UNIVERSIDADE FEDERAL DO RIO DE JANEIRO - UFRJ
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS - CCJE
FACULDADE NACIONAL DE DIREITO - FND

Matheus Bria da Silva Tavares

OS CRIMES CIBERNÉTICOS E A PANDEMIA DA COVID-19 NO BRASIL: A PROGRESSIVA ADAPTAÇÃO DO CRIME AO DESENVOLVIMENTO DO CIBERESPAÇO

Rio de Janeiro
2022

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO - UFRJ
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS - CCJE
FACULDADE NACIONAL DE DIREITO - FND

Matheus Bria da Silva Tavares

OS CRIMES CIBERNÉTICOS E A PANDEMIA DA COVID-19 NO BRASIL: A PROGRESSIVA ADAPTAÇÃO DO CRIME AO DESENVOLVIMENTO DO CIBERESPAÇO

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob orientação do Professor Dr. Carlos Eduardo Japiassú.

Rio de Janeiro
2022

MATHEUS BRIA DA SILVA TAVARES

OS CRIMES CIBERNÉTICOS E A PANDEMIA DA COVID-19 NO BRASIL: A PROGRESSIVA ADAPTAÇÃO DO CRIME AO DESENVOLVIMENTO DO CIBERESPAÇO

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob orientação do Professor Dr. Carlos Eduardo Japiassú.

Data da Aprovação: 14/07/2022

Banca examinadora:

Prof. Dr. Carlos Eduardo Japiassú

Ana Lúcia Tavares Ferreira

Beatriz Abraão de Oliveira

Rio de Janeiro
2022

AGRADECIMENTOS

Primeiramente, agradeço a Deus por ter sempre me proporcionado a força para seguir em frente, mesmo em meio a dificuldades da vida.

Tão importante quanto, agradeço a minha família, que me apoiou e acreditou em mim, ainda nos tempos de vestibular, sempre confiando no meu potencial e me ensinando tudo que sei, principalmente na figura da minha mãe, Renata, que me levou em seu colo na sua formatura, em 1998 e, desde cedo, me mostrou a importância da vida acadêmica, me acompanhando em cada etapa dessa jornada até aqui. Seu exemplo e carinho é o combustível que me move em todos os campos da minha vida. Sempre a prometi que eu batalharia muito para poder retribuir tudo que ela fez por mim.

Agradeço à minha avó Ângela, que sempre cuidou de mim e me mostrou o significado de nos dedicarmos a quem amamos. Se não fosse ela, não teria acesso a maioria dos livros que tive durante o período da graduação. Nunca imaginei que os parágrafos finais dessa monografia seriam escritos ao lado dela no hospital e que esses agradecimentos precisariam ser revistos um dia após a escrita, devido ao seu falecimento. Essa monografia representa não só uma conquista minha, mas também da minha amada avó, que tanto me ajudou a tornar todos os meus sonhos possíveis.

Agradeço ao meu avô, Antônio Carlos, que pôde acompanhar a minha felicidade em entrar na UFRJ, estando comigo, inclusive, no dia da minha matrícula, mas que não teve a oportunidade de vivenciar o desenvolvimento da minha graduação. Seu exemplo e força continuam me motivando a sempre correr atrás dos meus sonhos.

Agradeço ao meu irmão, Rafael, que nasceu no meu último ano do ensino médio e que cada aniversário dele simboliza meu tempo como estudante de direito da Faculdade Nacional de Direito.

Agradeço ao meu tio Roberto, meu padrasto, Renato e meu padrinho, Rodrigo, por serem homens justos, íntegros e que tanto me ensinaram no decorrer dessa jornada que é a vida.

Agradeço também à minha amada Camila, que sempre se esforça para me ajudar, cuidar de mim e que tanto admiro por sua forma única de me motivar, me fazendo acreditar que todas as minhas metas são possíveis de serem alcançadas. Ela teve uma participação crucial nesse momento da minha vida.

Presto, ainda, minha homenagem aos meus bons amigos Reyson Gabriel e Eduardo Branco, que me acompanharam durante boa parte dessa jornada acadêmica, mostrando que a Nacional de Direito proporciona mais que apenas um canudo de formatura, mas também amizades que serão levadas por toda a vida.

Por fim, e não menos importante, agradeço a cada um dos professores, amigos e todos aqueles que, de algum modo, me motivaram, ensinaram e incentivaram o meu desenvolvimento acadêmico e profissional.

RESUMO

A pandemia da COVID-19 e o isolamento social decorrente da mesma trouxe à tona a dependência humana à tecnologia. Por sua vez, o desenvolvimento da tecnologia, ao longo da história, fez surgir uma nova realidade virtual, denominada ciberespaço. Dessa maneira, se faz necessário entender como as infrações nesse novo espaço digital tiveram seu desenvolvimento, aperfeiçoamentos e as mudanças ocorridas durante o período de isolamento social, vez que a vida humana se pautou, majoritariamente, de forma online. Soma-se a isso a necessidade de entender como o estado brasileiro vem lidando com essa questão, bem como suas respectivas respostas legislativas concernentes ao tema.

Palavras-chaves: Direito penal; Pandemia; Tecnologia; Isolamento social; Ciberespaço; Cibercrimes.

SUMMARY

The COVID-19 pandemic and the resulting social isolation brought to light the human dependence on technology. On its turn, the development of technology, through out the history, gave rise to a new virtual reality, called cyberspace. In this way, it is necessary to understand how the infractions in this new digital space had their development, improvements and the changes that occurred during the period of social isolation, since human life was guided, mostly, online. Added to this is the need to understand how the brazilian state has been dealing with this issue, as well as their respective legislative responses concerning the subject.

Keywords: Criminal law; Pandemic; Technology; Social isolation; Cyberspace; Cybercrimes.

SUMÁRIO

INTRODUÇÃO

Com o passar dos anos e o desenvolvimento da tecnologia, artifícios criminosos foram se tornando cada vez mais sofisticados. A globalização – impulsionando esse desenvolvimento – foi fator importante para tornar as fronteiras mais diluídas e o acesso à informação, bem como a comunicação, cada vez mais facilitado.

Por sua vez, a pandemia global do COVID-19 fez com que o mundo ficasse isolado, demonstrando ainda mais a dependência da sociedade à tecnologia e um maior desenvolvimento da mesma em atividades básicas da vida humana, como a implementação, em larga escala, da modalidade de home office.

Ao longo da história, se tornou perceptível que a tecnologia evoluiu em larga escala. Se antes, computadores e comunicação em nível global eram artifícios de guerra, hoje em dia é impossível imaginar nossas vidas sem a internet. A maioria das pessoas não consegue passar mais de uma hora, sequer, sem acessar seus dispositivos tecnológicos, como os smartphones e computadores.

A pandemia do COVID-19, a partir do momento que fez com que a população mundial precisasse se manter isolada para conter a disseminação do vírus, revelou o quanto a tecnologia é importante, visto que se não houvesse a possibilidade de manutenção de empregos pela modalidade virtual, por exemplo, o impacto na economia certamente poderia ser ainda mais desastroso.

Nessa mesma linha, é perceptível que a atividade criminosa sempre consegue se adaptar ao meio, possuindo artifícios criativos para conseguir se moldar frente às especificidades fáticas em que a sociedade se encontra. Se de um lado ocorreu o avanço da tecnologia e a consequente crescente dependência da vida humana a mesma, também houve o fortalecimento de um fenômeno criminal característico do desenvolvimento tecnológico humano: os crimes cibernéticos.

Por conta disso, é extremamente importante tentar entender em que consiste os crimes cibernéticos, suas principais delimitações e como foi o seu

desenvolvimento no Brasil. Buscando, ainda, verificar como os criminosos se reinventaram para se adequarem ao ciberespaço e, mais especificamente, continuarem delinquindo frente ao isolamento social decorrente da pandemia no país.

CAPÍTULO 1: CIBERCRIMES – CONSIDERAÇÕES INICIAIS

O presente capítulo busca desenvolver o conceito clássico de crime, tentando compreender a definição da cibercriminalidade, analisando, em um parâmetro histórico, como se deu a relação entre o desenvolvimento da tecnologia e a inovação da conduta criminosa.

Após esse cenário inicial, será também analisada as transições de tipos penais já existentes à modalidade virtual, bem como as categorias existentes de cibercrime.

1.1 – CONCEITO DE CRIME

Antes de procedermos com a conceituação dos crimes cibernéticos, é necessário definir o que é o crime, adotando, para isso, a visão doutrinária desta definição, vez que o Código Penal é omisso em tratar acerca da conceituação do referido instituto.

Nesse sentido, o crime é definido, majoritariamente, como fato típico, antijurídico e culpável. Em uma corrente minoritária, podemos citar autores como Basileu Garcia e Mezger, que sustentam que a punibilidade integraria o conceito de crime. Rogério Greco, por sua vez, define o crime, sob uma visão analítica, como fato típico, ilícito e culpável somente.[1]

Para o referido autor, o fato típico se dividiria nos seguintes elementos: i) conduta dolosa ou culposa; ii) comissiva ou omissiva; iii) resultado; iv) nexo de causalidade entre conduta e o resultado e tipicidade[2].

A ilicitude é definida da seguinte forma pelo autor em comento:

> Ilicitude, ou antijuridicidade, é a relação de antagonismo, de contrariedade entre a conduta do agente e o ordenamento jurídico. Quando nos referimos ao ordenamento jurídico de forma ampla, estamos querendo dizer que a ilicitude não se resume à matéria penal, mas sim que pode ter natureza civil, administrativa, tributária etc. Se a conduta típica do agente colidir com o ordenamento jurídico penal, diremos ser ela penalmente ilícita.[3]

[1] GRECO, Rogério. Curso de Direito Penal – Parte Geral - Vol 1 - 17ª Ed. 2015, p 196
[2] GRECO, Rogério. Curso de Direito Penal – Parte Geral - Vol 1 - 17ª Ed. 2015, p 197
[3] GRECO, Rogério. Curso de Direito Penal – Parte Geral - Vol 1 - 17ª Ed. 2015, p 199

Consoante à culpabilidade, GRECO define que esta é “o juízo de reprovação pessoal que se realiza sobre a conduta típica e ilícita praticada pelo agente”.

BITTENCOURT, por sua vez, adota os elementos estruturais do conceito analítico de crime: ação típica, antijurídica e culpável, rechaçando a visão, que já foi majoritária na doutrina brasileira, do crime como “ação típica e antijurídica”, que admitia a culpabilidade somente como mero pressuposto da pena.

Desta forma, temos que a visão doutrinária mais aceita no país é de que crime é o fato típico, ilícito e culpável. Por mais que seja esta a teoria mais adotada, ela não é uníssona, vez que existem muitas outras conceituações, abraçadas por diversos autores, com definições distintas. Como este não é o objetivo do presente ensaio, ignoraremos a discussão doutrinária envolvendo o tema e partiremos ao cerne da questão aqui desenvolvida: a definição de crimes cibernéticos.

1.2 – CRIMES CIBERNÉTICOS

Estabelecido o panorama geral da visão doutrina acerca do que é o crime, buscaremos agora entender no que consiste os crimes cibernéticos e como o tema vem sendo tratado sob uma perspectiva doutrinária.

Irineu Francisco Barreto Júnior define os crimes cibernéticos da seguinte forma:

> Com o advento da Internet e da Sociedade da Informação, surgiu uma nova modalidade de crimes cometidos no espaço virtual da rede através de e-mails (correio eletrônico), web sites (sítios pessoais, institucionais ou apócrifo) ou mesmo ocorridos em comunidades de relacionamento na Internet, entre as quais a mais conhecida é o Orkut, propriedade do provedor de conteúdo americano Google. As transações comerciais eletrônicas, envolvendo compras que exigem a identificação do número de cartão de credito, as transações bancárias, que solicitam registro de dados referentes as contas correntes bancárias, além do uso de senhas e demais mecanismos de segurança, assim como a profusão de novas modalidades relacionais mantidas em sociedade, através da Internet, propiciaram o surgimento de novas modalidades de crimes na web, batizados de crimes virtuais.[4]

[4] BARRETO Júnior, Irineu. Atualidade do Conceito de Sociedade da Informação para a Pesquisa Jurídica. In: PAESANI, Liliana Minardi (Coord.). O direito na sociedade da informação. São Paulo: Atlas, 2007, p. 71.

Moisés de Oliveira Cassanti, por sua vez, adota a seguinte definição:

> Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido cibercrime. Outros termos que se referem a atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital.[5]

Nessa mesma linha, Miguel Coli define o instituto como:

> (...) aquele no qual um ou mais computador (es), equipamentos telemáticos ou dispositivos eletrônicos, interligados por meio de uma rede de comunicação, são utilizados, por um ou mais indivíduos, no cometimento de uma, ou mais conduta(s) criminalizada(s), ou são alvo(s) desta(s). O homem interagindo com uma máquina – retroalimentando-a com informações por meio de mensagens – através de uma rede de computadores (cibernética) interligados (ciberespaço), agindo conforme uma conduta previamente criminalizada (Crime informático) estereotiparia um modelo de cibercrime. [6]

Além disso, citamos também a definição apresentada por Ramalho Terceiro:

> [...] os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas (TERCEIRO, 2006).[7]

Augusto Rossini também leciona que:

> [...] o conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o 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 a confidencialidade (ROSSINI, 2004). [8]

É perceptível, então, que há, na doutrina nacional, o consenso de reconhecimento das condutas ilícitas praticadas, através da internet, envolvendo a utilização de computadores - em uma relação entre a tecnologia e a conduta criminosa humana - como cibercrime.

Não almejando percorrer algumas divergências doutrinárias de nomenclatura acerca desse respectivo conceito criminal, vez que já foi cumprido

---

[5] CASSANTI, Moisés de Oliveira. Crimes Virtuais: Vítimas Reais - Rio de Janeiro: Brasport, 2014, p. 3.

[6] COLLI, Maciel. Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos. Juruá Editora, 2010. P. 44.

[7] RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. Crimes virtuais. 2005. Disponível em:<http://www.advogadocriminalista.com.br>. Acesso em: 10 fev.

8 ROSSINI, Augusto Eduardo de Souza. Informática, telemática e direito penal. São Paulo: Memória Jurídica, 2004.

o objetivo de estabelecer parâmetro introdutório acerca da questão, passemos à análise de como o desenvolvimento da tecnologia contribuiu para a configuração do cibercrime.

1.3 – A GLOBALIZAÇÃO E O DESENVOLVIMENTO DA INTERNET

Frente às definições de cibercrime apresentadas na seção anterior, é perceptível que as recentes tecnologias possuem uma natureza dual, a depender da destinação que lhes é dado. Isto é, se de um lado temos um aspecto positivo de aproximação das pessoas, novas possibilidades de negócios e empregos, disseminação mais veloz da informação, dentre outros aspectos que serão melhor explorados em pontos posteriores do trabalho, há de ser pontuado também um relevante aspecto negativo: essas inovações colaboraram significativamente com a facilidade da prática de delitos à distância.

Busquemos agora, então, entender como se deu esse desenvolvimento tecnológico e a sua relação com o desenvolvimento das empreitadas criminosas na modalidade virtual.

Em primeiro lugar, é importante destacar o relevante papel que a globalização, ao estreitar os países do mundo, tornando fronteiras físicas cada vez menos importantes, teve com relação a isso.

Nesse sentido, de modo a explicar melhor a relação de tal fenômeno com o objetivo desta dissertação, é válido trazer à luz o entendimento doutrinário do sociólogo Stuart Hall a respeito da temática:

> A globalização se refere àqueles processos, atuantes numa escala global, que atravessam fronteiras nacionais, integrando e conectando comunidades e organizações em novas combinações de espaço-tempo, tornando o mundo, em realidade e em experiência, mais interconectado.[9]

Uma das principais heranças desse mundo conectado foi a fluidez das informações e a facilidade de comunicação.

Pensar nessas questões facilmente nos remete à internet, que foi um grande impulso para tornar o mundo cada vez interligado e interrelacionado. Se

[9] Hall, Stuart. 2011. A identidade cultural na pós-modernidade. Rio de Janeiro. DP&A.

pensarmos nas redes sociais e em aplicativos de mensagens eletrônicas, fica perceptível o quanto essa invenção contribuiu para que as fronteiras entre cidades, estados, países e continentes se tornasse cada vez menos significativa. O que pouco sabemos, no entanto, é que o início da internet se deu muito antes do processo de globalização, tendo, inclusive, forte relação com pesquisas militares.

A ideia por trás da internet, tal como conhecemos hoje, surgiu no início dos anos 60, durante o processo da Guerra Fria, relacionada aos esforços norte-americanos em pesquisas militares. Essa rede, por sua vez, recebeu o nome de ARPANET.

A concretização dessa ideia ocorreu somente no final dos anos 60, quando o Departamento de Defesa dos Estados Unidos concedeu a liderança a respeito das pesquisas de ciências e tecnologias das forças armadas à ARPA (*Advanced Research Projects Agency*).

O objetivo da Arpa é descrito, assertivamente, nas palavras de Costa Almeida (1998, p. 52-53):

> A Internet foi criada nos anos 60 nos EUA, como um projeto militar que buscava estabelecer um sistema de informações descentralizado e independente de Washington, para que a comunicação entre os cientistas e engenheiros militares resistisse a um eventual ataque à capital americana durante a Guerra Fria.[10]

Após esse período de guerra, a Universidade da Califórnia herdou um computador da força militar, o qual passou a permitir que essa universidade se interligasse, via *backbone* - trecho de maior capacidade da rede, que tem como objetivo a conexão de diversas redes locais – com outras universidades, criando assim uma associação denominada *Network Working Group* – NWG. Posteriormente, eles também se interligaram aos computadores das agências governamentais e militares norte-americanas, do Reino Unido e da Noruega. O que possibilitou, por sua vez, todo esse desenvolvimento foi justamente a

[10] COSTA ALMEIDA, André Augusto Lins da. A Internet e o Direito. Revista Consulex, São Paulo, ano II, nº 24, dez. 1988.

principal atividade desenvolvida na ARPANET: o correio eletrônico (ROSSINI, 2004, p. 26).[11]

Essa inovação rapidamente fez com que surgisse o interesse em ligar outras redes paralelas de comunicação à ARPANET. Para que isso ocorresse, foi preciso o desenvolvimento de protocolos de comunicação para interconexão de diversas redes.

Silva e Remoaldo descreve esse processo da seguinte forma:

> Rapidamente outros locais começaram a ver as vantagens das comunicações eletrônicas. Muito desses locais começaram então a encontrar formas de ligar as suas redes privadas à ARPANET. Isso levou a necessidade de ligar computadores que eram fundamentalmente diferentes entre si. Nos anos 70, a ARPA desenvolveu uma série de regras chamadas protocolos, que ajudaram a que esta comunicação fosse estabelecida.[12]

Pouco mais tarde, no início da década de 80, a ARPANET foi dividida em duas redes: i) *milnet*, destinada ao uso militar; ii) *arpanet*, destinada ao uso civil. De todo modo, elas ainda eram conectadas, permitindo troca de informação entre os usuários (ROSSINI, 2004, p. 27).

Como resultado disso, surgiu a CSNET (Computer Science Network), vez que havia discordância quanto ao domínio dos militares sobre essas redes.

Nos anos 90 surge, então, a nomenclatura tal conhecemos hoje, a partir da retirada do *backbone* ARPANET pelo Departamento de Defesa Norte-Americano, sendo substituído pelo *backbone* NSFNET, se eternizando com a nomenclatura internet.

Quanto ao Brasil, a internet deu seus primeiros passos no país em 1988, através da Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp) e Laboratório Nacional de Computação Científica (LNCC) no Rio de Janeiro. No entanto, foi só a partir do ano de 1991 que seu uso foi estendido ao público geral.

Estabelecido essa construção histórica, ideal para entendermos as premissas formadoras do ciberespaço, tal como conhecemos hoje, passemos

[11] ROSSINI, Augusto Eduardo de Souza. Informática, Telemática e Direito Penal. São Paulo: Memória Jurídica, 2004.
[12] SILVA, Libório; REMOALDO, Pedro. Introdução à Internet. 2. ed. São Paulo: Editorial Presença, 1995 p. 17.

agora à análise acerca dos impactos ocasionados pela disseminação da internet pelo mundo.

Canonga e Júnior analisa esse cenário da seguinte forma:

> É marcante a presença da alta tecnologia atrelada a constantes inovações com o domínio das empresas de países desenvolvidos. Esta convergência tecnológica vem nos bombardeando com novidades inimagináveis, como, por exemplo, o acesso à internet pelo celular, permitindo o envio de e-mails, a realização de transações financeiras, além de múltiplas aplicações, serviços e negócios que as TICs vêm proporcionando, e que são crescentes mundialmente.[13]

Dessa forma, é perceptível que, aos poucos, a presença da tecnologia foi se tornando cada vez mais relacionada à ideia de desenvolvimento, se infiltrando no cotidiano humano e se tornando parte essencial do mundo tal conhecemos hoje: temos smartphones, tablets, notebooks e diversos outros dispositivos que permitem as mais variadas operações, tais como: envio de informações, realização de transações financeiras e uma rápida e, muitas vezes, eterna, divulgação de opinião.

Não é de se espantar que esse inovador cenário começasse a atrair também criminosos, aproveitando-se dessa nova forma de viver o mundo para delinquir.

Nesse sentido, leciona Patrícia Peck Pinheiro:

> A possibilidade de visibilidade do mundo atual traz também riscos inerentes à acessibilidade, tais como segurança da informação, concorrência desleal, plágio, sabotagem por hacker, entre outros. Assim na mesma velocidade da evolução da rede, em virtude do relativo anonimato proporcionado pela internet, crescem os crimes, as reclamações devido a infrações ao Código de Defesa do Consumidor, as infrações à propriedade intelectual, marcas e patentes, entre outras.[14]

Dessa forma, fica perceptível que os referidos avanços, além das facilidades comentadas, também trouxeram significativos riscos aos usuários do ciberespaço, principalmente no tocante tanto à conversão de tipos penais já existentes à modalidade virtual, quanto surgimento de novas figuras típicas

[13] CANONGIA, Claudia; JUNIOR, Raphael Mandarino. Segurança cibernética: o desafio da nova Sociedade da Informação. Disponível em: <http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/349/342>. Acesso em: 20 fev. 2022.

[14] PINHEIRO, Patricia Peck. Direito Digital. 4ed. Ver., atual. eampl. São Paulo: Saraiva, 2011 p. 76.

relacionadas com essa nova realidade da vida humana – que é o ciberespaço - cujo maior aprofundamento será explorado na seção seguinte.

1.4 – O CIBERESPAÇO

Todo esse processo desenvolvimentista resultou em uma espécie de realidade paralela, que é o ciberespaço, podendo ser interpretado, basicamente, como um ambiente virtual que conecta dispositivos ao redor do mundo, incluindo-se aqui não somente os *personal computers* – PCs – mas também smartphones, tablets e outros dispositivos com funções semelhantes.

Luciana Boiteux define o ciberespaço da seguinte forma:

> O conceito de ciberespaço (cyberspace), ou espaço virtual alcançado pela rede mundial de computadores, a Internet, que reduziu as distâncias e aproximou as pessoas, foi concebido como uma nova dimensão espacial que transcende fronteiras, e permite a todos aqueles conectados à rede imediato contato com qualquer lugar do mundo em segundos, independentemente de fronteiras ou meios de transporte. [15]

É oportuno registrar que, paralelamente ao surgimento desse novo espaço virtual, foram surgindo também novas comunidades virtuais, gerando novas espécies de relacionamentos entre as pessoas, conforme bem definido por Corrêa:

> De qualquer modo, o ciberespaço potencializa o surgimento de comunidades virtuais e de agregações eletrônicas em geral que estão delineadas em torno de interesses comuns, de traços de identificação, pois ele é capaz de aproximar, de conectar indivíduos que talvez nunca tivessem oportunidade de se encontrar pessoalmente. Ambiente que ignora definitivamente a noção de tempo e espaço com barreiras.[16]

A autora também disserta que:

> A revolução tecnológica concentrada nas Tecnologias da Informação e da Comunicação (TICs), que possibilita a conexão mundial via rede de computadores, promove alterações significativas na base material da sociedade, ao estabelecer uma interdependência global entre os países e modificar as relações Estado-Nação e sociedade. O uso crescente de redes como a Internet resultou na criação de uma organização social, a sociedade em rede, que permite a formação de

[15] BOITEUX, Luciana: Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual, RBCCRIM n. 47, 2004, p. 147.
[16] CORRÊA, Cybthia Harumy Watanabe. Comunidades Virtuais gerando identidades na sociedade em rede. Universiabrasil.net, 2004.

> comunidades virtuais, grupos constituídos pela identificação de interesses comuns.[17]

Torna-se perceptível, portanto, que a internet não só possibilitou o surgimento de um novo espaço, como também permitiu o delineamento de variedades de relações sociais. Dessa forma, podemos ter indivíduos que se associam – inseridos na realidade do ciberespaço – para realizarem grupos de estudos, fazerem vídeos de danças na internet, jogarem jogos virtuais, bem como atividades mais destrutivas, como o aproveitamento desse novo espaço criado e novas relações sociais desenvolvidas, como um impulso para a criminalidade.

1.5 – CRIMINALIDADE E AMEAÇAS NO CIBERESPAÇO

Essas inovações na realidade e na forma de viver o mundo ocasionaram um fenômeno criminal interessante: alguns crimes, já previamente existentes e com consumação característica da realidade fática, tiveram desdobramentos, por meio da internet e dessa interrelação global, conforme foi trabalhado nos tópicos antecedentes, que tiveram importantes reflexos no ciberespaço.

Dessa forma, da mesma forma que a criminalidade é um fenômeno comum na realidade física, a cibercriminalidade aos poucos também se sedimentou da mesma forma com relação a essa nova realidade virtual.

Se de um lado a tecnologia trouxe essa possibilidade de interconexões, do outro também trouxe consigo uma grave consequência aos países conectados: a necessidade de lidar com essas novas facetas da criminalidade.

No tocante a essas empreitadas criminosas no ciberespaço, podemos citar como exemplos concretos: fraudes de instituições financeiras, desvio e lavagem de dinheiro, espionagem, violações de direitos de propriedade industrial, pornografia infantil, tráfico de bens e mercadorias ilícitas, crimes contra a hora, intolerância racial, invasão de dispositivos eletrônicos, por meio de ações de *hackers*, dentre outras variedades de ações do gênero.

[17] CORRÊA, Cybthia Harumy Watanabe. Comunidades Virtuais gerando identidades na sociedade em rede. Universiabrasil.net, 2004.

Além disso, as redes sociais, consequência direta dessas novas formas de socialização e formação de comunidades virtuais, também se mostrou um ambiente propício ao cometimento de crimes contra a honra.

Nesse sentido, Kunrath disserta que:

> Os crimes contra a honra, nas modalidades de calúnia, injúria e difamação, ocorrem com bastante frequência nas redes sociais e se alastram com extrema facilidade, pela ágil disseminação das ofensas postadas na rede, potencializando as consequências nefastas para as vítimas, ante as características da circulação dos conteúdos veiculados pela internet. Outros ilícitos graves, como a invasão de privacidade, ameaças, assédio sexual, assédio moral (*Bullying*), têm permeado constantemente os diversos sítios, correios eletrônicos e redes sociais. A falsificação de perfil é o ilícito mais comum em vários tipos de mídias, como blogs e sites de relacionamento.[18]

Para além disso, o ciberespaço, devido à sensação de aparente anonimidade também contribuiu para que o ser humano mostrasse seu lado mais cruel e perverso. Dessa forma, crimes envolvendo pornografia infantil e outras violações aos direitos de crianças e adolescentes também se tornaram, lamentavelmente, uma forte característica dessa modalidade de criminalidade. Nesse sentido, com relação à exploração sexual infantil, a mesma autora expõe que:

> Um dos mais terríveis crimes que envolvem a exploração sexual de crianças e adolescentes, a pedofilia virtual consiste em produzir, publicar, vender, adquirir e armazenar pornografia infantil pela rede mundial de computadores, por meio das páginas da web, e-mail, newsgroups, salas de bate-papo (chat) ou qualquer outra forma. Compreende, ainda, o uso da internet com a finalidade de aliciar crianças ou adolescentes para atividades sexuais ou para exposição pornográfica.

Além disso, cabe também destacar o crime de estupro, que com a alteração decorrente da Lei 12.015/09, ao alterar o antigo dispositivo, que consistia em “constranger mulher à conjunção carnal, mediante violência ou grave ameaça” (BRASIL, 1940) para “constranger alguém, mediante violência ou grave a ameaça, a ter conjunção carnal ou a praticar ou permitir que com ele se pratique outro ato libidinoso” (BRASIL, 2015), ampliou o escopo de proteção do tipo penal, permitindo também, segundo entendimento doutrinário e

[18] KUNRATH, Josefa Cristina Tomaz Martins. A expansão da criminalidade no ciberespaço: desafios de uma política criminal de prevenção ao cibercrime. 158 f. il. 2014. Dissertação (Mestrado) — Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2014.

jurisprudencial acerca do tema, que ele possa ser também praticado no meio virtual.

É perceptível, então, que não é necessário a existência de contato física entre o criminoso e a vítima, bastante a presença da grave ameaça do ofensor em relação à ofendida para que o crime possa se consumar. Uma das formas comuns que ele se dá é a ameaça de exposição de fotos e vídeos íntimos, caso a vítima não efetue determinado ato libidinoso, muitas vezes por meio de webcams. Dessa forma, a ofendida se vê obrigada, pelo medo da retaliação social que pode vir a sofrer, a realizar o ato libidinoso em si mesma, de modo a contribuir para o desejo libidinoso do criminoso.

Criminosos também costumam disseminar e propagar vírus de computador. Segundo a Cartilha de Segurança para a Internet, importante documento basilar do estudo da cibercriminalidade, o vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu equipamento seja infectado é preciso que um programa já infectado seja executado, tendo como principais finalidades: acesso às informações pessoais não autorizadas do usuário, senhas, abrir janelas indesejadas, além de afetar o desempenho do dispositivo. (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012). [19]

Outro *malware* comum, mas com algumas distinções bem características referentes ao vírus, é o *worm*:

> Worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores. Worms são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo

[19] COMITÊ GESTOR DA INTERNET NO BRASIL. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de segurança para internet. 2. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012 p. 24.

> que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores.[20]

Válido destacar, ainda, as ações de *Phishing*, técnica de engenharia social consistente, muitas vezes, num golpe de envio de mensagens eletrônicos, no qual os criminosos, fazendo-se passar por instituições bancárias, enviam comunicação semelhante ao padrão destas, de modo a obter senhas e informações pessoais das vítimas. (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012).[21]

Dessa forma, fica claro que as invenções humanas, por mais que tragam comodidades e facilidades para a vida cotidiana, também impulsionam, ainda que indiretamente, as inovações de condutas delitivas. Nesse sentido, será abordado a seguir quais os marcos normativos vigentes no Brasil relacionados à temática, de modo a entender como a legislação penal brasileira veio se adequando a essa nova realidade que nos encontramos.

[20] COMITÊ GESTOR DA INTERNET NO BRASIL. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de segurança para internet. 2. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012 p. 41.

[21] COMITÊ GESTOR DA INTERNET NO BRASIL. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de segurança para internet. 2. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012 p. 25.

CAPÍTULO 2: DESDOBRAMENTOS NORMATIVOS SOBRE CIBERCRIMINALIDADE NO BRASIL

Conforme demonstrado nos tópicos anteriores, o desenvolvimento tecnológico e a popularização da internet fizeram surgir diversas problemáticas relacionadas à criminalidade virtual.

Fato é que tal fenômeno fez com que fossem necessárias respostas estatais para lidar com isso. Ao redor do mundo, foram vislumbradas algumas iniciativas, dentre as quais é válido destacarmos a Convenção de Budapeste ou Convenção sobre o Cibercrime, criada em 2011, na Hungria. Pioneiro e importante tratado internacional sobre o tema, englobando mais de 20 países, que influenciou, certamente, o desenvolvimento de diversas legislações sobre a temática, nas mais diversas jurisdições ao redor do mundo, incluindo a brasileira, que será o foco de análise do presente ensaio.

Sendo assim, analisaremos os principais diplomas normativos brasileiros que abordam a temática, buscando entender como o Estado buscou lidar com a crescente realidade da criminalidade virtual.

2.1 – LEI AZEREDO (LEI Nº 12.735/2012)

A legislação em comento ficou conhecida por tal nomenclatura devido ao seu relator, o então senador mineiro, Eduardo Azeredo.

Ivan Paganotti ensina o seguinte sobre a temática[22]:

> A proposta original pretendia incluir no Código Penal brasileiro cibercrimes como a disseminação de vírus, o estelionato eletrônico (como o roubo de senhas), a divulgação inadvertida de dados pessoais e a criminalização não só da produção e divulgação de conteúdos que promovem a pedofilia, mas também o armazenamento desses materiais. O projeto também criava regras para identificar e armazenar dados de usuários para potencialmente identificar melhor os suspeitos de incorrer nesses crimes, obrigando provedores a preservar esses registros por 3 anos e ampliando suas obrigações de fiscalização e denúncia de crimes.

[22] PAGANOTTI, Ivan. Eptic online: revista eletrônica internacional de economia política da informação, da comunicação e da cultura, ISSN-e 1518-2487, Vol. 16, Nº. 2, 2014, págs. 139-156

A proposta de lei original (PL84/99) tinha uma forte carga de censura, motivo pelo qual chegou a ser apelidada, à época, de “AI-5 Digital”, em alusão ao famoso ato institucional instituído durante a ditadura militar brasileira, que fortalecia ainda mais o Executivo em detrimento dos outros poderes e contribuiu para que o regime militar se tornasse ainda mais rígido.

Em decorrência disso, houve uma significativa movimentação popular contrária à lei, motivo que ocasionou a mudança em diversos de seus artigos. Ainda assim, teve importante repercussão no regramento penal brasileiro, promovendo algumas alterações, que merecem ser pontuadas.

Foi incluída, no artigo 356 do Código Penal Militar, a expressão “dado eletrônico”. Dessa forma, o leque de proteção da referida norma jurídica, que dispõe sobre o crime próprio militar de traição, passou a incluir também, de forma expressa, informações de bases de dados militares. Dessa forma, se tornou claro que aquele militar que divulgasse dados de bases militares, também sofreria a punição correspondente do artigo ao crime de traição[23].

No tocante ao Código Penal, foi incluído, no artigo 298, o parágrafo único, que traz a equiparação dos cartões de crédito e débito como documentos particulares. Antes disso, a punição de indivíduos que praticavam fraudes com esses instrumentos era muito difícil de ocorrer, vez que a defesa costumava alegar a atipicidade da conduta. Essa alteração foi muito importante porque, conforme vimos, a interconexão global se tornou rapidamente uma realidade, assim como o desenvolvimento de formas de comércio online, sendo o pagamento com cartões de crédito a forma mais utilizada nessas plataformas.

Além disso, a Lei Azeredo também trouxe a seguinte previsão, em seu artigo quarto:

> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.[24]

[23] DE MATTOS, Alexandre Magalhães. Crimes na Internet (Kindle Locations 2028-2035). Alexandre Mattos. Kindle Edition.

[24] Lei n° 12.735. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em 03 de junho de 2022.

Dessa forma, as polícias judiciárias dos estados precisaram começar a estruturar setores e delegacias especializadas no combate aos cibercrimes. No entanto, isso ficou longe de ser uma realidade uníssona no país, tendo muitos estados que não possuem, ainda, um setor especializado para combater esses referidos delitos[25].

2.2 – LEI CAROLINA DIECKMANN (LEI Nº 12.737/2012)

A lei recebeu essa nomenclatura devido ao episódio ocorrido com a atriz Carolina Dieckmann, em 2011, que teve seu computador invadido por hackers que roubaram fotos íntimas suas e exigiram pagamento para não publicarem as fotos na internet, o que gerou uma grande repercussão midiática, trazendo à tona importantes discussões sobre privacidade na era digital.

O caso se tornou bastante emblemático para o estudo da cibercriminalidade devido ao fato de que o Brasil não tinha, à época, uma lei específica para crimes de informática, tendo sido os envolvidos indiciados por furto, extorsão qualificada e difamação.

Dentre as suas principais alterações, é válido destacarmos as alterações promovidas no artigo 154, acrescentando o 154-A e 154-B[26]:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
>
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado

[25] SAFERNET BRASIL. Delegacias cibercrimes. Disponível em: <http://www.safernet.org.br/site/prevencao/orientacao/delegacias>. Acessado em 03 de junho de 2022.

[26] Decreto Lei nº 2.848. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 03 de junho de 2022.

> do dispositivo invadido: Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
>
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

A inclusão desses artigos na normativa penal brasileira possibilitou que os indivíduos que agora cometessem crimes relacionados à invasão de dispositivos informáticos pudessem ter um dispositivo específico para enquadrar essas condutas delitivas. Válido destacar, ainda, que o caput do art. 154-A deixa claro que somente são enquadradas as formas dolosas de conduta, visto que exige uma finalidade do agente, não admitindo-se possibilidade de responsabilidade culposa.

Nesse sentido, Patrícia Peck Pinheiro afirma que[27]:

> Ainda, receberá as mesmas penas da invasão aquele que instala uma vulnerabilidade em um sistema de informação para obter vantagem indevida, por exemplo, um backdoor ou uma configuração para que algumas portas de comunicação à internet fiquem sempre abertas. O usuário de gadgets e dispositivos informáticos comuns estão protegidos contra hackers e pessoas mal intencionadas que abusam de confiança ou buscam intencionalmente devassar dispositivo para se apropriar de dados do computador ou prejudicar o seu proprietário, com a exclusão ou alteração de dados, para que fiquem imprestáveis, ou ainda, informações íntimas e privadas, como fotos, documentos e vídeos. As empresas possuem maior proteção jurídica contra a espionagem digital, pois a obtenção de segredos comerciais e ou informações sigilosas definidas por lei agora também se enquadram na lei.

Uma grande discussão que pairou sobre esses artigos, se deu justamente pelas penas impostas, consideradas muito brandas e que ainda manterão, de

[27] PINHEIRO, Patrícia Peck; HAIKAL, Victor Auilo. A nova lei de crimes digitais. 2013. Disponível em: <www.pppadvogados.com.br/Publicacoes.aspx?v=1&nid=1432>. Acesso em 05/06/2022.

certa forma, a sensação de impunidade daqueles que realizam essas condutas. Dessa forma, será mais difícil inibir as atividades dos hackers.

Além disso, é válido também ressaltar o impacto que teve no artigo 266, do Código Penal, que diz respeito à interferência em redes de tráfego na internet como uma forma de bloquear sinais telefônicos ou de rádio. Nesse sentido, Rogério Tadeu Romano ensina que[28]:

> Duas são as modalidades contidas no artigo 266, referentes ao serviço telegráfico, radioelétrico ou telefônico, em enumeração taxativa. A primeira modalidade é interromper, paralisar, fazer cessar, perturbar. A segunda, envolve serviço interrompido e a conduta do agente é impedir, dificultar. Assim a norma do artigo 266 do Código Penal visa ao serviço de forma que se o comportamento é interromper ou perturbar o aparelho telegráfico ou telefônico determinado, ou a comunicação de duas pessoas, não haverá enquadramento no artigo 266. Consuma-se o crime com a interrupção ou perturbação do serviço ou quando o agente logra impedir ou dificultar o seu restabelecimento.

Como última alteração feita, válido também destacar aquela feita no artigo 298, que prevê o crime de falsificação de documento particular, incorporando, por meio do parágrafo 4º, o crime de falsificação de cartão de crédito, ou cartão de débito, com pena de reclusão de 1 a 5 anos e multa.

Doutrinariamente, há certa discussão a respeito do crime envolvendo a falsificação de cartões, visto que ele abrange, simultaneamente, diversos crimes previstos na legislação brasileira. A respeito disso, Murilo Cezar Antonini Pereira discorre sobre quais são esses tipos penais:

> Por óbvio que o problema decorre principalmente do bem jurídico tutelado (patrimônio) e do elemento “fraude”, comum nos indigitados tipos penais. Uma coisa é certa, os referidos crimes não podem ser confundidos. Debruçando sobre a nossa legislação penal, pode-se notar que o furto mediante fraude está previsto no inciso II do §2º do art.155 do Código Penal. O furtador engana a vítima, buscando diminuir sua vigilância sobre a coisa, a qual é subtraída. Percebam que o agente nada mais faz do que aplicar “golpe patrimonial imperceptível” que recai sobre coisa alheia móvel da vítima. Analisando ainda o nosso Código Penal, o estelionato pode ser observado no art.171, caput, do referido estatuto penal repressivo. O estelionatário também engana a vítima, porém no sentido de mantê-la ou induzi-la em erro, com o fito de obter vantagem patrimonial ilícita.

Essa equiparação, trazida pela lei em referência, foi essencial para essa dinâmica da nova realidade do ciberespaço ficar ainda mais caracterizada,

[28] ROMANO, Rogério Tadeus. 2014. Furto de Fios Telefônicos. Disponível em: https://jus.com.br/artigos/32600/furto-de-fios-telefonicos. Acesso em 04 de junho de 2022.

sendo um claro exemplo de adaptação da normal penal à realidade trazida pela crescente ampliação desse espaço virtual.

2.3 – MARCO CIVIL DA INTERNET (Lei Nº 12.965)

Este é, sem dúvidas, um dos mais importantes e significativos instrumentos normativos a respeito da temática do presente trabalho.

Sua confecção contou com a participação de diversos setores da sociedade, tendo sido debatido de forma bem abrangente pelos mais diversos grupos sociais, valendo destacar: empresas, organizações da sociedade civil, ativistas e comunidade técnica.[29]

A Lei 12.965 foi aprovada em abril de 2014 pela presidente da República Dilma Rousseff e, com isso, trouxe ao ordenamento jurídico importantes direitos, deveres e garantias para todos aqueles que utilizam a internet no Brasil.

O texto final contou com 32 artigos, dentre os quais é válido nos debruçarmos em uma análise um pouco mais profunda de algum deles, buscando entender os impactos que teve no ordenamento jurídico brasileiro.

Por ser um diploma legal com uma linguagem bastante técnica, o artigo 5º é de suma importância, vez que traz a definição de alguns termos utilizados pelo presente instrumento normativo[30]:

> Art. 5º Para os efeitos desta Lei, considera-se: I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes; II - terminal: o computador ou qualquer dispositivo que se conecte à internet; III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais; IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País; V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP; VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP

[29] LEMOS, Ronaldo; SOUZA, Carlos Affonso. Marco civil da internet: construção e aplicação, Juiz de Fora; Editora Associada, 2016, p. 13.

[30] Lei n˚ 12.965 de 2014. <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acessado em 06/06/2022.

> utilizado pelo terminal para o envio e recebimento de pacotes de dados; VII aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Sobre o Marco Civil da Internet, Eduardo Tomasevicius Filho discorre que[31]:

> Pela leitura do texto convertido na Lei n.12.965/14, observa-se a preocupação de afastarem-se críticas de que se poderia restaurar a censura no país. Para isso, no art.2º, caput, afirmou-se que a disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, e pelo art.19 declara-se que "com o intuito de assegurar a liberdade de expressão e impedir a censura [...]", vez que tais referências não existiam no projeto primitivo. Assim, repetiu-se o que consta no art.3º, I, quando prevê que um dos princípios do uso da internet no Brasil é a "garantia da liberdade de expressão, comunicação e manifestação do pensamento, nos termos da Constituição Federal".

Dessa forma, percebe-se que parte da preocupação da época era que o Marco Civil da Internet, assim como a primeira versão da Lei Azeredo, conforme previamente mencionado, pudesse consistir em um documento de censura aos atos digitais. Justamente por conta disso, o próprio diploma legal tratou de, logo em seus artigos iniciais, afirmar o fundamento de respeito à liberdade de expressão e impedir a censura.

Soma-se a isso as palavras de Tomasevicius Filho acerca da proteção conferida pela referida lei ao direito de privacidade:

> Isso está previsto nos incisos I, II, III, VII e VIII do art.7º, ao elencarem-se como direitos dos usuários de internet a inviolabilidade da intimidade e da vida privada, a preservação do sigilo das comunicações privadas pela rede, transmitidas ou armazenadas; o não fornecimento de dados pessoais coletados pela internet a terceiros sem prévio consentimento do usuário, além de estabelecer o dever de informar os usuários acerca da coleta de dados sobre si, quando houver justificativa para tal fato. Do mesmo modo, o art.10 do Marco Civil da Internet estabeleceu que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet devem ser realizadas com respeito a intimidade, vida privada, honra e imagem das pessoas direta ou indiretamente envolvidas. O art.14 dispôs que o provedor de conexão à internet não pode guardar registros de acesso a aplicações da internet e o provedor de aplicação de internet não pode guardar os registros de acesso sem prévio consentimento do usuário, nem os dados pessoais desnecessários à finalidade para a qual se deu consentimento, nos termos do art.16. Pelo art.9°, §3º, proíbe-se que os provedores de

[31] Tomasevicius Filho, E. (2016). Marco Civil da Internet: uma lei sem conteúdo normativo . Estudos Avançados, 30(86), 269-285.

> conexão à internet, gratuitos ou onerosos, ou os responsáveis pela transmissão, comutação e roteamento de dados, realizem bloqueios, filtros ou análises de conteúdo dos pacotes de dados.

Tais disposições são extremamente pertinentes, visto que dados pessoais passaram a ter uma maior valorização com o advento e popularização da internet, sendo um comércio extremamente lucrativo, que veio lidando, nos últimos anos, com uma crescente regulamentação, a exemplo da Lei Geral de Proteção de Dados (LGPD), que teve forte influência do Marco Civil da Internet nesses aspectos apontados.

No tocante à responsabilidade do conteúdo compartilhado, o Marco Civil traz importantes disposições a respeito da temática, conforme ensina Tomasevicius Filho:

> O legislador tratou da responsabilidade civil dos provedores de internet por ofensa aos direitos da personalidade das pessoas, como honra, imagem, vida privada e intimidade das pessoas. O art.18 reconheceu a irresponsabilidade civil do provedor de acesso por danos causados pelos usuários. Por outro lado, o art. 19 regulamentou especificamente a responsabilidade civil dos provedores de conteúdo, por exemplo os armazenadores de arquivos fotográficos e musicais, bem como de páginas da internet, entre eles, os blogs. Estabeleceu-se, nesse caso, a responsabilidade subsidiária entre o usuário da internet que praticou o ato ilícito civil e o provedor de conteúdo. Dessa maneira, a responsabilidade primária é do usuário da internet e o provedor de conteúdo somente responde conjuntamente com o causador do dano quando descumprir ordem judicial para que tornasse indisponível o conteúdo ofensivo.

Percebe-se, portanto, que por mais que diversas críticas sejam feitas ao Marco Civil da Internet, principalmente em função da responsabilidade dos provedores, que é bastante atenuada, sendo caracterizada somente quando descumprir ordem judicial para remoção do conteúdo ofensivo, ele é um importante instrumento normativo que permitiu que a norma jurídica se aproximasse mais do ciberespaço, regulando condutas e estabelecendo regras para o que era, até pouco tempo atrás, uma “terra de ninguém”.

CAPÍTULO 3: COMO A CIBERCRIMINALIDADE SE PORTOU, NO BRASIL, DURANTE A PANDEMIA DA COVID-19?

A pandemia da COVID-19 teve um impacto global extremamente significativo. Dessa forma, o presente capítulo se debruçará sobre as alterações que esse período provocou na realidade da sociedade brasileira, em seus modelos econômicos e sociais, analisando como a criminalidade se adaptou frente a um cenário de isolamento social e uma ainda maior presença online.

Após discorrermos sobre toda a conceituação, construção e transformação do ciberespaço, bem como o movimento legislativo brasileiro recente, buscando regular algumas condutas concernentes ao mesmo, alcançaremos, enfim, o cerne do presente ensaio: buscar entender como a cibercriminalidade se desenvolveu durante esse período marcante de quase dois anos de total isolamento, procurando vislumbrar, ainda, as respectivas respostas legislativas frente a esse cenário.

3.1 – O ISOLAMENTO SOCIAL: UMA NOVA REALIDADE EM 2020

O ano de 2020 trouxe algo inesperado no mundo: uma disseminação, em larga escala, de uma epidemia global, alterando, de forma profunda, o *status quo* de definição de modelos de trabalhos e sociabilidade.

Diversos estados no Brasil, bem como países ao redor do mundo, decretaram *lockdown,* com exceção dos serviços ligados às atividades essenciais, como aqueles ligados à saúde.

Por conta disso, visando impedir que houvesse uma onda de desemprego nunca antes vista, diversas empresas adotaram um modelo de trabalho remoto. Dessa forma, os serviços poderiam continuar movimentando a economia e mantendo o emprego desses profissionais, ainda que em tempos de rígido isolamento social.

Nesse sentido, Luiz Sergio Dutra Nagli disserta que[32]:

[32] Luiz Sergio Dutra Nagli. 2020. PANDEMIA NA PANDEMIA: A ESCALADA DE ATAQUES CIBERNÉTICOS PÓS COVID-19. Disponível em:

> A escalada do COVID-19 forçou as empresas a alterar abruptamente a maneira com que conduziam suas operações. Estas mudanças têm como resultado imediato a alocação de um grande volume de trabalhadores no regime de Home Office, aumentando exponencialmente a exposição dos trabalhadores, e suas famílias, a internet. Esta exposição, por motivos de trabalho ou lazer criou uma grande oportunidade para a ação de criminosos digitais. Com os trabalhadores em casa, convivendo com toda à família, também em casa e disputando os recursos de Internet para trabalho, estudo e lazer, o tempo de exposição à rede se multiplicou. Vale dizer, que em muitos casos, o Home Office não contou com o reforço educacional e de segurança digital necessário, longe da segurança das redes corporativas, os trabalhadores se tornaram presa fácil para os criminosos.

Dessa forma, tivemos um cenário nunca antes visto: adultos trabalhando virtualmente, crianças estudando por aulas à distância e, até mesmo o entretenimento, também adquiriu um formato digital: válido ressaltar, inclusive, a onda de *lives* patrocinadas, onde diversas marcas contrataram artistas para shows com transmissões ao vivo gratuitas, de modo a estimular o isolamento social.

Percebemos, então, que tanto as atividades laborais, essenciais à sobrevivência, bem como as atividades de lazer, acabaram se concentrando em um único lugar: o ciberespaço.

Se de um lado ocorreu a concentração da maior parte da população brasileira em um ambiente virtual, por outro lado, as ruas e ambientes físicos ficaram cada vez menos habitados. Dessa forma, nasce a pergunta norteadora do presente ensaio: como a atividade criminosa se comportou frente a essa repentina mudança?

Com relação aos crimes virtuais, é notório que eles podem possuir alguns enfoques, que analisam sua razão de ser, bem como os respectivos antígenos para combatê-los.

Dessa maneira, Gordon e Ford (2006)[33] separam o crime digital em duas categorias: uma com foco na tecnologia e outra com foco no fator humano. O crime digital relacionado à tecnologia possui seu antídoto na mesma tecnologia, como um maior desenvolvimento de ferramentas de software e hardware para

<http://bibliotecadigital.fgv.br/ocs/index.php/ctd/ctd2020/paper/view/7614/0> Acesso em 08 de junho de 2022.

[33] Gordon, S.; Ford, R. COVID-19: On the Definition and Classification of Cybercrime. Journal of Computing Virology, 2006.

proteção. Com relação aos crimes focados nos fatores humanos, o antídoto está na educação. Como elo mais fraco, o fator humano deve ser fortalecido por treinamento contínuo e, no caso da atual pandemia, reforçado para as questões de adaptação do ambiente remoto e higiene digital.

Segundo Darcianne Diogo[34]:

> Aproveitando-se da crise sanitária, criminosos que atuam pela internet intensificaram as ações [...]. Em 2020, houve registro de 17.843 casos, aumento de 87,1% em comparação com 2019. Em relação a estelionatos, o crescimento foi de 209%.

Martins também disserta nesse sentido[35]:

> De fato, o isolamento social foi capaz de reduzir significativamente a prática de roubos e furtos nas cidades brasileiras, como consequência do zelar da população, ao preferir a segurança do ambiente domiciliar. No entanto, estas mesmas circunstâncias, serviram para a desenvoltura de crimes cibernéticos. Criminosos percebendo o uso massivo da rede mundial de computadores por grande parte da população mundial procuraram, rapidamente, adaptar-se à nova realidade para cometer fraudes eletrônicas, aproveitando-se do estado de medo e ansiedade que a pandemia e a necessidade de isolamento causam as pessoas.

É perceptível, portanto, que esse cenário de isolamento social decorrente da pandemia trouxe à luz uma problemática que, conforme analisado, foi se desenvolvendo de forma progressiva e acompanhando a própria formação do ciberespaço: os crimes virtuais.

3.2 – O ENTRETENIMENTO EM TEMPOS DE PANDEMIA: A CRESCENTE ONDA DOS SERVIÇOS DE STREAMING E A PIRATARIA

Quando o primeiro serviço de streaming, a popular Netflix, chegou ao Brasil em 2011, aquilo pareceu inovador e muito interessante financeiramente: ampla variedade de filmes, séries, documentários e, principalmente, preço acessível.

[34] DIOGO, Darcianne. Com 17.843 ocorrências, crimes cometidos pela internet sobem 87,1% em 2020. Correio Braziliense, 13 fev. 2021. Dsponível em: https://www.correiobraziliense.com.br/cidades-df/2021/02/4906387-com-17- 843-ocorrencias-crimes-cometidos-pela-internet-sobem-871--em-2020.html. Acesso em: 08 de junho de 2022.

[35] MARTINS, Humberto. Seminário virtual: Criminalidade em tempo de Covid. Atuação do Sistema de Justiça. Junho de 2020.

Em pouco tempo, houve um exponencial crescimento do número de usuários no país. Dessa forma, ser assinante do serviço rapidamente se tornou um item essencial de entretenimento da família brasileira.

O streaming adquiriu, então, de forma rápida, uma significante relevância: diversas grandes produções originais, nível técnico dos grandes estúdios, contratação de atores consagrados e tendo, até mesmo, importantes indicações a prêmios televisivos e cinematográficos.

Se antes da era dos streamings, a maioria dos usuários recorria ao uso dos *torrents* para consumirem conteúdos audiovisuais, isso não era mais vantajoso agora: por uma mensalidade acessível, não precisariam mais expor suas máquinas a vírus, não teriam o trabalho de procurar os arquivos de vídeo ou buscar legendas. Tudo estava disponível de forma legal e instantânea.

Em consequência disso, filmes e séries, que contavam com sua disponibilização nas referidas plataformas, sofreram uma grande diminuição de circulação de cópias irregulares. O resultado disso parecia, então, fornecer uma animadora lógica: seria o streaming o caminho lógico de modernização do combate à pirataria?

No entanto, o período da pandemia provou ser justamente o contrário.

A partir de 2020, houve uma onda de novos serviços por streaming que chegaram no país, de tal modo que as principais séries e filmes também se fragmentaram, sendo divididas em diversos catálogos. Para ter acesso ao portfólio completo, seria necessário, então, pagar por isso.

Em períodos de crescente isolamento social, boa parte do entretenimento se deu por meio de telas de computadores e monitores televisivos. A demanda por serviços do gênero aumentou e, com isso, esse contexto abriu margem para uma maior circulação de cópias irregulares de obras autorais, infringindo direitos de propriedade intelectual.

Dessa forma, destaca-se a seguinte reportagem:

> Não foi somente o consumo de streaming que disparou durante a pandemia. O consumo de pirataria das plataformas de vídeo seguiu a tendência. Mas o que até algum tempo era um problema secundário para boa parte das empresas, que viam a prática como uma maneira de divulgar seus produtos, agora é um dos maiores problemas do setor. No mundo, nos dois primeiros meses da pandemia, o crescimento dos dez maiores sites de pirataria foi de, em média, 19% (dados SimilarWeb).
>
> No Brasil, chegou a quase 50% de aumento no mesmo período. Um dos principais sites piratas no país viu seu tráfego crescer de 8,5 milhões de usuário para 13,75 milhões entre fevereiro e março de 2020.[36]

Nesse sentido, é válido fazer referência à Lei do Software (Lei nº 9.609), que "Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências." e à Lei dos Direitos Autorais (Lei nº 9.610), que dispõe sobre direitos autorais e outras providências.

O direito autoral também é expressamente assegurado no inciso XXVII do Artigo 5º da Constituição Federal (BRASIL, 1988): "aos autores pertence o direito exclusivo de utilização, publicação ou reprodução de suas obras, transmissível aos herdeiros pelo tempo que a lei fixar".

Além disso, a problemática não se resume apenas à distribuição irregular de obras protegidas por direitos autorais[37]:

> Plataformas como Netflix, Disney+, Amazon Prime e Globoplay estão entre os principais alvos para distribuição de malware, adware, roubo de senhas e lançamento de ataques de spam e phishing. Essas ameaças virtuais são mais frequentemente baixadas quando os usuários tentam obter acesso por meios não oficiais, seja comprando contas com desconto, obtendo um "hack" para manter seu teste gratuito ou tentando acessar uma assinatura sem pagar. Muitas vezes, esses links ou arquivos não oficiais vêm com outros programas maliciosos, como trojans e backdoors.

[36] Netflix, Disney, Amazon e Globo lutam contra disparada da pirataria. Guilherme Ravanche <disponível em: https://www.uol.com.br/splash/colunas/guilherme-ravache/2021/04/20/netflix-disney-amazon-e-globo-lutam-contra-disparada-da-pirataria.htm?cmpid=copiaecola>. Data de acesso: 13 de junho de 2022.

[37] Netflix, Disney, Amazon e Globo lutam contra disparada da pirataria. Guilherme Ravanche <disponível em: https://www.uol.com.br/splash/colunas/guilherme-ravache/2021/04/20/netflix-disney-amazon-e-globo-lutam-contra-disparada-da-pirataria.htm?cmpid=copiaecola>. Data de acesso: 13 de junho de 2022.

Percebe-se, portanto, que criminosos cibernéticos se aproveitaram dessa crescente expansão do streaming no período da pandemia para fomentar novas espécies de golpes virtuais, amoldando-se bem a essa demanda do mercado para conseguir atrair e formar novas vítimas.

3.3 – PEDOFILIA NO CIBERESPAÇO

Um grande problema que o desenvolvimento da internet ocasionou, agravando conforme o acesso à tecnologia foi se tornando cada vez mais difundido no corpo social, foi a questão dos crimes sexuais direcionados a crianças e adolescentes.

O início do século XXI e a chegada dos primeiros fóruns e sites de bate-papo trouxeram consigo uma problemática que possui incidência até os dias atuais: o aliciamento de menores no ambiente virtual, a chamada ciberpedofilia[38]:

> A ciberpedofilia nada mais é do que crimes sexuais praticados contra crianças e adolescentes através da internet. Os ciberpedófilos criam mecanismos para atrair a sua vítima utilizando-se de diversas linguagens infantis para conhecer e conquistar a criança e/ou o adolescente, com o propósito da prática sexual. Alguns outros meios utilizados pelos ciberpedóflios, são a criação de perfis falsos, para que consigam se passar por crianças e assim ter uma desenvoltura maior no diálogo com a vítima sem que a mesma perceba qualquer diferença num primeiro momento. Posteriormente, ocorre as chamadas chantagens emocionais, onde conseguem através disso, o que almeja da vítima, inclusive o chamado “estupro virtual”.

Com relação a isso, o Estatuo da Criança e do Adolescente (Lei nº 8069), passou a trazer disposições para coibir práticas como as descritas:

> O ECA agora ampliou o rol das situações que envolvesse a pornografia infantil, para que abrangesse os cibercrimes, como se observa no artigo 241-A do ECA, ao punir aquele que oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente, poderá pegar de 3 a 6 anos de prisão e multa.

Disciplinando também a situação em que o pedófilo armazena ou compra fotos de sites ou baixa de sites de pedofilias, o artigo 241-B do ECA, regulamenta

[38] MORAIS, Lucas Andrade de. Ciberpedofilia: os crimes de pedofília praticados através da internet. Conteúdo Jurídico, Brasília-DF: 06 maio 2021. Disponível em: <https://conteudojuridico.com.br/consulta/Artigos/51597/ciberpedofilia-os-crimes-de-pedofilia-praticados-atraves-da-internet>. Acesso em: 13 de junho de 2022.

tal conduta e assim dispõe que será punido quem adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.

Percebe-se, portanto, que há punição a todo aquele que troca, disponibiliza, transmite, distribui, publica ou divulga foto, vídeo ou outro registro que contenha cena de sexo envolvendo criança ou adolescente, bem como aquele que armazena, compra ou baixa esses registros de sites de pedofilia.

Nesse sentido, percebe-se que a problemática em comento já é latente há um tempo, visto que possuiu, inclusive, regulamentação especial para trazer punições aos abusadores que agem no meio virtual.

Por conta disso, é essencial também entender como essas práticas se comportaram frente à pandemia, já que o tráfego de crianças e adolescentes online se tornou mais intensificado, visto que muitas escolas adotaram modelo de EAD e até mesmo o entretenimento, conforme comentado no tópico antecedente, se desenvolveu de forma virtual.

Destaca-se, nesse sentido, os seguintes dados coletados pela Safernet Brasil durante o período analisado[39]:

> Entre janeiro e abril de 2021 foram denunciadas à Safernet Brasil 15.856 páginas relacionadas com pornografia infantil, das quais 7.248 foram removidas por indício de crime. O número mostra um crescimento de 33,45% nas denúncias em relação ao mesmo período do ano passado, quando 11881 páginas haviam sido denunciadas, das quais 6938 foram removidas.
>
> Ano passado, primeiro ano da pandemia de covid-19, a Safernet Brasil recebeu 98.244 denúncias anônimas de páginas de internet contendo pornografia infantil - recorde histórico desde que é feita a medição (iniciada em 2006). O número é mais do que o dobro (102,24%) em relação às 48.576 páginas reportadas por usuários da internet pela mesma razão em 2019.

Percebe-se, portanto, que a maior exposição de crianças e adolescentes no ambiente virtual, ocasionou também um aumento das práticas de ciberpedofilia, intensificando o número de uploads e downloads deste tipo de conteúdo, tendo um aumentou de 33,45% em 2021, quando comparada ao

[39] SAFENET. Denúncias de pornografia infantil cresceram 33,45% em 2021, aponta a Safernet Brasil. Disponível em:<https://new.safernet.org.br/content/denuncias-de-pornografia-infantil-cresceram-3345-em-2021-aponta-safernet-brasil> 15.08.2021. Acesso em: 14 de junho de 2022.

primeiro período do mesmo ano de 2020, quando as medidas de isolamento social ainda não haviam sido implementadas.

Destaca-se, ainda, que o primeiro ano de pandemia teve um recorde mundial de 98.244 denúncias anônimas, tendo um aumento de 102,24% quando comparado ao ano anterior.

Os dados trazem, então, uma preocupante preocupação: o aumento da presença de menores no ciberespaço faz surgir novas oportunidades para os ciberpedófilos, que intensificam seus ataques diante do cenário apontado.

Em um constante modelo de desenvolvimento tecnológico, tal como apontamos durante todo o desenvolvimento do presente ensaio, é preocupante observar o quanto essa rede se articula e se desenvolve, tendo, atualmente, poucos mecanismos de fiscalização para a identificação e penalização desses criminosos.

3.4 – O PIX: INOVAÇÃO BRASILEIRA E O GOLPE DO PIX

O PIX se popularizou muito durante o período de pandemia no Brasil, podendo ser definido como, de acordo com o Banco Central do Brasil (BCB) “o meio de pagamento instantâneo brasileiro em que os recursos são transferidos entre contas em poucos segundos, a qualquer hora ou dia. É prático, rápido e seguro. O Pix pode ser realizado a partir de uma conta corrente, conta poupança ou conta de pagamento pré-paga.”

Devido à sua praticidade e por não conter custos, bastando como cadastro um CPF junto à plataforma bancária, ele rapidamente se popularizou no país. A expressão “faz um pix” se tornou muito popular em todas as camadas sociais. Diversas plataformas de marketplace, inclusive, passaram a incluir essa possibilidade de pagamento em seus produtos, de modo que após a compra é gerado um QR Code, com um prazo de validade de 30 minutos, substituindo o monopólio dos cartões de crédito, que perdurava desde o início do desenvolvimento deste tipo de plataforma.

No entanto, esse novo meio de pagamento digital acabou servindo também como um instrumento para a realização de crimes cibernéticos, como por exemplo: roubo de dados de cartão, envio e recebimento de e-mails com

códigos maliciosos, invasão de contas bancários, clonagem de contas em redes sociais, etc.

Todas essas modalidades são, portanto, espécies de estelionato, definido da seguinte forma pelo Código Penal:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.

Dessa forma, abordaremos alguns dos principais golpes utilizados por esses estelionatários.

Com relação aos links maliciosos, esse tipo de golpe ocorre quando o usuário recebe um link, geralmente através de mensagem no celular, e-mail ou redes sociais e, ao clicá-lo, é infectado pelo vírus oculto no link, que invade o aparelho utilizado e retira informações pessoais. Dessa forma, o criminoso pode ter acesso aos dados bancários da vítima e realizar transferências, via pix, como se fosse o dono da conta.

Há também o golpe da falsa central de atendimento, em que o golpista faz contato com a vítima e se identifica como funcionário de banco ou empresa em que a vítima é cliente. A partir disso, o estelionatário oferece ajuda ou algum serviço e, quando o cliente divulga seus dados, o golpista utiliza para outras finalidades e pode solicitar pagamentos ou transferências por meio do pix. Essa prática ficou conhecida e popularizada em noticiários como o Golpe do Pix.

Algo que também se desenvolveu foram as clonagens de whatsapp, na qual o estelionatário clona uma conta na plataforma e entra em contato com os contatos mais frequentes, inventando alguma história que justifique o pagamento via pix, geralmente alegando algum problema urgente.

Na plataforma Instagram, também se tornou comum anúncios de produtos com preços muito abaixo do mercado. Em alguns casos, os estelionatários utilizam contas de pessoas conhecidas da vítima, o que facilita o golpe. Após isso, elas pagam antecipadamente, via pix, pelo valor do produto, que sequer existe.

Percebe-se, portanto, que por mais que o pix tenha sido um avanço que veio para ficar, também trouxe consigo novas preocupações com relação à segurança dessas transferências.

3.5 – RESPOSTAS ESTATAIS

Feito um recorte de algumas das problemáticas que surgiram durante o período da pandemia, com relação aos crimes virtuais, é oportuno ver que o estado não ficou inerte, mas também trouxe novas legislações para regular essa temática, conforme analisaremos em seguida.

3.5.1 – LEI N. 14.155, DE 27 DE MAIO DE 2021

A legislação em comento alterou o Código Penal para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Código de Processo Penal para definir a competência em modalidades de estelionato.

Dentre suas alterações, válido comentar aquela referente ao artigo 154-A do Código Penal, que foi originalmente previsto pela Lei Carolina Dieckmann, previamente comentada no presente ensaio, que criminaliza a invasão de dispositivo informático. Na redação original, o núcleo do tipo penal designava uma invasão com uma das finalidades enumeradas nos elementos subjetivos especiais do tipo.

Com a alteração dada pela Lei nº 14.1552021, para a criminalização do crime basta agora que o dispositivo seja de uso alheio e sem a exigência que a invasão ocorra mediante violação indevida de mecanismo de segurança.

Além disso, a pena anterior era mais branda, de 3 meses a 1 ano e multa, sendo, portanto, um crime de menor potencial ofensivo, de competência dos Juizados Especiais Criminais. Com a alteração dada pela lei em referência, ocorreu um aumento dessa pena, passando a ser de 1 a 4 anos de reclusão e multa, deixando, dessa forma, de ser um crime de menor potencial ofensivo, devendo ser processado pelo juízo comum.

3.5.2 - FURTO QUALIFICADO POR MEIO ELETRÔNICO

Também ocorreram alterações com relação ao crime de furto, passando a trazer uma forma qualificada e novas formas majoradas:

> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
>
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
>
> I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
>
> II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.

Percebe-se, então, que foi trazida uma nova forma de furto, sendo aquele furto mediante fraude cometido por dispositivo eletrônico, não sendo necessária a violação de mecanismo de segurança ou a utilização de programa malicioso.

Nessa mesma linha, inclui-se as formas majoradas quando o crime é cometido mediante servidor mantido fora do território nacional e quando o crime é praticado contra idoso ou vulnerável.

É interessante que essas formas majoradas tenham sido incluídas, visto que esses são dois dos maiores problemas enfrentados quando falamos em cibercriminalidade: a dificuldade de punição extraterritorial e a presença, em massa, cada vez maior de idosos e vulneráveis nesse ambiente de ciberespaço, que são vítimas mais fáceis para caírem nestes artifícios criminais.

3.5.3 - ESTELIONATO VIRTUAL

Com relação ao crime de estelionato, ocorreram as seguintes inclusões, de uma forma qualificada e figuras majoradas:

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
>
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

> Estelionato contra idoso ou vulnerável
>
> § 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.

A figura qualificada do estelionato virtual foi uma resposta estatal à crescente improvisação de mecanismos de estelionato por meio virtuais, que se impulsionaram, conforme demonstrado, durante o período da pandemia. Dessa forma, foi acertada a decisão em trazer uma figura qualificada para aquelas fraudes realizadas por meio de redes sociais, contatos telefônicos ou envio de e-mails fraudulentos ou, ainda, qualquer outro meio análogo a estes.

As formas majoradas a respeito do servidor mantido fora do território nacional e praticado contra idoso ou vulnerável também seguem a mesma linha daquilo discutido com relação às alterações no crime de furto.

Também houve alteração no artigo 70 §4º do Código de Processo Penal, vejamos:

> § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.

Percebe-se, então, que a competência para o processamento de crimes de estelionato vai ser no domicílio da vítima quando “praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores”.

CONCLUSÃO

Percebe-se, portanto, que o desenvolvimento da tecnologia e a ampliação do ciberespaço trouxe facilidades para a vida humana, mas também gerou novas preocupações: o desenvolvimento da cibercriminalidade, que acompanha, na mesma proporção, o progresso e difusão do ambiente virtual.

A pandemia do COVID-19 no Brasil trouxe uma nova realidade que também revelou, de forma prática, o quanto a relação entre popularização e aumento do número de tráfego virtual faz surgir novas problemáticas relacionadas aos crimes virtuais.

Desde o início da formação do ciberespaço, houve um movimento legislativo para buscar regular algumas condutas, todas elas, de certo modo, relacionadas com o contexto fático em que a sociedade se encontrava naquele momento.

Essa mesma linha foi observada durante o período da pandemia, que trouxe alguns movimentos legislativos, como os destacados em tópico anterior.

É de se esperar, portanto, que a cibercriminalidade seja tratada não só por uma repressão estatal, mas também por meio de programas de educação que orientem os internautas a como se protegerem desse tipo de atividade criminosa, já que a expectativa, nos próximos anos, é que o número de pessoas com dispositivos eletrônico se torne cada vez maior, vez que a linha de progresso da tecnologia tem sido uma contínua curva ascendente.

Entender a cibercriminalidade, seus protocolos e suas principais formas de atuação é essencial para conseguirmos combatê-la, ainda que ela talvez se revele algo tão em desenvolvimento e em curvas tão ascendentes quanto o próprio avançar da tecnologia.

Como todas as relações de antítese, o dia e a noite, o preto o branco, o yan e o yang, o bom e o mal, temos os opostos que acabam se desenvolvendo em conjunto. Com toda a certeza, o desenvolvimento do ciberespaço encontra o seu antagonismo justamente neste avanço da cibercriminalidade.

REFERÊNCIAS

BARRETO Júnior, Irineu**. Atualidade do Conceito de Sociedade da Informação para a Pesquisa Jurídica**. In: PAESANI, Liliana Minardi (Coord.). O direito na sociedade da informação. São Paulo: Atlas, 2007.

BOITEUX, Luciana: **Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual**, RBCCRIM n. 47, 2004.

CANONGIA, Claudia; JUNIOR, Raphael Mandarino. **Segurança cibernética: o desafio da nova Sociedade da Informação**. Disponível em: <http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/349/342>

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

COLLI, Maciel. **Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos.** Juruá Editora, 2010. P. 44.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de segurança para internet**. 2. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012.

CORRÊA, Cybthia Harumy Watanabe. **Comunidades Virtuais gerando identidades na sociedade em rede**. Universiabrasil.net, 2004.

COSTA ALMEIDA, André Augusto Lins da. **A Internet e o Direito**. Revista Consulex, São Paulo, ano II, nº 24, dez. 1988.

DE MATTOS, Alexandre Magalhães. **Crimes na Internet (Kindle Locations 2028-2035).** Alexandre Mattos. Kindle Edition.

Decreto Lei nº 2.848. Disponível em: <**Erro! A referência de hiperlink não é válida.**>.

DIOGO, Darcianne. **Com 17.843 ocorrências, crimes cometidos pela internet sobem 87,1% em 2020**. Correio Braziliense, 13 fev. 2021. Disponível em: https://www.correiobraziliense.com.br/cidades-df/2021/02/4906387-com-17- 843-ocorrencias-crimes-cometidos-pela-internet-sobem-871--em-2020.html.

Gordon, S.; Ford, R. COVID-19: **On the Definition and Classification of Cybercrime**. Journal of Computing Virology, 2006.

GRECO, Rogério. **Curso de Direito Penal – Parte Geral - Vol 1 - 17ª Ed**. 2015

Hall, Stuart. 2011. **A identidade cultural na pós-modernidade**. Rio de Janeiro. DP&A.

KUNRATH, Josefa Cristina Tomaz Martins. **A expansão da criminalidade no ciberespaço: desafios de uma política criminal de prevenção ao cibercrime**. 158 f. il. 2014. Dissertação (Mestrado) — Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2014.

Lei n˚ 12.735. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em 03 de junho de 2022.

Lei n˚ 12.965 de 2014. <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

LEMOS, Ronaldo; SOUZA, Carlos Affonso. **Marco civil da internet: construção e aplicação**, Juiz de Fora; Editora Associada, 2016.

Luiz Sergio Dutra Nagli. 2020. **PANDEMIA NA PANDEMIA: A ESCALADA DE ATAQUES CIBERNÉTICOS PÓS COVID-19**. Disponível em: **Erro! A referência de hiperlink não é válida.**.

MARTINS, Humberto. Seminário virtual: **Criminalidade em tempo de Covid**. Atuação do Sistema de Justiça. Junho de 2020.

MORAIS, Lucas Andrade de. **Ciberpedofilia: os crimes de pedofília praticados através da internet**. Conteúdo Jurídico, Brasília-DF: 06 maio 2021. Disponível em: <https://conteudojuridico.com.br/consulta/Artigos/51597/ciberpedofilia-os-crimes-de-pedofilia-praticados-atraves-da-internet>.

Netflix, Disney, Amazon e Globo lutam contra disparada da pirataria. Guilherme Ravanche <disponível em: https://www.uol.com.br/splash/colunas/guilherme-ravache/2021/04/20/netflix-disney-amazon-e-globo-lutam-contra-disparada-da-pirataria.htm?cmpid=copiaecola>.

PAGANOTTI, Ivan. **Eptic online: revista eletrônica internacional de economia política da informação, da comunicação e da cultura, ISSN-e 1518-2487, Vol. 16, Nº. 2,** 2014.

PINHEIRO, Patricia Peck. **Direito Digital. 4ed**. Ver., atual. eampl. São Paulo: Saraiva, 2011.

PINHEIRO, Patrícia Peck; HAIKAL, Victor Auilo. **A nova lei de crimes digitais**. 2013. Disponível em: <www.pppadvogados.com.br/Publicacoes.aspx?v=1&nid=1432>.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **Crimes virtuais**. 2005. Disponível em:<http://www.advogadocriminalista.com.br>.

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

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SAFENET. **Denúncias de pornografia infantil cresceram 33,45% em 2021, aponta a Safernet Brasil**. Disponível em:<https://new.safernet.org.br/content/denuncias-de-pornografia-infantil-cresceram-3345-em-2021-aponta-safernet-brasil> 15.08.2021. Acesso em: 14 de junho de 2022.

SAFERNET BRASIL. **Delegacias cibercrimes**. Disponível em: <http://www.safernet.org.br/site/prevencao/orientacao/delegacias>.

SILVA, Libório; REMOALDO, Pedro. **Introdução à Internet**. 2. ed. São Paulo: Editorial Presença, 1995.

Tomasevicius Filho, E. (2016). **Marco Civil da Internet: uma lei sem conteúdo normativo. Estudos Avançados**.