CIBERCRIMES E PANDEMIA

Breves reflexões

CYBERCRIMES AND PANDEMIC

Brief reflections

JOÃO MARCELO DE PAIVA BRANDÃO[1]

MARIA EDUARDA VIEIRA MOURA[2]

Resumo: O presente artigo trata da ocorrência de crimes cibernéticos no contexto da pandemia da COVID-19 no Brasil. Em função da atipicidade desse período de crise sanitária, mostra-se válido analisar qualitativamente de que maneira fatores intrínsecos ao momento atual, tais como a vulnerabilidade emocional, o distanciamento social, o *e-commerce*, o trabalho remoto e a maior virtualização de atividades em geral criaram condições favoráveis para a realização desses delitos. Pontuam-se, mediante a citação de cada tipo de crime, fatores – alvos, meios, finalidades e facilitadores – que perpassam a atuação dos criminosos, esclarecendo inclusive a engenharia social diretamente envolvida nos ilícitos. Traça-se uma pormenorização sobre a fraude no Auxílio Emergencial, crime peculiar ao cenário de excepcionalidade de saúde pública, advinda pela circulação do novo coronavírus. Diante de todas essas questões, evidencia-se a crescente necessidade de informar e conscientizar a população sobre os riscos da utilização da *internet*, alertando para os graves perigos e efeitos nocivos dos cibercrimes, que debilitam não só a sociedade civil, mas as instituições privadas e o Estado Brasileiro como um todo.

Palavras-chave: cibercrimes; pandemia; *internet*; covid-19.

Abstract: This article addresses the occurrence of cybercrimes in the context of the COVID-19 pandemic in Brazil. Given the atypical situation noted in this period of sanitary crisis, it is valid to analyze qualitatively how factors related to the current moment, such as emotional vulnerability, social distance, e-commerce, remote work and the greater virtualization of most activities, created propitious conditions to the carrying out of these crimes, which were intensified in the year of 2020. It examines, in each type of crime, factors - targets, means, purposes and facilitators - that surround the activities of criminals, clarifying even the social engineering directly involved in the illicit acts. For example, it is given a criminal detail about the fraud in Emergency Aid, a typical and exclusive crime in the exceptional public health scenario, due to the circulation of the new coronavirus. In light of all these issues, there is a growing need to inform and make the population aware of the risks of using the Internet, alerting to the serious dangers and harmful effects of cybercrimes, which weaken not only civil society, but private institutions and the Brazilian State as a whole.

Keywords: cybercrimes; pandemic; internet; covid-19.

[1] Graduando em Direito pela UFMG. E-mail: jmarcelopaiva@gmail.com.

[2] Graduanda em Direito pela UFMG. E-mail: mariaeduardav.moura@hotmail.com.

1. INTRODUÇÃO

As últimas décadas do século XX e mais especialmente o século XXI trouxeram consigo uma mudança paradigmática sem precedentes: a implementação do que o alemão Klaus Schawab convencionou chamar, no Fórum Econômico Mundial de 2016, como 4ª Revolução Industrial. Nas palavras dele, "*technological Revolution that will fundamentally alter the way we live, work, and relate to one another*"[3] (SCHAWAB, 2016), ou seja, a ascensão de sistemas tecnológicos nunca vistos em termos de alcance, velocidade e impacto transformou a existência do ser humano, havendo uma constante necessidade de adaptação a novos contextos e desafios que se projetam na vivência individual e coletiva.

Se nos anos 1800, verificou-se a supremacia de máquinas operadas manualmente nas fábricas inglesas, apenas duzentos anos depois, a mente humana é força direta de produção, não apenas um elemento decisivo no sistema produtivo (CASTELLS, 1999, p. 69). Nesse sentido, o chamado "terceiro milênio" é marcado pela centralidade de múltiplas formas de tecnologias desenvolvidas e aprimoradas pelo o homem, que passam a figurar indissociavelmente da vida cotidiana das pessoas, designando ferramentas indispensáveis para a sobrevivência moderna.

Grande exemplo é a própria *internet*. Desenvolvida nos Estados Unidos no contexto da Guerra Fria, só foi mais popularizada no nosso país a partir dos anos 2000 e hoje representa aparato básico e primordial na realização de atividades do dia a dia da maioria dos brasileiros. Segundo dados coletados no levantamento TIC DOMICILIOS 2019, relevante pesquisa exercida pelo Centro Regional para o Desenvolvimento de Estudos sobre a Sociedade da Informação (Cetic.br), três a cada quatro brasileiros usam a *internet*, o que representa cerca de 134 milhões de pessoas conectadas constantemente.

Se por um lado, a democratização do acesso à *internet* no Brasil permitiu interações em rede de boa parte da população, por outro, foi circunstância preponderante para a potencialização dos perigos e ilícitos no ambiente virtual. Tomando por base a premissa de que "boa parte das ameaças a que os cidadãos estão expostos provêm de decisões que outros cidadãos adotam no manejo dos avanços tecnológicos" (Aragão, 2014, p.15), vislumbra-se o incremento maciço da ocorrência dos chamados crimes cibernéticos no país, havendo, assim, uma crescente necessidade de implementação de políticas públicas que possam atenuar a disseminação dessas práticas danosas, típicas de uma "sociedade de riscos", tal como cunhou o sociólogo alemão Ulrich Beck na década de 80.

---

[3] Tradução livre: Revolução tecnológica que alterará a forma de viver, trabalhar e relacionar uns com os outros.

Sem efetivo consenso de denominação e nomenclatura na doutrina jurídica, segundo a Organização para a Cooperação Econômica e Desenvolvimento (OECD) da Organização das Nações Unidas (ONU), o "crime de computador é qualquer comportamento ilegal, aético, ou não autorizado envolvendo processamento automático de dados e, ou transmissão de dados" (ARAS, 2001). Já a jurista Maria de La Luz (1984) pontua que, em uma perspectiva ampla, o delito eletrônico seria a conduta criminal que conta com o emprego de tecnologia como método, meio ou fim enquanto, em um recorte específico, o crime digital seria qualquer ato ilícito no qual os computadores, suas técnicas e funções atuem como método, meio e fim.

Em verdade, a busca pela conceituação da criminalidade cibernética vai diretamente de encontro com as múltiplas formas de conectividade em consonância com as recentes tecnologias ainda em desenvolvimento. Verifica-se, desse modo, um contato ainda prematuro do Direito com essa vasta gama de conceitos e bens jurídicos, que passam a demandar o desenvolvimento de uma tutela especial de proteção.

No âmbito da normatização já existente, como as práticas ilícitas que defrontam com os direitos advindos da era das tecnologias não constavam, naturalmente, no Código Penal Brasileiro de 1940, foi pertinente a criação de legislação específica para versar sobre tais questões, o que só começou a acontecer a partir do ano de 2012. Dessa forma, esse atraso na positivação de leis que abordem os cibercrimes demonstra a tratativa ainda pouco consolidada do aparato estatal brasileiro no combate aos delitos na *internet*.

No entanto, é importante ressaltar que, dados os constantes avanços e aprimoramentos em termos de domínio tecnológico, os crimes são altamente dinâmicos e mutáveis, o que justifica a dificuldade dos códigos em realizar tipificações precisas e que abarquem todo o arcabouço dos ilícitos virtuais, gerando, desse modo, uma constante necessidade de complemento ou até mesmo modificação das leis já positivadas no ordenamento jurídico.

Em primeira análise, a ex-presidente Dilma Rousseff sancionou a Lei dos Crimes Cibernéticos (12.737/2012), que tipifica criminalmente delitos informáticos, como violação de dados, a invasão de computadores e a derrubada de sites. Popularmente denominada como lei Carolina Dieckmann, a legislação teve grande repercussão em virtude do caso de divulgação de fotos íntimas da atriz. No mesmo ano, também recebeu a sanção presidencial a Lei 12.735/12, que, por sua vez, tipifica as práticas realizadas a partir da utilização de sistemas digitais, eletrônicos e afins em detrimento de sistemas informatizados. Tal lei estipula ainda o estabelecimento de delegacias especializadas, importante passo na ofensiva de combate e apuração dos cibercrimes.

Dois anos depois, já em 2014, foi promulgada a Lei do Marco Civil (LMC), que modificou a nossa legislação atribuindo direitos e deveres aos usuários das redes, às organizações e ao aparato estatal. Trata-se de uma normatização fundamental para a tutela jurídica de dados e de arquivos privativos dos internautas, informações essas que só podem ser obtidas mediante ordem judicial de quebra de dados. Em paralelo, pela Lei 12.965/2014 também ficou instituído que a retirada de conteúdos da *internet* deve ocorrer por meio de ação judicial. Em resumo,

> Essa lei estabelece normas para a proteção da privacidade, seja em relação à guarda e ao tratamento de registros, dados pessoais ou comunicações por sites ou empresas que prestem serviços de acesso à *internet*, seja em relação à forma como essas informações devem ser disponibilizadas ao cidadão (MPMG, 2019, p. 7).

Apesar das citadas adequações na legislação brasileira para o preenchimento de lacunas normativas no que diz respeito ao combate e a punição de crimes cibernéticos, após a instauração do Marco Civil, notou-se um acréscimo alarmante dos registros absolutos de delitos virtuais. Essas práticas cresceram significativamente na segunda metade da segunda década do século XXI, urgindo a realização de mais iniciativas por parte do Poder Público para o enfrentamento da problemática.

No presente artigo, optou-se pelo direcionamento do enfoque analítico para o contexto da pandemia da Covid-19, momento histórico de exacerbação de dilemas sociais que já assolavam a humanidade mesmo antes da excepcionalidade sanitária. Segundo dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), só no primeiro semestre de 2020, foram reportados 318.697 casos de cibercrimes. A maior novidade nesse levantamento refere-se ao registro de notificações que dizem respeito exclusivamente a temáticas da pandemia, como por exemplo, a incidência de tentativas de fraudes no Auxílio Emergencial.

A modalidade de crimes cibernéticos que será abordada pode ser classificada como engenharia social, ou seja, prática na qual criminosos utilizam de técnicas específicas e personalizadas para cada tipo de delito, visando com que a vítima acredite nas informações transmitidas e se convença a fornecer dados ou realizar transações financeiras (JORGE, WENDT, 2013). Há nessa modalidade, a utilização de dois mecanismos para que a vítima creia na veracidade da relação desenvolvida. O primeiro trata-se da utilização da identidade de instituições confiáveis, como grandes lojas, bancos, órgãos do governo. Por outro lado, a depender do cibercrime, o criminoso investe nas vulnerabilidades da vítima e do sistema informatizado. Ambas as formas são potencializadas pela desinformação acerca de como utilizar a *internet* de forma segura (JORGE, WENDT, 2013).

Dessa maneira, o objetivo deste artigo consiste na exposição qualitativa da ocorrência de cibercrimes no período de ascensão do novo coronavírus. Busca-se enfatizar, sobretudo, o entrelaçar entre a disseminação de atos criminosos pela *web* e a nova dinâmica social advinda do cenário restritivo de isolamento. Além disso, vale ponderar que não se trata de um estudo que tem por intuito esgotar a temática, pelo contrário: por ser uma relação de causas e consequências ainda pouco delineadas em suas múltiplas dimensões, evidencia-se como necessária a elaboração de abordagens científicas posteriores que possam continuar as reflexões e proposições aqui iniciadas.

Utilizando como ferramenta metodológica a explanação pormenorizada de alguns exemplos de delitos virtuais altamente contabilizados no contexto pandêmico, o estudo por nós desenvolvido anseia traçar rotas de encontro entre os cibercrimes e o quadro brasileiro de excepcionalidade no ano de 2020. Um efeito possível a partir dessa incipiente análise é o incentivo ao aguçamento do olhar de juristas e cientistas sociais acerca de como a mudança significativa de hábitos e costumes da população brasileira pôde contribuir frontalmente para a multiplicação de atos ilícitos na esfera virtual.

Ainda imersos na calamidade, vale, em síntese, dizer do imenso valor de investigações que se aventurem em debruçar sobre processos históricos ainda em andamento, o que agrega ainda mais relevância na tentativa de pareamento teórico-pragmático entre a pandemia e os cibercrimes.

2. A PANDEMIA E SUAS IMPLICAÇÕES

Segundo a revista científica inglesa *The Lancet*, no dia 1º do mês de dezembro de 2019, foi registrada, pela primeira vez, a ocorrência de uma "pneumonia" de características bastante singulares em Wuhan, na China. Apesar de uma imprecisão na delimitação de uma data exata, consenso entre os pesquisadores é que os relatos iniciais fornecidos às autoridades sanitárias locais já alertavam para o surgimento de uma infecção altamente contagiosa, que se espalhava rapidamente para dezenas de pessoas na capital da província de Hubei.

Tragédia anunciada, cerca de um mês depois de um dos primeiros registros de contaminação, a Organização Mundial da Saúde (OMS) foi notificada da ocorrência de uma doença altamente infecciosa, que ocasionava febre, dores no corpo, tosse seca e grave falência dos pulmões. Mediante o acréscimo descontrolado do número de contaminados e de mortos por todo o planeta, em fevereiro, a organização denominou a enfermidade como Covid-19 e decretou o estabelecimento de uma pandemia, dando início ao contexto de calamidade sanitária que vai marcar profundamente o século XXI.

Desde então, a dinâmica de vida das pessoas alterou-se essencialmente. Constatado que a transmissão do novo coronavírus ocorre principalmente por intermédio de gotículas de saliva de indivíduos contaminados, fez-se necessária a implementação do uso contínuo de máscara e do distanciamento social. Desse modo, já em março de 2020, duas práticas entraram com destaque nos noticiários brasileiros: a quarentena e o *lockdown*.

O primeiro termo citado diz respeito à postura a ser adotada por quem esteve em regiões com alto índice de infecções por Covid 19 ou teve contato direto com algum doente, buscando-se com isso a não propagação do vírus, em eventual caso de infecção do indivíduo em questão. Já o *lockwonw* refere-se a uma medida mais drástica adotada pelas cidades para minimizar a curva de infectados, aliviando o sistema de saúde municipal. Permite-se o funcionamento apenas do serviço essencial, como farmácias, açougues, supermercados e padarias, havendo o fechamento de todo o restante do comércio, com o intuito de diminuir aglomerações.

Assim sendo, muitas foram as consequências geradas pelas múltiplas imposições na circulação de pessoas. Sob esse ponto de vista, vale ponderar o quanto as mudanças no fluir natural da vida dos brasileiros trouxeram consigo cenário favorável para o alargamento da ocorrência de cibercrimes. O cerne dessa questão pandêmica reside na utilização de aparato digital para a prática de objetivos delituosos que já estavam presentes no Código Penal, como a fraude, a extorsão e o abuso sexual etc., vindo à tona não só uma realidade de calamidade pública de saúde como de ameaça ao uso seguro de plataformas tecnológicas.

De imediato, o efeito talvez mais notável da pandemia da Covid-19 foi a maior permanência das pessoas dentro de suas residências. Mediante o fechamento de escolas e faculdades, a restrição no funcionamento do comércio em geral e o estabelecimento do trabalho remoto, dentre outros aspectos, os brasileiros mudaram a rotina, permanecendo muito mais tempo em casa. No município de Belo Horizonte, por exemplo, em meados de março de 2020, o índice de isolamento chegou ao patamar de 62% (G1, 2020), demonstrando uma permanência de cidadãos nas ruas muito abaixo dos parâmetros convencionais dos "tempos de normalidade".

Tal confinamento ocasionou um acréscimo no tempo de ócio das pessoas, que, sem as suas habituais atividades cotidianas, passaram a recorrer à *internet* e muito especialmente às redes sociais para simplesmente "passar o tempo". Segundo pesquisa da Kantar, empresa de consultoria de mercado, a utilização do aplicativo de mensagens *WhatsApp* aumentou, em índices de até 76% pelo mundo. O *Facebook* e o *Instagram*, por sua vez, contaram com acréscimos de uso na casa dos 40%, aproximadamente. Assim sendo, o maior consumo de redes virtuais de relacionamento abriu espaço para a expansão dos delitos que são próprios dessas plataformas, tal como subtração

financeira de estelionatários e a própria pornografia infantil, crimes cibernéticos mais bem destrinchados no próximo tópico do artigo.

Além disso, não podemos nos esquecer que o panorama geral de anormalidade e o confinamento coletivo propiciaram uma degradação sem precedentes da saúde mental das pessoas. O fenômeno foi identificado como "fadiga pandêmica" pela OMS e diz respeito a uma desmotivação exacerbada frente a todas as pautas ligadas ao contexto de disseminação da Covid-19. Piorando ainda mais a estabilidade emocional, o isolamento do convívio em sociedade também contribuiu para o acirramento das vulnerabilidades e carências das pessoas, que, sentindo-se sozinhas, passaram a ser alvos mais suscetíveis a crimes na *internet* no âmbito dos "golpes do amor" e afins.

Em um viés mais econômico, a pandemia do novo coronavírus acirrou a desestabilização financeira mundial, demandado enérgicas ações dos governos para contornar a problemática. Só no Brasil, 879 mil pessoas ocupadas e afastadas deixaram de receber remuneração e 19,6% das pessoas ocupadas tiveram rendimento menor do que o normalmente recebido (IBGE, 2020). Esse cenário gerou a criação do chamado Auxílio Emergencial, instituído pela Lei nº 13.982, de 2020, que se trata de um benefício concedido pelo Governo Federal destinado aos trabalhadores informais, microempreendedores individuais (MEI), autônomos e desempregados. A solicitação do auxílio é, também, condicionada à maioridade, desemprego e pertencimento à família cuja renda mensal por pessoa não ultrapasse meio salário-mínimo (R$ 522,50), ou cuja renda familiar total seja de até 3 (três) salários-mínimos (R$ 3.135,00). Segundo o IBGE, 41% dos domicílios brasileiros receberam o benefício (IBGE, 2020). Sendo o dinheiro fornecido por meio online, observou-se também a multiplicação de crimes de usurpação da quantia.

Em seguida, vale notar que as restrições aos grandes centros comerciais (como shoppings e grandes lojas) propulsionaram a opção dos consumidores pela compra de serviços e produtos ofertados via *internet*, inaugurando o triunfo do chamado *e-commerce*. Considerando ainda o contexto de menor circulação de bens físicos em paralelo com a injeção de dinheiro na economia em função do auxílio emergencial, segundo o Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE), o *e-commerce* tornou-se a melhor opção de venda, pois o consumidor recebe o produto em casa, sem contato físico (SEBRAE, 2020). Apesar dos enormes ganhos em termos de praticidade, essa maior recorrência às denominadas compras online ocasionou a multiplicação de delitos virtuais ligados à prestação virtual de serviços, dentre os quais cita-se o golpe do site fraudulento e do falso e-mail. Como as centrais de atendimento de consumidores passaram a ser

digitais, podemos citar ainda o alargamento da clonagem de *WhatsApp* como produto da hegemonia do *e-commerce*.

Por fim, no ano de 2020, a utilização do teletrabalho como medida de segurança sanitária foi uma realidade para muitas empresas em todo o mundo. Somente no Brasil, cerca de 7,9 milhões de pessoas trabalharam remotamente de maio a setembro de 2020 (IBGE, 2020). Essa necessidade ocasionou na implantação de sistemas, redes e aplicativos com vistas a adaptar a atuação das empresas ao novo modelo de trabalho. Tal questão será explanada adiante a fim de mostrar que é, também, um dos fatores decorrentes do período pandêmico que possibilitaram a ocorrência maior de crimes cibernéticos.

3. EXEMPLOS DE CRIMES CIBERNÉTICOS NA PANDEMIA

População, instituições e empresas têm utilizado novas tecnologias, subsidiadas pela *internet*, para tornar quaisquer tipos de relações mais ágeis, econômicas e menos burocráticas a partir da virtualização de processos. No período pandêmico, essa demanda fez-se potencialmente mais necessária, tendo em vista as medidas de restrição do comércio e da circulação de pessoas. O comércio virtual, por exemplo, mostrou-se uma alternativa a empresas que tiveram sua atuação presencial prejudicada pelas políticas de isolamento social. Proporcionalmente, o aumento da utilização de serviços virtuais provocou intensificação na ocorrência de cibercrimes (INTERPOL, 2020, p.4). Diante disso, criminosos aproveitam dessa conjuntura de aumento de trocas financeiras em ambiente virtual e das vulnerabilidades decorrentes do período de crise sanitária para aplicar diversas modalidades de crimes.

Dentre eles, é possível pontuar o golpe do site fraudulento que é de grande recorrência e tem como alvo clientes de um site de comércio eletrônico. Os golpistas desenvolvem um site semelhante a um determinado site de vendas verídico e as vítimas, atuando em erro por acreditar se tratar do site original, efetuam compras e realizam pagamentos via boleto bancário, cartão de crédito, depósito em conta ou transferência. Entretanto, os compradores não recebem as mercadorias compradas ou contratadas (ACADEPOL, 2020) tornando-se vítimas ao serem induzidos a esses sites fraudulentos por meio de spams, propagandas via links patrocinados, anúncios em sites de compras coletivos, bem como por ofertas de produtos muito procurados com preços muito inferiores àqueles adotados no mercado (CERT.br, 2017). Nesse âmbito, a concretização do crime é potencializada em função da falta de informações sobre a necessidade de conferir os requisitos básicos de segurança, a fim de atestar a veracidade dos sites.

Ainda na modalidade de vendas virtuais, outro delito cometido se dá por meio do golpe do falso e-mail em sites de vendas online. A vítima, nesse caso, é aquela pessoa que anuncia algum produto em plataformas digitais, como Mercado Livre. Assim, o criminoso, sob falsa pretensão de obter mais informações sobre o produto, solicita o telefone e e-mail da vítima. Com isso, o vendedor recebe um e-mail semelhante ao do site no qual seu produto foi anunciado informando que a venda foi concluída e o produto deve ser enviado para determinado endereço (ACADEPOL, 2020). A vítima, portanto, envia o produto para o golpista e só se dá conta do golpe ao não receber o pagamento pelo produto vendido.

Ademais, a pandemia fez com que serviços de atendimento ao consumidor também fossem realizados de forma virtual, pois diversas empresas de telemarketing tiveram que reduzir o pessoal em trabalho remoto. Essa condição favoreceu a ocorrência de outro cibercrime, a clonagem de *WhatsApp*. Nesse delito, o golpista entra em contato com a vítima por meio das redes sociais se passando pela empresa e oferece serviços de atendimento ao consumidor. Para consumação do atendimento, o infrator solicita o número de telefone da vítima e diz que a empresa enviará um código que deverá ser informado no chat. Porém, o que realmente acontece é que, mediante o número de telefone, o golpista tenta acessar a conta de *WhatsApp* da pessoa, o que automaticamente envia para esta um torpedo SMS com um código que libera o acesso ao aplicativo. Quando esse código é informado ao criminoso, ele tem acesso ao *WhatsApp* da vítima e passa-se por ela em conversas com amigos e família e solicita o pagamento de algum boleto ou depósito bancário, afirmando estar com dificuldades financeiras ou ter dificuldades de realizar transações monetárias virtualmente. Assim, os contatos da vítima, acreditando estar conversando com ela, realizam o pedido e o crime é consumado.

Criminosos, ainda, aproveitam-se do aumento da vulnerabilidade e redução da segurança dos sistemas empresariais, decorrentes dos impedimentos impostos pela pandemia, para roubar dados (INTERPOL, 2020). Essa modalidade de crime é popularmente conhecida como *Sniffer* e objetiva monitorar, bem como interceptar todos os dados processados em uma rede. Com isso, os cibercriminosos tomam conhecimento de logins e senhas de usuários de determinados sites, além de informações sobre conteúdos de e-mails, áreas de redes vulneráveis e informações sigilosas (JORGE, WENDT, 2013, p.34). Esses dados são utilizados para fraudes e obtenção de vantagens financeiras.

Como já supracitado, outro fenômeno comum em decorrência da pandemia é a busca de contato virtual para suprir relações pessoais que foram limitadas pelo isolamento social, uma necessidade para conter o avanço da doença. Crimes provenientes de relacionamentos na *internet* já

eram comuns, porém, nesse período, o aumento de relações virtuais, proporcionalmente, intensificou a ocorrência de crimes dessa natureza. Isso se dá, pois esse período de crise de saúde alterou as relações sociais, o que tornou as pessoas emocionalmente vulneráveis e sensíveis, já que muitas delas foram afastadas de seus empregos presenciais, do contato com a família e amigos e de momentos de lazer. Por um lado, as vítimas buscam as redes sociais e o ambiente virtual para sanar a necessidade de contato com outras pessoas, mas, por outro lado, os golpistas de aproveitam desse momento para abusar e extorquir indivíduos fragilizados.

Jovens, que já representavam um significativo contingente de usuários da *internet*, aumentaram sua exposição nas redes em função de medidas de isolamento social (COUTINHO, DESLANDES, 2020, p.4). Além disso, a OMS, por meio do guia "COVID-19 *parenting*" recomenda que o uso da *internet* é essencial para o desenvolvimento social nesse período de pandemia. Entretanto, os criminosos aproveitam desse panorama com o fim de abusar de crianças. Segundo relatório da *The International Criminal Police Organization* (INTERPOL) sobre crimes cibernéticos na pandemia, o continente americano registrou um aumento de imagens no comércio virtual de exploração infantil (INTERPOL, 2020). A pornografia infantil é crime estabelecido pelos artigos 240 a 241-E do Estatuto da Criança e do Adolescente (Lei nº 8.069, de 13 de julho de 1990). Esses dispositivos normativos criminalizam a prática de produzir, fotografar, filmar, vender, oferecer, trocar, divulgar ou publicar, adquirir, possuir ou armazenar em qualquer meio de comunicação, incluindo a *internet*, esse tipo de conteúdo.

As investigações acerca desse tipo de delito verificam que os criminosos interceptam vítimas por meio de jogos virtuais, redes sociais e aplicativos de mensagens (ACADEPOL, 2020). Eles fazem uso de perfis falsos e se passam por crianças e adolescentes e, a partir disso, obtém informações sobre rotina e gostos das vítimas, criando, assim, uma relação íntima. Isso gera um ambiente de confiança, adequado para induzir o fornecimento de imagens íntimas. Em alguns casos, o abusador ameaça a família e amigos da criança por meio de chantagem com informações que foram acumuladas durante as conversas com a vítima (ACADEPOL, 2020).

No entanto, não só crianças são vítimas de cibercriminosos na *internet*, o golpe do amor pode ser exemplificado nesse contexto de pandemia. Ele se trata da abordagem por criminosos por meio de perfis falsos em redes sociais ou sites de relacionamentos e, após certa intimidade, constroem com a vítima uma falsa relação de namoro virtual. Os golpistas, diante de diversas declarações de amor, relatam problemas financeiros à vítima, alegam precisar de dinheiro para alguma finalidade específica – que muitas vezes é dotada de caráter emocional – e pedem ajuda para resolver o problema. A vítima, iludida e apaixonada, envia a quantia solicitada ao infrator por

meio de transferências bancárias. Esse crime prolonga-se por muito tempo sem ser descoberto até que os falsos namorados desaparecem, porém, nesse momento, já houve perda de muito dinheiro.

Em outra vertente de análise, seguindo a tendência de virtualização do fornecimento de diversos serviços, em decorrência do isolamento social na pandemia, o recebimento do Auxílio Emergencial deu-se, exclusivamente, de forma online por meio de um aplicativo ou site do programa. A partir da aprovação do benefício, o pagamento era efetuado em uma Conta Poupança Social também por um aplicativo, o Caixa Tem (CAIXA ECONÔMICA FEDERAL, 2020). A virtualização do processo de fornecimento da quantia emergencial pelo governo favoreceu a ocorrência de cibercrimes mediante processo de fraude no recebimento do auxílio. Os crimes aconteciam, geralmente, a partir da obtenção do CPF da vítima e, com ele, os fraudadores entravam no aplicativo e solicitavam o auxílio. A partir do recebimento, eles faziam transferências ou pagamento de boletos emitidos pelos golpistas em nome deles. Dessa forma, o auxílio chegava na conta do infrator, lesando não só o Estado, mas, também, aquele indivíduo que ficou impedido auxílio.

O Governo Federal determinou que a Polícia Federal (PF) e o Ministério Público Federal atuassem em casos graves de fraudes no recebimento do auxílio e que envolvam grupos criminosos por meio de um banco de dados que conteria renda, patrimônio pessoal e participação em empresa. A Caixa Econômica Federal (CEF) ficou responsabilizada pela confirmação da ocorrência de pagamento fraudulento do auxílio emergencial. Se o banco confirmar que houve fraude no pagamento, remeterá os dados à PF para integrar a Base Nacional de Fraudes ao Auxílio Emergencial (BNFAE), criada pela PF, que possibilitará a investigação da atuação de grupos criminosos (GOVERNO DO BRASIL, 2020). Operações de prisão e busca e apreensão foram realizadas em 14 estados e conseguiu bloquear 3,82 milhões de pedidos fraudados do auxílio, que somam o valor de R$ 2,3 bilhões (G1, 2020).

Segundo a Organização dos Estados Americanos (OEA), em conjunto com a empresa de segurança cibernética Symantec, o Brasil está dentre os principais países da América Latina que mais geraram atividades nocivas pela *internet*. Porém, é o país que menos registra denúncias e punições para a prática dos cibercrimes (OEA, SYMANTEC, 2014). Essa conjuntura de poucas denúncias e punições é causada, pois vítimas de crimes virtuais não comunicam a ocorrência desses delitos às autoridades competentes (SILVA, 2020), o que é somado à insuficiência estatal na aplicação da legislação vigente. No contexto pandêmico, essa realidade tende a se acentuar, já que apesar da possibilidade da realização dos Boletins de Ocorrência de forma virtual, poucas pessoas conhecem essa possibilidade, tendo em vista que a significativa parte das denúncias são feitas

presencialmente por meio de Boletim de Ocorrência em delegacias especializadas e, ao adotar medidas de segurança, as pessoas tendem a evitar sair de casa por motivos que não sejam essenciais.

A falta de denúncias acerca de delitos cibernéticos corrobora para um contexto que viabiliza a incidência desse tipo de crime, bem como traz ônus para as vítimas e, também, para o Estado. Com as fraudes do auxílio emergencial, por exemplo, a Polícia Federal recuperou mais de dois bilhões de reais que, caso os crimes se efetivassem de forma impune, seriam perdidos, o que impossibilitaria a plena execução de garantias sociais e usurparia direitos de indivíduos vulneráveis. Além disso, a recorrente falta de informações sobre como identificar e não ser vítima desses golpes possibilita, cada vez mais, a ocorrência dessa modalidade de crime.

CONSIDERAÇÕES CONCLUSIVAS

A 4° revolução industrial promoveu significativa alteração social com aporte de novas tecnologias, entre elas a *internet*, que se tornou ferramenta essencial para a realização de diversas tarefas, sejam elas de cunho industrial, comercial e, até mesmo, pessoal. Essa conjuntura de centralidade da *internet* potencializa a ocorrência de diversos ilícitos no ambiente virtual, que utilizam da conectividade como meio, método e fim para obter determinada vantagem. Os criminosos aproveitam da desinformação acerca desses delitos, que, por se portarem em um ambiente dinâmico, atualizam-se constantemente, o que dificulta o processo de informação acerca das medidas preventivas por parte da sociedade. Além disso, há grande problemática acerca da dificuldade do ordenamento em se alterar constantemente conforme o surgimento dos novos tipos delituosos, a fim de tipificá-los. Nesse contexto, o Brasil, somente em 2012, tomou medidas centralizadas no contexto dos delitos informáticos, o que demonstra uma reação tardia no combate à essa modalidade de crime.

O contexto pandêmico, no entanto, potencializou a ocorrência desses delitos, isso em função de diversos fatores já existentes, mas que foram potencializados em decorrência das medidas adotadas para a contenção da doença, tais como *lockdowns* e isolamento social. A *internet* tornou-se mais essencial para garantir a continuidade de atividades corriqueiras que encontraram diversos obstáculos na pandemia e, proporcionalmente a isso, houve aumento da ocorrência de cibercrimes. A partir desse contexto, foi possível associar diretamente características próprias da pandemia com delitos virtuais, a fim de exaltar os fatores que potencializaram essa conjuntura.

O que se percebe nos diversos crimes citados é que a *internet* é uma ferramenta meio para alcançar os fins delituosos e mostra-se como facilitadora desse processo. A vulnerabilidade das

pessoas em função da crise sanitária, do isolamento social e da impossibilidade acessar serviços presencialmente foram fatores determinantes para que os criminosos executassem suas atividades. Além disso, a virtualização de processos em caráter de urgência para executar atividades que foram limitadas deixou arestas nos quesitos de segurança, facilitando a ocorrência de delitos. Ilustrando a conjuntura do cibercrime na pandemia, a fraude do Auxílio Emergencial apresenta a correlação de fatores próprios da pandemia sendo utilizados como propiciadores para crimes informáticos.

Segundo a Academia de Polícia Civil de Minas Gerais (ACADEPOL), o conhecimento acerca dos riscos aos quais o mundo virtual expõe a sociedade, bem como ter informações sobre medidas de prevenção é de suma importância para amenizar não só as ocorrências desse tipo de delito, mas os impactos que causam. Porém, inexistem políticas públicas voltadas ao enfrentamento dessa questão por meio da informação à sociedade, especialmente à parcela civil que carece de instrução digital. Percebe-se, diante disso, que a pandemia somada à falta de informações são fatores determinantes para que os criminosos obtenham sucesso na realização dos delitos. Além disso, a falta de denúncias à essas ocorrências, que foram ainda menos realizadas na pandemia, viabilizam o aumento da incidência desse tipo de crime, que traz ônus à todas as esferas da sociedade.

Salienta-se, por fim, que os crimes cibernéticos constituem uma temática recente tanto para as discussões doutrinárias acerca do delito, bem como para a legislação brasileira, que caminha lentos passos para a tipificação dessa modalidade de crime. Junto a isso, é importante pontuar que a pandemia se trata de um momento atual que ainda não teve fim, o que dificulta a delimitação dos fatores inerentes a esse período. Diante disso, ressalta-se a importância de posteriores estudos científicos e doutrinários acerca da temática com fim de esgotar a questão dos cibercrimes relacionados à pandemia da Covid-19.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAGAO, Davi Farias. **Crimes cibernéticos na pós-modernidade: Direitos fundamentais e a efetividade da investigação criminal de fraudes bancárias eletrônicas no Brasil.** Universidade Federal do Maranhão, 2015. Disponível em: <https://tedebc.ufma.br/jspui/bitstream/tede/667/1/Dissertacao-%20DavidFariasAragao.pdf>. Acesso em: 24 jan. 2021.

ARAS, Vladimir. **Crimes de informática. Uma nova criminalidade**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 6**,** n. 51**,** 1out.2001**.** Disponível em:<https://jus.com.br/artigos/2250>**.** Acesso em: 26 jan. 2021

BORTOT, Jéssica Faria. **Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com Base nas Legislações Brasileira e Internacional.** VirtuaJus, Belo Horizonte, v.2, n.2, p.338-362,1º sem. 2017.

CAIXA ECONÔMICA FEDERAL. **Auxílio Emergencial**. Disponível em: <https://www.caixa.gov.br/auxilio/PAGINAS/DEFAULT2.ASPX>. Acesso em: 20 jan. 2021.

CASTELLS, Manuel. **A Sociedade em rede – a era da informação: economia, sociedade e cultura**. v.1. Trad. Roneide Venancio Majer. Atualização para 6ª edição: Jussara Simões. 6ª ed. São Paulo: Paz e Terra, 1999.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). Cartilha de Segurança para a Internet. Disponível em: <https://cartilha.cert.br/seguranca/>. Acesso em: 20 jan. 2021.

CNJ, Conselho Nacional de Justiça. **Crimes digitais: o que são, como denunciar e quais leis tipificam como crime?** Notícias CNJ, Brasília, 22 de jun. 2018. Disponível em: <https://www.cnj.jus.br/crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime/>. Acesso em: 24 jan.2021.

DANTAS, Miguel. **Farto da pandemia e das restrições? É preciso evitar a fadiga pandêmica.** Público, 30 out. 2020. Disponível em: <https://www.publico.pt/2020/10/30/sociedade/noticia/farto-pandemia-restricoes-preciso-evitar-fadiga-pandemica-1937059>. Acesso em: 28 jan.2021.

DESLANDES, Suely; COUTINHO, Tiago. **O uso intensivo da internet por crianças e adolescentes no contexto da COVID-19 e os riscos para violências auto infligidas**. Ciência e Saúde Coletiva, vol. 25, Rio de Janeiro, junho de 2020. Disponível em: <https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-81232020006702479&tlng=pt>. Acesso em: 20 jan. 2021.

GOVERNO DO BRASIL. **PF cria banco de dados contra fraudes no Auxílio Emergencial.** Notícias Justiça e Segurança, 23 de agosto de 2020. Disponível em: <https://www.gov.br/pt-br/noticias/justica-e-seguranca/2020/07/pf-cria-banco-de-dados-contra-fraudes-no-auxilio-emergencial>. Acesso em: 20 jan. 2021.

IBGE, Instituto Brasileiro de Geografia e Estatística. **O IBGE apoiando o combate à COVID-19**. Disponível em: <https://covid19.ibge.gov.br/pnad-covid/saude.php>. Acesso em 20 jan. 2021.

INTERPOL. **Cybercrime: COVID-19 Impact**. Agosto, 2020. Disponível em: <https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>. Acesso em: 20 jan. 2021.

JORGE, Higor; WENDT, Emerson. **Crimes Cibernéticos: Ameaças e procedimentos de investigação**. 2° Edição, Editora Brasport Livros e Multimídia Ltda, 2013.

KANTAR. **COVID-19 Barometer: Consumerattitudes, média habits and expectations.** Londres, 03 abr. 2020. Disponível em: <https://www.kantar.com/Inspiration/Coronavirus/COVID-19-Barometer-Consumer-attitudes-media-habits-and-expectations>. Acesso em 27. jan. 2021

MINISTÉRIO PÚBLICO DE MINAS GERAIS. **Navegar com Segurança: por uma internet mais segura, ética e responsável**. 4 ed. Belo Horizonte: MPMG, 2019.

POLÍCIA CIVIL DE MINAS GERAIS**. Crimes cibernéticos: os principais riscos e as técnicas básicas de prevenção**. Belo Horizonte: PCMG, 2020.

SEBRAE, Serviço Brasileiro de Apoio às Micro e Pequenas Empresas. **Coronavírus: o impacto nas vendas online**. Portal SEBRAE, 15 de março de 2020. Disponível em: <https://www.sebrae.com.br/sites/PortalSebrae/artigos/coronavirus-o-impacto-nas-vendas-online,ed84f8e520f71710VgnVCM1000004c00210aRCRD>. Acesso em: 20 de janeiro de 2021.

SILVA, Debora. **Cibercriminalidade e a (in) suficiência legislativa pátria para a repressão dos crimes cometidos por meio da Internet**. Trabalho de Conclusão de Curso, Florianópolis, 2020.

SYMANTEC; ORGANIZAÇÕES DOS ESTADOS AMERICANOS. **Tendências de Cibersegurança na América Latina e no Caribe**. 2014. Disponível em: <http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamcannex.pdf >. Acesso em: 20 jan. 2021.

VALENTE, Jonas. **Brasil tem 134 milhões de usuários de internet, aponta pesquisa.** Agência Brasil, Brasília, 26 de maio de 2020. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa>. Acesso em: 23 jan. 2021.

WORLD HEALTH ORGANIZATION, UNICEF. **COVID-19 parenting**. Disponível em: <https://www.covid19parenting.com COVID PARENTING>. Acesso em: 20 de janeiro de 2021.