PUCSP – Pontifícia Universidade Católica de São Paulo

WILLIAN ANDRADE LO

A (IN)EFICÁCIA DA PRODUÇÃO DE PROVAS ORIUNDAS DO AMBIENTE DIGITAL EM FACE À CRIMES CIBERNÉTICOS

São Paulo

2022

WILLIAN ANDRADE LO

A (IN)EFICÁCIA DA PRODUÇÃO DE PROVAS ORIUNDAS DO AMBIENTE DIGITAL EM FACE À CRIMES CIBERNÉTICOS

Artigo apresentado como requisito parcial para obtenção do título de Especialista no Curso de Direito Penal e Direito Processual Penal.

Orientador:

Prof. Dr. Antonio Carlos da Ponte

São Paulo

2022

A (IN)EFICÁCIA DA PRODUÇÃO DE PROVAS ORIUNDAS DO AMBIENTE DIGITAL EM FACE À CRIMES CIBERNÉTICOS

Willian Andrade Lo[1]

Resumo: Este trabalho tem como objetivo analisar o surgimento dos principais crimes digitais, advindos do fenômeno da globalização digital e expansão das tecnologias e o respectivo reflexo no direito penal e processual penal. Busca-se em um primeiro momento avaliar as características que perfazem um crime digital, seus meios de disseminação e impactos causados as vítimas. Também se almeja discorrer acerca das atuais e possíveis formas de produção de provas no combate e repressão aos cibercrimes como forma de atuação dentro dos parâmetros jurídicos, em consonância com os princípios aplicáveis para que de forma eficiente possa oferecer segurança aos cidadãos que estão expostos a essas novas formas de criminalidade, as quais apresentam alto e rápido potencial de disseminação. Por fim, será analisada a efetividade das provas produzidas relativas ao ambiente digital.

Palavras-chave: Crimes digitais. Tecnologia. Cibercrime. Fraude.

Abstract: This paper aims to analyze the emergence of the main digital crimes, arising from the phenomenon of digital globalization and expansion of technologies and their respective impact on criminal law and criminal procedure. At first, it seeks to evaluate the characteristics that build a digital crime, its means of dissemination and impacts caused to the victims. It is also intended to discuss the current and possible ways of producing evidence in the fight and repression of cybercrime as a way of acting within the legal parameters, in line with the applicable principles so that it can efficiently offer security to citizens who are exposed to these new forms of criminality that have a high and fast potential for dissemination. Finally, the effectiveness of the evidence produced relating to the digital environment.

Keywords: Digital Crimes. Technology. Cybercrimes. Fraud.

1 INTRODUÇÃO

A evolução da sociedade por si só muda o modo como as pessoas convivem entre si, se relacionam e usufruem do ambiente ao qual estão inseridas. E o que observamos hoje é que as mudanças acontecem com mais frequência, haja vista que, conforme preceitua BAUMAN[2], a sociedade atual apresenta contornos fluídos, onde tudo ocorre com muita agilidade e que as estruturas sociais não foram feitas para serem estáticas ou ainda para durar muito tempo. Essa fluidez constante tende a gerar impactos e conflitos, os quais nem sempre são resolvidos em

[1] Possui Graduação em Direito pela Pontifícia Universidade Católica de São Paulo. Certificado em Compliance (CCEP-I) pela *Society of Corporate Compliance em Ethics*. Membro efetivo da Comissão de Estudos de Compliance da OAB SP. Experiência em empresas multinacionais de segmentos distintos na implementação de programas de compliance e proteção de dados.

[2] BAUMAN, Zygmunt. **Modernidade líquida** – tradução Plínio Dentzien. Rio de Janeiro. Zahar: 2001.

autocomposição, mas sim imputando ao Estado a incumbência de mediar a situação para que seja dada uma solução adequada e de acordo com as leis vigentes.

O direito penal e processual penal tradicional se deleitaram em reflexões acerca de teorias para aplicação da lei penal no tempo e no espaço, as quais comumente levam em consideração aspectos mais objetivos e possíveis de determinarem as características de competência de um delito cometido, assim como seus demais reflexos práticos. E sob a mesma ótica seguiu-se as premissas de produção de provas no devido processo legal, buscando-se evidências factíveis que pudessem formar o livre convencimento do magistrado, seja com a oitiva de testemunhas, documentos físicos, perícias etc., mas que de forma geral possuem essência sólida e sedimentada dentro dos ditames jurídicos.

Contudo, o surgimento da internet e os avanços tecnológicos trouxeram incertezas e situações dúbias tanto no que concerne a determinação do local do crime, quanto das provas aplicáveis ao caso concreto, na medida em que possibilitaram novas formas de criminalidade com os chamados cibercrimes ou simplesmente um novo ambiente para a prática de crimes já tipificados. Essas novas formas de delitos trazem consigo um cenário cinzento ao local fático do crime, haja vista que ocorrem em um espaço virtual, assim como a possibilidade de novos meios de prova para serem apresentados e utilizados na persecução penal, que por sua vez não estão totalmente sedimentados no tange a sua aceitação, confiabilidade e adesão aos princípios jurídicos aplicáveis.

Em 2020, com o surgimento da pandemia de covid-19, a era da informação ganhou ainda mais força do que até então havíamos presenciado, e o mundo se viu interconectado de suas casas devido ao *lockdown* ou outras restrições que implicaram no distanciamento físico das pessoas, e isso fez com que quase todos os aspectos da vida humana fossem tratados por meio da tecnologia. Diversos foram os avanços, que apesar já existirem, talvez não fossem tão explorados, como no caso da telemedicina, do estudo a distância, do teletrabalho regulamentado, e no ramo do direito não podemos deixar de dar destaque a implantação de audiências virtuais e tantas outras facilidades tecnológicas disponíveis por meio de aplicativos, programas de computador e softwares.

Destarte, diante do crescimento das diversas formas de cibercrimes, é imperioso realizar um estudo de formas de combate e repressão pelo direito de tais ações que se mostram tão prejudiciais aos usuários que navegam na internet, e avaliar como endereçar as situações dessa modalidade de crime que traz circunstâncias próprias, muitas vezes de difícil reparação. E em

que pese existir diversas formas de produção de provas, este artigo terá como foco a análise da das provas produzidas no ambiente digital e a consequente ponderação da (in)eficácia de tais documentos como parte do processo penal e do livre convencimento do magistrado.

2 ASPECTOS CONTEMPORÂNEOS DA CRIMINALIDADE CIBERNÉTICA

2.1 A evolução da tecnologia o impacto no direito brasileiro

A rede de conexão internet é um marco histórico e impactante nas diversas interações sociais, a qual surgiu ao final dos anos 60, quando em meio a Guerra Fria, os Estados Unidos buscaram uma forma de comunicação em diferentes locais que pudesse dar suporte as suas ações militares. Foi nesse cenário que surgiu a Arpanet, rede de conexão criada pela empresa ARPA, que a princípio funcionava interligando centros universitários.

Mais tarde, nos anos 80, houve a expansão da internet e o surgimento de exploração por empresas privadas de tal tecnologia para que os particulares pudessem ter acesso a essas novas ferramentas. Nesse interim surgiram empresas como a IBM, a Apple e a Microsoft, que até hoje se destacam no mercado e pela oferta de produtos e serviços, que têm sido muito presentes para os usuários de internet e de dispositivos tecnológicos.

No entanto, o grande marco da tecnologia pode ser compreendido como o início dos anos 2000, período em que diversos foram os portais de conteúdo criados, tais como o Yahoo, AOL, salas de bate papo, mensagens instantâneas, sites de busca como o Google e redes sociais como o Orkut, Facebook (atualmente conhecido como "Meta"[3]), Twitter e tantos outros que quebraram as fronteiras geográficas físicas e tornaram o mundo um lugar mais próximo.

De 1960 até os dias atuais, muita coisa mudou em relação ao mundo digital, que continua em constante evolução, e diversas foram as inovações que se encontram de fácil acesso aos internautas, as quais são aplicáveis a quase tudo que fazemos diariamente, desde fazer compras, acessar serviços públicos, fazer locação de imóveis, e tudo e por meio um smartphone, tablet ou computador.

Entretanto, sob uma ótima jurídica, não podemos nos ater somente aos benefícios e facilidades hoje dispostos aos cidadãos, mas aos riscos que elas trazem e aos impactos no direito, que tem a função de atuar frente aos dilemas e definir regras que sejam capazes de

[3] CNN. Facebook muda nome para Meta. Disponível em: https://www.cnnbrasil.com.br/business/facebook-muda-nome-para-meta/. Acesso em 05 mar. 2022.

endereçar com a devida diligência, e em consonância com os princípios aplicáveis e o arcabouço jurídico já existente.

Nesse diapasão, o direito é impactado em todos os seus ramos, seja no tributário, administrativo, penal, empresarial, internacional e outros e precisam ser adaptados para a realidade moderna que nos envolve. Podemos citar de forma resumida problemas que envolvem direitos autorais, fraudes em comércio eletrônico, direitos à intimidade, atendimento a direitos do consumidor por produtos adquiridos de forma online, a tributação de produtos e serviços exclusivamente digitais ou relacionados a criptomoedas.

Contudo, é inegável que a internet e o mundo digital se tornaram indispensáveis para as rotinas da humanidade, cabendo então ao mundo jurídico acompanhar o funcionamento da sociedade e trazer as soluções legais mais adequadas para avanço constante – e necessário – seja acompanhado de segurança.

2.2 Conceito e características dos crimes cibernéticos

Um dos primeiros impasses enfrentados quando o assunto é crime cibernético reside na própria nomenclatura utilizada para abarcar de maneira completa os delitos pertencentes a essa categoria, os quais ocorrem por meio da rede de dados em que pessoas se conectam para realizar diversas ações, desde as mais simples como uma comunicação corriqueira, mas também as mais complexas e que envolvem criação de contas bancárias de forma totalmente online, e portanto possuem sistemas de segurança da informação e mecanismos antifraude mais robustos.

No Brasil, verificamos que as próprias autoridades policiais que atuam na repressão de tais crimes não apresentam um consenso de identificação adotada, fato esse que é evidenciado ao analisar que no Distrito Federal temos a Delegacia Especial de Repressão aos Crimes Cibernéticos (DRCC), na Bahia temos o Grupo Especializado de Repressão aos Crimes por Meio Eletrônicos, no Maranhão temos o Departamento de Combate aos Crimes Tecnológicos, dentre outros.

Nesse sentido, ZANIOLO[4] adota uma posição interessante e engloba os crimes cibernéticos como crimes modernos, em uma acepção meramente semântica, para abordar os crimes atuais e recentes, os quais se destacam justamente pelo vínculo com a tecnologia, e desta maneira ter um entendimento mais genérico. Com essa definição e como bem pontuado pelo

[4] ZANIOLO, Pedro Augusto. **Crimes Modernos: O impacto da tecnologia no direito**. 4ª ed. Salvador: JusPodvm, 2021, p. 42

autor, não há correlação no sentido filosófico de “moderno”, e sua inserção dentro de um contexto histórico, pois se assim fosse, o termo mais adequado seria o crime “pós-moderno”.

Apesar de diversas serem as formas e nomenclaturas possíveis, para os fins desse trabalho, utilizaremos as expressões crimes digitais ou crimes cibernéticos, as quais refletem maior sinergia com os aspectos ocorridos dentro do ambiente digital, bem como por estarem alinhadas aos termos legislativos e doutrinários.

Porém, o que são crimes cibernéticos, afinal? Para CRESPO[5], são condutas típicas criminais, nos quais os aparatos tecnológicos são utilizados para este fim, seja considerando que o alvo do ato ilícito seriam sistemas informatizados ou até mesmo que a tecnologia foi utilizada com um meio do cometimento do crime, mesmo que o crime pudesse ter sido cometido de outra maneira.

Nesse sentido, há duas categorias de crimes digitais que merecem nossa devida atenção e que nos auxiliarão a compreender suas consequências, tratativas e agentes envolvidos. Quando o crime digital é cometido contra um sistema informacional em si, como no caso de invasões *crackers* para acessar dados confidenciais, copiá-los, reproduzi-los, a disseminação de vírus ou qualquer outro tipo interferência no *software* ou *hardware*, estamos diante do que chamamos de crimes digitais próprios ou puros, que por sua vez se consumam no próprio meio eletrônico.

No entanto, se o crime digital apenas utiliza a internet como meio de realização de um crime, muitas vezes de bens jurídicos já protegidos pelo ordenamento pátrio, como no caso da vida, liberdade, patrimônio etc., estaremos diante de um crime digital impróprio ou misto. Neste caso, os crimes tradicionais que já conhecemos, tais quais a calúnia, difamação, ameaça, são cometidos pelos diversos aparatos tecnológicos, seja via redes sociais no caso do Facebook, Instagram, Twitter ou via aplicativos de mensagens instantâneas como WhatsApp ou Telegram, dentre outros.

Sob a análise dos sujeitos envolvidos no delito, quando estamos diante de crimes cibernéticos próprios, destacamos o sujeito ativo como sendo comumente, pessoas os chamados de “hackers”, contudo, do olhar técnico, o mais adequado seria “cracker”. Nesse sentido:

> "Hacker" e "cracker" duas palavras bastante parecidas, mas possuem significados diferentes no mundo da tecnologia. De forma geral, hackers são indivíduos que elaboram e modificam softwares e hardwares de computadores, seja desenvolvendo

[5] CRESPO, Marcelo. **Crimes digitais: do que estamos falando?** Disponível em: https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/. Acesso em: 30 out. 2021.

> funcionalidades novas ou adaptando antigas. Já cracker é o termo usado para designar quem pratica a quebra (ou cracking) de um sistema de segurança.[6]

Em relação aos crimes virtuais impróprios, o sujeito ativo não guarda tanta especificidade técnica, haja vista ser um meio para o cometimento para diversos crimes como estelionato, furto, terrorismo, ameaça, difamação e tantos outros, e por isso pode ser compreendido como o sujeito que pratica o delito típico, mas que se utiliza do meio digital para sua ação.

Acerca do sujeito passivo, cabe destacar como sendo uma pessoa física ou jurídica, a qual a ação ou a omissão, se aplicável, tiver recaído, ou seja, qualquer pessoa que tenha sido lesada pela prática do crime digital, em que teve algum bem juridicamente protegido, afetado, seja o desvio de bens, deterioração do patrimônio ou até mesmo violação de informações e dados pessoais.

Alguns avanços foram observados no ordenamento jurídico brasileiro em função de situações que ao se tornarem públicas, causaram grande repercussão na mídia, fazendo com que a aprovação de dispositivos legais apresentasse mais celeridade, como foi o caso da chamada "Lei Carolina Dieckmann" em 2012, que se deu como resultado de uma invasão que a atriz Carolina Dieckmann sofreu eu seu computador e teve fotos pessoais íntimas acessadas por um criminoso, que por sua vez exigiu uma quantia em dinheiro para não tornar os arquivos públicos. Ocorre que a atriz não cedeu a chantagem e teve suas fotos tornadas públicas na internet[7].

A Lei Carolina Dieckmann, Lei nº 12.737/2012 implicou em uma alteração do Código Penal Brasileiro e instituiu o crime de invasão de dispositivo informático, conforme previsto no artigo. 154-A, e também alterou o artigo 266 para prever as mesmas consequências para quem dificultar serviços de informação que sejam públicos e o artigo 298 para equiparar cartão de crédito e débito como documentos particulares em crimes de falsificação de documento.

Por seu turno, a Lei nº 12.735/2012, conhecida como Lei Azeredo, também trouxe mudanças ao cenário de combate aos crimes virtuais ao introduzir a criação de delegacias especializadas no combate aos crimes digitais, conforme artigo 4º da referida norma, e de estabelecer que a indução ou incitação de discriminação ou preconceito de raça, cor, etnia,

---

[6] PRIVACY, Tech. Hacker x Cracker qual a diferença? Disponível em: https://privacytech.com.br/protecao-de-dados/hacker-x-cracker-qual-a-diferenca,359858.jhtml. Acesso em 15 jan.2022.

[7] FMP, Fundação Escola Superior do Ministério Público. Lei Carolina Dieckmann: você sabe o que essa lei representa? Disponível em: https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/. Acesso em: 15. Jan. 2022.

religião ou procedência nacional, praticados por intermédio dos meios de comunicação social ou publicação de qualquer natureza, tenham a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio. Imperioso mencionar, no entanto, que tal lei sofreu diversas críticas em seu texto original devido a diversos pontos polêmicos que continha como por exemplo sobre a guarda de logs pelos provedores de internet, e por isso restou aprovada com apenas 4 artigos.

No Brasil, em agosto de 2020, entrou vigor a Lei Geral de Proteção de Dados, Lei nº 13.709/2018 ou simplesmente "LGPD"[8], a qual dispõe sobre o tratamento de dados pessoais, com a finalidade de dar autonomia sobre o uso dos dados pelos seus titulares, bem como lhes fornecer privacidade, liberdade e livre desenvolvimento da personalidade da pessoa natural. Verificamos na própria lei a definição do que é considerado um dado pessoal:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Em âmbito constitucional, também é plausível destacar a recente Emenda Constitucional aprovado que tornou a proteção de dados pessoais um direito fundamento no Brasil.[9] Com isso, o tema obtém o status de grande relevância e assim como as demais garantias constitucionais, fica sob a responsabilidade da União legislar sobre o tema e que assim proporcionar maior segurança jurídica em sua aplicação e busca evitar retrocessos legais a matéria de proteção de dados.

Pelo exposto, conclui-se que diversos foram os avanços legislativos na busca de tentar trazer mecanismos no combate aos crimes cibernéticos, mas que ainda não há um arcabouço robusto o bastante para prevenir e combater as condutas delituosas no ambiente digital, fator

---

[8] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 15 jan. 2022.

[9] DEPUTADOS, Câmara dos; Agência Câmara de Notícias. **Promulgada PEC que inclui a proteção de dados pessoais entre direitos fundamentais do cidadão.** Disponível em: https://www.camara.leg.br/noticias/850028-promulgada-pec-que-inclui-a-protecao-de-dados-pessoais-entre-direitos-fundamentais-do-cidadao/. Acesso em 05 mar. 2022.

que por sua vez pode contribuir com a impunidade. Tampouco há um consenso mínimo acerca de conceitos técnicos de crimes cibernéticos, os quais são têm surgido na medida que a sociedade evolui e avança em tecnologia. Por essa razão, no próximo capítulo faremos uma breve análise de alguns crimes virtuais muito comuns na atualidade.

2.3 Principais crimes cometidos no ambiente virtual

A prática de crimes cibernéticos em face de grandes empresas, seja para algum tipo de invasão cracker, acesso a informações sigilosas e outros, é uma tarefa mais complexa, pois devido ao risco envolvido da atividade econômica, as empresas costumam implantar diversas camadas de proteção de seus sistemas informativos. Com isso, as pessoas físicas que navegam pela internet e fazem uso de dispositivos de tecnologias no dia a dia acabam sendo vítimas potenciais, em que o êxito do golpe almejado pode ser alcançado de maneira mais fácil e sem grande aplicação de expertise de tecnologia.

Importante mencionar que o fato de cidadãos comuns serem alvos mais fáceis, isso não quer dizer que as grandes empresas não sofram com os delitos informativos, e inclusive quando ocorre, os prejuízos são altíssimos, pois envolve não somente a indisponibilidade de seus sistemas e consequentemente do oferecimento de seus produtos e serviços, mas também de riscos financeiros pelos valores gastos com a remediação dos problemas e vulnerabilidades encontradas, e por fim a reputação, um valor quase que imensurável para uma marca e de difícil reparação.

Neste capítulo, veremos alguns dos principais crimes cometidos pela internet e que têm apresentado relevância, mas de modo algum os tópicos abaixo são capazes de esgotar a lista de delitos que podem ser cometidos de maneira virtual.

2.3.1 Clonagem do WhatsApp

Primeiramente cabe destacar que o WhatsApp é um aplicativo que permite o contato via mensagem e chamadas de voz para celulares para todos aqueles que possuem o aplicativo no mundo, sendo ainda possível compartilhar fotos, vídeos, localização. Atualmente, os usuários já somam mais de dois bilhões de pessoas, em mais de 180 países[10].

[10] WhatsApp. **Sobre o WhatsApp**. Disponível em: https://www.whatsapp.com/about/?lang=pt_br. Acesso em: 15 jan. 2022.

No tocante ao crime de clonagem do referido aplicativo, é preciso que façamos a sua divisão em duas principais partes. O primeiro objetivo do criminoso é obter acesso ao aplicativo da vítima, e para tanto, é necessário ter o número do celular em questão, o qual muitas vezes fica disponível em redes sociais ou como forma de contato em sites de compra e venda, mas o criminoso também necessita da senha de acesso ao WhatsApp, que é um código de 6 dígitos criado pelo próprio usuário, como um mecanismo de segurança chamado de "confirmação em duas etapas".

Com o número do celular da vítima, o criminoso entra em contrato com ela e, de maneira geral alega ser de alguma entidade pública, instituição bancária ou site que a vítima faz a venda de produtos e solicita a confirmação de alguns dados, e dentre eles o código de segurança recebido via SMS pela vítima, mas que foi solicitado pelo golpista que está tentando acesso ao WhatsApp por meio de um outro celular. Ao passar esse código, o acesso foi totalmente concedido ao criminoso e neste momento o usuário perde o acesso imediato ao aplicativo.

Assim, a partir do acesso fraudulento, se inicia a segunda parte do golpe, que reside na tentativa de obtenção de uma vantagem financeira, a qual é realizada pelo contato direto com os amigos, parentes, colegas; e se passando pela vítima, o golpista menciona que está com dificuldades de pagar um boleto, fazer uma transferência ou usar o cartão de crédito, e por isso pede que essas pessoas realizem a transação financeira com a promessa de que serão reembolsadas brevemente. No momento que o parente ou amigo realização a transação financeira solicitada, mais um crime é consumado.

2.3.2 Sites de comércio eletrônico fraudulentos

A venda de produtos por meio de sites ou até mesmo aplicativos e redes sociais, é uma prática comum e que está cada vez mais presente na vida dos brasileiros. Destaca-se ainda que a pandemia de covid-19 contribuiu fortemente para o incentivo de aquisição de produtos pela via digital, uma vez que as pessoas se viram compelidas a evitar ambientes públicos e também em decorrência das legislações que determinaram o fechamento de estabelecimentos comerciais, de forma parcial ou total.

Segundo a Associação Brasileira de Comércio Eletrônico (ABComm), em parceria com a Neotrust, o ano de 2020 representou um crescimento de 68% nas vendas online em relação a 2019. A estimativa apresentada pela associação indica que cerca de 20 milhões de consumidores

realizaram uma compra pela internet pela primeira vez e que 150 mil lojas passaram a vender em plataformas virtuais[11].

E apesar do desenvolvimento econômico que se observa com o crescimento de vendas pelo mercado eletrônico, junto a ele, observamos os crimes que envolvem sites fraudulentos. Aqui estamos diante de um criminoso cria um site quase que idêntico a um outro site de alguma empresa regular no comércio de produtos. Com isso, o criminoso induz que as vítimas acessem e façam a aquisição de produtos no site falso, pensando estarem comprando em algum site verdadeiro, e ao concluir a compra e realizar o pagamento, não recebem o produto.

2.3.3 Sextorsão

A sextorsão é uma espécie de extorsão mediante ameaça de divulgar imagens ou vídeos íntimos das vítimas na internet com o objetivo de forçar uma pessoa a fazer algo para satisfazer a vontade do criminoso dentro de um curto período de tempo, como forma de vingança, humilhação ou até mesmo para obter uma vantagem financeira.

Nesse tipo de crime, o autor muitas vezes não tem conteúdo algum da vítima, entretanto, por meio argumentos convincentes, como no caso de possuir alguns dados pessoais e sobretudo diante do pânico causado, a vítima acaba acreditando no ofensor e cedendo as ameaças.

Cabe aqui ressaltar que este crime se diferencia da prática de "Pornografia de Vingança", que por sua vez engloba condutas de transmissão, venda, destruição relacionadas a cenas de estupro, sexo, nudez ou pornografia, as quais não possuem o consentimento da vítima, conforme previsto no artigo 218-C do Código Penal.

2.3.4 Sequestro de Dados ou Ransomware

Outro crime que tem afetado o ambiente virtual é o sequestro de dados, ou também chamado de *ransomware*, que é um tipo de malware capaz de causar inúmeros prejuízos as vítimas, conforme explica a empresa AVAST[12] (2021):

> O ransomware é um tipo de malware, ou software maligno, que sequestra arquivos e, às vezes, computadores ou dispositivos móveis inteiros. Podemos definir ransomware por esse

[11] G1. Com pandemia, comércio eletrônico tem salto em 2020 e dobra participação no varejo brasileiro. Disponível em: https://g1.globo.com/economia/noticia/2021/02/26/com-pandemia-comercio-eletronico-tem-salto-em-2020-e-dobra-participacao-no-varejo-brasileiro.ghtml. Acesso em: 15 jan. 2022.

[12] AVAST. Guia essencial sobre ransomware. Disponível em: https://www.avast.com/pt-br/c-what-is-ransomware#gref. Acesso em: 16 jan. 2022.

> comportamento: os cibercriminosos solicitarão um pagamento de resgate em troca de acesso ou descriptografia de seus arquivos.

Assim, o *ransomware* acarreta um crime em que o autor se utiliza de um software malicioso para infectar servidores e computadores, bem como criptografar, ou seja, codificá-los para que o usuário não tenha mais acesso aos seus dados e caso as vítimas não tenham cópias de seus arquivos e dados, o que chamamos de "backup", então acabam perdendo todas as informações referentes ao dispositivo afetado.

Como consequência da indisponibilidade dos dados, o criminoso solicita um pagamento para que a devolução das informações seja feita, ação que se mostra muito insipiente, haja vista que não há garantias da efetiva devolução dados e tampouco que não haverá uma outra invasão.

2.3.5 Golpe do boleto falso

O golpe do boleto falso é uma modalidade de crime que pode ocorrer, tanto pelo envio do boleto adulterado de maneira impressa para a vítima, quanto por vias digitais, situações e que é o comum por mensagens SMS, WhatsApp ou e-mail, mas em ambos o objetivo é o mesmo: induzir a vítima a pagar um documento fraudado.

A prática do crime nos revela que o fraudador busca produzir um documento que é muito similar ao que seria o documento original, e que inclusive vem acompanhado de alguns dados pessoais como nome, endereço e CPF. Dessa maneira, a vítima acredita fielmente que está pagando uma despesa da qual, de fato, utilizou do serviço ou adquiriu um produto, e então prossegue com o pagamento. Ocorre que nestes casos, valor pago é direcionado para a conta do fraudador, ou até mesmo de "laranjas" ao invés do verdadeiro credor.

2.4 A produção de provas em crimes cibernéticos

A produção de provas relacionadas aos crimes cibernéticos é, com efeito, uma grande dificuldade no que tange a condenação de tais delitos. Isso decorre pela própria essência da prova dentro do devido processo legal que nos remete a algo que supostamente aconteceu do modo como um conjunto de evidências nos leva a crer. Nesse sentido, destaca NUCCI[13]:

> Há fundamentalmente, três sentidos para o termo prova: a) ato de provar: é o processo pelo qual se verifica a exatidão ou a verdade do fato alegado pela parte no processo (ex.: fase probatória); b) meio: trata-se do instrumento pelo qual se demonstra a verdade de algo (ex.: prova testemunhal); c) resultado da ação de provar: é o produto extraído da análise

[13] NUCCI. Guilherme de Souza. Curso de Direito processual penal. 17. Ed. – Rio de Janeiro: Forense. 2020

> dos instrumentos de prova oferecidos, demonstrando a verdade de um fato.

Para que não ocorram injustiças, o direito deve se pautar por uma análise completa, levando em consideração tanto a materialidade quanto a autoria e mesmo assim o que se alcançará é uma convicção de que uma situação tenha ocorrido ou não da forma que é suscitada nos autos pelas partes, não significando assim, que serão encontrados exatamente os fatos ocorridos na realidade.

Há de se tomar grande cautela ainda no tocante as provas ilícitas (art. 157, CPP), que são aquelas que violam as disposições de direito material ou princípios penais. O mesmo deve ser observado sobre as provas ilegítimas, ou seja, aquelas não atendem os requisitos de direito processual e os princípios constitucionais. Em casos como este. No Brasil, A Constituição determina que provas obtidas por meios ilícitos são inadmissíveis no processo, conforme art. 5º inc. LVI.

O Superior Tribunal de Justiça firmou entendimento de que as provas obtidas diretamente de smartphones, oriundas, por exemplo de SMS, aplicativos como WhatsApp ou de mensagens recebidas e enviadas por e-mail, obtidas no momento do flagrante, mas sem que haja prévia autorização legal para a análise dos dados do dispositivo móvel, serão consideradas como ilícitas. [14]

Em relação ao local do crime, o ambiente se mostra como um território insipiente que pode ser rapidamente modificado, como no caso de alguém cometer um crime de calúnia via postagem em uma rede social, porém antes que isso seja devidamente salvo por alguém, o autor pode deletar a publicação e dificultar a condenação pela referida infração. Por isso, a utilização de ferramentas adequadas e, sobretudo, lícitas para a coleta e produção de provas no meio cibernético deve ser algo realizado de maneira eficaz e condizente com cada crime em questão.

Dentre as inovações surgidas como meio de prova, pode-se ressaltar o que comumente se chama de "printscreen", que se caracteriza por uma captura de tela de algum dispositivo informático, a qual é largamente utilizada atualmente em decorrência da sua facilidade de produção e armazenamento. No entanto, a validade do printscreen por vezes é questionada, uma vez que é produzida de forma unilateral e não é capaz de guardar os metadados necessários a comprovação do conteúdo ali disposto. Ademais, esse tipo de documento não goza de fé pública e é facilmente passível de ser alterado.

[14] STJ, 5ª Turma, HC 372.762, Rel. Min. Felix Fischer, publ. 16.10.2017

Como alternativa as fraquezas do printscreen, há a possibilidade de salvamento de toda a página da internet, por exemplo, na qual um eventual delito teria sido cometido, de forma que fossem preservadas as informações da URL (Uniform Resource Locator), que pode ser compreendido como o endereço virtual no qual se encontra algum conteúdo informático. Também existem softwares que auxiliam nesse quesito, como no caso do HTTrack, que está disponível de forma gratuita e permite o armazenamento de todo um site, incluindo as imagens, fontes, html e outras fontes do servidor.

Visando a preservação das provas e a manutenção da legitimidade e licitude dos materiais relacionados ao potencial crime, ainda há algumas alternativas usualmente já conhecidas pelo direito. Acerca dos mecanismos já aplicados, podemos destacar a ata notarial, que está prevista no art. 384 do CPC e que é um documento dotado de fé pública, lavrado por um tabelião, de modo que os fatos nela assinalados possuem presunção relativa de veracidade, podendo assim, ser utilizada para preservar a evidência cibernética.

Uma outra forma, é a certidão do escrivão, que também é um documento dotado de fé pública, mas que é lavrado por servidor público, como no caso do escrivão das delegacias de polícia, e, portanto, também é capaz que guardar o conteúdo ali discutido de uma forma que seja útil ao processo da parte interessada que requerer a produção do documento.

Cabe ainda ressaltar que as plataformas e provedores de tecnologias, possuem algumas obrigações legais sobre a manutenção de certas evidências e informações, conforme previso no Marco Civil da Internet em seu 13 §2º e 15 §2º bem como de compartilhá-las quando solicitado pelas autoridades competentes, como no caso do Ministério Público, autoridade policial ou administrativa. Esse acesso pode ser solicitado por ofício extrajudicial.

Também é interessante destacar a tecnologia *blockchain*, comumente conhecida por sua aplicação em criptomoedas como forma de documentação e rastreio. Ocorre que sua abrangência vai muito além disso, pois ela funciona como espécie de um livro contábil em que são feitos registros de operações e que os mantém imutáveis, ou até mesmo para o arquivamento de documentos ou contratos.

A cooperação das empresas com o poder público também é algo essencial no combate à criminalidade cibernética e que trouxe por exemplo a criação do que se conhece por *"plataforma records"*, que é uma espécie de canal de atendimento das empresas com o Poder Público que vem facilitando o envio de informações para auxiliar as autoridades em suas

investigações. Algumas empresas como Facebook, WhatsApp e Instagram já utilizam essa modalidade de serviço.

Nota-se, portanto, que há formas de produção de provas que podem apoiar os cidadãos e dar suporte as autoridades quando diante de uma investigação, mas que também surge uma preocupação em relação a celeridade que isso acontece ou simplesmente da eficiência diante da constante e ágil mudança no ambiente digital. A tecnologia surge rodeadas de fraquezas e pontos de atenção que precisam ser combatidos para que a sociedade não se veja diante da impunidade, em decorrência da ausência de materialidade probatória suficientemente capaz de nos mostrar os argumentos para punir ou absolver os envolvidos.

3 CONCLUSÃO

Diante da análise apresentada, verificou-se a importância do estudo da criminalidade cibernética, assim como da necessidade de uma forte atuação policial e judicial, principalmente no tocante ao combate célere de um crime que em sua essência é ágil e perspicaz. Essa modalidade de crime, que vem se aperfeiçoando cada vez mais com o avanço da tecnologia, afeta diariamente pessoas físicas e jurídicas, fazendo-as de vítimas desses delitos, as quais necessitam de um aparato robusto do Estado frente as mazelas e prejuízos auferidos.

Pelo exposto, é evidente que há algumas formas de produção de provas mais rápidas e que são capazes de captar e guardar o exato conteúdo e momento do possível crime cibernético, como no caso do printscreen, mas que por sua vez, oferece riscos a confiabilidade do material, uma vez que são produzidos de maneira unilateral e passível facilmente de adulteração, e não sendo possível a análise dos metadados como forma de validação do conteúdo.

Por outro lado, o direito já possui mecanismos robustos que podem dar sustentação aos materiais coletados no ambiente digital, tais como a ata notarial, a perícia ou ofício extrajudicial, dentre outros, mas que podem não apresentar a celeridade necessária e acompanhar a rápida mudança que é comumente vista neste tipo de crime, de modo que os conteúdos possam ser perdidos, deletados ou simplesmente modificados.

Por fim, temos a clara compreensão que este trabalho não esgota todas as formas de criminalidade digital e tampouco é exaustiva em correlacionar a (in)eficiência de alguns tipos de meio de prova que podem ser aplicáveis e úteis ao ambiente cibernético. Apenas buscamos trazer para debate a necessidade de avançar tanto no aspecto normativo, quanto no aspecto tecnológico, o combate a criminalidade digital, já que, em sua essência, retroceder não é uma

opção, e a humanidade certamente já incorporou uma ânsia por constantemente implantar mecanismos de tecnologia e inovação que possam tornar a vida mais produtiva, com mais qualidade e menos barreiras a globalização.

REFERÊNCIAS

AVAST. **Guia essencial sobre ransomware**. Disponível em: https://www.avast.com/pt-br/c-what-is-ransomware#gref. Acesso em: 16 jan. 2022.

BARRETO, Alessandro Gonçalves. KUFA, Karina. SILVA, Marcelo Mesquita. **Cibercrimes e seus reflexos no direito brasileiro**. São Paulo: JusPodvm, 2021.

BAUMAN, Zygmunt. **Modernidade líquida** – tradução Plínio Dentzien. Rio de Janeiro. Zahar: 2001.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 15 jan. 2022.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 15 jan. 2022.

BRASIL. **Lei nº 12735, de 30 de novembro de 2012.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 15 jan. 2022.

CNJ, Conselho Nacional de Justiça. **Crimes digitais: o que são, como denunciar, e quais leis tipificam como crime?** Disponível em: https://www.cnj.jus.br/crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime/. Acesso em: 30 out. 2021

CRESPO, Marcelo. **Crimes digitais: do que estamos falando?** Disponível em: https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/. Acesso em: 30 out. 2021.

DEPUTADOS, Câmara dos; Agência Câmara de Notícias. **Promulgada PEC que inclui a proteção de dados pessoais entre direitos fundamentais do cidadão.** Disponível em: https://www.camara.leg.br/noticias/850028-promulgada-pec-que-inclui-a-protecao-de-dados-pessoais-entre-direitos-fundamentais-do-cidadao/. Acesso em 05 mar. 2022.

FEBRABAN. **As fraudes e os golpes mudam todo dia, a melhor forma de prevenção é se manter informado.** Disponível em: https://antifraudes.febraban.org.br/?gclid=CjwKCAiA_omPBhBBEiwAcg7smUUZD26QcH2JZCmFaraJIxezgMWI_S2hscCk2BfMOe6SksiFoy86exoCrPMQAvD_BwE. Acesso em 15 jan. 2022.

FILHO, Paulo Roberto Aguiar de Lima. **O direito penal na quarta revolução industrial: A expansão razoável frente aos crimes cibernéticos**. Delictae Revista De Estudos Interdisciplinares Sobre O Delito, 6(10). Disponível em: https://doi.org/10.24861/25265180.v6i10.150. Acesso em: 30 out. 2021.

FMP, Fundação Escola Superior do Ministério Público. **Lei Carolina Dieckmann: você sabe o que essa lei representa?** Disponível em: https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/. Acesso em: 15. Jan. 2022.

FORBES. **Coronavírus acelera migração para ecommerce no Brasil**. Disponível em: https://forbes.com.br/negocios/2020/05/coronavirus-acelera-migracao-para-ecommerce-no-brasil/. Acesso em: 15 jan. 2022.

GAMON, Vicente Pons. **Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad**. URVIO. Revista Latinoamericana De Estudios De Seguridad, (20), 80-93. Disponível em: https://doi.org/10.17141/urvio.20.2017.2563. Acesso em: 30 out. 2021.

G1. **Com pandemia, comércio eletrônico tem salto em 2020 e dobra participação no varejo brasileiro.** Disponível em: https://g1.globo.com/economia/noticia/2021/02/26/com-pandemia-comercio-eletronico-tem-salto-em-2020-e-dobra-participacao-no-varejo-brasileiro.ghtml. Acesso em: 15 jan. 2022.

NUCCI. Guilherme de Souza. **Curso de direito processual penal**. 17. Ed. – Rio de Janeiro: Forense. 2020

PRIVACY, Tech. **Hacker x Cracker qual a diferença?** Disponível em: https://privacytech.com.br/protecao-de-dados/hacker-x-cracker-qual-a-diferenca,359858.jhtml. Acesso em 15 jan.2022.

SERASA. **Como saber se meu WhatsApp foi clonado?** Disponível em: https://www.serasa.com.br/premium/blog/como-saber-se-seu-whatsapp-foi-clonado. Acesso em: 15 jan. 2022.

WHATSAPP. **Sobre o WhatsApp**. Disponível em: https://www.whatsapp.com/about/?lang=pt_br. Acesso em: 15 jan. 2022.

ZANIOLO, Pedro Augusto. **Crimes Modernos: O impacto da tecnologia no direito**. 4ª ed. Salvador: JusPodvm, 2021.