CRIMES CONTRA O PATRIMÔNIO NA INTERNET: GOLPES FINANCEIROS E A ATUAÇÃO ESTATAL NA APLICAÇÃO DA LEI PENAL

Larissa dos Santos Sena[1]
Deivid Lopes de Oliveira[2]
Fábio da Silva Santos[3]

RESUMO

Os crimes contra o patrimônio no âmbito da internet ou com auxílio de sistemas informatizados representam uma modalidade criminosa que tem crescido na atualidade, demando a necessidade de implementação de políticas públicas e leis que possam criar melhores condições para a efetividade da atuação estatual no que tange a aplicação da lei penal. Avaliando esses aspectos, este estudo teve por objetivo analisar a atuação do Poder Público para mitigar a prática de crimes contra o patrimônio no âmbito virtual, especificamente no que tange aos golpes financeiros. No Brasil, embora existam leis com significativo papel no apoio a repressão desses crimes, se verifica a necessidade de suas respectivas atualizações, ampliando as condutas cabíveis, bem como oferecendo meios que reforcem a coleta de provas de forma mais ágil, contribuindo para a identificação do criminoso e da cobrança pelo ressarcimento as vítimas pelos danos causados. Noutro giro, é imperativo a necessidade de que os usuários da internet e de suas ferramentas tenham conhecimento dos riscos associados ao compartilhamento de dados e se conscientizem quanto as medidas de segurança no acesso à internet e sistemas a esta interligados.

Palavras-chave: Crimes virtuais. Patrimônio. Aplicação da Lei Penal.

1 INTRODUÇÃO

O presente artigo tem como escopo contextualizar a sociedade pós-moderna e o crescimento das ferramentas digitais, construindo uma análise acerca das novas modalidades de crimes realizados no universo cibernético que atingem o bem jurídico patrimônio.

Os crimes cibernéticos possuem relação intrínseca com o ambiente digital e, na contemporaneidade, devido utilização exacerbada dos meios tecnológicos,

[1] Graduanda em Direito, Centro Universitário Nobre de Feira de Santana (UNIFAN), larysena82@gmail.com
[2] Mestre em Direito (Universidade Federal da Bahia), Centro Universitário Nobre (UNIFAN), deivid_dlo@hotmail.com
[3] Professor Orientador da disciplina Trabalho de Conclusão de Curso (TCC) II do Centro Universitário Nobre (UNIFAN), fabiosantos.direito@gruponobre.edu.br

.

verifica-se elevação da ocorrência desses tipos de crime, que podem ser denominados de cibercrimes. Nesse sentido “o crime eletrônico é, em princípio, um crime de meio, isto é, utiliza-se de um meio virtual” (PINHEIRO, 2013, p. 164).

Nessa premissa, é de extrema importância que o Direito Penal consiga se adequar às inovações jurídicas trazidas no âmbito digital para efetivamente regular e coibir os delitos praticados nessa esfera. Uma vez que ainda impera a crença de que o meio digital é um ambiente marginal, um submundo em que a ilegalidade impera.

Logo, a importância do presente artigo consiste na construção de uma análise sobre a eficácia do *jus puniendi* estatal na esfera cibernética. Desde o contexto da investigação criminal até a aplicação da sanção correspondente, à Luz do Código Penal, da doutrina e de legislações extravagantes de modo que seja possível desenvolver um estudo atualizado e com fundamento na realidade enfrentada pela sociedade atualmente.

Por fim, o trabalho tem como objetivo geral analisar a atuação do Poder Público para mitigar a prática de crimes contra o patrimônio no âmbito virtual, especificamente no que tange aos golpes financeiros. Tem-se como objetivos específicos: descrever o papel do Poder Público como órgão regulador e fiscalizador da utilização das ferramentas digitais; identificar tipos e incidência dos crimes contra o patrimônio na esfera virtual; e analisar a eficácia do *jus puniendi* estatal no âmbito cibernético e virtual quanto aos crimes contra o patrimônio.

As ferramentas de pesquisa utilizadas no presente estudo, que fazem parte do embasamento teórico deste artigo, consistem na pesquisa documental e bibliográfica acerca do tema proposto. Bem como, em uma análise de legislação de direito material e processual penal, especificamente o Código Penal, dos julgados relacionados aos crimes contra o patrimônio no âmbito virtual e legislações correlatas.

2 OS CRIMES CONTRA O PATRIMÔNIO FACE AO NOVO PARADIGMA DA CRIMINALIDADE DIGITAL

Os avanços das ferramentas tecnológicas introduziram mudanças significativas nas ações humanas, mas trouxeram consigo algumas preocupações relacionadas aos atos ilícitos praticados no ambiente virtual. Este tópico busca elucidar quais são esses crimes e como eles se materializam, sendo apresentada a

distinção entre crimes virtuais próprios e impróprios, e suas tipificações, bem assim as vulnerabilidades presentes no ambiente informático que são utilizadas pelos criminosos, conforme se observa nos subtópicos seguintes.

2.1 DISTINÇAO ENTRE CRIMES VIRTUAIS PRÓPRIOS E IMPRÓPRIOS

Para a construção de uma análise acerca da temática, é de salutar relevância a exposição das diferenças conceituais entre os crimes virtuais, informáticos ou digitais, uma vez que o universo cibernético apesar de fazer parte do contexto social e das relações interpessoais, ainda tem seus conceitos pouco explorados, seja no universo acadêmico ou na informalidade.

Nesse sentido, os crimes de informática constituem condutas, decorrentes da evolução da internet, das redes sociais e das diversas possibilidades de acessos aos sistemas de grandes empresas ou de terceiros por criminosos, que favoreceram a prática de condutas delituosas com a intenção de obtenção de vantagem econômica. Em geral são executados, por indivíduos especializados no ramo tecnológico (CASTRO, 2003; CAMPELO; PIRES, 2019).

Quanto ao conceito, pode-se dizer que:

> Crime virtual ou crime digital pode ser definido como sendo termos utilizados para se referir a toda a atividade onde um computador ou uma rede de computadores são utilizados como uma ferramenta, uma base de ataque ou como meio de crime. Infelizmente, esta prática tem crescido muito já que esses criminosos virtuais têm a errada impressão que o anonimato é possível na Web e que a Internet é um “mundo sem lei (BRASIL,.2008, p.23).

Logo compreende-se, que os crimes virtuais representam condutas ilícitas que são realizadas com a intermediação de dispositivos de informática e da internet.

Trazendo uma explicação mais abrangente, Sidow (2009, p. 52) menciona que:

> Na criminalidade da informática, os bens jurídicos atacados serão ou (a) um sistema de processamento de dados, transmissão de dados ou (b) qualquer outro bem jurídico, desde que especificamente violado pelo intermédio do recurso do processamento automático de dados ou sua transmissão.

Sydow (2009) destaca ainda que os crimes virtuais são crimes específicos, com comportamento próprio e que se diferenciam dos crimes “reais” por não possuírem em sua conduta típica uma ação física ou violenta, já que ocorre por meio eletrônico, não tem local, ou padrão que possa explicar de fato a sua ocorrência.

Alessandro Barata (2002) diferencia crimes de informática e crimes cibernéticos. Para o autor o primeiro representa ações criminosas praticas com computador e outros recursos de informática com intenção de expor alguém ou prejudicar, enquanto o segundo são aqueles cometidos por meio da internet, sendo derivado do primeiro, mas restrita a intermediação por meio das redes sociais, sites, entre outros.

Quanto a caracterização, sabe-se que nestes tipos de crimes o acesso a sistemas de informações não permitidos, constitui o principal elemento para sua realização e são classificados em crimes próprios e crimes impróprios.

Damásio Evangelista de Jesus e José Antônio Milagres (2016, p.17) relatam que:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado.

Os crimes dessa natureza são aqueles em que o componente de informática tem papel importante na sua caracterização, englobando assim, aqueles contra software ou hardware, uso de dados armazenados em computador, entre outros.

Quanto aos crimes considerados impróprios, Damásio Evangelista de Jesus e José Antônio Milagres (2016, p.18) mencionam que:

> são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço “real”, ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.

Nessa segunda modalidade, embora a máquina seja um meio utilizado para realização de condutas elas se materializam por meio da rede e sistemas de informática, são exemplos nesses casos a pedofilia, estelionato, entre outros.

Na tipificação dos crimes virtuais, o sujeito ativo é a pessoa que realizou o ato criminoso, ou seja, quem invadiu dados, adulterou informações, difamou, entre

outros. O sujeito passivo é a vítima da ação danosa, podendo ser o Estado, pessoas físicas ou jurídicas (PINHEIRO, 2013).

Oliveira (2002) relaciona diversas condutas já consagradas pela legislação penal brasileira como delituosas, que também são consideradas crimes quando ocorridas por intermédio do ambiente virtual, são elas: pirataria, dano ao patrimônio, sabotagem informática, pornografia infantil, apropriação indébita, estelionato, entre outros, o Quadro 1 a seguir resume seus principais aspectos.

Quadro 1- Caracterização dos Principais crimes ocorridos no ambiente virtual

Crime	Característica	Pena
Pirataria	Copiar dados em CDs, DVDs ou qualquer base de dados sem prévia autorização do autor é percebido como pirataria em conformidade com a Lei 9.610/98.	2 meses a 4 anos e multa.
Dano ao patrimônio	Previsto no art. 163 do Código Penal. O dano pode ser simples ou qualificado, sendo estimado qualificado quando "o dano for contra o patrimônio do público, de empresa de empresa concessionária de serviços públicos ou de sociedade de economia mista.	No dano simples cabe detenção, de um a seis meses, ou multa. No dano qualificado, a pena prevista é detenção de seis meses a três anos e multa.
Sabotagem informática	Invasão de determinado estabelecimento, objetivando prejudicar e/ou roubar dados.	A lei apenas prevê punição de 1 a 3 anos de prisão e multa.
Pornografia infantil	Ato de apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, de modo inclusivo na rede mundial de computadores ou Internet, fotografias ou imagens com pornografia ou cenas de sexo explícito abrangendo criança ou adolescente	Detenção de 2 a 6 anos e multa.
Apropriação indébita	Apropriação indébita de bens materiais, como por exemplo CPU, mouse e monitor.	Reclusão de 3 a 6 anos e multa.
Estelionato	Obtenção de vantagem ilícita em razão de prejuízo alheio.	Reclusão de 1 a 5 anos e multa.

Fonte: Elaborado a partir de Oliveira (2002)

Nota-se que as principais modalidades de condutas ilícitas tipificadas sob a modalidade de crimes virtuais, também possuem uma abordagem voltada ao crime “real”. Ao refletir sobre esse aspecto Patury e Lopes (s.d,p.2) mencionam que:

> Já é perceptível que o uso da internet acompanha diferentes condutas passíveis de causar lesões a diversos bens jurídicos, razão pela qual se

> suscita a possibilidade de se enquadrar condutas praticadas no meio virtual aos tipos penais já existentes. Sendo assim, o conjunto norma-sanção é tão necessário no mundo digital quanto no real.

Nesse diapasão, apesar de haver uma variedade de condutas que podem ser percebidas no meio virtual como práticas criminosas, ainda há diversos casos que a legislação não acompanhou a tipificação de forma proporcional, deixando lacunas legais que tem contribuído em muitos aspectos para manter tais criminosos a margem da lei. São exemplos desses crimes o uso de e-mails simulando órgãos públicos ou empresas, o compartilhamento de links que clonam dados de celular, ou mesmo o uso de *Whatsapp* e *Telegram* com a finalidade enganosa (ZAPAROLLI, 2020).

2.2 O AMBIENTE INFORMÁTICO E AS VULNERABILIDADES UTILIZADAS PELOS CRIMINOSOS

O meio digital propicia que seus usuários se deparem com diversas situações em que tem seus dados expostos e vulneráveis frente as diversas manobras utilizadas por criminosos para auferir vantagens econômicas ilícitas, seja induzindo a potencial vítima ao erro ou se beneficiando das próprias falhas dos sistemas de proteção de dados na esfera virtual. Nessa premissa, denota-se que o ambiente informático ainda possui deficiências na sua regulamentação, bem como na rede de proteção de dados, o que torna precária a tutela dos indivíduos enquanto sujeitos de direitos e consumidores.

Assim, segundo Wolfgang (2021), nos Estados Democráticos de Direito, as variadas possibilidades vinculadas ao acesso de dados no ambiente virtual e a seu processamento para influenciar condutas, incluindo o comprometimento dos direitos de liberdade, bem como a influência no desenvolvimento social, necessitam de controle jurídico que deve ser exercido pelo Estado através das normas. Com isso, observa-se que, em que pese a sociedade esteja vivenciando a cultura da hiperconectividade digital, são notórias as dificuldades do legislador em acompanhar as inovações no que tange as condutas ilícitas praticadas no âmbito da criminalidade virtual.

Nessa linha de atividade criminosa, se destaca a atuação de dois tipos de delinquentes: o *cracker* e o *carder*. O primeiro utiliza seu conhecimento informática e em tecnologias virtuais para invadir sistemas, criar vírus, com a intenção de causar prejuízo alheio, além de realizarem captação de dados visando angariar lucros ilícitos. O segundo, considerado um estelionatário virtual, é um poderoso conhecedor das falhas dos sistemas de segurança de empresas ou das vulnerabilidades dos consumidores, assim cria programas que realizam compras utilizando-se de dados alheios obtidos ilegalmente (ROCHA, 2013 *apud* LEHFELD, 2021).

No Brasil essa realidade tem reforçado a busca por empresas especializadas em segurança cibernética, já que a ausência de um adequado sistema de proteção pode favorecer a perpetuação de diversos crimes, a exemplo, dos ataques cibernéticos ocorridos contra a Natura e a montadora Honda em junho de 2020. De acordo com as informações fornecidas pela multinacional russa de cibersegurança Kaspersky, foi registrado 1,6 bilhão de tentativas de invasões de dados no Brasil entre fevereiro e abril, do mesmo ano (ZAPAROLLI, 2020).

Zaparolli (2020) destaca os ataques de *ransomware* que englobam o uso de *malwares* para invadir e assumir o controle de computador ou do smartphone, como um dos principais crimes praticados no país. Para o autor, o que contribui para que essas ameaças continuem por aí, está diretamente relacionado ao baixo investimento em cibersegurança, que também culmina com a escassez de mão-de-obra qualificada nesta área.

Para Gomes, Nunes e Wilmers (2020) o principal dilema vivenciado pelo crime de *ransomware* é o fato de que este se consuma por uma conduta que se assemelha a prática de extorsão, no qual o invasor de dados após obter o acesso ao sistema informático da vítima, utiliza uma espécie de bloqueio para que o dono dos dados acessados, seja impedido de retomar o controle sobre as suas informações, e ao fim, exige quantia para devolver o acesso a vítima. Diante disso, o ordenamento jurídico pátrio se depara com uma lacuna, já que o crime de sequestro de dados não é tipificado na lei penal, além disso, há uma enorme dificuldade em se identificar diretamente o beneficiário da vantagem indevida, já que não há legislação específica que controle ou regule transações dessa natureza.

Para Lehfeld et al. (2021) a disseminação e crescimento de casos de crimes virtuais encontram respaldo na vulnerabilidade do consumidor no meio eletrônico, e

se dá pela falta de proficiência informática e ausência de saberes básicos na compreensão da tecnologia utilizada. Por sua vez, o distanciamento entre os sujeitos do mundo real, aliado à falta de regulamentação e proteção do ciberespaço deu força para a possibilidade de que novos crimes pudessem ser praticados nesse ambiente.

É importante destacar, que dentre as fragilidades observadas o compartilhamento exacerbado de informações pessoais nas redes sociais, a troca de informações em sites não seguros, são as mais comuns. Em muitos casos, o criminoso utiliza as próprias redes sociais, utilizando a identidade da vítima, para solicitar quantias para parentes e amigos próximos.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT (2012) enumera alguns dos principais riscos relacionados a utilização da internet e das redes sociais, são eles:

a)Acesso a conteúdos impróprios ou ofensivos: visualização de páginas com conteúdos pornográficos durante a navegação.

b)Contato com pessoas mal-intencionadas: pessoas podem usar identidades falsas ou o anonimato da internet para aplicar golpes.

c)Furto de identidade: pessoas podem roubar identidade de outra pessoa

d)Furto e perda de dados: consiste em furtar e apagar dados presentes em equipamentos conectados à internet pela ação de ladrões e atacantes com códigos maliciosos.

e)Invasão de privacidade: divulgação de informações pessoais comprometendo a privacidade alheia.

f) Vazamento de informações: divulgação de conteúdos sigilosos de empresas, detalhes técnicos de novos produtos antes mesmos de sua aprovação final.

g)Disponibilização de informações confidenciais: troca de informações como endereços, senhas e números de cartão de crédito.

h)Uso de equipamentos sem programas de antivírus e combate a ação criminosa: a utilização da internet sem o devido respaldo em segurança eletrônica é um alto risco a proteção de dados.

Os golpistas financeiros têm intensificado cada vez mais as condutas utilizadas, e exploram as fragilidades dos usuários para enganar e persuadir, utilizando-se de estratégias diversas para obter dados financeiros e,

consequentemente, angariar vantagens ilícitas. Normalmente, o golpe pode ocorrer a partir de um link compartilhado por e-mail ou rede sociais, que podem trazer mensagens de assuntos como dieta, vagas de emprego, pesquisas de mercado, sempre com o nome de alguma empresa consolidada ou grupo conhecido, no entanto, se trata de vírus ou programas construídos para invadir o computador da vítima ou seu *WhatsApp* e levantar seus dados com a intenção de realização de fraudes financeiras (CERT, 2012).

Em geral, conclui-se que os riscos e a grande maioria dos crimes virtuais ocorrem pela falta de conhecimento, negligência e imprudência dos usuários que não utilizam práticas de segurança adequadas durante o uso da internet, de suas ferramentas ou canais de comunicação. Por outro lado, a fragilidade legal, e a escassez de ferramentas e qualificação na investigação policial, contribuem para dificultar a caracterização da conduta delituosa e a identificação do criminoso, assim, esses aspectos dificultam a proteção do bem jurídico tutelado, bem assim, corroboram para a sensação de impunidade, já que em grande parte dos casos, não há um desfecho com aplicação da sanção correspondente ou restituição do prejuízo financeiro.

3 O TRATAMENTO ESTATAL DISPENSADO AS NOVAS FORMAS DE ATUAÇÃO CRIMINOSA

Nesta seção, apresentamos um breve relato sobre os atuais instrumentos legais existentes para promover a repressão e combate aos crimes virtuais, bem como sobre seus entraves no processo de persecução penal e as inovações legislativas que podem auxiliar na melhor forma de inibir e punir os crimes virtuais.

3.1 OS INSTRUMENTOS ESTATAIS DE REPRESSÃO E COMBATE AOS CRIMES CIBERNÉTICOS PATRIMONIAIS

Os constantes relatos de crimes cibernéticos têm forçado a necessidade do Estado de coibir práticas que concorrem para sua consumação. Diante, de não ser permitido no Direito Penal se utilizar analogias que prejudiquem o autor da infração, em relação as tipificações já existentes, se torna imperativo a criação de leis que possam classificar essas condutas (POLEGATTI; KAZMIERCZAK, 2012).

Nesse tocante, coube ao Direito Penal evoluir para abarcar novos tipos de crimes, incluindo as práticas de delitos ocorridos no ambiente virtual ou que se efetivam por meio dele, com a finalidade de resguardar os direitos dos cidadãos protegendo-os de atos que possam lhe causar danos financeiros, morais ou a imagem (MONTEIRO NETO, 2008).

No Brasil, a primeira legislação que trouxe como objeto a punição de crimes virtuais propriamente dita foi a Lei nº 12.737/2012, batizada de Lei Carolina Dieckmann devido a ser resultado da repercussão da exposição de fotos íntimas da atriz na internet de forma maliciosa. A referida legislação atualizou o Código Penal, introduzido tipificação para algumas condutas criminosas vinculadas ao ambiente virtual, são elas: a invasão de dispositivo informático, interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, falsificação de documento particular e de cartão. As penas aplicáveis são progressivas de acordo com a gravidade e especificações da conduta descritas na lei e podem variar de 3 meses a 3 anos, com multa prevista.

O marco civil da internet é a Lei nº 12.965/2014 que entrou em vigor no desde o dia 23 de junho de 2014 e regulamenta o uso da internet no país, bem assim trata as condições para acessibilidade, conexão, troca e divulgação de dados, resguardando o direito do sigilo de dados privados, bem como da adoção de medidas de segurança para a proteção de dados de terceiros pelas empresas prestadoras de serviços dessa natureza.

Posteriormente em 2018, a Lei nº. 13.709, tratou da primeira proposição da Lei Geral de Proteção de Dados (LGPD), que posteriormente foi alterada pela Lei nº 13.853 de 2019, e disciplina a proteção de dados pessoais e tem como fundamentos:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

A importância da LGPD para o contexto atual está no fortalecimento de práticas que venham ampliar as condições para que seja implementado um cenário de segurança jurídica vinculado ao uso e compartilhamento de dados no ambiente virtual, sobretudo, para se resguardar os direitos e garantias prevista na constituição e estimular meios de prevenção a crimes virtuais.

Outro ponto importante na repressão contra os crimes virtuais se dá a partir da Lei nº. 14.155 de 2021 que aumentou as penas vinculadas aos crimes cibernéticos de invasão de dispositivo informático, fraude eletrônica, estelionato praticado no ambiente virtual contra idoso ou vulnerável, passando as penas destas condutas delituosas a variar entre 1 a 8 anos, podendo ultrapassar a 13 anos, caso seja aplicada majoração pela gravidade do ato.

Além dessas legislações supracitadas, vale destacar a existência da Lei nº 9.296/1996 que versa sobre a interceptação de comunicação telemática ou informática; da Lei nº 9.609/ 1998, que regula a proteção da propriedade intelectual do programa de computador, da Lei nº 9.983/2000, que tipificou os crimes relacionados ao acesso indevido a sistemas informatizados da Administração Pública, da Lei nº 11. 829/2008 que versa sobre o combate a pornografia infantil na internet e a Lei nº 12.034/2009, que delimita os direitos e deveres dentro da rede mundial, durante as campanhas eleitorais, como instrumentos legislativos que convalidam as legislações mais recentes, e demonstram que a preocupação do Estado em resolver questões pertinentes a crimes envolvendo tecnologias e a internet não é uma questão tão nova, mas que teve lento processo de sistematização e atualmente atravessa a emergência de evoluir para atender as constantes demandas de atos ilícitos praticado no ambiente virtual (BORLOT, 2017).

3.2 INOVAÇOES LEGISLATIVAS

Apesar de existirem tipificações penais para os crimes virtuais, sabe-se que estas ainda não são suficientes para alcançarem todas as condutas danosas existentes, o que torna necessário implementação por parte do Estado de uma estrutura que possibilite investigações mais eficazes, como também, meios de prova e identificação do ocorrido, possibilitando melhor segurança jurídica para os usuários do mundo virtual e eletrônico (SMITH; SANCHES; BORBA, 2020).

Um dos primeiros passos, seria então promover a implementação de uma política criminal específica para os crimes virtuais, que pudessem atualizar as legislações existentes, implementando medidas de segurança e punibilidade para as condutas ainda não previstas especificamente, bem como visando assegurar meios para que as provas e a identificação do criminoso pudessem ocorrer de forma mais ágil.

Outro possível caminho está na participação do Brasil na Convenção de Budapeste, que objetiva a promoção de medidas de proteção da sociedade contra os crimes ocorridos pela internet, designando leis e a cooperação de seus países-membros. A possibilidade de adoção de protocolos internacionais de segurança e de um padrão legal para o combate aos crimes virtuais em nível internacional torna mais robusta as políticas atuais e é algo necessário, já que esses crimes podem atingir diferentes partes do mundo (SOUZA; PEREIRA, 2009).

Quanto a este aspecto, um avanço foi dado em 14 de dezembro de 2021 por meio da promulgação do Projeto de Decreto Legislativo (PDL) 255/2021 que trata da adesão do Brasil a Convenção de Budapeste, que já foi assinada por mais de 60 países (MINISTÉRIO PÚBLICO FEDERAL, 2021).

3.3 OS ENTRAVES BUROCRÁTICOS DE PERSECUÇÃO CRIMINAL NA RESOLUÇÃO DESTES CRIMES

Os crimes virtuais são complexos e apresentam grande dificuldade de comprovação. Aspectos como a fragilidade na produção de provas, na determinação dos locais em que estes se consumam, bem como na identificação do infrator, fomentam um cenário de impunidade e aumento de casos subnotificados, sobretudo diante de existir poucas equipes técnicas qualificadas para apurar esses tipos de delitos (MORAES; SILVA; SANTIAGO, 2020).

Carvalho, Souza e Costa (2017) elencam como uma das principais dificuldades a ausência de leis específica, e muito embora exista uma corrente doutrinária que acredite que todos os tipos penais poderiam ser aplicados no ambiente dos crimes virtuais, em que pese, esse caminho afrontar a própria aplicação da lei penal que veda a analogia *in malam partem*, por esta ferir o princípio da taxatividade.

Vidal (2015) tece críticas a fragilidade presente na identificação de provas nos crimes virtuais e isso se deve ao fato delas serem extremamente voláteis, podendo ser apagadas ou perdidas facilmente. Noutro giro, há casos em que as evidências podem se encontrar envoltas a uma grande quantidade de dados legítimos, demandando uma análise técnica e pericial apurada para identificar os possíveis criminosos.

Quanto ao perfil do criminoso, tem-se também uma dificuldade em sua caracterização. Na atualidade o fácil acesso à informação e as novas tecnologias, tem inserido diversos perfis de usuários na internet. Embora seja notório que certas práticas criminosas demandam muito conhecimento e habilidades em sistemas, tais aspectos não estão restritos apenas a pessoas com capacidade penal, o que reflete a possibilidade de que estes infratores possam ser ainda menores, demandando que a política criminal também possa contemplar esses crimes no âmbito penal da infância e juventude (MORAES. SILVA; SANTIAGO, 2020).

Outra questão relevante, citada por Moraes, Silva e Santiago (2020), ocorre nos casos em que o crime atinge vítimas difusas, a exemplo de grandes empresas, que mesmo sendo confirmado o delito, preferem não acionar a justiça e a investigação do Estado, devido ao fato de que a publicidade das informações seria negativa, havendo um prejuízo maior a sua imagem, com repercussões incalculáveis ao longo prazo quando comparado ao dano já sofrido.

4 ANÁLISE DAS ATUALIZAÇÕES NECESSÁRIAS AO ENFRENTAMENTO DS INOVAÇÕES CRIMINOSAS

Neste tópico visando ampliar a discussão sobre as dificuldades enfrentadas na caracterização dos crimes virtuais, é necessário tecer um breve relato sobre os meios digitais visto como maior desvalor de condutas, bem como apresentar uma breve explanação sobre a realidade existente no processo de reparação de danos causados por crimes virtuais, conforme se observa no subtópicos seguintes.

4.1 MEIO DIGITAL VISTO COMO MAIOR DESVALOR DE CONDUTA

Conforme expõe Stephan Doering Darcie (2020) o desvalor de conduta, constitui uma das dimensões essenciais do crime, porque para que este seja

tipificado é necessário a materialização de uma conduta estabelecida como ilícita. Por outro lado, o juízo sobre o aumento de uma pena ou exclusão de um crime depende da relação material entre o grau de desvalor revelado pelo caso concreto e aquele caracterizado nos dispositivos legais potencialmente aplicáveis.

No entanto, no plano virtual, essa materialização nem sempre é possível, como também nem em todos os casos estão previamente estabelecidas as condutas delituosas ocorridas, fato que concorre, em grande parte, para que o criminoso se mantenha impune ou seja apenas alcançado pelos delitos menores praticados que possuem previsão legal.

Dias e Dias (2012) ao relatar sobre estes aspectos consideram como uma problemática ocorrida quanto aos crimes virtuais a limitação de sua tipificação e extensão de sua conduta, o que permite que punições deixem de ser executados.

Busato e Huapaya (2007) destacam que o *jus puniendi* responde a um desvalor de conduta e de resultado ao mesmo tempo, sendo necessário para ocorrência de um crime a existência de uma conduta que afeta um bem jurídico. Nesse sentido, o merecimento da pena estaria condicionado a relação entre conduta e dano, cabendo ao Estado estabelecer uma sanção adequada para proteção do bem jurídico.

Por essa visão, o crime cibernético contra o patrimônio, só ocorreria de fato se da conduta resultasse lesão ao bem da vítima, mas há que se considerar, o risco que a tentativa desse ato também poderia ter como resultado. Isso porque, no roubo de dados de cartão de crédito, acesso a contas, documentos pessoais, por exemplo, mesmo que não tenha se chegado à conclusão do feito, a mera tentativa já seria uma condição delituosa, devido aos possíveis efeitos futuros que este compartilhamento de dados poderia causar, até porque, ninguém sabe que se da exposição de dados, quantas pessoas poderiam utilizar a mesma informação, mesmo que em momentos diferenciados.

Buscando elucidar essa situação, Dias e Dias (2012) mencionam sobre o crime de extorsão, que está descrito no art. 158 do código penal, que muito embora tenha se massificado no ambiente cibernético por meio de acesso de dados pessoais, imagem em sites ou clonagem de WhatsApp, não encontra materializada sua conduta criminosa quando se refere a crimes praticados por intermédio de sistemas informatizados conectados à internet.

Na prática, as particularidades que englobam os crimes virtuais, não podem deixar de ser avaliadas durante a descrição da conduta delituosa, não apenas o desvalor do resultado imediato associado a conduta deveria ser o caminho para se determinar ou não a sua tipificação, como também a possibilidade subjetiva do desvalor do resultado, quando este tem chances de se tornar objetivo, causando um dano futuro. Um exemplo dessa problemática pode ser verificado nos crimes em que, por exemplo, o sujeito pratica a infração ao disponibilizar na internet imagens confidenciais de outrem, a exemplo, cenas de sexo ou nudes. Em muitos casos, o desvalor do resultado vai além da exposição de imagem não autorizada, quando devido ao constrangimento, por exemplo, a vítima comete suicídio. No entanto, não se vê previsão legal para esse tipo de situação.

Nessa premissa, crimes de imagem contra as empresas, normalmente trazem danos patrimoniais muitas vezes incalculáveis, porque não se trata apenas de se perder um contrato atual, mas o de se perder a credibilidade no mercado. Para esses tipos de crimes, resta o questionamento se o desvalor da conduta e a pena admitida concorrem realmente para punibilidade eficaz. Dessa forma, são essas situações que fazem com que, em muitos casos, essas organizações prefiram omitir o crime, porque não encontram na lei, uma diretriz equitativa que garanta um equilíbrio entre o dano causado e a possibilidade de reparação.

4.2 ATUAÇÃO ESTATAL VOLTADA AO ALCANCE DO PATRIMÔNIO DO AUTOR E RESSARCIMENTO DA VÍTIMA

De acordo com o art. 927 do Código Civil (2002): “aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo”. Nesse caso, convém destacar que para isso ocorrer, deve primeiro ser confirmado o delito praticado.

Sanseverino (2010, p. 58), acrescenta que:

> A plena reparação do dano deve corresponder à totalidade dos prejuízos efetivamente sofridos pela vítima do evento danoso (função compensatória), não podendo, entretanto, ultrapassá-los para evitar que a responsabilidade civil seja causa para o enriquecimento injustificado do prejudicado (função indenitária), devendo-se estabelecer uma relação de efetiva equivalência entre a indenização e os prejuízos efetivos derivados dos danos com avaliação em concreto pelo juiz (função concretizadora do prejuízo real). Os prejuízos efetivamente sofridos pelo lesado constituem não apenas o piso mínimo da indenização (função compensatória), mas também estabelecem

> o seu teto máximo (função indenitária), balizando concretamente a atividade judicial voltada à sua quantificação (função concretizadora).

Em outras palavras, compreende-se que a instituição de reparação ou restituição do dano visa manter o equilíbrio na relação entre o autor e vítima, não permitindo que se mantenha, mesmo após a condenação penal, alguém prejudicado em favor de outrem.

Quanto ao valor mínimo admitido para reparação dos danos, a Lei nº 11.719/2008 estabelece que este deverá ser fixado pelo juiz, considerando-se os prejuízos sofridos pelo ofendido e isso poderá ser proferido pelo juízo criminal ao estabelecer a sentença condenatória. Assim, compreende-se que a cobrança do dever de ressarcimento do dano material pode ser solicitada tanto pelo juízo cível quanto criminal no decurso do processo penal (GANGONI, 2018).

Convém esclarecer que não cabe reparação a dano hipotético ou eventual, assim se torna necessário a comprovação efetiva dos danos, emergentes (efetivos) ou os lucros cessantes (que se deixou de lucrar), sendo apresentada prova comprobatória do seu valor (TARTUCE, 2018). Nos casos de lucros cessantes, o interessado deve realizar os cálculos e devidamente confirmadas a relação entre receitas, custos do negócio evidenciar o resultado que deixará de receber, a fim de que lhe seja concedida após vistas do juízo, que deverá avaliar se a reparação ocorre na medida da extensão do dano, para proceder a cobrança da respectiva indenização.

Nos casos de crimes virtuais, a compreensão da extensão do dano é complexa, porque não são em todas as situações que o prejuízo patrimonial é reconhecido diretamente. Em processos de crimes em que houve violação de dados, segredos, que podem ter sido, por exemplo, compartilhados, com terceiros, a própria vítima não tem condições de avaliar sua extensão, e poderá sofrer o impacto da ação criminosa por um longo período.

5 CONCLUSÃO

Os crimes virtuais tem apresentado crescimento significativo na atualidade e introduzido para o campo do Direito, algumas preocupações, sobretudo no que se

refere ao estabelecimento de meios legais que possam assegurar sua repressão e proteção a vítima, bem como estabelecer condições para sua adequada punibilidade e reparação de danos.

Embora no contexto brasileiro a existência de Leis voltadas à punição de crimes virtuais representem um passo importante no combate a esses crimes, que tem como meio ou fim a utilização da internet ou de sistemas informatizados na internet, percebeu-se pela crítica dos diversos autores, que a atual arcabouço jurídico-legal, no âmbito penal é frágil, não comporta adequadamente as condutas criminosas e não tem avançado para reprimir as novas modalidades de crimes que tem se intensificado no ambiente virtual.

A necessidade de se ter uma renovação legislativa que seja capaz de atribuir as respectivas sanções para as infrações ocorridas no ambiente virtual é emergente, e impõe ao Estado a responsabilidade de reformular suas práticas repressivas atualmente existentes. Um ponto importante a ser destacado nesse sentido, é a busca pela ampliação das delegacias especializadas em crimes virtuais e no estabelecimento de medidas que possam dar maior celeridade aos processos penais e cíveis dessa natureza, como também contemplando a volatilidade das provas e evidências, para, assim, contribuir com a agilidade na persecução penal, desde a conclusão do inquérito policial até o julgamento.

Observando-se que em alguns casos, os crimes de internet ocorrem por falta de adoção de medidas de segurança por parte da vítima, se faz oportuno que se invistam em práticas educativas que orientem aos diversos usuários da internet e de sistemas informatizados que utilizam o ambiente virtual para serem operacionalizados, a importância de estarem atentos as diversas formas de ataques virtuais, e isso pode ser iniciado e intensificado nas escolas de ensino fundamental e médio, uma vez que o uso de ferramentas de tecnologia da informação e comunicação, bem assim da internet se iniciam de forma cada vez mais precoce.

Por derradeiro, a introdução do Brasil em pactos ou convenções internacionais de proteção contra crimes virtuais também é uma estratégia que pode potencializar as ações de combate a tais crimes, bem como auxiliar na atualização de práticas que podem combater a ocorrência das suas novas modalidades, visto que, em uma sociedade interligada pela globalização, o combate à criminalidade virtual necessita ser de interesse dos principais países que integram a comunidade internacional.

REFERÊNCIAS

BARATTA, Alessandro. **Criminologia crítica e crítica do direito penal introdução à sociologia do direito penal.** 3. ed. Rio de Janeiro: Revan, 2002.

BORLOT, Jéssica Fagundes. 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

BRASIL. **Manual de cooperação jurídica internacional e recuperação de ativos: cooperação em matéria penal.** Brasília: Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, 2008.

BRASIL. **Lei nº 12. 737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 05 abr. 2022

BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 07 mai. 2022.

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: 07 mai. 2022.

BRASIL. **Lei nº 14.155,** de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 05 abr. 2022.

BUSATO, Paulo César; HUAPAYA, Sandro Montes. **Introdução ao direito penal.** Fundamentos para um sistema penal democrático. 2 ed. Rio de Janeiro: Editora Lumen Juris, 2007.

CAMPELO, Larissa; PIRES, Pamela de Freitas. **Crimes Virtuais.** 13/03/2019. Disponível em: https://jus.com.br/artigos/72619/crimes-virtuais. Acesso em: 04 mai. 2022.

CARVALHO, Daniel Leal de. SOUZA, Marta Alves; COSTA, Helder Rodrigues da. **Crimes Virtuais:** crescimento e falta de leis específicas. 2017. Disponível em: https://silo.tips/download/crime-virtual-crescimentoefalta-de-leis-especificas-daniel-leal-de-carvalho-ma. Acesso em 01 mai. 2022.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais.** 2ª ed. Rio de Janeiro: Lumen Juris, 2003.

CERT, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança No Brasil (Org.). **Cartilha de Segurança para Internet**. 2º. ed. São Paulo: Comitê Gestor da Internet No Brasil, 2012. 140 p. Disponível em: <https://cartilha.cert.br/livro/>. Acesso em: 06 mai. 2022.

DARCIE, Stephan Doering. **O desvalor da conduta no direito penal.** 2020. 56 f Tese (Doutorado em Direito) - Universidade de São Paulo. São Paulo: USP, 2020.

GANGONI, Bruno Correa. A Reparação do Dano Material e Moral à Vítima da Criminalidade. Revista do Ministério Público do Rio de Janeiro nº 70, p. 37-81, out./dez. 2018.

GOMES, Luiz Eduardo dos Santos Pereira; NUNES, Luan Esteche; WILMERS, Michael Felipe. Natureza jurídica do crime de ransomware e a utilização da criptomoeda como meio de impunidade**. Escola Superior do Ministério Público do Ceará -** Ano 12, nº2, p. 215- 234, Jul./Dez. 2020.

HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital**. Rio de Janeiro: Grupo GEN, 2020. 9788530992262. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992262/. Acesso em: 22 mai. 2022.

JESUS, Damásio Evangelista de; **MILAGRES**, José Antônio**. Manual de Crimes Informáticos**. 1ª Edição. ed. São Paulo: Saraiva, 2016.

LEHFELD, Lucas de Souza et al. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. **Rev. Eletrônica Pesquiseduca**. Santos, V.13, N. 29, p.236-255, jan-abril 2021.

MINISTÉRIO PÚBLICO FEDERAL. **Brasil aprova adesão à Convenção de Budapeste que facilita cooperação internacional para combate ao cibercrime**. 23/12/2021. Disponível em: http://www.mpf.mp.br/pgr/noticias-pgr/brasil-aprova-adesao-a-convencao-de-budapeste-que-facilita-cooperacao-internacional-para-combate-ao-cibercrime. Acesso em: 07 mai. 2022.

MONTEIRO NETO, João Araújo. **Aspectos Constitucionais e Legais do Crime Eletrônico.** Fortaleza, 2008. 192 f. Dissertação (Mestrado em Direito Constitucional) –Universidade de Fortaleza. Fortaleza: UNIFOR, 2008.

MORAES, Alexandre Rocha Almeida de; SILVA, Isabela Tucci; SANTIAGO, Bruno. Os cibercrimes e investigação digital: novos paradigmas para a persecução penal. **Momentum**, Atibaia, v. 1, n. 18, p. 1-34, 2020.

OLIVEIRA, Felipe Cardoso Moreira de. **Criminalidade informática.** 2002. 95 f. Dissertação (Mestrado em Ciências Criminais), Faculdade de Direito, PUCRS, Porto Alegre, 2002.

PATURY, Fabrício; LOPES, Elizângela Nogueira. **Cyberbullying**. Disponível em: https://www.mpba.mp.br/sites/default/files/biblioteca/criminal/artigos/diversos/ciberbullying_-_fabricio_rabelo_patury_e_elizangela_nogueira_lopes.pdf?download=1. Acesso em: 03 mai. 2022.

POLEGATTI, B. C.; KAZMIERCZAK, L. F. **Crimes Cibernéticos: O Desafio do Direito Penal na Era Digital.** Ourinhos, 2012.

PINHEIRO, Patrícia Peck. **Direito digital**. 5ª ed. São Paulo: Saraiva, 2013.

SANSEVERINO, Paulo de Tarso Vieira. **Princípio da reparação integral-indenização no código civil.** São Paulo: Saraiva, 2010.

SOUZA, Gills Lopes Macêdo, **PEREIRA**, Dalliana Vilar. **A Convenção de Budapeste e as Leis Brasileiras.** João Pessoa, Paraíba. Maio 2009. Disponível em: https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574aconvencao-de-budapesteeas-leis-brasileiras. Acesso em 06 de mai. 2022.

SMITH, Virginia Luna; SANCHES, Janaina Aparaecida Soares Gaspar. Extorsão Virtual velho crime, novas práticas. **REVISTA JurES** - v.13, n.24, p. 19-35, dez. 2020.

SYDOW, Spencer Toth. **Delitos informáticos próprios:** uma abordagem sob a perspectiva vitimo dogmática. 2009. 282 f. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009. Disponível em: Acesso em: 04 mai. 2022.

TARTUCE, Flavio. **Manual de Direito Civil**. 9 ed. Rio de Janeiro: Editora Método, 2018.

VIDAL, Rodrigo de Mello. **Crimes virtuais**. 2015. Disponível em: http://arquivos.integrawebsites.com.br/69477/7c8afc410a4aa166c24cebf0a062b335.pdf. Acesso em: 05 mai. 2022.

ZAPAROLI, Domingos. Vulnerabilidades da internet. **Pesquisa Fapesb**, n.295, p. 75-77, 2020.