2022
FLUXO CONTÍNUO
Ed. 37 - Vol. 1. Págs. 166-184

JNT - FACIT BUSINESS AND TECHNOLOGY JOURNAL ISSN: 2526-4281 - QUALIS B1

CRIMES CIBERNÉTICOS EM TEMPOS DE PANDEMIA: O ISOLAMENTO SOCIAL COMO PROPULSOR DA VULNERABILIDADE DA POPULAÇÃO E DO AUMENTO DOS CASOS

CYBERCRIMES IN TIMES OF A PANDEMIC: SOCIAL ISOLATION AS A DRIVER OF POPULATION VULNERABILITY AND THE INCREASE IN CASES

Carlos Alberto Cardoso WANDERLEY
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: cacwanderley@gmail.com

Rodrigo Silva da COSTA
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: rodrigosilvadacosta0@gmail.com

Lara de Paula RIBEIRO
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: lara.ribeiro@unitpac.edu.br

RESUMO

O presente artigo tem por finalidade discutir o motivo do vertiginoso aumento do número de casos de crimes praticados na internet, sobretudo no período pandêmico. Para isso faz-se uma análise desse tipo penal, dito como cibercrime, apontando as principais características dessa prática, bem como as legislações vigentes e a deficiência no processo de investigação e punição. É certo que os crimes dessa natureza crescem gradualmente a cada dia, porém, foi durante a pandemia da Covid-19 que houve um explosivo crescimento da cibercriminalidade, motivado principalmente pelo isolamento social, o qual foi um dos principais propulsores a esse irrefreável crescimento. Devido ao isolamento, as pessoas foram obrigadas a se refugiarem em suas casas, limitando o contato com o mundo externo, que só se tornou possível por meio da internet. Daí, com o elevado número de usuários logados na web, a incidência de delitos virtuais aumentaram, pois havia um maior número de possíveis vítimas. A pesquisa demonstrou que de fato está correlacionado, o isolamento social como causa do aumento da cibercriminalidade, mas também, entra nessa conta a deficiência da legislação penal, que não acompanhou a evolução tecnológica.

Palavras-chave: Aumento dos casos. Ciovid-19. Crimes Cibernéticos. Internet. Isolamento Social.

ABSTRACT

This article aims to discuss the reason for the vertiginous increase in the number of cases of crimes committed on the internet, especially in the pandemic period. For this, an analysis of this criminal type, called cybercrime, is made, pointing out the main characteristics of this practice, as well as the current legislation and the deficiency in the investigation and punishment process. It is true that crimes of this nature grow gradually every day, however, it was during the Covid-19 pandemic that there was an explosive growth of cybercrime, mainly motivated by social isolation, which was one of the main drivers of this unstoppable growth. Due to isolation, people were forced to take refuge in their homes, limiting contact with the outside world, which was only possible through the internet. Hence, with the high number of users logged into the web, the incidence of virtual crimes increased, as there were a greater number of possible victims. The research showed

that, in fact, social isolation is correlated as a cause of the increase in cybercrime, but also the deficiency of criminal legislation, which has not followed technological evolution.

Keywords: Covid-19. Cybercrime. Increase in cases. Internet. Social isolation.

INTRODUÇÃO

A tecnologia avança a passos largos e a cada dia toma mais espaço frente à sociedade, fazendo com que o mundo se torne mais globalizado e conectado, marginalizando aqueles que não aderem a essa nova realidade. Essa conectividade far-se-á, principalmente, pela internet, que trouxe vários benefícios à evolução do processo de comunicação e do encurtamento de distâncias entre as pessoas, atualmente, representa um dos principais meios de comunicação e interação social, atraindo cada vez mais usuários.

Contudo, a internet também se mostra um campo extremamente propício a práticas de diversos atos ilícitos. Esse novo lócus da criminalidade se mostra favorável em razão do elevado número de possíveis vítimas, que aliado ao anonimato e a deficiência da atuação jurídica nessa área, acarretam o cometimento de diversas práticas delitivas, as quais se denominam cibercrimes e se disseminaram em larga escala no decorrer dos últimos anos.

Os maiores índices de incidência desses crimes foram registrados a partir do ano de 2020, quando houve um aumento explosivo na quantidade de crimes cometidos na internet e o motivo por detrás desse fator se relaciona ao cenário mundial daquele período, no qual houve o surgimento e acometimento da pandemia da Covid-19. No final do ano de 2019, o mundo foi assolado pela doença, a qual rapidamente se alastrou por diversos países, ganhando status de pandemia e espalhando caos e desespero à população, uma vez que afetou não só a saúde pública, como os demais setores sociais.

Assim, o presente artigo tem o intuito de relacionar o contexto pandêmico ao aumento vertiginoso dessa modalidade delitiva. Inicialmente, apresentando um contexto sobre a pandemia, sobretudo no que diz respeito às medidas de combate e controle da doença, como o isolamento social, que é o principal ponto a ser discutido, haja vista que, com as pessoas a se refugiadas em suas casas, limitando o contato e interação social, estas se voltaram para internet como único meio de escape. Daí se extrai um dos motivos pelos quais os crimes cibernéticos foram tão incidentes nesse período, em função da massiva quantidade de usuários que estavam logados na rede.

BREVE CONTEXTO SOBRE A PANDEMIA DA COVID-19

Conceito de Pandemia

Segundo a Organização Mundial de Saúde (OMS), o termo pandemia está associado a uma disseminação em larga escala de uma enfermidade que se alastra por diferentes países e continentes com transmissão sustentada de pessoa para pessoa, ou seja, é dizer que, quando uma doença atinge níveis mundiais com alta taxa de contaminação, esta, pode ser declarada como uma pandemia. Contudo, não basta apenas que haja contágio em escala global, é necessário também analisar o potencial ofensivo da enfermidade, bem como o ritmo de contaminação, haja vista que há doenças endêmicas ao redor do globo que apesar de atingirem diferentes países, não são consideradas pandemias, pois são estáveis e de menor potencial lesivo, como é o caso das gripes sazonais.

Desse modo, resta dizer que uma pandemia é a disseminação em larga escala de um patógeno (agente causador da doença) com intenso ritmo de contaminação e potencial ofensivo à saúde humana. Dentre estas, pode-se citar como referência, a gripe espanhola e a Covid-19.

Análise Panorâmica da Pandemia Causada pelo Novo Coronavírus (Covid-19)

No dia 31 de dezembro de 2019 a Organização Mundial de Saúde (OMS) foi alertada sobre um surto de pneumonia ocorrido na cidade de Wuhan, na República Popular da China. Uma semana depois, restou identificado que se tratava de contágio pelo SARS-CoV-2, uma variação do coronavírus, causador da COVID-19 (*coronavirus disease 2019*), a qual possuía elevada taxa de infectividade o que fez com que sua propagação se fizesse de maneira extremamente rápida, e o número de casos cresceu exponencialmente.

Em razão da expansão da doença e de seus efeitos catastróficos, no dia 11 de março de 2020 a Organização Mundial de Saúde (OMS) a classificou como Emergência Pública de Interesse Internacional (EPII) e desde seu início já foram identificados casos da doença em mais de 180 países e o número de infectados é de 478.790.847. No Brasil, o primeiro caso foi registrado em 26 de fevereiro de 2020 e no decorrer de 2 anos, 29.380.063 pessoas foram infectadas e 655.249 mortes relacionadas a Covid-19 foram atestadas.

Segundo Maia e Dias (2020) toda pandemia é causadora de grandes impactos sociais, econômicos e políticos. Não obstante, o Brasil registrou a maior queda em seu PIB (produto interno bruto) na história recente, registrando déficit de 4,1% no referido ano. Assim, foi publicado o Decreto Legislativo n° 6, de março de 2020, que reconhecia o estado de calamidade pública e autorizava gastar acima do teto orçamentário previsto àquele ano, bem como foi implementado também medidas preventivas como isolamento e distanciamento social, uso obrigatório de máscaras e fechamento de locais públicos, a fim de se evitar aglomerações e a consequente propagação da doença. Tais medidas visavam refrear o contágio do vírus, haja vista que o sistema público de saúde não conseguiria suprir toda a demanda, no epicentro, as unidades de tratamento intensivo (UTIs) apresentavam quadros de superlotação, e, havia carência de equipamentos respiratórios e até mesmo de equipamentos básicos, tais quais luvas, máscaras, álcool em gel, etc.

Essa situação começou a ser revertida após a criação das primeiras vacinas, o que trouxe um vislumbre de um contra ataque ao vírus. A Rússia foi pioneira nesse quesito, fabricando a primeira vacina no mundo contra o SARS-CoV-2, iniciando sua produção em agosto de 2020. No Brasil, a vacinação somente teve início em 17 de janeiro de 2021. Segundo dados divulgados pela "*Our World In Data",* até a data de 24/03/2022 foram aplicadas 411 milhões de doses de vacina, estando 160 milhões de brasileiros totalmente imunizados, cerca de 75% da população.

Todavia, mesmo durante o avanço da vacinação, fez-se necessário a implantação de medidas preservativas para combater o avanço da doença, uma vez que, mesmo com a vacinação ocorrendo, o vírus ainda se propagava. Com isso, mais de 98% dos municípios do Brasil adotaram o isolamento social, onde pessoas estavam obrigadas a usar máscaras, manter distância, em grande parte dos casos trabalharem de suas casas, e até ficou proibida a circulação de pessoas nas ruas, ficando estas, obrigadas a utilizar internet e televisão como principal meio de comunicação e interação social. Contudo, a Organização Mundial de Saúde ainda mantém o status de pandemia, haja vista que o número de casos ainda é alarmante e os efeitos e duração da Covid-19 ainda é incerto.

Definição e Formas de Isolamento Social Impostos Durante a Pandemia da COVID-19 e o Impacto Dessas Medidas Frente à População

Pode-se definir o isolamento social como uma ação voluntária ou não, com o fito de manter um indivíduo afastado do convívio com os demais. É dizer que uma pessoa é retirada do meio social para que seja resguardada a sua integridade ou a das outras que a cercam. Partindo dessa premissa, entende-se que o isolamento social pode ser voluntário, quando o indivíduo por sua própria decisão e vontade decide afastar-se do convívio social, e, o isolamento involuntário, meio no qual o Estado atua e coage o indivíduo, restringindo alguns de seus direitos, de modo a retirá-lo do meio social.

Durante a pandemia da Covid-19, boa parte da população, por si só, decidiu pelo isolamento social, fato este ocorrido pelo temor à doença, em razão da carência de informação, sobretudo pela incerteza do tratamento. Não obstante, o Estado interveio aplicando suas próprias medidas restritivas, essenciais ao controle epidemiológico, inicialmente impondo o distanciamento social, a fim de evitar aglomerações, o que se fez com a suspensão de transporte público e eventos, regulamentação de horário de funcionamento do comércio e suspensão de aulas presenciais em escolas e universidades. Nesse meio, foi publicada a portaria n° 454, que declarou estado de transmissão comunitária da Covid-19, fazendo assim entrar em vigor a Lei n° 13.979, denominada lei da quarentena e implementada com o fito de frear a contaminação e propagação da doença.

Frente ao irrefreável aumento da doença, o governo brasileiro impôs o isolamento social, de modo que apenas as atividades consideradas como essenciais foram mantidas em funcionamento. Ocorre que apesar de necessário, o chamado *lockdown*, se mostrou bastante severo, trazendo consequências psicológicas e sociais, provocando doenças como depressão e ansiedade, bem como, influenciando no aumento dos casos de violência doméstica.

Destarte, em meio à medida inquisitiva, a única forma de "escape" tornou-se a internet, que passou a ser a principal forma de interação social, haja vista que outras formas de contato estavam restritas. Desse modo, a maioria das atividades diárias passou a ser exclusivamente por meio remoto e essa significativa mudança na convivência social, acentuou a vulnerabilidade, muito em razão de doenças psicológicas, como depressão e ansiedade, ocasionadas, sobretudo pelo temor ao vírus, bem como pelo tempo em que as pessoas se mantinham logadas na rede.

Estudos apontam que a maioria das pessoas isoladas apresentam quadros de morbidades psicológicas, muito em razão do fechamento de escolas e locais públicos, associado também à proibição de eventos festivos ou comemorativos. Segundo Wang, C. et al (2020), num estudo realizado na China, nos primeiros meses da pandemia, 53,8% dos entrevistados relataram que o impacto psicológico era moderado ou grave, e outros 28,8% revelaram sofrer sintomas de ansiedade e estresse.

Nesse ínterim, as medidas restritivas incidiram diretamente na saúde psicológica das pessoas, agravando complicações preexistentes. Contudo, é mister dizer que apesar das severidades das medidas de isolamento social, até então, estas se mostraram a melhor forma de enfrentamento à pandemia e mesmo após a vacinação em larga escala, tais medidas continuaram a ser aplicadas.

CRIMES CIBERNÉTICOS

Conceito de Cibercrime

O termo mais utilizado e atualmente aceito pela doutrina internacional teve origem no final da década de 1990, advindo de uma reunião de um subgrupo das nações do G8, denominado de "Grupo de Lyon", para informar as formas de crimes cometidos por meio da internet, denominando-os como "Cibercrimes". A reunião foi realizada especificamente para discutir formas para combater os atos ilícitos praticados na internet ou através desta, que podem envolver desde invasões de sistema, roubo de dados pessoais, falsidade ideológica, até práticas de injúria cometidas na internet. Segundo Correia (2020), pode-se conceituar cibercrime como "a conduta ilícita manifestada por meio eletrônico, em que se é utilizado o da internet como meio para práticas delituosas".

Assim, compreende-se como Cibercrime a prática de ato ilícito na internet, utilizando de aparelhos eletrônicos para, através da internet, fraudar sistema de comunicações, invadir computadores e redes corporativas (INTERPOL, 2015). Dessa forma, Cibercrime é a conduta ilícita realizada por meio de computador e da internet (Rosa, 2002, pp. 53-57.). Tais condutas podem ser praticadas de diversas formas, tantos os crimes tradicionais, ou seja, os que não precisam de conhecimento técnico sobre informática, como os crimes contra a honra e imagem ou ainda delitos patrimoniais, bem como os casos que exigem conhecimento técnico ou o bem jurídico é especificamente da informática, como crimes contra softwares, que o bem jurídico é autoral.

Tipos de Crimes e as Principais Características da Cibercriminalidade

Os crimes cibernéticos são caracterizados principalmente pelo anonimato, que pode ser real, aqueles em que o criminoso é uma *hacker* ou *cracker*, verdadeiros "*experts*" que possuem conhecimento técnico nas áreas de informática, ou, simplesmente pelo fato de o criminoso estar por detrás de uma tela, longe da vítima, uma vez que munido com um dispositivo eletrônico, seja um computador, *tablet* ou *smatphone*, e, através de um ponto de conexão qualquer usuário pode praticar uma série de delitos dentro da web.

Outro ponto importante é que a principal rede de comunicação, planejamento e atuação de criminosos, encontra-se na chamada *Dark Web* que é uma parte da *Deep Web*, um domínio obscuro, de difícil acesso, que corresponde a 90% da internet e se mantém invisível aos usuários comuns. Nessa esfera, não são utilizados os *browsers* comuns, é preciso receber *links* específicos que direcionam aos domínios ali presentes.

É nesse ambiente que se concentra a base de operações dos criminosos, onde é possível ter acesso a todo e qualquer ilícito, tais como drogas, armas, materiais de pedofilia, encomendar assassinatos e outros tantos crimes violentos e cruéis. Um dos principais meios de acesso a essa parte da web far-se-á mediante o TOR (*The Onion Router*), um *software* de código livre que direciona o tráfego da internet, capaz de ocultar a localização e a identidade dos usuários, fazendo com que os domínios e páginas ali presentes sejam quase impossíveis de serem rastreados.

Todavia, embora utilizada como meio de fornecimento, os criminosos precisam atuar dentro da *Surface* da web que é parte da internet que é disponível para todos e acessada por usuários comuns, local em que suas vítimas estão logadas, e dentre os delitos mais frequentes, destacam-se o *phising*, *cyberbullying*, *ransomware*, *cyberstalking* e estelionato eletrônico.

O ***pishing*** é uma das práticas mais recorrentes no ambiente virtual, consiste na captação de dados pessoais da vítima. Para isso, o criminoso se vale de falsos e-mails e mensagens, quase sempre informando que a pessoa é a ganhadora de algum prêmio e para recebê-lo é necessário enviar suas informações pessoais. Há também a reprodução de ambientes digitais de forma quase perfeita, muda-se detalhes na URL (link do site), assim o internauta nem desconfia e deixa os dados, é comum em sites de compra e venda ou páginas de programas sociais, nas quais é necessário preencher os dados do usuário.

Já o ***cyberbullying*** consiste na humilhação, intimidação, exposição vexatória e difamação sistêmica da vítima em ambientes virtuais tais como aplicativos de mensagem e redes sociais. Na prática é dizer que se trata de delitos contra honra e imagem, porém que alcançam maior potencial ofensivo ao serem praticados na internet.

O ***Ransomware*** é um tipo de extorsão digital na qual dados ou sistemas computacionais das vítimas são criptografados através de *software* e apenas liberados mediante o pagamento por meio de moedas digitais, em outras palavras, o golpe consiste em sequestrar dados de seu aparelho eletrônico, por meio de programas maliciosos, tornando os referidos dados inacessíveis, assim, os criminosos exigem um pagamento para liberação desses dados, por isso o nome popular de "sequestro de dados".

Por sua vez, o ***cyberstalking*** ocorre quando há uma perseguição ou assédio à vítima, por meio de cerceamento da sua liberdade e privacidade, de modo a ameaçar-lhe a integridade física ou psicológica, invadindo ou perturbando sua liberdade e privacidade. Já o **estelionato eletrônico** é o mesmo crime tradicional, qual seja, de obter vantagem indevida por meio de fraude, mas nesse caso a fraude se faz por meio eletrônico.

A Vulnerabilidade da População e a Sensação de Impunidade

Estima-se que haja cerca de 3,9 bilhões de internautas na internet, de modo que o número de criminosos e de vítimas é exorbitante. Nesse mister é imperioso destacar que é absurdamente minoritária a parcela de usuários que utilizam dos meios de proteção e segurança básicos quando navegam pela Web, por isso se tornam presas fáceis para os cibercriminosos, que se utilizam dessa vulnerabilidade para roubar dados pessoais e promover as mais diversas práticas delituosas.

Como cediço essa modalidade delitiva se caracteriza pelo anonimato e somado a isso há uma carência na legislação pátria, bem como no processo investigativo, fato este traduzido pelas poucas delegacias especializadas de repressão ao crime cibernético que existem, as quais não conseguem suprir a quantidade absurda de demanda. Ademais, a transnacionalidade adiciona um quê a mais de complexidade, pois não existem fronteiras dentro da web e um cibercriminoso pode atingir sua vítima em qualquer lugar do planeta.

Esses fatos somados consubstanciam a situação de vulnerabilidade da população, pois a grande maioria das vítimas são pessoas com idade avançada ou que possuem pouco conhecimento sobre proteção de dados, de modo que se expõe em sites não seguros. E não

bastasse, ainda se tem a deficiência do ordenamento jurídico brasileiro sobre o tema, com dispositivos legais ultrapassados que pouco dispõe sobre essa nova modalidade de crime e as penas aplicadas são irrisórias, de modo que a grande maioria dos casos sequer chega a ser investigados, tampouco punidos.

Nesta senda, entende-se que há cibercrimes próprios e impróprios, esta é a definição trazida por Fichtelberg, ou seja, é dizer que o chamado cibercrime se divide na modalidade propriamente dita que são os casos em que os delitos são praticados e voltados a dispositivos eletrônicos e a internet em si. De outra sorte, os demais cibercrimes, ditos impróprios, tratam-se meramente de delitos comuns, porém que são praticados por meio da rede mundial de computadores e ali alcança maior potencial ofensivo.

Nota-se que a própria doutrina encontra dificuldade em definir e qualificar esse tipo penal, assim se torna difícil criar normativas específicas quando sequer há uma tipificação própria a cada delito. Ademais, quando se olha pelo aspecto dos cibercrimes impróprios, por assim dizer, que são crimes tradicionais, porém, na esfera digital se tornam mais lesivos e com alcance absurdamente maior, aqui, tem-se outro grave problema jurídico, pois não se pode tratá-los da forma tradicional.

Nota-se, portanto, que até mesmo as autoridades encontram dificuldades frente a essa questão, fato este que só reforça a vulnerabilidade das vítimas, as quais são ainda mais despreparadas e desnorteadas. Numa analogia esdrúxula, é o mesmo que entrar numa zona de guerra, sem nenhum equipamento e sem nenhuma noção do que acontece ao redor, isso é o que ocorre com a esmagadora maioria dos usuários comuns que navegam na internet.

O IRREFREÁVEL AUMENTO DO CIBERCRIME EM DECORRÊNCIA DA VULNERABILIDADE ACENTUADA DA POPULAÇÃO DURANTE A PANDEMIA DA COVID-19

O Isolamento Social como Fator Potencializador do Aumento do Número de Casos de Crimes Cibernéticos

Diante a situação de calamidade pública em decorrência da Covid-19, houve grande aumento nos casos de crimes digitais, esse é o diagnóstico feito pelo delegado e coordenador do Laboratório de Operações Cibernéticas do Ministério da Justiça e Segurança Pública, Alesandro Barreto, que em seu relato, fez uso do termo pandemia de crimes digitais, ressaltando que o cibercrime envolve diversos tipos de delitos, desde ataques a sistemas bancários até exploração sexual infantil.

Anterior a pandemia, em 2019, o Brasil já ocupava o terceiro lugar no ranking dos que sofrem mais ataques cibernéticos, de acordo com um relatório global divulgado pela *Symantec*. Porém, no ano seguinte, os números de casos de ciberataques cresceram consideravelmente, de acordo com a *Fortinet Threat Intelligence Insider Latin America*, empresa que analisa incidentes de segurança cibernética, o Brasil foi alvo de mais de 3,4 bilhões de tentativas de ataques na internet, de janeiro a setembro de 2020.

A pandemia da covid-19 causou uma série de problemas não só na questão da saúde, mas trouxe complicações severas em todos os setores sociais. Fato é que pouco se sabia, à época, sobre a doença, o que provocou medo e insegurança à população, que buscava de todas as formas se proteger do temível vírus. Deste modo, se operou um estado de pânico social em nível global, que somado ao isolamento social desencadeou os sentimentos de angústia, insegurança e medo, que podem se estender até mesmo após o controle do vírus (HOSSAIN *et al*., 2020).

No início da pandemia, houve registros do aumento em 41.000% de sites com termos relacionados a "coronavírus" e a "Covid" em seu domínio, notadamente, as pessoas buscavam na internet qualquer informação sobre a doença, e o medo e o desespero tornaram as vítimas ainda mais vulneráveis, o que facilitou a atuação criminosos. Outro ponto digno de menção, em pesquisa realizada pelo site CyberNews, no mesmo período, foi registrado um aumento de 66% na busca por páginas com conteúdos relacionados a golpes e invasões de dispositivos eletrônicos, mediante uso de pesquisas e buscas por expressões como, “como hackear” ou “como acessar a deepweb”, dentre outras.

Nesse ínterim, com o rápido e irrefreável avanço da pandemia, o governo foi forçado a adotar medidas extremas de controle e prevenção da doença, sendo determinado as medidas de isolamento social. É nesse ponto onde se encontra a principal relação entre o contexto pandêmico e o aumento do número de casos de crimes cibernéticos. Notadamente com o isolamento social, a população foi forçada a ficar em casa, permitindo sair apenas em situações de emergência, ou para repor suprimentos, porém, mesmo com a situação extrema, não se pode simplesmente parar a vida cotidiana, mesmo isolada a população ainda precisava trabalhar, estudar, se comunicar e interagir, o que só foi possível por meio da internet.

Segundo pesquisa realizada Comitê Gestor de Internet no Brasil, bem como pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação

(Cetic.br), a pandemia teria impactado diretamente no número de pessoas e domicílios com acesso à internet, de modo que no ano de 2020, cerca de 152 milhões de brasileiros estava conectados, o que representa 81% da população nacional com mais de 10 anos de idade, um aumento de 12 pontos percentuais. Por sua vez, a Agência Nacional de Telecomunicações (Anatel), pontuou que o uso da internet no Brasil cresceu algo em torno de 40% a 50%, durante o período de isolamento social.

Nesse mister é imperioso destacar que a internet se tornou o principal meio de trabalho, estudo e interação social, durante o período de isolamento, isso gerou um aumento no número de usuários, bem como no tempo em que as pessoas se mantinham conectadas, assim, a maioria dos serviços se operou por meio digital, principalmente os serviços de comunicações, compra e venda e movimentações financeiras. Durante esse mesmo período, cerca de 67% das transações bancárias foram realizadas por meios digitais, são dados da Febraban (Federação Brasileira de Bancos). Nesse passo, a instituição também apontou que as instituições financeiras registraram um aumento de 80% nas tentativas de ataques virtuais.

Proveitoso também destacar que o isolamento social trouxe uma série de problemas à população, que intensificou o estado de vulnerabilidade. Segundo pesquisas realizadas Laboratório Delete-Detox Digital e Uso Consciente de Tecnologias, da Universidade Federal do Rio De Janeiro (UFRJ), o isolamento social intensificou o estado de dependência tecnológica, fato este, que traz consigo uma série de psicopatologias, tais como estresse, depressão e ansiedade. Os fatores psicológicos só complementam o quadro de vulnerabilidade da população, atingido seu ápice durante o isolamento social, de modo que, não bastasse utilizar a internet para estudo e trabalho, a maioria das pessoas passou a utilizar dessa ferramenta de maneira desenfreada, e, quanto mais tempo conectado, mais exposto se torna.

De tal sorte, as pessoas de idade avançada e aqueles com pouco conhecimento tecnológico foram os mais impactados com essa mudança repentina, uma vez que foram forçados a se inserir no mundo digital. O impacto dessa mudança acentuou ainda mais a vulnerabilidade desse público, fazendo com que se tornem presas fáceis de golpes, ao acessarem sites falsos ou simplesmente por clicarem em links fraudulentos (*Phishing*). Um dado apresentado pela empresa Axur, que atua em monitoramento na internet, revela um ponto crucial que demonstra ainda mais a vulnerabilidade da população frente à

cibercriminalidade, que é a falta de informação e o descuido com os meios básicos de proteção, segundo estudo, no ano de 2021 a senha mais usada por brasileiros foi a sequência “123456”.

Diante todo esse contexto, é muito apropriada a denominação feita por Alesandro Barreto, de que se vive uma “pandemia de criminalidade digital”. Frente ao elevado número de pessoas conectadas e forçadas a utilizar a internet para quase todos os tipos de serviços, somando-se ainda com as questões psicológicas, tem-se a conjectura de que o isolamento social foi o principal propulsor do aumento da cibercriminalidade nos últimos dois anos.

Dados Sobre o Aumento do Número de Casos de Crimes Cibernéticos

Com o fito de corroborar a relação entre pandemia e cibercriminalidade, sustentando a tese de que o isolamento social foi agente motivador do aumento massivo do número de pessoas usando a internet e consequentemente gerou o aumento do número de casos. Segundo pesquisa da Fortinet Threat Intelligence Insider Latin America, o Brasil foi alvo de mais de 3,4 bilhões de tentativas de ataques na internet, durante a pandemia, foram registradas 156.692 denúncias anônimas, sendo estas lideradas pela pornografia infantil, 98.244 registradas, dados estes que levam em conta as notificações recebidas pela Central Nacional de Denúncias de Crimes Cibernéticos, uma parceria, da ONG Safernet Brasil com o Ministério Público Federal (MPF). Já os crimes cibernéticos de natureza financeira como invasão de computadores, roubo de senhas e dados bancários, além de golpes gerais de extorsão também aumentaram, conforme dados disponibilizados pela Federação Brasileira de Bancos (Febraban) houve um aumento de 80% nas tentativas de ataques virtuais na modalidade *Phishing*, bem como, cerca de 70% em de golpes de falso funcionário e de falsas centrais telefônicas e de 60% em tentativas de fraudes contra idosos.

Em relatório sobre Crimes Criptográficos da Chainalysis, empresa especializada em blockchain e que analisa o uso de criptomoedas em transações criminosas, revelou que durante a pandemia houve aumento de 311% nos pedidos de resgate por dados e sistemas sequestrados e que pelo menos 350 milhões de dólares foram pagos a grupos criminosos. Nas pesquisas realizadas pela ABINC (Associação Brasileira de Internet das Coisas),

revelam que houve aumento de 116% de casos de *ransomwares* registrados no Brasil, somando perdas alarmantes.

Por sua vez, Arthur Sabbat, Diretor do Conselho Diretor da ANPD (Autoridade Nacional de Proteção de Dados), pontuou que os crimes cibernéticos tiveram aumento de cerca de 300%, desde o início da pandemia. Relevante menção aos casos de crimes digitais praticados especificamente contra mulheres, os quais aumentaram vertiginosamente durante o período de isolamento social, com aumento de cerca de 80%, registrados 12.698 casos, envolvendo delitos contra honra e dignidade, ameaças, pornografia, uso indevido de imagem e *stalking.*

Outrossim, no ano de 2021, os números se continuaram crescendo em velocidade alarmante, conforme aponta pesquisa da consultoria alemã Roland Berger, o Brasil ocupou o quinto lugar no ranking de ataques por crimes cibernéticos, sendo registrados cerca de 9,1 milhões de ocorrências, apenas no primeiro trimestre, números estes maiores que os registrados em todo o ano anterior. Ainda equiparando os anos de 2020 e 2021, neste último houve aumento de, incríveis, 950%, uma vez que o país foi alvo de 88,5 bilhões de tentativas de ciberataques, conforme dados apontados pelo FortiGuard Labs (Laboratório de Inteligência de Ameaças da Empresa). Conforme dados da Axur, somente no ano de 2021 houve prejuízo mundial estimado em 6 trilhões de dólares, decorrentes da cibercriminalidade.

Ainda, pelos registros da Axur, em seu "Relatório de Atividade Criminosa Online no Brasil", revela que o Brasil liderou o ranking mundial em vazamento de dados, sendo registrados cerca de 2,8 bilhões de dados sensíveis expostos. O relatório registra também a exposição indevida de 273 milhões de credenciais, login e senha, no mesmo período.

Em contínuo, dados da empresa de cibersegurança Kaspersky, demonstram que no mesmo período foi registrado aumento de 23% nos casos de crimes cibernéticos no Brasil. Ademais, foi apontado que os cibercriminosos brasileiros atuaram diretamente em 481 milhões de tentativas de infecção por *malwares*, o que equivale a 1.395 tentativas por minuto. Desta forma, os dados apontados notadamente atestam o exponencial crescimento do número de casos de crimes cibernéticos durante o período pandêmico, não obstante, estes números apontam que a incidência desse tipo delitivo tende a crescer ainda mais, daí a importância de se discutir e criar medidas de combate ao cibercrime.

As Legislações Vigentes e Políticas Públicas Sobre o Tema

Em se tratando da legislação brasileira, cumpre destacar inicialmente o Marco Civil da internet, lei 12.965/2014, que possui 32 artigos que tratam sobre temas como os direitos e garantias dos usuários da internet e trouxe consigo dez princípios elaborados pelo Comitê Gestor da Internet brasileira, estabelecendo direitos e deveres aos usuários da rede. Destarte, a lei também estabeleceu um ponto extremamente importante, que diz respeito ao armazenamento de registros de acesso e de conexão, dados estes cruciais no processo investigativo para a identificação dos criminosos.

A legislação brasileira somente passou a prever condutas ilícitas praticadas por meio digital com a edição da Lei 12.737/2012, conhecida como Lei Carolina Dieckman, em razão da repercussão do caso envolvendo a atriz brasileira, a qual teve seu computador invadido e furtadas imagens pessoais de cunho íntimo, que foram utilizadas para extorsão. Outra normativa implementada no mesmo ano, também notória sobre o tema, é a lei 12.735, que dentre suas inovações também determinou a criação de delegacias especializadas em crimes digitais.

Assim, o Código Penal Brasileiro passou a tipificar o crime de Invasão de Dispositivo Informático, com a adição do artigo 154-A, aplicando pena de detenção, de 3 meses a 1 ano, e multa, a quem invadir dispositivo informático alheio, mediante violação de mecanismo de segurança para obter ou alterar informações. Todavia, apesar de a normativa ter sido considerada um avanço, ainda assim se mostra frágil e incompleta, pois para a conduta ser tipificada como crime, há a necessidade de violação de dispositivo de segurança para configurá-lo, ou seja, o delito fica condicionado à presença de barreira de segurança. Ademais, verifica-se que o acesso indevido, por si só não é punido, haja vista que o texto do artigo menciona a invasão como uma conquista ou meio para obtenção de dados ou informações, sendo necessário o invasor adultere ou destrua, tais dados sem o consentimento do proprietário. E não obstante o *quantum* da pena em abstrato é ínfimo, não condiz com a gravidade dos delitos dessa ordem.

Recentemente, na tentativa de suprir essas falhas foi promulgada a Lei 14.155, de 2021, que alterou o artigo 154-A, de modo a ampliar a incidência do tipo penal, bem como majorou a pena, que passou a ser de reclusão de 1 a 4 anos, e multa. A nova tipificação penal incorre quando há invasão de dispositivo de "uso alheio", e não há mais a condição de mecanismo de segurança, assim, a mera invasão, sem consentimento do usuário do

dispositivo já basta para configurar o tipo penal. Com efeito, a invasão propriamente dita, agora é vista como violação à privacidade alheia, e é punida nos termos do artigo, noutro aspecto, o crime do artigo 154-A deixa de ser de menor potencial ofensivo, como antes era tratado. A lei também alterou os artigos 155 e 171, acrescentando a fraude eletrônica como qualificadora.

No entanto, em que pese os avanços da normativa penal vigente, esta ainda não é suficiente e em razão disso tramita no Congresso Nacional o projeto de lei n° 236/2012, que tem por finalidade de instituir um novo Código Penal Brasileiro, uma vez que o código vigente foi publicado ainda na década de quarenta e até então houve substanciosas mudanças na sociedade, sobretudo no que diz respeito aos cibercrimes.

O referido projeto institui sete artigos específicos sobre delitos digitais, elencados do 213 ao 219, por exemplo o artigo 214 tipifica o delito de “acesso indevido”, ampliando ainda mais a incidência do tipo penal do artigo 154-A, em razão de que o atual preceitua a “invasão”. Nos demais artigos se discutem a obtenção de dados privados e sua divulgação, bem como a punição a quem comercializa, manipula ou vende artefatos maliciosos por meio da internet. E ainda pelo artigo 213, há a tipificação de diversos delitos, tais como o acesso indevido qualificado, dano a dados informatizados, fraude informatizada e obtenção indevida de credenciais de acesso a dados e artefato maliciosos, Além do que elenca as causas de excludente de ilicitude, com o fito de preservar os profissionais da informática e segurança eletrônica.

Cumpre ainda destacar também o Senado aprovou o projeto de decreto legislativo 255/2021, o qual faz a adesão do Brasil a Convenção sobre Crime Cibernético, conhecida por Convenção de Budapeste, que tem por finalidade facilitar a cooperação internacional no combate a esses delitos, implementando tipificação de condutas, normas para investigação e produção de provas. Este representa o primeiro tratado internacional sobre cibercriminalidade e já foi assinado por mais de sessenta países e já é utilizado como base e orientação para a legislação, representando um avanço no combate à nova era da criminalidade.

CONSIDERAÇÕES FINAIS

É inegável que a tecnologia se tornou imprescindível para a sociedade atual. Hoje, não se vislumbra o mundo sem a internet, uma vez que ela representa um dos principais

meios para a realização de diversas atividades. Contudo é de se registrar que por meio da internet adveio o grave problema dos cibercrimes, que são práticas crescentes e ganham cada vez mais adeptos em razão do elevado número de possíveis vítimas, bem como o anonimato do agente e a transnacionalidade, uma vez que o autor do delito pode praticá-lo de qualquer lugar do globo, pois não há fronteiras na internet.

De certo que durante a pandemia do novo coronavírus, a incidência de crimes cibernéticos alcançou números estratosféricos, fato este ocorrido em razão da própria pandemia. O isolamento social adotado como forma de controle da doença, deixou as pessoas confinadas em suas casas, forçando-as a utilizarem a internet, que se tornou o único meio de comunicação, estudo, trabalho, lazer e interação social. Desse modo, com o elevado número de pessoas logadas na rede, sobretudo pela acentuada vulnerabilidade causada pelo isolamento social, os criminosos se voltaram para a internet, pois era ali onde as pessoas se encontravam e realizavam suas atividades diárias. Não obstante, cumpre destacar que a própria população pouco sabe sobre o cibercrime e pouco faz para se proteger dele, isso se demonstra quando a senha mais utilizada por brasileiros no ano de 2021 foi a sequência de “1,2,3,4,5 e 6”.

Não bastasse o alto grau de exposição da maioria dos usuários da internet, a legislação pátria também não tomou a devida ciência da gravidade desses crimes, que representam a nova era da criminalidade e só tendem a crescer ainda mais. Das legislações vigentes, a lei 14.155/2021 é a mais expressiva, porém só prevê dois tipos penais, mas, ainda assim, a normativa representa um avanço, haja vista que a lei anterior era ainda menos incisiva.

Nessa seara, nota-se que o Brasil vêm buscando se adequar a essa nova realidade, sobretudo pelo projeto de lei 236/2012, o qual prevê uma reformulação do Código Penal brasileiro, que já se mostra obsoleto e não acompanha a evolução social. O referido projeto traz consigo ao menos sete artigos referentes a crimes cibernéticos, tipificando vários delitos que até então não são previstos no ordenamento jurídico pátrio.

Ademais, o Brasil recentemente aderiu a Convenção de Budapeste, a qual tem por finalidade a investigação e repressão do cibercrime, o que se fará mediante a cooperação internacional, haja vista que essa modalidade delitiva se caracteriza pela transnacionalidade, assim é necessário estreitar laços entre os países no intuito de maximizar o processo investigativo e punitivo.

REFERÊNCIAS

ANPD participa de seminário que discute o combate aos crimes cibernéticos. Gov.br, 2021. Disponível em <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-de-seminario-que-discute-o-combate-aos-crimes-ciberneticos/>. Acesso em: 02 de maio de 2022.

BALL, Peter. (2022). **Covid, 2 anos depois: 5 coisas que descobrimos desde o início da pandemia**. Disponível em <https://www.bbc.com/portuguese/brasil-59785767>. Acesso em: 08 de maio de 2022.

BARRETO, A. G., SANTOS, H. **Deep Web: investigação no submundo da internet**. 1. Ed. Rio de Janeiro: Editora Brasport. 2019.

BARRETO, A. G., KUFA, K., SILVA, M. M. **Cibercrimes e seus reflexos no direito brasileiro**. 2. ed. Salvador: Editora JusPODIVM. 2020.

BATISTA, João Pedro Thimotheo *et al* (2020). **Isolamento vertical e horizontal: entenda as diferenças.** Disponível em <https://coronavirus.saude.mg.gov.br/blog/74-isolamento-vertical-e-isolamento-horizontal>. Acesso em: 26 de março de 2022.

BATISTA, Rodrigo. (2021). **Lei com penas mais duras contra crimes cibernéticos é sancionada**. Agência do Senado. Disponível em <https://www12.senado.leg.br/noticias/materias2021/05/28/>. Acesso em: 09 de maio de 2022.

BEZERRA, Carina B. *et al*. (2020). **Impacto psicossocial do isolamento durante pandemia de covid-19 na população brasileira: análise transversal preliminar**. Disponível em <https://scielosp.org/article/sausoc/2020.v29n4/e200412/>. Acesso em: 26 de março de 2022.

BRASIL. Decreto-lei n° 2.848, de 07 de dezembro de 1940. **Código Penal**. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em 8 de maio de 2022.

BRASIL. Lei n° 12.737, de 30 de novembro de 2012. **Dispões sobre a tipificação de delitos informáticos**. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 08 de maio de 2022.

BRASIL. Lei n° 12.965, de 23 de abril de 2014. **Institui o Marco Civil da Internet**. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 08 de maio de 2022.

BRASIL. Lei n° 14.155, de 27 de maio de 2021. **Altera o Código Penal para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet**. Disponível em

<http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm>. Acesso em: 08 de maio de 2022.

CAMPOS, Ana Cristina. (2021). **Covid-19, 98,6% dos municípios adotaram o isolamento social**. Agência do Brasil. Disponível em <https://agenciabrasil.ebc.com.br/saude/noticia/2021-11/covid-19-986-dos-municipios-adotaram-isolamento-social-em-2020>. Acesso em: 26 de março de 2022.

COSTA, Dionatan. (2020). **A incidência dos crimes virtuais em tempos de isolamento social**. Disponível em < https://jus.com.br/artigos/85629/a-incidencia-dos-crimes-virtuais-em-tempos-de-isolamento-social >. Acesso em: 09 de maio de 2022.

Crimes cibernéticos triplicam em 2021 e extorsão digital entra na rotina do brasileiro. tiinside.com.br, 2021. Disponível em <https://tiinside.com.br/26/08/2021/crimes-ciberneticos-triplicam-em-2021-e-extorsao-digital-entra-na-rotina-do-brasileiro/>. Acesso em 08 de maio de 2022.

Denúncias de crimes cometidos pela internet mais que dobram em 2020. G1.globo.com, 2021. Disponível em <https://g1.globo.com/economia/tecnologia/noticia/2021/02/09/numero-de-denuncias-de-crimes-cometidos-pela-internet-mais-que-dobra-em-2020.ghtml>. Acesso em 02 de maio de 2022.

FICHTELBERG, Aaron. **Crime without borders: an introduction to international criminal justice**. New Jersey: Pearson Prentice Hall. 2008.

GASTAL, Mariana. (2021). **Crimes Cibernéticos e a pandemia de Covid-19**. Disponível em <https://www.wlm.org.br/crimes-ciberneticos-e-a-pandemia-de-covid-19/>. Acesso em: 02 de maio de 2022.

LÉON, Lucas Pordeus. (2021). **Brasil tem 152 milhões de pessoas com acesso à internet**. Agência do Brasil. Disponível em <https://agenciabrasil.ebc.com.br/geral/noticia/2021-08/brasil-tem-152-milhoes-de-pessoas-com-acesso-internet>. Acesso em: 02 de maio de 2022.

MAIA, B. R., DIAS, P. C. (2020). **Ansiedade, depressão e estresse em estudantes universitários: o impacto da COVID-19**. Estudos de Psicologia (Campinas), 37, e200067. Disponível em <http://dx.doi.org/10.1590/1982-0275202037e200067>. Acesso em 26 de março de 2022.

NOVO, Benigno Nuñez. **A primeira vacina contra o coconavírus(COVID-19): Rússia parte na frente**. Disponível em <https://meuartigo.brasilescola.uol.com.br/saude/a-primeira-vacina-contra-o-coronavirus-covid-19-russia-parte-na-frente.htm>. Acesso em: 26 de março de 2022.

PORFIRIO, Francisco. **Cyberbullying.** Mundo educação. Disponível em <https://mundoeducacao.uol.com.br/sociologia/cyberbullying.htm>. Acesso em 02 de maio de 2022.

SANTANA, esther. (2020). **Isolamento social**. Disponível em <https://www.educamaisbrasil.com.br/enem/sociologia/isolamento-social>. Acesso em: 26 de março de 2022.

SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**. São Paulo: Revista dos Tribunais, 2003.

Vacinação contra a COVID-19 no Brasil. Wikipédia.org. Disponível em <https://pt.wikipedia.org/wiki/Vacinação_contra_a_COVID-19_no_Brasil>. Acesso em: 26 de março de 2022.

ZORETTO, Ricado. (2020). **Mudanças causadas pela covid-19 aumenta o sofrimento e transtornos mentais**. Disponível em <https://www.uol.com.br/vivabem/noticias/redacao/2020/08/10/mudancas-caudas-pela-covid-19-aumentam-sofrimento-e-transtornos-mentais.htm>. Acesso em: 26 de março de 2022.