PRÁTICAS ILÍCITAS EM MÍDIAS DIGITAIS E SUAS CONSEQUÊNCIAS JURÍDICAS, NO PERÍODO DA PANDEMIA

UNLAWFUL PRACTICES IN DIGITAL MEDIA AND THEIR LEGAL CONSEQUENCES, DURING THE PANDEMIC PERIOD

Adsson Rodrigues Nobrega
Estudante de Direito na Universidade Federal da Paraíba (UFPB).

Alicia Pereira de Albuquerque
Estudante de Direito na Universidade Federal da Paraíba (UFPB).

Resumo: O presente artigo tem como objeto examinar as práticas ilícitas no meio digital no período da pandemia do coronavírus e as inovações legislativas, buscando indagar enquanto problema se é possível afirmar que o distanciamento social intensificou os cibercrimes com que defende a hipótese que o direito normativo ampliado nesse período não foi suficiente para lidar com esse cenário, devendo-se ampliar os meios de investigação dos crimes e modificar o comportamento dos usuários como forma de prevenção. Trata-se, quanto a metodologia, de pesquisa bibliográfica tendo como objeto de estudo a legislação, doutrina, jurisprudência e pesquisas jornalísticas, partindo de uma documentação indireta. Assim, visa como objetivo geral, chamar a atenção para o crescimento dos delitos digitais na pandemia, o que se desdobra em objetivos específicos, provar essa relação, discutir quais legislações foram criadas ou modificadas para atender o anseio social por segurança e estabelecer quais crimes são preferíveis e quais grupos estão mais vulneráveis a eles.

Palavras-chave: Aumento Cibercrimes. Pandemia. Isolamento social. Ampliações legislativas.

Abstract: This article aims to examine the illicit practices in the digital environment in the period of the coronavirus pandemic and the legislative innovations seeking to question as a problem if it can be said that social distancing has intensified cyber crimes with which it defends the hypothesis that normative law expanded in this period was not enough to deal with this scenario, making it necessary to expand the means of investigating crimes and modifying the behavior of users as a form of prevention. As for the method, it is a bibliographic research having as object of study the legislation, doctrine, jurisprudence and journalistic research, starting from an indirect documentation. Thus, its generais objective is to draw attention to the growth of digital crimes in the pandemic, which unfolds in specific objectives, prove this relationship, discuss which laws were created or modified to meet the social desire for security and establish which crimes are preferable and which groups are most vulnerable to them.

Keywords: Increase Cybercrime. Pandemic. Social isolation. Legislative expansions.

Sumário: 1. Introdução – 2. O aumento de usuários na internet no período da pandemia – 3. Quem são os mais vulneráveis a esses crimes? – 4. Atualização legislativa em relação aos crimes cibernéticos no Brasil – 5. Os índices criminais que obtiveram maior frequência: 5.1. Phishing; 5.2. Golpes envolvendo cartão de crédito; 5.3. Fraudes bancárias; 5.4. Golpe do relacionamento virtual – 6. Atuação policial no combate aos crimes cibernéticos – 7. Considerações finais – Referências.

1. INTRODUÇÃO

A pandemia ocasionada pela disseminação do Sars-Cov-2 (Coronavírus) proporcionou uma mudança mundial em relação ao comportamento humano, por gerar a necessidade do isolamento social, pelas restrições impostas pelos decretos que visavam conter a propagação desse vírus, foi decretado o distanciamento.

Nesse aspecto, o objetivo deste trabalho será elucidar se houve crescimento dos crimes digitais no período da pandemia e se as mudanças legislativas, para suprir a existência de insegurança nesse espaço digital, surtiram efeitos, observando-se as modificações significativas na matriz policial para atender a demanda social por segurança digital, partindo de uma análise das vítimas que se encontram mais vulneráveis à esses delitos e como os criminosos se sentiram atraídos por esse meio, demonstrando quais atos são preferidos e como eles atuam.

Pois bem, a problemática levantada se refere acerca da fragilidade da segurança digital, impulsionada pelo período de isolamento e as ampliações legislativas que buscam impedir esse avanço, será que produziram de fato alguma modificação benéfica nesse cenário e como os usuários devem se portar nesse ambiente a fim de evitar serem vítimas de um delito digital. Com o início da pandemia causada pelo coronavírus, o distanciamento social tornou-se regra para atenuar a disseminação da COVID-19. Por esse ângulo, pode-se afirmar que o distanciamento social intensificou os delitos cometidos por meios eletrônicos?

A pesquisa se encaminhará de um estudo exploratório bibliográfico, no conceito de Prodanov e Freitas, com enfoque em fontes distintas que explicitam a relação entre o acesso à internet e a pandemia, e como essa relação provocou um quadro de insegurança online, assim como também apresentará exemplos de casos que compunham esse contexto por meio de uma documentação indireta, tendo como objeto de estudo a legislação, doutrina, jurisprudência e pesquisas jornalísticas[1].

Divide-se a estrutura, deste ensaio, em quatro partes principais. A primeira trará uma breve

[1][...] elaborada a partir de material já publicado, constituído principalmente de: livros, revistas, publicações em periódicos e artigos científicos, jornais, boletins, monografias, dissertações, teses, material cartográfico, internet, com o objetivo de colocar o pesquisador em contato direto com todo material já escrito sobre o assunto da pesquisa. (PRODANOV; FREITAS, 2013, p. 54).

introdução e especificará a relação da pandemia com os crimes cibernéticos, e se esse entrelaço proporcionou alguma mudança. Em sequência, será abordado as preferências dos delituosos no meio digital e as características das vítimas mais vulneráveis. Dando continuidade, explanar-se-á às inovações legislativas ocorridas no período da pandemia, em conjunto da atuação policial e com uma análise dos crimes que obtiveram maiores índices no isolamento. Por fim, será apresentado o cenário de fragilidade e insegurança e a importância do ponto anterior como solução para a amenização dessa realidade.

Pretende-se, ao final, evidenciar as colocações apontadas e notabilizar a importância da ampliação da atuação policial e de medidas de controle contra os cibercrimes, com o intuito de amenizar o quadro de irresolução e alargamento desses índices.

2. O AUMENTO DE USUÁRIOS NA INTERNET IMPULSIONADO PELO PERÍODO DA PANDEMIA

A pandemia do Covid-19, decretada oficialmente pela Organização das Nações Unidas (ONU) em março de 2020, modificou totalmente os hábitos e costumes humanos. A partir do momento que nos encontramos obrigados a nos segregar em nossos ambientes domésticos, pelo bem-estar da saúde pública, várias mudanças foram necessárias para continuar com as habitualidades a que já estávamos acostumados. Com isso, métodos de ensino a distância, homework, e manuseio da internet como fonte primordial para a circulação de informações, foram de extrema importância para seguir com a vida, visto que as medidas restritivas impediam as relações presenciais dos seres humanos, sendo assim os indivíduos tiveram que se adaptar às condições e buscar formas de amenizar o cenário de isolamento social em que se encontrava, achando na internet o seu principal aliado.

Dessa maneira, ocorreram aumentos significativos nos números de acesso à internet estudado pelo TIC Domicílios, pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros (TIC Domicílios), com o objetivo de analisar a difusão dos meios de comunicação e acesso à internet na população brasileira, pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), órgão do Comitê Gestor da Internet no Brasil (CGI.br):

> “Em 2020, a proporção de domicílios com acesso à Internet chegou a 83%, o que representa aproximadamente 61,8 milhões de domicílios com algum tipo de conexão à rede. Houve um aumento de 12 pontos percentuais em relação a 2019 (71%)” (TIC domicílios, 2021).

Segundo a pesquisa citada é notório o crescimento do acesso ao ambiente digital proporcionado pelo aumento de domicílios que passaram a ter conexão com a internet no período da pandemia. Esse crescimento teve como causa principal a necessidade de adaptação, devido a migração das atividades presenciais para o ambiente digital, pois muitas pessoas passaram a viver totalmente de forma online, ou seja, trabalhar remotamente, estudar, comunicar-se, pagar contas, e até fazer compras.

Nesse cenário, para manter-se na ativa os criminosos tiveram que se aprimorar à realidade, dado o aumento de usuários na internet, fazendo com que os crimes que possuíam maior incidência de forma física se tornassem agora uma preocupação para os usuários digitais, imersos em um cenário de insegurança e vulnerabilidade.

3. QUEM SÃO OS MAIS VULNERÁVEIS A ESSES CRIMES?

Na contemporaneidade, a internet tem papel fundamental na estrutura da sociedade moderna, podendo ser usada como meio de comunicação; ambiente de trabalho; meio de entretenimento e até mesmo como sede de instituições bancárias. Nessa perspectiva, as adaptações provocadas pelo confinamento proporcionam uma facilidade para o manuseio de dados pessoais, isto é, aquelas pessoas que costumavam ir presencialmente aos bancos e caixas passaram a controlar tudo por meio de aplicativos baixados em seus dispositivos de forma online. A internet move o mundo e sua importância foi ressaltada durante a pandemia que assolou a sociedade nos últimos anos. A rede mundial de computadores tornou-se um ambiente propício para a propagação de atividades delituosas.

A princípio, é necessário definir o significado de cibercrime. Nesse sentido, há um conflito na jurisprudência brasileira sobre o conceito de crime cibernético, também conceituado como delito de informática ou crimes digitais, entretanto, a definição majoritária abrange todo crime que é praticado por meio da internet ou meio digital análogo. Desse modo, pode-se subdividir esses crimes em delitos cibernéticos próprios e impróprios, esses dizem respeito a uma forma de virtualizar os crimes já tipificados na legislação pátria como, por exemplo, calúnia, difamação, furto, estelionato, estupro entre outros delitos. Já aquele, relaciona-se com os crimes que necessitam de uma forma eletrônica para existirem, como o crime de invasão de dispositivo informático, art. 154-A do CP, registro não autorizado da intimidade sexual, art. 216-B do CP e inserção de dados falsos em sistema de informação art. 313-A do CP.

Dessa forma, a possibilidade de praticar um delito sem as intromissões de barreiras físicas, visto que o ambiente digital possibilita a conexão entre diferentes partes do planeta, além de ter a facilidade de manter-se no anonimato com a criação de falsas identidades de perfis nas redes sociais, faz com que a internet seja um ambiente propício para os criminosos atuarem, eles se sentem à vontade, pois existem grandes dificuldades para punir os crimes cibernéticos, pelos motivos já citados. Com isso, tendo em vista o avanço do uso das tecnologias é evidente o perigo que se tornou esse ambiente no decurso da pandemia demonstrado pela reportagem divulgada pelo G1:

> “Foram 156.692 notificações anônimas de janeiro a dezembro do ano de 2020, contra 75.428 em 2019. Ocorrências foram lideradas, pela pornografia infantil, com quase 100 mil acusações”. Os dados 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)" (G1.com, 2021).

É primordial se ater aos principais métodos usados pelos criminosos e quais os crimes apresentam maior incidência, de acordo com o Relatório Semestral sobre Crimes Cibernéticos, de 2020, da LexisNexis Risk Solutions, quem tem menos de 25 anos e as pessoas acima dos 75 são os dois grupos mais vulneráveis. Os primeiros recebem mais ataques, enquanto o segundo grupo perde mais dinheiro. Com isso, é possível afirmar que as vítimas dos cibercrimes afetadas financeiramente disponham de uma maior idade, pois os criminosos encontram nesse grupo a fragilidade, mas que, no entanto, as pessoas mais jovens e com mais experiência na internet não estão livres desses ataques.

Os criminosos se apropriam da facilidade com que o meio digital apresenta de esconder sua identidade, desse modo eles criam falsos perfis, se passam por órgãos de pesquisa, enviam e-mails fraudulentos, tudo isso com o intuito de enganar a vítima para obtenção de dados, como também eles compartilham conteúdos ilícitos como o comércio de pornografia infantil, além de disseminar ofensas contra outros usuários. Nesse aspecto, o anseio social por segurança no meio digital é alarmante fazendo com que surgissem ampliações e inovações legislativas com o intuito de atender a necessidade de segurança digital.

> "As vítimas são crianças e adolescentes, mas também jovens e pessoas idosas que estão expostas a todo tipo de golpe, principalmente, utilizando dados pessoais e violação de senhas e outros tipos de invasões que tenham acontecido tanto em celulares, como em computadores", diz o diretor-presidente da Safernet Brasil, Thiago Tavares (SANTANAFM, 2021).

4. ATUALIZAÇÃO LEGISLATIVA EM RELAÇAO AOS CRIMES CIBERNÉTICOS NO BRASIL

O ordenamento jurídico brasileiro já conta, há certo tempo, com meios de coibir as ações de criminosos na internet, bem como leis que versam a respeito desses delitos como a Lei n° 12.737 de 2012, conhecida como Lei Carolina Dieckmann atribuiu-se a lei esse nome após um criminoso invadir o computador pessoal da atriz Carolina Dieckmann e extorqui-la com o material obtido. Tal legislação aborda crimes como dispersão de códigos maliciosos, falsificação de documentos digitais e invasão de dispositivos eletrônicos, delitos estes que ganham cada vez mais relevância em nossa sociedade e receberam uma atenção maior desde o início da pandemia de Covid-19 visto o cenário de distanciamento social imposto à população e a virtualização antecipada de diversas atividades como trabalho, comércio, cadastros públicos, entre outras.

> **A pandemia acelerou a digitalização de empresas e o processo não deve parar por aí**
>
> A pandemia restringiu o canal de venda presencial, forçando as empresas a intensificarem ou até mesmo anteciparem a virtualização do negócio, por meio de canais alternativos de venda, como redes sociais, sites próprios, marketplaces, entre outros. A pesquisa aponta que 28% dos negócios, sendo parte ou o todo, migraram para o ambiente digital durante o período da

> COVID-19. No período da pandemia, mais de 40% tiveram aumento nos acessos de seus sites e meios digitais de venda. A mesma pesquisa mostra que 97% das empresas têm presença on-line, desses, 65% atuam de forma totalmente digital e 32% ainda alternam entre físico e on-line (híbrido) [...] (PUCPR, 2021).

Ao passo que essa ferramenta proporcionou uma facilidade para nossas vidas, ela se tornou um alvo para os mais diversos fatos ilícitos desde os patrimoniais como também os relacionados, tendo em vista esse fato o Senado aprovou a adesão do Brasil à Convenção sobre o Crime Cibernético, celebrada em Budapeste, na Hungria, em novembro de 2001 (Projeto de Decreto Legislativo 255/2021). A matéria, que teve como relator o senador Nelsinho Trad (PMDB-MS), foi publicada no Diário Oficial da União a Lei nº 14.155, de 2021, sancionada pelo presidente Jair Bolsonaro. Ademais, essa lei tipificou a conduta de difundir códigos que permitam invadir dispositivos alheios, esses programas são usados comumente em golpes conhecidos como "phishing" o qual será abordado mais à frente em nossa pesquisa, outra mudança relevante foi a inserção no Código Penal de uma nova qualificadora para o crime de furto que foi denominada de “furto eletrônico” o qual se configura pela subtração de um bem por meio de um dispositivo informático. Em suma, temos o delito de fraude eletrônica, art. 171, § 2º-A, § 2º-B e § 4º, que é um dos crimes de maior incidência no período da pandemia, visto que esse delito pode ser praticado por meio de engenharia social, contatos telefônicos, e-mail fraudulento ou até mesmo por meio das redes sociais onde o criminoso consegue atingir um número demasiado de vítimas, simultaneamente, que também teve sua pena ampliada pela Lei nº 14.155, de 2021, tendo em vista a explosão de casos nos últimos anos.

Além disso, como visto a Lei nº 12.737/12 foi criada com o intuito de defender qualquer cidadão vítima de algum crime praticado por meio digital e com o avanço da digitalização, já exposto anteriormente, a legislação mostrou-se insuficiente para acompanhar a quantidade crescente de crimes cibernéticos no Brasil. Desta forma, o legislador fez notáveis alterações no *caput* do art. 154-A do Código Penal, suprimindo o trecho: “mediante violação indevida de mecanismo de segurança”. Com essa inovação da Lei nº 14.155 de 2021 o criminoso não precisa violar nenhum mecanismo de segurança da vítima, bastando para a consumação do delito a violação das informações, nessa lógica, a pena máxima também foi modificada e passou de 1 ano de detenção para 4 anos de reclusão dando assim uma reprimenda maior para esse crime.

5. OS ÍNDICES CRIMINAIS QUE OBTIVERAM MAIOR FREQUÊNCIA

Consoante pesquisa sobre segurança digital feita pela TransUnion, mostra que o número de fraudes digitais envolvendo serviços financeiros aumentou 457% desde o início da pandemia, há um ano. Além disso, segundo o estudo "Global Consumer Pulse", 20% dos consumidores foram alvo de fraudes relacionadas à Covid-19. Segundo o levantamento, o número de tentativas de transações digitais fraudulentas originadas no Brasil aumentou 10,99% no último ano, em relação ao período anterior. As cidades com maior porcentagem de transações fraudulentas foram Rio de Janeiro, São Paulo e Brasília.

Os fraudadores estão sempre procurando tirar proveito de eventos mundiais significativos. A pandemia da Covid-19 e sua correspondente e rápida aceleração digital, trazida pelas ordens de permanência em casa, é um evento global sem rival na era on-line, disse Shai Cohen, vice-presidente sênior da Global Fraud Solutions na TransUnion. “Analisando bilhões de transações, examinamos indicadores de fraude durante o ano passado e tornou-se claro que a guerra contra o vírus também trouxe uma guerra contra a fraude digital”. Entre as fraudes relacionadas à COVID-19, a pesquisa ouviu 1.101 consumidores brasileiros, dos quais 20% disseram terem sido alvo de fraudes relacionadas à doença.

Os principais golpes tiveram como objetivo o roubo de dados de cartões de crédito e as cobranças fraudulentas. “A pandemia mudou os hábitos financeiros dos consumidores, com mais compras e entretenimento movendo-se online. Isso atraiu fraudadores digitais, que transferiram suas atividades para indústrias relacionadas”, disse Leal. “Apesar dessas ameaças, os consumidores esperam que as empresas sejam capazes de proteger suas transações, mas ainda assim manter experiências digitais convenientes” (EXAME, 2021).

Viu-se até aqui que o meio virtual proporciona a prática de quase qualquer crime, como já exposto, mas alguns delitos ganharam mais relevância durante toda a pandemia de COVID-19 devido a sua recorrência, dentre os golpes com maior reincidência temos:

5.1. PHISHING

É um gênero bastante abrangente de fraude cibernética, esse golpe é muito comum pela facilidade dos criminosos em atraírem suas vítimas. A finalidade é fazer a vítima entregar seus dados de forma espontânea. A vítima pressupõe que está respondendo um e-mail ou acessando um site legítimo de alguma empresa; órgão; entidade, mas está cadastrando seus dados em uma página falsa. Também pode ocorrer quando o criminoso entra em contato com a vítima informando-a que ela ganhou um prêmio ou sorteio. Durante a pandemia, os casos de *Phishing* aumentaram consideravelmente.

Segundo a Kaspersky, empresa notoriamente conhecida no ramo de segurança da informação, de fevereiro a março de 2021 o número desses ataques aumentaram 120% no Brasil. Reforçando esse entendimento, um relatório produzido pela Axur Proteção Digital, feito no último trimestre de 2021, onde a instituição identificou 8569 casos de *phishing*, o que representou um aumento de 18,52% em comparação ao trimestre anterior. A empresa reiterou a tendência de aumento desses golpes no Brasil.

5.2. GOLPES ENVOLVENDO CARTÃO DE CRÉDITO

Golpes envolvendo cartões de crédito podem acontecer de diversas formas. À medida que a tecnologia avança, os golpistas encontram novos artifícios para ludibriar as vítimas. Entre os modos temos a engenharia social quando os criminosos se passam por funcionários do banco e a clonagem de dados. Vale evidenciar que a Lei nº 12.737/12 equiparou a falsificação de cartão

de crédito ao art. 298 do Código Penal, falsificação de documento particular.

De acordo com a Axur, existem mais de 2.842.779 cartões com dados expostos na deep web, somente no último trimestre de 2021 a instituição detectou mais de 325.250 cartões expostos. Os dados mostraram que houve uma redução de 67% em comparação ao trimestre anterior. Entretanto, essa diminuição não foi notada no Brasil, o qual assumiu o primeiro lugar no ranking de países com mais vazamentos de cartões de crédito. O Brasil representa 45,4% dos cartões vazados no mundo, mais de 10% a mais que o segundo colocado os Estados Unidos com 34,3%. Pode-se afirmar que as fracas políticas de segurança dos bancos brasileiros aliada ao pouco conhecimento de segurança da informação dos usuários contribuem para esse número tão expressivo.

5.3. FRAUDES BANCÁRIAS

Fraudes as quais envolvam instituições financeiras estão cada vez mais comuns, visto a capacidade dos golpistas de inovarem em seu "*modus operandi*", já que o médio digital oferece uma vastidão de possibilidades. Desse modo, as fraudes bancárias mais recorrentes são aplicadas por telefone onde o fraudador se passa por um funcionário da instituição financeira. Nesse golpe o criminoso usa dados que a própria vítima, por descuido, acaba deixando exposto na internet e assim facilitando a atuação dos golpistas. Essa fraude pode até mesmo contar com a atuação de motoboys que fazem a intermediação dos criminosos com a vítima buscando cartões bancários, documentos ou entregando boletos fraudulentos.

Em conformidade com a pesquisa de segurança digital da Federação Brasileira de Bancos - Debraban. Houve um aumento de 70%, no período da pandemia, dos golpes que visem obter dados bancários das vítimas. A mesma pesquisa estimou um crescimento de 300% no vazamento de dados pessoas desde o início da pandemia. Ademais, notou-se uma maior recorrência nos boletos fraudulentos enviados por e-mail.

5.4. GOLPE DO RELACIONAMENTO VIRTUAL

Este golpe ocorre geralmente por meio de aplicativos de relacionamento ou pelas redes sociais. Nele o golpista usa um perfil falso de uma pessoa bem sucedida e visa atingir pessoas que estão passando por algum tipo de vulnerabilidade emocional. Nesse golpe o criminoso tem, entre outras, as finalidades de exigir transferências bancárias, praticar sequestros e assaltos ou extorsão por fotos íntimas da vítima.

De acordo com um relatório da empresa Psafe, entre fevereiro e março de 2022, das pessoas ouvidas 34,38% confirmaram que já mantiveram um relacionamento com alguém que conheceram pela internet. Das pessoas que já mantiveram um relacionamento online, 25,5% tiveram perdas financeiras decorrentes de falsos relacionamentos. Nesse sentido, conforme dados da Federal Trade Commission em 2021 os danos patrimoniais em decorrência desses golpes chegaram a ultrapassar 304 milhões de dólares, isso significa um aumento de 51% na

comparação com o ano anterior.

6. ATUAÇÃO POLICIAL NO COMBATE AOS CRIMES CIBERNÉTICOS

Tendo em vista todo esse quadro de crimes digitais foi necessário que as polícias tanto civis quanto federal se reestruturarem de modo a combater esses ilícitos. Desse modo, serão citadas as principais mudanças e se elas proporcionaram uma melhora nos índices criminais.

No estado da Paraíba no ano de 2021 foi criada uma delegacia especializada na apuração de crimes cibernéticos com sede em João Pessoa, mas com expansão para todo o Estado, essa mudança facilita o processo de punição dos criminosos, pois visa sua atuação específica e qualificada para delitos digitais.

> "Estamos tratando de uma das modalidades criminosas mais ativas da atualidade no Brasil e até mesmo em outros países. Hoje, com o avanço da tecnologia, o crime ficou, de certa forma, mais fácil. Principalmente quando as vítimas são pessoas que não têm muita experiência com as ferramentas tecnológicas e acabam caindo em golpes diversos. Por isso, uma nova delegacia voltada exclusivamente para atender essa demanda é de extrema importância para a sociedade", disse o delegado-geral da Paraíba, André Luís Rabelo (REPÓRTERPB, 2021).

Outrossim, procedimentos como a infiltração de policiais no ambiente digital são de extrema importância no combate aos crimes digitais, no qual a pornografia infantil é mais visada por esse processo para repreende-la, o problema central é que deve ser autorizado judicialmente e para se obter essa autorização se torna requisito a exigência do esgotamento de todos os outros meios de obtenção de prova e de que os policiais tenham qualificação para atuar nesses meios, o que infelizmente não é a realidade das delegacias brasileiras, que contam com uma carência de profissionais na área computacional.

Além disso, a Polícia Federal já dispunha da Unidade Especial para Investigação a Crimes Cibernéticos, que conta com uma força tarefa especializada para essa atuação investigativa de crimes nos meios digitais. Outra possibilidade para a vítima de crimes digitais é prestar o boletim de ocorrência online no site da Delegacia Virtual do Ministério da Justiça e da Segurança Pública, o que facilita o contato da vítima com a polícia.

Ademais, pesquisa realizada pela SaferNet Brasil, associação civil de direito privado sem fins lucrativos, e pelo Ministério Público Federal, apontam um crescimento de 102% no número de denúncias de abuso online de crianças e adolescentes em 2020, comparado a 2019. Houve também um aumento expressivo de pedidos de ajuda relacionados à saúde mental (ideação suicida e auto-mutilação), problemas com dados pessoais, exposição de imagens intimas, cyberbullying, fraudes, golpes e spam. Essa pesquisa demonstra o crescimento das denúncias no período de pandemia e a necessidade de se ampliar os meios de combate a esses ilícitos, pois os já existentes se mostram insuficientes ou ineficazes, não basta apenas criar inovações legislativas que aumentem as penas, é importante atuar na investigação para que se possa

punir os criminosos.

Com isso, para se ter uma efetividade no combate à criminalidade virtual é necessário o conjunto da população com a polícia, por meio da denúncia pelo boletim de ocorrência com a junção de todas as informações possíveis do caso, que muitas pessoas não fazem por acreditar não ter solução ou ser perda de tempo, e da atuação policial na investigação, nesse ponto se faz necessário a ampliação de mais delegacias especializadas e a existência de concursos públicos voltados a contratação de especialistas no meio digital para atender as demanda sociais por justiça e amenizar os quadros de insegurança elevados durante o período de pandemia.

Assim, portanto, a hipótese que aqui se levanta é a de que para que os impactos gerados pelos aumentos do acesso à internet e a criminalidade sejam imunizados, faz-se urgente a atuação no aprimoramento dos métodos de investigação pela qualificação tanto dos policiais quanto das delegacias, com a disponibilidade de equipamento e força tarefa qualificada e capacitada para esse trabalho.

Além disso, é importante que os próprios usuários estejam cientes de que a internet é um local visado por criminosos e com isso tenha cautela ao disponibilizar seus dados pessoas ou contas bancárias, a fim de manter-se protegido dos possíveis golpes, por meio de mecanismo disponibilizados pelas próprias redes sociais que permite que um usuário denunciar um perfil falso ou com conteúdo ou atos ilícitos ou suspeitos. Dessa forma, poderá ser amenizado o cenário de insegurança no meio digital alargado durante a pandemia.

7. CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo relacionar os crescimentos dos crimes digitais com o isolamento social e visualizar as medidas que foram tomadas e se de fato tiveram efeitos. Com isso, é preciso, por todo exposto, admitir-se as falhas no combate contra os crimes digitais e toda a problemática já citada. Com base na ampliação da disseminação de crimes de informática, proporcionado pelo período da pandemia do coronavírus, que teve como causa o isolamento social, que tornou um ambiente propício para o crescimento do acesso à internet.

Desse modo, os usuários passaram a se sentir constantemente ameaçados nesse ambiente, tendo em vista o aumento dos casos e a ineficácia das medidas de punição. Desse modo, mesmo as inovações legislativas que tipificam e ampliam essas condutas não foram capazes de desestimular os praticantes desses ilícitos.

Ademais, mostrou-se as preferências dos criminosos quanto às vítimas e os delitos mais frequentes, com esse levantamento busca-se a atenção dos usuários em relação ao seu comportamento nas redes sociais. Enfim, o período pandêmico pelo qual passamos apenas acelerou um problema que já seria previsto, tendo em vista o avanço tecnológico em nossas vidas, e nesse contexto é necessário que as medidas de combate sejam ampliadas para que

sejam freadas as consequências dos delitos digitais.

REFERÊNCIAS

Agência de Notícias, nova delegacia irá atender uma das modalidades criminosas mais ativa. **Polícia Civil da Paraíba**, 11 de jun. 2021. Disponível em: https://www.policiacivil.pb.gov.br/noticias/nova-delegacia-ira-atender-uma-das-modalidades-criminosas-mais-ativas-no-brasil-afirma-delegado-geral-da-policia-civil

Agência Senado. Penas mais duras contra crimes cibernéticos. **Senado Federal**, 28 mai. 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada

Blog Banco Inter, como não cair no golpe do cartão de crédito. **Inter**. Disponível em: https://blog.bancointer.com.br/golpe-do-cartao-de-credito

Conteúdo Axur, Atividade criminosa online no Brasil. **AXUR**, 21 jan. 2021. Disponível em: https://conteudo.axur.com/hubfs/E-books/Relat%C3%B3rios%20trimestrais/Relatorio_Axur_Q4_2020+year-in-review.pdf

Datasafer, Central nacional de Denúncias de Crimes cibernéticos. **Safernet**. Disponível em: https://indicadores.safernet.org.br/

Eduardo Boni, vazamentos de dados crescem 785%. **Security Business**, 24 mai. 2021. Disponível em: https://securitybusiness.com.br/vazamentos-de-dados-crescem-785-no-primeiro-trimestre/

G1.com, crimes cometidos pela internet mais que dobram. **Globo**, 09 fev. 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

Gov.br, ANPD participa de seminário que discute o combate aos crimes cibernéticos. **Presidência da República**, 01 de dez. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-de-seminario-que-discute-o-combate-aos-crimes-ciberneticos

Kaspersky Daily, brasileiros são principais alvos de ataques de phishing no mundo. **Kaspersky**, 2 mar. 2021. Disponível em: https://www.kaspersky.com.br/blog/brasileiros-maiores-alvos-phishing-mundo/17045/

Pesquisa TIC Dominicio, resumo executivo edição COVID-19. **CETIC**, 13 dez. 2020. Disponível em: https://cetic.br/media/docs/publicacoes/2/20211124201505/resumo_executivo_tic_domicilios_2020.pdf