CRIMES CIBERNÉTICOS / *CYBER CRIMES* [*]

Jessica Ayumi Matushita

Matheus Heron Martins[**]

SUMÁRIO: *1 Introdução. 2 Conceito de internet e de crime cibernético. 3 Breve histórico da internet no mundo e no Brasil. 4 A evolução histórica dos crimes virtuais e a legislação. 5 Classificação dos crimes cibernéticos. 6 Motivação da criação da Lei nº 14.155/2021. 7 Estatísticas dos crimes cibernéticos no Brasil. 8 A importância da tutela nos crimes cibernéticos. 9 Considerações finais. Referências.*

RESUMO: O presente artigo volta-se ao estudo dos crimes cibernéticos, tendo em vista a constante evolução da tecnologia, que mudou a forma de como um indivíduo comunica-se e vive-se em sociedade, assim como também mudou as formas de se cometer delitos. Diante deste cenário, os crimes cometidos na *internet* têm se tornado alvo de insegurança, pois trata-se de um meio virtual comumente utilizado nos dias atuais, sendo necessária uma atenção maior nas normas para combatê-los. Para tanto, em um primeiro momento, busca-se definir o conceito de *internet* e crime cibernético, relatar um breve histórico destes no mundo e no Brasil, indicar os tipos de crimes cibernéticos existentes no ordenamento jurídico brasileiro, bem como a motivação da criação da Lei nº 14.155/2021, que introduziu no Código Penal dispositivos que punem mais rigorosamente aqueles que cometem tais delitos, a estatística dos crimes cibernéticos no período compreendido entre 2018 até os dias atuais, e, por fim, analisar sobre a importância da tutela nos crimes cibernéticos. Desse modo, realizou-se pesquisa exploratória,

---

[*] Trabalho de Conclusão do Curso apresentado como requisito parcial para obtenção do grau de Bacharel em Direito, orientados pela Professora Caroline Bittencourt da Silveira.

[**] Acadêmicos do Curso de Direito no Centro Universitário Integrado de Campo Mourão – PR. E-mail jessica.ayuumi@gmail.com; heron1306@gmail.com.

com análise qualitativa, quantitativa e pesquisa bibliográfica, com a utilização de material específico em publicação de artigos científicos. Concluiu-se com o presente que a legislação brasileira ainda não está preparada para combater os crimes cibernéticos, fazendo-se necessária a implementação de novas leis para suprir essa lacuna apresentada.

PALAVRAS-CHAVE: Crimes cibernéticos. Tutela. *Internet*. Ambiente virtual.

ABSTRACT: *This article turns to the study of cybercrimes, in view of the constant evolution of technology, which changed the way an individual communicates and lives in society, as well as changed the ways of committing crimes. Given this scenario, crimes committed on the Internet have become the target of insecurity, because it is a virtual medium commonly used today, and greater attention is needed in the norms to combat them. To this end, at first, we seek to define the concept of internet and cybercrime, to report a brief history of these in the world and in Brazil, to indicate the types of cybercrimes existing in the Brazilian legal system, as well as the motivation for the creation of Law No. 14,155/2021, which introduced into the Penal Code devices that punish those who commit such crimes more rigorously, the statistics of cybercrime in the period from 2018 to the present day, and finally analyze the importance of guardianship in cybercrimes. Thus, exploratory research was carried out, with qualitative, quantitative analysis and bibliographic research, with the use of specific material in the publication of scientific articles. It was concluded with the present that the Brazilian legislation is not yet prepared to combat cybercrime, making it necessary to implement new laws to fill this gap presented.*

KEY-WORDS: *Cybercrimes. Guardianship. Internet. Virtual Environ.*

1 INTRODUÇÃO

Atualmente a *internet* faz parte do cotidiano da grande maioria das pessoas de todo o planeta, essa grande evolução tecnológica inovou a forma em que o mundo, é observado, e também a maneira que se vive atualmente. Este envolvimento criou um aspecto de dependência, o que a torna imprescindível para o contexto social hodierno.

Com a facilidade de acesso, não resta dúvidas que a *internet* é envolvente, sendo praticamente infinita; a quantidade de coisas que podem ser feitas a partir dela, além de conectar pessoas do mundo todo, não esquecendo sua ampla possibilidade de ser utilizada para estudos, trabalhos, lazer e diversas outras coisas.

Infelizmente, toda a facilidade de acesso oferecida por essa evolução tecnológica vem acompanhada de riscos sérios ao ambiente virtual. Da mesma forma que existem os crimes no mundo real, a *internet* também possui uma vasta quantidade de delitos

cometidos por lá. Conhecidos como crimes virtuais ou cibercrimes, os delitos no ambiente virtual se espalham cada vez mais, deixando todos preocupados e com medo de serem a próxima vítima.

Com toda a evolução da tecnologia, vive-se em tempos onde o acesso à informação e a dados no ambiente virtual se tornou comum, pois a *internet* mudou a forma de como comunica-se e vive-se em sociedade, assim como também mudou as formas de se cometer delitos.

Diante dessa mudança, os crimes cometidos na *internet* vêm cada dia mais se tornando comuns no cotidiano das pessoas que a utilizam, gerando insegurança e medo e, por se tratar de um ambiente em constante evolução, é necessária uma atenção maior nas normas para combatê-los.

2 CONCEITO DE *INTERNET* E DE CRIME CIBERNÉTICO

A *internet* conceitua-se como uma rede de computadores interligados em regiões de todo o planeta, capaz de trocar dados e mensagens entre os dispositivos de computação distintos. Ainda, é possível dizer sobre seus aspectos principais, ou seja, todos os componentes básicos que a formam (KUROSE E ROSS, 2013, p. 2).

Pode-se dizer, também, que a *internet* é "o maior acervo de informações disponíveis publicamente", tendo em vista o seu aspecto informativo em nível global (MORAIS, LIMA E FRANCO, 2012, p. 42).

Segundo o entendimento de Inellas (2004, p. 3):

> A *Internet* é uma Rede de computadores, integrada por outras Redes menores, comunicando entre si, os computadores se comunicam através de um endereço lógico, chamado de endereço IP, onde uma gama de informações são trocadas, surgindo aí o problema, existe uma quantidade enorme de informações pessoais disponíveis na rede, ficando a disposição de milhares de pessoas que possuem acesso à *internet*, e quando não disponíveis pelo próprio usuário, são procuradas por outros usuários que buscam na rede o cometimento de crimes, os denominados Crimes Virtuais.

Com o avanço da modernidade tecnológica, os crimes cibernéticos, doravante crimes virtuais, têm surgido abruptamente, desestabilizando a segurança da rede.

Por se tratar de algo novo e diferente, a sensação de liberdade fez com que as pessoas perdessem um pouco da noção do que era real, facilitando a utilização do ambiente virtual como meio de praticar delitos.

Bittencourt (2016) alega que existem dois lados na tecnologia, segundo seu ponto de vista, do mesmo jeito que a tecnologia dá aos seus usuários uma liberdade mais ampla e igualdade individual maximizada, ela também consegue retirar dos indivíduos a habilidade de distinguir as pessoas com as quais se relacionam de maneira virtual, além de inibir a capacidade de diferenciar a sensação de segurança da ideia com a de segurança real.

A globalização, a facilitação de comunicação e diversas outras possibilidades que a *internet* proporciona é de fato algo espantoso, entretanto, a sensação de liberdade e de impunidade faz com que ela se torne um ambiente vulnerável, onde quem tem um maior conhecimento pode usar de forma indevida para prejudicar terceiros.

Por conta dessa globalização, começaram a surgir os crimes virtuais, e como a *internet* se mostrava como um ambiente novo, não foi difícil que se propagasse, gerando de certa forma, uma insegurança aos usuários da rede.

Deste modo, os crimes virtuais, conhecidos também como crimes cibernéticos, no entendimento dos autores Jesus e Milagre (2016, p. 9), refere-se a fatos típicos e antijurídicos cometidos por meio da, ou contra a tecnologia da informação, ou seja, um ato típico e antijurídico, cometido através da informática em geral.

Nessa mesma linha de raciocínio, segundo Rossini (2004, p. 110), o conceito de “delito informático” poderia ser descrito como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por uma pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou até mesmo fora dele, e que ofenda, de forma direta ou indiretamente, a segurança da informática, que tem por elementos a integridade, a disponibilidade a confidencialidade.

A prática criminal é algo tão antigo que acompanha a humanidade desde o início de sua existência, atualmente essa criminalidade passou de nível e está em escala global, com diversas organizações criminosas com atividades espalhadas em todo o mundo. Esse fenômeno afeta toda a economia em nível nacional e internacional, além de repercutir também sobre a política, na segurança e na sociedade de forma geral (CASTELLS, 2000, p. 202). Por incrível que pareça, atualmente existem grupos especializados em computação e que utilizam dessa inteligência para atuar de forma criminosa.

Deste modo, passar-se-á a um breve histórico da *Internet* e dos crimes cibernéticos, que relatem sua evolução no mundo e no Brasil.

3 BREVE HISTÓRICO DA *INTERNET* NO MUNDO E NO BRASIL

A história da *internet* se dá com a Guerra Fria – conflito político-ideológico travado entre Estados Unidos da América (EUA) e União Soviética (URSS), no período compreendido entre 1945 a 1991 –, onde estas duas super potências disputavam poderes e hegemonias, tendo a primeira alinhada ao capitalismo, e a segunda, ao comunismo (TODA MATÉRIA, 2019).

De acordo com esta mesma fonte, em 07 de fevereiro de 1958, nos EUA, foi criada a ARPA Agência de Projetos de Pesquisa Avançada[1], uma empresa que revolucionaria o mundo, pois a mesma foi a responsável pela pesquisa e pelo desenvolvimento das novas tecnologias, em especial, para facilitar a troca de informações, tendo em vista temer os ataques soviéticos – como o lançamento do satélite Sputnik, em outubro de 1957 (CARVALHO, 2006, p. 28) –, e facilitar as estratégias de guerra.

Em 23 de março de 1972, alterou-se o nome da agência para DARPA - Agência de Projetos de Pesquisa[2], permanecendo até o ano de 1993, quando então o Presidente Bill Clinton determinou a retomada do nome para ARPA. Posteriormente, em 10 de fevereiro

[1] *Advanced Research Projects Agency*.
[2] *Defense Advanced Research Projects Agency*.

de 1996, reassumiu em definitivo a designação DARPA, nome este que persiste até hoje (INFOPEDIA, 2022).

A *internet* já havia evoluído consideravelmente para a época em questão, mas ainda não tinha atingido o auge.

Por volta do ano de 1966, Robert Kahn entrou na DARPA, juntamente com Howard Frank, criaram o plano ARPANET – Rede de Agências de Projetos de Pesquisa Avançada[3]. Seu primeiro protótipo foi feito em 1967, entretanto, somente ganhou visibilidade quando um computador da Universidade da Califórnia (UCLA) se conectou com outro do SRI Instituto de Pesquisa de Stanford[4], fato esse que ocorreu em 29 de outubro de 1969 (ROCK CONTENT, 2020).

Segundo Kurose e Ross (2013, p. 45):

> Roberts publicou um plano geral para a ARPAnet [Roberts, 1967], a primeira rede de computadores por comutação de pacotes e uma ancestral direta da *Internet* pública de hoje. Em 1969, no Dia do Trabalho nos Estados Unidos, foi instalado o primeiro computador de pacotes na UCLA (Universidade da Califórnia em Los Angeles) sob a supervisão de Kleinrock. Pouco tempo depois, foram instalados três computadores de pacotes adicionais no Stanford Research Institute (SRI), na Universidade da Califórnia em Santa Bárbara e na Universidade de Utah. O incipiente precursor da *Internet* tinha quatro nós no final de 1969. Kleinrock recorda que a primeiríssima utilização da rede foi fazer um login remoto entre a UCLA e o SRI, derrubando o sistema [Kleinrock, 2004].

Ainda, de acordo com KUROSE e ROSS (2013), no ano de 1972, a ARPANET tinha cerca de 15 nós e foi apresentada publicamente pela primeira vez por Robert Kahn. O primeiro protocolo fim a fim entre sistemas finais da ARPANET, conhecido como NCP – Protocolo de Controle de Rede[5], estava concluído. Por conta desse protocolo, a escrita de aplicações tornou-se possível. Em 1972, Ray Tomlinson, da BBN, escreveu o primeiro programa de e-mail.

---

[3] *Advanced Research Projects Agency Network.*
[4] *Stanford Research Institute.*
[5] *Network-Control Protocol.*

Em 1974, foi desenvolvida por Robert Kahn e Vinton Cerf uma nova versão de protocolo, respondendo a um ambiente de rede de arquitetura aberta, TCP/IP – Protoloco de controle de transmissão/Protocolo da internet[6] foi o nome recebido por esse novo protocolo (ROCK CONTENT, 2020).

Segundo a mesma fonte, o intuito do protocolo TCP/IP ia além de apenas ser um controlador, pois visava facilitar a comunicação entre as redes sem a necessidade de alterações na sua interface, por isso ganhou destaque. Também garantia uma maior estabilidade sem que houvesse perda nos pacotes de informação e verificava a chegada e a ordem que haviam sido enviados.

Após um tempo, mais precisamente em 1983, a ARPANET adere ao novo protocolo, mudando do antigo NCP para o TCP/IP. Dois anos depois, a *internet* já estava consolidada no mundo e era a principal rede de comunicação com alcance global (ROCK CONTENT, 2021).

De acordo com o Netion Telecom (2020), até hoje é utilizado o *WWW* – Rede Mundial de Computadores[7], mas a história dele começa em 1989, quando Tim Berners-Lee o desenvolveu com o intuito de facilitar o trabalho colaborativo no CERN. Pode-se dizer que o *WWW* funciona como um protocolo de distribuição de documentos de hipertexto – HTTP – Protocolo de Transferência de Hipertexto[8] –, interconectados e acessíveis por meio de um navegador da web conectado na rede de *internet*.

De acordo com o site Toda Matéria (2019):

> A década de 90 ficou conhecida como o "boom da *internet*", pois foi quando ela se popularizou pelo mundo, com o surgimento de novos browsers ou navegadores — *Internet* Explorer, Netscape, Mozilla Firefox, Google Chrome, Opera, Lynx — e o aumento do número de usuários, navegadores da *internet*. Diante disso, ocorre uma grande proliferação de sites, chats, redes sociais — Orkut, Facebook, Msn, Twitter —, tornando a *internet* a rede ou teia global de computadores conectados.

---

[6] *Tranmission Control Protocol/Internet Protocol.*
[7] *World Wide Web.*
[8] *Hypertext Transfer Protocol.*

No Brasil, a chegada da *internet* ocorreu em setembro de 1988, com o desenvolvimento no meio acadêmico e científico, sendo que, no começo, apenas professores e funcionários de universidades e instituições de pesquisa tinham acesso a ela. De acordo com Guizzo (2002), a *internet* tem início no Laboratório Nacional de Computação Científica (LNCC), quando conseguiram acesso à BITNET, onde foi possível estabelecer uma conexão de 9.600 bits com a Universidade de Maryland.

No ano de 1995 a *internet* passou a ter acesso público, deixando de ser um privilégio das universidades. Após se tornar pública, o número de provedores que oferecem o serviço e número de usuários que usam a *internet*, vem aumentando vertiginosamente a cada ano. De acordo com Takahashi (2000, p. 133):

> Uma primeira versão de serviços *Internet* com pontos em 21 estados no País foi implantada pela Rede Nacional de Pesquisa (RNP) de 1991 a 1993, a velocidades baixas. Entre 1995 e 1996, esses serviços foram atualizados para velocidades mais altas. Paralelamente, a partir de junho de 1995, uma decisão do Governo Federal definiu as regras gerais para a disponibilização de serviços *Internet* para quaisquer interessados no Brasil.

A comercialização da *internet* tem início no final de 1994 quando a Embratel elaborou um projeto piloto, por conta desse projeto, foi permitido o acesso à *internet* por linhas discadas e, em 1995 através de RENPAC ou linhas E1. No mesmo tempo em que isso acontecia, foi iniciada pela RNP (Rede Nacional de Pesquisas) um processo de implantação da *internet* no comércio brasileiro. De acordo com o site Brasil Escola (2021):

> [...] a partir de abril/1995 foi iniciada pela RNP um processo para implantação comercial da *Internet* no Brasil, com uma série de etapas, entre as quais a ampliação do *backbone* RNP no que se refere a velocidade e número de POP's, a fim de suportar o tráfego comercial de futuras redes conectadas a esses POP's; esse *backbone* a partir de então passou a se chamar *Internet*/BR.

Atualmente, conforme consta no site Gov.br, de acordo com a Pesquisa Nacional por Amostra de Domicílios (PNAD), feita no ano de 2021, cerca de 90,0% dos domicílios nacionais acessam a *internet*, número este que representa um aumento de 5,8% em relação ao ano de 2019.

Mesmo com o aumento de pessoas que passaram a utilizar a *internet*, o IBGE mostrou que cerca de 7,3 milhões ainda não possuem acesso a esta tecnologia. Os principais motivos para a não utilização são a falta de interesse (29,3%), o alto custo nos valores do serviço (28,8%) e o fato de nenhum morador da casa saber usar a *internet* (27,1%) (IBGE, 2022).

4 A EVOLUÇÃO HISTÓRICA DOS CRIMES VIRTUAIS E A LEGISLAÇÃO

A *internet* teve sua origem na década de 60, e tinha como objetivo principal servir como um meio de comunicação mais seguro e de combate à guerra, além de proporcionar maior proteção de dados para a segurança nacional. Entretanto, paralelamente, surgem evidências de casos de manipulação e sabotagem em sistemas de computadores, ocorrendo, assim, os chamados crimes virtuais (TODA MATÉRIA, 2019).

Segundo Albuquerque (2006, p. 35):

> [...] os primeiros casos de crimes cibernéticos foram na década de sessenta. Eram utilizados computadores como forma de cometimento do crime virtual, como o estelionato. Na referida década foi que começaram a ser relatados pela imprensa os primeiros casos de crimes cibernéticos. A partir da década de setenta, começaram os primeiros estudos empíricos sobre a criminalidade cibernética.

Na década de 70, foi criado o TCP/IP, protocolo que permitia a comunicação de outros usuários, além dos centros de pesquisas dos EUA (ROCK CONTENT, 2020).

Dessa forma, surgem também a figura do *hacker*, relacionado a crimes tais como invasão de sistemas, furto de *software*, entre outros., conforme leciona Inellas (2004, p. 15):

> Os ataques cibernéticos, praticados pelos *hackers*, iniciaram-se nos Estados Unidos da América e alcançaram outros países, inclusive o Brasil. O *hacker* é considerado o intruso do mundo virtual. A invasão dos Sistemas alheios, pelo *hacker*, geralmente deve-se a um mero desejo de demonstração de sua perícia em informática e à curiosidade. Normalmente, não possui um fim ilícito específico. Todavia, sua conduta, por si só, já é considerada ilícita. Seu conhecimento lhes permite avaliar as falhas de Sistema e violá-lo. O termo *hacker* surgiu por volta de 1960, e era usado para designar as pessoas que se interessavam em programação de computadores. Após o surgimento e

> expansão da *Internet*, o sentido do termo mudou, passando a significar os invasores dos computadores alheios. Os *hackers* sabem que todo Sistema de Segurança possui alguma falha. Então, dedicam-se a procurar, até encontrar, essa falha, denominada porta, para uma vez localizada, violar o Sistema daquele usuário. Dessa forma, poderá comandar computadores alheios à distância, invadir Sistemas de empresas e de Governos, alterar Sites e ter acesso aos mais diversos tipos de informação.

Em 30 de novembro de 2012 foi criada a Lei nº 12.737, que tipificou como crime a invasão de dispositivo informático. Esta lei ganhou força por conta de um episódio marcante envolvendo a atriz Carolina Dieckmann, que teve suas fotos íntimas expostas na *internet*, após uma subtração de arquivos pessoais em seu computador (FMP, 2021).

Com toda a modernização, cada dia que passa a sociedade está mais inserida no ambiente virtual. Um ponto que deve ser muito discutido é que o Direito – especialmente o Direito Penal – não está conseguindo acompanhar esse crescimento da evolução cibernética. Existem tentativas de modernização da legislação criminal, como, por exemplo, o artigo 154-A do Código Penal (BRASIL, 1940), que tipifica o comportamento do indivíduo com má intenção, que invade dispositivo eletrônico alheio para que possa obter, adulterar ou até mesmo destruir dados ou informações com o intuito de deixar a vítima vulnerável e, assim, obter uma vantagem ilícita.

Criou-se, então, outra lei para apoiar o combate de crimes virtuais, aprovada pelo governo brasileiro em 2014, que é a Lei nº 12.965, mais conhecida como Marco Civil da *Internet*, que estabelece princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil (BRASIL, 2014).

Segundo Siqueira et al. (2017, p. 126):

> A lei do Marco Civil foi criada para suprir as lacunas no sistema jurídico em relação aos crimes virtuais, num primeiro momento tratando dos fundamentos, conceitos para sua interpretação e objetivos que o norteiam, além de enumerar os direitos dos usuários, tratar de assunto polêmicos como por exemplo a solicitação de histórico de registros, a atuação do poder público perante os crimes virtuais e por último garante o exercício do direito do cidadão de usufruir da *internet* de modo individual e coletivo estando devidamente protegido.

Assim, o Marco Civil da *Internet* serve para nortear a *internet*, colocando os usuários como os principais beneficiados na rede. O foco principal da lei é a tutela dos direitos fundamentais, e, por esse motivo, é considerada a constituição da *internet* (RAMOS, 2021).

5 CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Com o avanço da tecnologia cada vez mais rápido, tornou-se questão de tempo para que começassem a aparecer os delitos cometidos no ambiente virtual, desestabilizando a segurança da rede.

A prática criminal é algo tão antigo que acompanha a humanidade desde o início de sua existência, e, atualmente, essa criminalidade passou de nível e está em escala global, com diversas organizações criminosas com atividades espalhadas em todo o mundo. Esse fenômeno afeta toda a economia em nível nacional e internacional, além de repercutir também sobre a política, na segurança e na sociedade de forma geral (CASTELLS, 2000, p. 202).

Atualmente, dentre as diversas classificações para crimes virtuais, a mais adotada é aquela que se aproxima da realidade dos fatos, sendo dividida em crimes cibernéticos próprios e impróprios (CAMPELO E PIRES, 2019).

Por um lado, os crimes cibernéticos próprios são aqueles em que o próprio objetivo do sujeito ativo é a utilização do computador como objeto e meio para execução do crime, a fim de atingir o sistema informático do sujeito passivo (vítima), portanto, tanto a execução quanto a consumação acontecem no próprio meio digital, necessariamente (ALMEIDA et al., 2015, p. 224). Siqueira et al. (2017, p. 122) corroboram:

> [...] o infrator pratica a conduta ilícita utilizando o próprio computador da vítima, para extrair dados que possam modificar, alterar ou causar dano ao funcionamento do sistema informático, de maneira que atinja o software ou hardware do aparelho.

Por outro lado, os crimes cibernéticos impróprios são aqueles em que o objetivo do sujeito ativo é a utilização computador como meio para a prática de um ato ilícito final já tutelado (ALMEIDA et al., 2015, p. 225), embora não seja o elemento essencial para a

conduta criminosa, assim como acontece nos crimes virtuais próprios. Segundo Siqueira et al. (2017, p. 122):

> [...] o infrator pratica o crime por meio do computador, utilizando a máquina como um instrumento para a realização da conduta ilícita, de modo que passe a causar efeitos além da informática, podendo o ato ser consumado não só pelo computador mas também fora dele.

Ainda acerca dos crimes virtuais impróprios, conforme o site Slaplaw (2021), pode-se citar, a exemplo, a falsificação de documentos, crimes contra a honra, ameaças, crime de perseguição ou *stalking*, *cyberbulling*, entre outros.

6 MOTIVAÇÃO DA CRIAÇÃO DA LEI Nº 14.155/2021

A Lei nº 14.155/2021, que foi sancionada pelo Presidente da República no dia 27 de maio de 2021, torna mais rigorosa a punição de crimes de violação de dispositivo informático, furto e estelionato cometidos pela *internet* ou por qualquer dispositivo eletrônico. (BRASIL, 2021).

As alterações buscam atualizar o Código Penal, em razão das mudanças que estão ocorrendo no mundo, principalmente os delitos cometidos no ambiente virtual, responsabilizando de maneira mais gravosa os indivíduos que vierem a cometer delitos específicos, como, por exemplo, o furto e o estelionato realizado por meio de aparelhos eletrônicos.

Dada a tamanha importância de normas para o combate dos crimes virtuais e por se tratar de um tema em constante evolução, faz-se necessário que o Código Penal acompanhe de perto e de forma rigorosa cada vez mais este assunto.

Essa inovação na legislação veio em um ótimo momento, tendo em vista o crescimento elevado do número de fraudes virtuais no Brasil. Por conta da pandemia do Covid-19 e do distanciamento social, os meios digitais, que já eram muito utilizados no dia a dia, passaram a ser utilizados também no ambiente de trabalho, contribuindo para o crescimento desses números (ODC, 2022).

Com o grande aumento dos delitos no ambiente virtual, a segurança de todos está correndo risco, apesar de não cessar todos os perigos que existem na *internet*, essa nova lei traz para todos uma sensação de esperança para que, posteriormente, o legislador continue criando normas para tipificar esses delitos e não deixar impune quem os comete.

7 ESTATÍSTICAS DOS CRIMES CIBERNÉTICOS NO BRASIL

A tecnologia trata-se de algo relativamente inovador e diferente, de modo que a sensação de liberdade fez com que as pessoas perdessem um pouco da noção do que era real, facilitando a utilização do ambiente virtual como meio de praticar delitos.

A humanidade tem passado por tempos difíceis, atualmente, existe o medo da contaminação na vida real e, de certa forma, no ambiente virtual não é diferente. No ano de 2019, antes mesmo do início da pandemia do COVID-19, o Brasil já estava em terceiro lugar no ranking de países que mais sofreram com ataques cibernéticos, ficando atrás apenas das superpotências como a China e os Estados Unidos, segundo o relatório global feito pela Symantec (FOLHA DE SÃO PAULO, 2019; CONTEÚDO JURÍDICO, 2022).

Segundo a Gazeta de São Paulo (2020), devido à utilização elevada de celulares, computadores e equipamentos eletrônicos, no ano de 2020 os números de casos envolvendo os crimes virtuais cresceram consideravelmente. Por mais que esses delitos não sejam novidade no Brasil, os maiores índices que já foram registrados se deram durante a pandemia do COVID-19, tendo em vista o aumento do uso de novas ferramentas tecnológicas para funções de trabalho, estudo e lazer (REVISTA COBERTURA, 2022).

De acordo com a empresa *Fortinet Threat Intelligence Insider Latin American*, que analisa os incidentes de segurança cibernética, o Brasil sofreu cerca de 3,4 bilhões de tentativas de ataques na *internet*, entre os meses de janeiro e setembro de 2020. (GASTAL, 2021).

Segundo esta mesma fonte, foi constatado, pela Federação Brasileira de Bancos, um aumento de 80% nas tentativas de *phishing* (obtenção de forma fraudulenta de informações confidenciais de usuários da *internet*), cerca de 70% nos golpes de falso

funcionário e de falsas centrais eletrônicas e 60% em tentativas de fraudes contra idosos. Outro grande aumento referente aos crimes virtuais foi em relação às mulheres, com considerável aumento de delitos no contexto doméstico e familiar, também ocorreu no ambiente virtual. Entre os anos de 2019 até 2020 foi registrado um aumento saindo de 7.112 para 12.698, valor esse que atinge o percentual de quase 80%. Os principais delitos cometidos foram as ameaças, os crimes contra a honra, o *stalking* (bisbilhotar, perseguir alguém) e a pornografia de vingança. Os números apresentados representam apenas a fração que chegou ao conhecimento das autoridades, diante disso, a perspectiva de delitos cometidos em sua totalidade chega a ser ainda mais assustadora.

No ano de 2021, foram registrados 88,5 bilhões de tentativas de ataques na *internet*, de acordo com o levantamento realizado pela empresa *Fortinet Threat Intelligence Insider Latin American*, o que perfaz mais de 950% em relação ao ano anterior (REVISTA COBERTURA, 2022; LGPDBRASIL.COM.BR, 2022; VALOR ECONÔMICO, 2022).

Por um lado, o site R7 (2022) enfatiza que, no ano de 2021, o Brasil estava em segundo lugar no *ranking* de países que mais sofreram ciberataques, com mais de 439.000 ataques cibernéticos (7,1% de um total de 6,4 milhões realizados em todo o mundo), ficando atrás somente dos Estados Unidos, com mais de 1,33 milhão de ataques (21,7%), conforme relatório realizado pela empresa especializada *Netscout*.

Ressalta-se ainda que os sites CanalTech (2021) e ISTOÉ Dinheiro (2021) enfatizam que o Brasil estava em quinto lugar no *ranking* de países que mais sofreu crimes cibernéticos no ano de 2021, sendo que no primeiro trimestre houve um total de 9,1 milhões de ocorrências, mais que o ano inteiro de 2020, levando em conta somente os crimes de sequestro digital (*ransomware*), conforme consultoria alemã *Roland Berger*, ficando atrás somente dos Estados Unidos, Reino Unido, Alemanha e África do Sul.

Ainda que haja uma divergência quanto ao ano de 2021, as duas posições apresentadas demonstram a gravidade das condutas, tendo em vista o Brasil se enquadra entre os cinco países que mais sofreram crimes cibernéticos.

E ainda, conforme o site ISTOÉ Dinheiro (2021):

> Já a empresa holandesa de cibersegurança *Surfshark* divulgou que o Brasil foi o sexto país mais atingido por vazamento de dados no ano: foram 24,2 milhões de usuários expostos entre janeiro e novembro deste ano. A *Surfshark* estima que 1 em cada 5 pessoas em todo o mundo teve dados vazados em 2021.

Importante ressaltar que os crimes virtuais e PIX impulsionaram aumento de 179% dos estelionatos. Conforme o site Correio do Povo (2022):

> Os casos de estelionato quase triplicaram no Brasil desde 2018, de cerca de 426, 8 mil naquele ano à taxa de 1,2 milhão de registros em 2021 — um aumento percentual de 179% no período. Desde então, o crime não diminuiu em nenhum dos 26 estados e no Distrito Federal. É o que revelam estudos da 16ª edição do Anuário do Fórum Brasileiro de Segurança Pública [...] Além disso, o Pix e a tecnologia bancária atual também podem facilitar a prática pela rapidez com que permitem a transferência de valores e a criação de contas — às vezes, com o nome e dados das próprias vítimas. Outras estatísticas coletadas, de assaltos e furtos de veículos, celulares e dos dados no geral reforçam essa percepção dos autores. "Estamos vivenciando mudanças significativas nas dinâmicas dos crimes contra o patrimônio, em direção à sua digitalização. A queda de roubos a transeuntes (-7,5%) e o crescimento de roubos e furtos de celulares (1,8%) estão, muito possivelmente, associados a esta dinâmica", defendem em artigo do anuário os pesquisadores David Marques e Amanda Lagreca.

Denota, portanto, que com o avanço da tecnologia cada vez mais rápido, foi questão de tempo para que ocorresse o aumento exponencial dos delitos cometidos no ambiente virtual, desestabilizando a segurança da rede.

8 A IMPORTÂNCIA DA TUTELA NOS CRIMES CIBERNÉTICOS

As normas jurídicas, de maneira geral, são medidas necessárias à manutenção da vida social, tanto para manter a segurança, quanto para evitar que atrocidades venham a ocorrer. Da mesma forma que acontece no dia a dia, no “mundo real”, na *internet* também se faz necessária a criação de normas para regulamentar o uso e deixar o ambiente virtual mais seguro.

O avanço da tecnologia é constante e, de certo modo, aqueles que tendem a se fixar no passado, ficam cada vez mais desatualizados, da mesma forma que as normas que regulamentam a vida em sociedade ficam cada vez mais ultrapassadas.

O Direito precisa se amoldar às necessidades atuais, e no cenário em que vivemos – a era da tecnologia –, nada mais justo do que se voltar para a regulamentação do ambiente virtual.

Com este avanço da tecnologia, é inevitável que grande maioria das pessoas recorram a ferramentas eletrônicas para resguardar seus arquivos pessoais ou até mesmo profissionais. Neste sentido, ressalta-se a importância de uma legislação com poder suficiente para proteger e assegurar a acessibilidade do material pelos seus proprietários, tendo uma punição severa para quaisquer invasores, além de garantir segurança em todo o ambiente virtual.

Como os crimes virtuais são cometidos por pessoas que vivem escondidas para não serem apanhadas, além as normas, devem ser modificadas as formas de investigação para que, desse modo, consiga rastrear, identificar e punir o indivíduo que comete tais delitos.

Segundo Maia (2017):

> [...] solução para o combate à criminalidade é a mudança desse paradigma: Nota-se que a velha política de segurança pública de tentar combater o crime com medidas clássicas, tais como o aumento do número de policiais militares, não funciona mais. O crime há muito tempo se organizou e, se o Estado não investir com inteligência na inteligência da polícia investigativa para que os criminosos sejam identificados e levados à justiça, de nada vai adiantar aumentar o efetivo da Polícia Militar nas ruas. Isso por uma razão muito simples: é impossível que tenhamos policiais em todos os lugares e também os criminosos não querem conflitos diretos com o aparato de segurança do Estado. Os criminosos atuam onde a polícia não está, pois sabem que, de fato, não serão investigados, ou seja, se não forem presos em flagrante, não serão depois. Isso gera para a população um sentimento de impunidade e desestímulo até em noticiar os crimes que sofre, pois do que vai adiantar perder horas em uma delegacia a espera da realização de um B.O. se aquele crime não será investigado? Gera ainda um efeito contrário para o criminoso, o qual passa a se sentir estimulado a cometer novos crimes.

Os crimes sempre existirão, seja dentro ou fora do ambiente virtual. Por esse motivo, o combate aos crimes virtuais deve ser constante, para que possa surtir melhor efeito, sendo necessário que se propague cada vez mais as informações de como se prevenir, assim como o que fazer nesses casos. Além disso, para regulamentar a vida em sociedade, as normas

de combate a esses delitos precisam ser mais rígidas e específicas, para que, dessa forma, aqueles que o cometem, sejam punidos de maneira adequada.

9 CONSIDERAÇÕES FINAIS

De acordo com o que foi demonstrado, percebe-se que a *internet* é um meio de comunicação muito importante, que vem crescendo cada vez mais, em razão da grande quantidade de pessoas que a utilizam, compartilhando informações de cunho pessoal ou profissional.

A quantidade de possibilidades que a *internet* proporciona é imensurável, mas da mesma forma que existem os benefícios, ela também possibilita a prática de delitos as quais prejudicam os usuários que estão conectados na rede.

O maior problema que se encontra na legislação é a falta de normas específicas para o combate dos delitos cometidos em ambiente virtual. Mesmo com a existência de normas regulamentadoras, ainda é pouco quando se leva em consideração a dimensão da *internet*.

Por se tratar de um assunto em constante evolução, as normas que já existem estão ficando ultrapassadas, levando em consideração a época em que foram elaboradas, e, por esse motivo, se faz necessária a criação de novas normas que se amoldem de acordo com o desenvolvimento da sociedade.

Conforme analisado, conclui-se que a legislação brasileira, no que diz respeito aos crimes virtuais, não está adequada e, muitas vezes, o crime prescreve sem que haja uma punição dos autores do delito.

Avanços significativos nas investigações seriam um mecanismo que poderia ajudar na busca dos criminosos, mas a tecnologia avançou e a legislação não a acompanhou.

Com a criação da Lei nº 14.155/2021, o legislador modernizou o Código Penal com a implementação da tipificação dos delitos específicos que se utilizem de equipamentos eletrônicos ou que atinja o ambiente virtual, tornando mais rigorosas as penas e

criando uma maior sensação de segurança. Mas, ainda falta muito para uma regulamentação adequada que conte com leis mais específicas, no intuito de combater os crimes virtuais, da mesma forma, aumentando os investimentos voltados para a proteção e a segurança das informações dos dados dos usuários.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. **A Criminalidade Informática**. São Paulo: Juarez de Oliveira, 2006.

ALMEIDA, J. J.; MENDONÇA, A. B.; CARMO, G. P.; SANTOS, K. S.; SILVA, L. M. M.; AZEVEDO, R. R. D.. **Crimes cibernéticos**. Caderno de Graduação – Ciências Humanas e Sociais – Unit, v. 2, p. 215-236, 2015.

BITTENCOURT, Rodolfo Pacheco Paula. **O anonimato, a liberdade, a publicidade e o direito eletrônico**. *Jusbrasil*, 2016. Disponível em: <https://rodolfoppb.jusbrasil.com.br/artigos/371604693/o-anonimato-a-liberdade-apublicidade-e-o-direito-eletronico>. Acesso em: 30 set. 2022.

BLOG NETION. **Dia do internauta: conheça a história do WWW**. *Blog Netion*, 2020. Disponível em: <https://www.netiontelecom.com.br/dia-internauta>. Acesso em: 29 set. 2022.

BRAIDA, Fernando Henrique Menezes da Silva. **Crimes cibernéticos: tipificação e legislação brasileira**. *Conteúdo Jurídico*, 2020. Disponível em: <http://www.conteudojuridico.com.br/consulta/Artigos/54506/crimes-cibernticos-tipificao-e-legislao-brasileira>. Acesso em: 20 out. 2022.

BRANCO, Dácio Castelo; YUGE, Claudio. **Brasil é o 5º maior alvo de crimes digitais no mundo em 2021**. *Canaltech*, 2021. Disponível em: <https://canaltech.com.br/seguranca/brasil-e-o-5o-maior-alvo-de-crimes-digitais-no-mundo-em-2021-195628/>. Acesso em: 19 out. 2022.

BRASIL. **90% dos lares brasileiros já tem acesso à *internet* no Brasil, aponta pesquisa**. *Gov.br*, 2022. Disponível em: <https://www.gov.br/casacivil/pt-br/assuntos/noticias-2022/setembro/90-dos-lares-brasileiros-ja-tem-acesso-a-*internet*-no-brasil-aponta-pesquisa>. Acesso em: 06 out. 2022.

BRASIL. **Decreto-Lei nº 2.848/1940 (Código Penal)**. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 12 out. 2022.

BRASIL. **Lei nº 12.965/2014 (Marco Civil da *Internet*)**. Diário Oficial da União, Brasília, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm#art32>. Acesso em: 12 out. 2022.

BRASIL. **Lei nº 14.155/2021**. Diário Oficial da União, Brasília, 28 mai. 2021. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm>. Acesso em: 12 out. 2022.

CAMPELO, Larissa; PIRES, Pamela de Freitas. **Crimes virtuais**. *Jus.com.br*, 2019. Disponível em: <https://jus.com.br/artigos/72619/crimes-virtuais>. Acesso em: 12 out. 2022.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da *Internet* no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança** [Rio de Janeiro]: *Cos.ufrj.br*, 2006. Disponível em: <https://www.cos.ufrj.br/uploadfile/1430748034.pdf>. Acesso em: 06. out. 2022.

CASTELLS, Manuel. **A Sociedade em Rede. A Era da Informação: Economia, Sociedade e Cultura**. vol. 1. Paz e Terra. São Paulo, 2000.

CORREIO DO POVO. **Crimes virtuais e Pix impulsionam aumento de 179% dos estelionatos**. *R7 In: Correio do Povo*, 2022. Disponível em: <https://www.correiodopovo.com.br/not%C3%ADcias/pol%C3%ADcia/crimes-virtuais-e-pix-impulsionam-aumento-de-179-dos-estelionatos-1.847362>. Acesso em: 20 out. 2022.

CRUZ, Lara Melana Galice. **Aumento de crimes cibernéticos durante a pandemia do covid-19 no Brasil**. *Conteúdo Jurídico*, 2022. Disponível em: <https://conteudojuridico.com.br/consulta/artigo/58466/aumento-de-crimes-cibernticos-durante-a-pandemia-do-covid-19-no-brasil#:~:text=Segundo%20relat%C3%B3rio%20global%20divulgado%20pela,parte%20dos%20brasileiros%20tem%20permanecido>. Acesso em: 19 out. 2022.

DANTAS, Tiago. **Especialista analisa aumento de crimes cibernéticos durante a pandemia**. *ODC*, 2022. Disponível em: <https://olhardacidade.com.br/especialista-analisa-aumento-de-crimes-ciberneticos-durante-pandemia/>. Acesso em: 12 out. 2022.

DIANA, Daniela. **História da *Internet***. *Toda matéria*, 2019. Disponível em: <https://www.todamateria.com.br/historia-da-*internet*/>. Acesso em: 29 set. 2022.

ESCOLA, Equipe Brasil. ***Internet* no Brasil**. *Brasil Escola*, 2021. Disponível em: <https://brasilescola.uol.com.br/informatica/*internet*-no-brasil.htm>. Acesso em: 06. out. 2022.

FERNANDA, Danielle. **Após pandemia, ataques cibernéticos crescem e causam preocupação**. *LGPDBrasil.com.br*, 2022. Disponível em: <https://www.lgpdbrasil.com.br/apos-pandemia-ataques-ciberneticos-crescem-e-causam-preocupacao/>. Acesso em: 19 out. 2022.

FONSECA, Aline. **Brasil sofreu mais de 3,4 bilhões de tentativas de ataques cibernéticos em 2020**. *Gazeta do Povo In: Diário do Litoral*, 2020. Disponível em: <https://www.diariodolitoral.com.br/brasil/brasil-sofreu-mais-de-34-bilhoes-de-tentativas-de-ataques/140286/>. Acesso em: 19 out. 2022.

FMP. **Lei Carolina Dieckmann: Você sabe o que essa Lei Representa?** *FMP*, 2021. Disponível em: <https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/>. Acesso em: 12 out. 2022.

GASTAL, Mariana**. Crimes Cibernéticos E A Pandemia De Covid-19**. *Women in Law Mentoring Brazil*, 2021. Disponível em <https://www.wlm.org.br/crimes-ciberneticos-e-a-pandemia-de-covid-19/>. Acesso em: 19 out. 2022.

GUIZZO, Erico Marui. ***Internet*: o que é, o que oferece, como conectar-se**. São Paulo: Ática, 2002.

IBGE. Pesquisa Nacional por Amostra de Domicílios (PNAD). **Acesso à *Internet* e à televisão e posse de telefone móvel celular para uso pessoal 2021**. *IBGE*, 2022. Disponível em: < https://biblioteca.ibge.gov.br/visualizacao/livros/liv101963_informativo.pdf>. Acesso em: 06 out. 2022.

INELLAS, Gabriel Cesar Zaccaria. **Crimes na *internet***. São Paulo: Juarez de Oliveira, 2004.

INFOPÉDIA – Dicionários porto Editora. **ARPA** na *Infopédia*, 2022 [em linha]: Porto Editora. Disponível em: <https://www.infopedia.pt/$arpa>. Acesso em: 29 set. 2022.

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

KUROSE, Jim.; ROSS, Keith. **Redes de computadores e a *Internet*: uma abordagem topdown**. 6. ed. São Paulo: Pearson Addison Wesley, Brasil, 2013.

LIMA, Leonardo Barcellos. **Crimes Virtuais: Próprios e Impróprios**. *Slaplaw*, 2021. Disponível em: <https://slap.law/os-crimes-virtuais-proprios-e-improprios/?utm_source=rss&utm_medium=rss&utm_campaign=os-crimes-virtuais-proprios-e-improprios>. Acesso em: 13 out. 2022.

MAIA, Daniel. **Criminalidade: A culpa é de quem?** *Daniel Maia Advocacia*, 2020. Disponível em: <https://www.danielmaiaadvocacia.com.br/p-u-b-l-i-c-a-c-o-e-s>. Acesso em: 12 out. 2022.

MORAIS, Carlos Tadeu Queiroz de; LIMA, José Valdeni de; FRANGO, Sérgio R. K. **Conceitos sobre *Internet* e *Web***. Porto Alegre: Editora da UFRGS, 2012.

PRADO, Filipe. **Brasil foi 5º país com mais ataques cibernéticos no ano: relembre os principais**. *ISTOÉ Dinheiro*, 2021. Disponível em: <https://www.istoedinheiro.com.br/brasil-foi-5o-pais-com-mais-ataques-ciberneticos-no-ano-relembre-os-principais/>. Acesso em: 19 out. 2022.

R7. **Brasil é 2º maior alvo mundial de ciberataques, revela estudo**. *Tecnologia e Ciência | Por Agência EFE In: R7*, 2022. Disponível em: <https://noticias.r7.com/tecnologia-e-ciencia/brasil-e-2-maior-alvo-mundial-de-ciberataques-revela-estudo-27062022>. Acesso em: 20 out. 2022.

RAMOS, Rahellen. **O que é o Marco Civil da *Internet*?** *Politize!*, 2021. Disponível em: <https://www.politize.com.br/marco-civil-da-*internet*/>. Acesso em: 12 out. 2022.

REDATOR ROCK CONTENT. **Conheça a história da *Internet*, sua finalidade e qual o cenário atual**. *Rock Content*, 2020. Disponível em: <https://rockcontent.com/br/blog/historia-da-*internet*/#:~:text=Conhe%C3%A7a%20a%20hist%C3%B3ria%20da%20*Internet*,mundo%20nos%20%C3%BAltimos%2040%20anos.>. Acesso em: 29 set. 2022.

ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal**. São Paulo: Memória Jurídica, 2004.

SEGS.COM.BR. **Crimes digitais aumentaram significativamente nos últimos dois anos**. *Revista Cobertura In: SEGS.com.br*, 2022. Disponível em: <https://www.segs.com.br/seguros/353243-crimes-digitais-aumentaram-significativamente-nos-ultimos-dois-anos>. Acesso em: 19 out. 2022.

SIQUEIRA, Marcela Scheuer. OLIVEIRA, Natalia. OLIVEIRA, Bruna Machado. MATTOS, Karoline Reis. **Crimes virtuais e a legislação brasileira**. (Re)Pensando o Direito – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13 (2017). Disponível em: <https://core.ac.uk/download/pdf/229767447.pdf>. Acesso em: 12 out. 2022.

SOPRANA, Paula. **Brasil é o 3º maior alvo de ataques a objetos conectados, diz Symantec**. *Folha de S. Paulo*, 2019. Disponível em: <https://www1.folha.uol.com.br/tec/2019/02/brasil-e-o-3o-maior-alvo-de-ataques-a-objetos-conectados-diz-symantec.shtml>. Acesso em: 19 out. 2022.

TAKAHASHI, Tadao (org.). **Sociedade da informação no Brasil: livro verde**. Brasília: Ministério da Ciência e Tecnologia, 2000.

VALOR ECONÔMICO. **Crimes digitais crescem pós-pandemia e provocam corrida por ciberseguros**. *Dino In: Valor Econômico*, 2022. Disponível em: <https://valor.globo.com/patrocinado/dino/noticia/2022/06/27/crimes-digitais-crescem-pos-pandemia-e-provocam-corrida-por-ciberseguros.ghtml>. Acesso em: 19 out. 2022.