida, como mecanismo de discriminação de conflitos, tem-se recorrido, por ausência de opção mais objetiva, à fragilidade da legislação no que diz respeito apos crimes cibernéticos no direito penal brasileiro, âmago do presente trabalho.

Em terceiro, abordando enfim a questão do objeto de discussão do presente trabalho, a percepção de que o mencionado processo de transformação e evolução das relações sociais traz consigo também o surgimento de novos bens e valores que demandam, naturalmente, por específicas formas de tutela e proteção judicial, independente, com o teor cultural de cada nação, dentro desta nova configuração de relacionamento social de inexistentes delimitações, posto que o advento da tecnologia, especial e principalmente, dos meios de comunicação, é fator globalizado.

A possibilidade de um panorama embassado em uma sociedade tutelada judicialmente no ambiente virtual é determinada por força da própria conjuntura da

sociedade em constante transformação, absolutamente utópica no amiente virtual, como também, no caso especificamente brasileiro, no ambiente físico, face a sua retratada reativa natureza legislativa e judicial.

Destarte, também é categórica a conclusão de que o ordenamento jurisdicional penal brasileiro, no que diz respeito ao ambiente virtual, não está nem sincronizado, e tampouco capacitado para combater as surgentes condutas delituosas, uma vez que, no ambiente virtual, a legislação possui apenas algumas leis que são pontuais, mas notoriamente dúbios e falhos, instrumentos inerentes à fatos específicos.

Dentro deste viés, demonstramos o esforço internacional que conotou no tratado da Convenção de Bruxelas, e no caso brasileiro, além das pontuais e reativas inserções legislativas, também a ampla fragilidade da legislação existente, além de reativos e pontuais projetos que objetivam cercar alguns aspectos demandados pela sociedade para os crimes cibernéticos, como por exemplo, o projeto de Lei nº 76/00, que em seu teor, a lembrar, tenciona promover alterações no Código Penal, no Código Penal Militar, no Código de Processo Penal, no Código de Defesa do Consumidor, e na Lei que trata da interceptação telefônica, dentre outras providências, que naturalmente, não dizem respeito exclusivamente ao caso em tela.

A única conclusão passível de se chegar, frente ao todo exposto, é de que, além de não ter por encerrado a discusssão a respeito do tema, é que ter-se-ia como solução do problema da fragilidade na legislação quanto crimes cibernéticos no direito penal brasileiro, seria o desenvolvimento de uma legislação específica que ter-se-ia como objetivo essencial regularizar os golpes e definir os crimes no ambiente virtual, contendo, claro, previsibilidade de proporcional punibilidade para os mesmos, elementos que no ordenamento penal brasileiro, possuem complexa aplicabilidade, para que não incorra justamente, em possibilidade de inconstitucionalidade.

É definitivamente este, o então desafio *mor* do contemporâneo processo evolucional humano, e claro, dos legisladores e operadores do direito Brasileiro.

REFERÊNCIAS

ABSTRATIVIZAÇÃO. In: Dicionário inFormal. Disponivel em: https://www.dicionarioinformal.com.br/abstrativiza%C3%A7%C3%A3o/. Acesso em: 23 nov. 2022.

ALBUQUERQUE, Priscilla Batista de. A Teoria da Abstrativisação do Controle Difuso de Constitucionalidade e o Supremo Tribunal Federal. **Conteúdo Jurídico**, 2017. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/50181/a-teoria-da-abstrativizacao-do-controle-difuso-de-constitucionalidade-e-o-supremo-tribunal-federal. Acesso em: 23 nov. 2022.

ALBUQUERQUE, Roberto Chacon de. Os Objetos Intangíveis na Era da Criminalidade Informática. **Espaço Jurídico Jornal Of Law**. [online], v. 7, n. 2, p. 165-178, 2006. Disponível em: https://editora.unoesc.edu.br/index.php/espaco juridico/article/view/8794. Acesso em: 09 maio 2018.

ANGELO, Ana Elisa; SNACHES, Ademir Gasques. Insuficiência das leis em relação aos crimes cibernéticos no Brasil. **Jus.com.br,** 2018. Disponível em: https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil. Acesso em: 22 out. 2022.

ARAS, Vladimir. Crimes de informática: uma nova criminalidade. **Jus Navigandi**, Teresina, v. 5, n. 51, out. 2001. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=2250. Acesso em: 23 nov. 2022.

ASSOCIAÇÃO DAS DEFENSORAS E DEFENDORES PÚBLICOS DO ESTADO DO CEARÁ. Código de Defesa do Consumidor completa 30 anos nesta sexta-feira, dia 11: O que avançou?. **ASCOM/-CE**, 10 set. 2020. Disponível em:https://www.anadep.org.br/wtk/pagina/materia?id=45808#:~:text=A%20Lei%208.078%2C%20de%2011,consumidores%20como%20basilares%20na%20sociedade. Acesso em: 18 nov. 2022.

ASSUNÇÃO, Ayume da Silva. **A tipicidade dos crimes cibernéticos no direito penal brasileiro:** um estudo sobre o impacto da Lei nº 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos. 2021. Trabalho de Conclusão de Curso - Centro Universitário Faculdade Guanambi, Guanambi, 2021.

BARBAGALO, Fernando Brandini. O novo crime de fraude eletrônica e o princípio da legalidade. **Tribunal de Justiça do Distrito Federal e Territórios**, 2022. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2022/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade#:~:text=Conforme%20a%20defini%C3%A7%C3%A3o%20legal%2C%20colacionada,qualquer%20outro%20meio%20fraudulento%20an%C3%A1logo%22. Acesso em: 20 nov. 2022.

BARROS, Marco Antonio de. Tutela Punitiva Tecnológica. *In*: PAESANI, Liliana Minardi (coord.) **O Direito na Sociedade da Informação**. São Paulo: Atlas, 2007.

BRASIL**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Rio de Janeiro: Presidência da República, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 01 nov. 2022.

BRASIL. **Lei nº 12.737, de 23 de abril de 2014**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasilia: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 12 maio 2022.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasilia: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 30 maio 2023.

COSTA, Marco Aurélio Rodrigues da. Crimes de informática. **Revista eletrônica Jus Navegandi,** 2017**.** Disponível em: http://www.jus.com.br/doutrina/crinfo.html. Acesso em: 20 nov. 2022.

CRESPO, Marcelo. Crimes digitais: do que estamos falando? **Canal Ciências Criminais,** 2022. Disponível em: https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/. Acesso em: 20 nov. 2022.

CRIMES de ódio têm crescimento de até 650% no primeiro semestre de 2022. Safer Net, 2022. Disponível em: https://new.safernet.org.br/content/crimes-de-odio-tem-crescimento-de-ate-650-no-primeiro-semestre-de-2022. Acesso em: 31 maio 2023.

FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do Estado e a realidade. **Rev. Fac. Direito UFMG,** Belo Horizonte, n. 62, p. 139 - 178, jan./jun. 2013. GARBOSSA, Daniella D'Arco. Crimes informáticos e o Projeto de Lei n°. 76/00 do Senado Federal. **Revista FMU Direito,** São Paulo, v. 24, n. 32, 2010.

GIMENES, Emanuel Alberto Sperandio Garcia. Justiça e segurança: crimes virtuais e condutas criminosas cometida via rede mundial de computadores – Brasil. **Revista de Doutrina da 4ª Região**, Porto Alegre, n. 55, ago. 2013. Disponível em: https://www.topsulnoticias.com.br/news/justi%C3%A7a-e-seguran%C3%A7a%3A-crimes-virtuais-e-condutas-criminosas-cometidas-via-rede-mundial-de-computadores-brasil/. Acesso em: 31 maio 2023.

IBGE Educa. Desenvolvido pelo Instituto Brasileiro de Geografia e Estatistica, 2023. Apresenta informações sobre educação com conteúdos atualizados e lúdicos sobre o Brasil. Disponível em: https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html. Acesso em: 24 nov. 2022.

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

LÉVY, P. **A inteligência coletiva por uma antropologia do ciberespaço** (L. P.

Rouanet, Trad.). São Paulo: Loyola. 1998

MUGGAH, Robert. O problema do cibercrime no Brasil. **El País Brasil**, 22 out. 2015. Opinião. Disponível em: https://brasil.elpais.com/brasil/2015/10/23/opinion/1445558339_082466.html. Acesso em: 23 nov. 2022

PINHEIRO, Daline Bento. Crimes computacionais na esfera penal jurídica brasileira. **Conteudo Juridico**, Brasilia-DF, 2017. Disponivel em: https://conteudojuridico.com.br/consulta/Artigos/51026/crimes-computacionais-na-esfera-penal-juridica-brasileira. Acesso em: 23 nov. 2022

QUEM somos. Safernet. Disponivel em: https://www.safernet.org.br/site/institucional. Acesso em: 16 nov. 2022

ROSA, Fabrízio. **Crimes de informática.** 2. ed. Campinas: Bookseller, 2005.

SHMIDT, Guilherme. Crimes cibernéticos. **JusBrasil,** 2014. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. Acesso em: 18 out. 2022.

SILVA, Taziane Mara da; TEIXEIRA, Talita de Oliveira; FREITAS, Sylvia Mara Pires de. Ciberespaço: uma nova configuração do ser no mundo. **Psicol. rev.**, Belo Horizonte, v. 21, n. 1, p. 176-196, jan. 2015 . Disponível em: http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1677-11682015000100012&lng=pt&nrm=iso. Acesso em: 24 nov. 2022.

TATEOKI, Victor Augusto. Classificação dos Crimes Digitais. **JusBrasil,** 2015 Disponivel em: https://victortateoki.jusbrasil.com.br/artigos/307254758/classificacao-dos-crimes-digitais. Acesso em: 20 nov. 2022.