CRIMES VIRTUAIS: UMA ABORDAGEM JURÍDICA ACERCA DAS LIMITAÇÕES NO COMBATE AOS CRIMES CIBERNÉTICOS

JUSTINO SOARES DOS SANTOS FILHO:
Graduando do curso de Direito da Universidade de Gurupi – UnirG.

FERNANDO PALMA PIMENTA FURLAN[1]

(orientador)

RESUMO: Os avanços tecnológicos encontrados na área da informática causaram e ainda causam um significativo impacto na sociedade, que os consomem diariamente. Esse impacto pode também ser percebido quando se utiliza das ferramentas trazidas por essa área no cometimento de crimes. No caso em tela, fala-se em crimes cibernéticos ou virtuais, que são crimes realizados por meio da internet. Frente a isso, o presente estudo possui a finalidade de analisar o desenvolvimento dos crimes virtuais, apresentando as suas particularidades e mostrando a sua punibilidade. De igual modo, também se discute quais dificuldades são encontradas na instrução probatória e na identificação do agente. Na metodologia, tem como técnica de pesquisa a referência bibliográfica e como meio de pesquisas, sites de busca, livros, artigos científicos e a norma brasileira. Nos resultados ficou evidente constatar que os crimes virtuais trazem além do prejuízo financeiro ao Estado, gera insegurança social. Portanto, é urgente que se tenha leis mais específicas que tratem desses crimes e uma maior modernização dos equipamentos de investigação.

Palavras-chave: Crimes virtuais. Combate. Legislação brasileira. Limitações.

ABSTRACT: Technological advances found in the area of information technology have caused and still cause a significant impact on society, which consumes them daily. This impact can also be seen when using the tools brought by this area in the commission of crimes. In the present case, we are talking about cyber or virtual crimes, which are crimes carried out through the internet. In view of this, this study aims to analyze the development of virtual crimes, presenting their particularities and showing their punishment. Likewise, it is also discussed which difficulties are found in the evidentiary instruction and in the identification of the agent. In the methodology, the bibliographic reference is used as a research technique and as a means of research, search sites, books, scientific articles and the Brazilian standard. In the results, it was evident to verify that virtual crimes bring, in addition to the financial loss to the State, it generates social insecurity. Therefore, it is urgent to have more specific laws that deal with these crimes and a greater modernization of investigation equipment.

Keywords: Virtual crimes. Combat. Brazilian legislation. Limitations.

[1] Professor Orientador do curso de Direito da Universidade de Gurupi – UnirG..

1. INTRODUÇÃO

O avanço tecnológico na área da informática e dos meios digitais trouxe para a sociedade um significativo impacto, principalmente na forma de comunicação. Esses avanços se encontram por meio de aparelhos digitais, tais como Smartphones, tablets e principalmente pelas redes sociais, assim como sites e demais ferramentas. Esses aparatos são utilizados diariamente e constantemente pelo indivíduo, pra fins de toda ordem.

Devido ao seu uso de forma constante por qualquer indivíduo, no âmbito digital tem-se percebido juntamente com o seu crescimento, o aumento da prática de crimes dessa espécie. Diariamente diversos cidadãos, empresas e até o Estado são vítimas de ataques oriundos do meio digital (TRUZZI, 2013).

Em razão da ocorrência cada vez mais numerosa de crimes de toda ordem na área digital, o Direito vem voltado seus olhos para esse cenário. Denominado de crimes cibernéticos ou virtuais, a legislação brasileira, juntamente com as equipes de investigação vem ampliando o trabalho na penalização, combate e prevenção desses crimes em solo brasileiro.

É com base nesse cenário que a presente pesquisa busca discorrer. Desse modo, objetiva-se analisar o real impacto que os crimes cibernéticos possuem para o Direito, apresentando o seu conceito e o seu *modus operandi*. Além disso, num objetivo mais específico, discute-se de que forma a linha investigativa pode trabalhar para elucidar a autoria e desenvolvimento de tais atos delituosos. Elaborado esses objetivos, também se discorre a respeito dos efeitos que os crimes cibernéticos trazem para o cenário jurídico.

Portanto, no decorrer de sua análise procura-se responder: quais os efeitos jurídicos e sociais dos crimes cibernéticos no âmbito do Direito? E quais as limitações impostas na busca por provas?

Cabe destacar que tal temática é de suma importância em razão das muitas situações passíveis de verificação com relação aos crimes cibernéticos, que vem prejudicando cada vez mais pessoas e órgãos públicos.

2. METODOLOGIA

Esse trabalho se configura como uma revisão de literatura, ao qual foi formulado por meio de dados bibliográficos e documentos. Os materiais foram constituídos pelas leis nacionais, de artigos científicos, de periódicos, de reportagens jornalísticas e demais materiais relacionados ao tema.

A coleta de dados é resultado de uma busca feita em bases de dados, tais como: Scielo; Google Acadêmico, dentre outros, entre os dias 10 a 28 de agosto de 2021.

3. DOS CRIMES VIRTUAIS: ASPECTOS GERAIS

Antes de se adentrar no tema central desse estudo, é necessário inicialmente discorrer em linhas gerais sobre os crimes virtuais. Os crimes virtuais ou também chamados de crimes cibernéticos se originam por meio da rede de computadores. É por meio desse aparato que é possível aferir este tipo de crime.

Importante explicar que existem ações ilícitas que são realizadas contra o computador, enquanto há outras que são feitas por "meio" dele, sendo esse último o enquadramento do crime virtual (GOMES, 2000).

Para realizar um crime virtual é necessário que haja uma rede conectada, e para isso necessita-se de internet. Esse termo, surgido durante a década de 1960, é entendia como uma "estrutura onde são passados milhares de terabytes de dados diariamente entre servidores e computadores pessoais, smartphones, tablets, consoles, televisores, etc." (CIRIACO, 2016, p. 02).

É portanto, uma rede de computadores que compartilham informações e dados entre si. Isso ocorre através do *World Wide Web* (www) que é como uma teia mundial, onde se permite que o usuário possa utilizar o conteúdo passado pela internet (CIRIACO, 2016).

É por meio da rede de computadores que o crime virtual é realizado. Em termos conceituais, Rosa (2016, p. 55) diz que o crime cibernético é "todo aquele ato que venha a prejudicar outrem por meio de dados armazenados, compilados, transmissíveis ou em transmissão". Alves (2020, p. 12) por sua vez, explica que é "o uso de um sistema de informática cujo objetivo é atingir um bem ou interesse que seja tutelado pelo Direito, pertencente ao Estado, ao direito privado ou ainda à integridade física, moral, individual de outrem".

Para Gonçalves (2017) os crimes virtuais são as ações ilegais praticadas por criminosos através de várias ferramentas eletrônicas, como por exemplo, um computador, um celular, um notebook, dentre outros. O criminoso busca com isso produzir, distribuir, vender ou qualquer outra atitude que venha expor o conteúdo adquirido de modo ilegal.

Continuando, desde o crescimento e a efetivação do uso da internet na sociedade, nas últimas décadas tem-se percebido um aumento significativo de crimes que são praticados por meio da rede de computadores. A título de exemplo, cita-se abaixo um trecho de uma reportagem jornalística que mostra os recentes dados sobre a criminalidade na internet:

> [...] O número de denúncias anônimas de crimes cometidos pela internet mais que dobrou em 2020. De janeiro a dezembro do ano passado, foram 156.692 denúncias anônimas, contra 75.428 em 2019. 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). O total de 156.692 é o maior número da série histórica desde que o levantamento começou, em 2014.[2]

Com os dados acima apresentados, fica evidente constatar que a prática do crime cibernético ainda é nos dias atuais muito frequente. Isso mostra que os cibercriminosos (nome dado aqueles que praticam o presente delito) tem utilizado da internet para realizar diversos crimes, causando prejuízos a terceiros, a empresas e ao Estado.[3]

Esses crimes podem ser divididos em três categorias principais; a saber:

> **Cibercrimes puros:** são aqueles em que o computador é o alvo dos infratores. Ou seja, quando o sistema (pessoal ou corporativo) sofre um ataque.
>
> **Cibercrimes mistos:** acontecem quando o sistema de computador é usado como "arma" para a prática dessas ações.
>
> **Cibercrimes comuns:** são aqueles em que o computador é usado como um acessório, apenas para guardar informações ilegais e roubadas.
>
> (PINHEIRO, 2021, p. 25)

Além dos citados acima, tem-se também os crimes virtuais impróprios (uso de equiparados eletrônicos para efetuar o crime, mas não danificando algum dado) e os crimes virtuais próprios (é preciso haver a quebra de sigilo de dados). (CUNHA, 2020).

Cabe destacar que o aumento da prática de crimes na internet também se deu por conta da popularização das redes sociais e da facilidade em resolver questões financeiras por meio de sites e aplicativos de banco. Nesses locais, a troca constante de imagens pessoais, de informações financeiras e sigilosas, de vídeos, de senhas e mensagens facilitou a continuidade de práticas delituosas nesses locais.

Como bem ressalta Bittencourt (2017, p. 12), de um lado a tecnologia trouxe "aos seus usuários uma maior liberdade e igualdade individual, em contrapartida tirou-lhes a habilidade de distinguir as pessoas com as quais se relacionam virtualmente, não sabendo exatamente se está lidando com um criminoso ou não".

O fato é que os crimes virtuais são o grande destaque da sociedade moderna. Como milhares de pessoas fazem uso de qualquer aparato eletrônico nos dias de hoje, naturalmente o número de ataques e de cometimento de crimes acaba sendo elevado. Cabe salientar que muitos indivíduos acabam por ajudar o cibercriminoso na consumação do crime, na forma de exposição dos seus dados pessoais (senhas,

---

[2] Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/02/09/numero-de-denuncias-de-crimes-cometidos-pela-internet-mais-que-dobra-em-2020.ghtml. Acesso em: 24 ago. 2021.

[3] Há ainda de se mencionar o *cracker* e o *hacker*, que também estão presentes nos crimes cibernéticos. O primeiro possui enorme conhecimento de sistemas operacionais e linguagens de programação, e faz uso desse conhecimento para tirar vantagens e lucros financeiros ou de dados pessoais, para posteriormente destruir e roubar. O segundo, também detém um conhecimento elevado sobre informática, mas o faz apenas em benefício próprio, como para provar a si mesmo que é capaz de praticar tais crimes (TAVARES, 2013).

imagens, vídeos, localização, etc.) o que se torna uma fonte de informação fundamental para que os crimes dessa natureza ocorram.

No entanto, a legislação brasileira tem promulgado normas que visem coibir essas práticas, conforme se expõe o tópico seguinte.

4. LEGISLAÇÃO BRASILEIRA FRENTE AOS CRIMES VIRTUAIS

Uma das principais imagens que se tem a respeito dos crimes virtuais é em relação a "falsa" impunidade. Diz-se falsa porque mesmo que não sendo plenamente eficiente na prática, o Brasil dispõe de normas e de projetos de leis que tenham como objetivo punir e prevenir que novos atos delituosos sejam realizados no campo informático.

A principal lei que rege sobre o presente tema é a Lei nº. 12.737/2012 conhecida como a Lei Carolina Dieckmann. Essa lei surgiu em razão do fato de que a popularmente atriz Carolina Dieckmann sofreu ameaças de um cibercriminosos que detinha em seu arquivo (que foram hackeadas) suas fotos intimas. Mesmo não cedendo às ameaças, as fotos acabaram por serem expostas a toda a rede. Diante da repercussão que esse caso tomou, o Congresso Nacional se movimentou até que fora criada a presente lei.

O objetivo da lei em comento é criminalizar a invasão de computadores, o "roubo" de senhas e arquivos, além da exposição de fotos e vídeos íntimos dos usuários. Nestas situações a penalidade prevista é de 03 meses a 01 ano, conforme regula o caput do art. 154-A:

> **Art. 154-A.** Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
>
> Pena - detenção, de 03 (três) meses a 01 (um) ano, e multa.
>
> (BRASIL, 2012)

O que se percebe neste artigo acima citado é a tutela da privacidade e da intimidade, bens tão valiosos ao ser humano, como também a proteção de dados particulares do proprietário deste dispositivo. Cabe lembrar que na respectiva lei, "prevê que o dono de seus próprios dados deva colocar meios ou medidas que impeçam ou dificultem a invasão desses dados, gerando assim a sua proteção, para que assim, demonstre que esses arquivos não sejam de conhecimento público" (TAVARES, 2013, p. 40).

Ainda nessa lei, também é importante mencionar que ela trouxe penas para os casos conde há possibilidade de invasão, com o intuito de conseguir dados pessoais das vítimas. A sua normatização é decorrente da observância do principio constitucional da privacidade. Sendo assim, visa esta norma a segurança de dispositivos eletrônicos, como o Smartphone, por exemplo.

> Art. 154-A [...]

> §2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> §3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> §4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão à terceiro, a qualquer título, dos dados ou informações obtidas.
>
> (BRASIL, 2012)

Pela lei em destaque, nota-se que ela é muito clara ao fazer entender a responsabilização do indivíduo que invadir, enganando as ferramentas de segurança, com o intuito de violar a intimidade digital de terceiro. Essa norma, portanto, é um importante instrumento normativo no combate aos crimes cibernéticos (BRASIL, 2012).

Além da supracitada lei, há de se mencionar a Lei nº 12.965/2014 que instituiu o Marco Civil da Internet. Assim como a lei anterior mencionada, essa também veio em decorrência do aumento de ataques a websites oficiais do governo, de empresas públicas e de contas privadas. Por essa situação, buscou-se por meio do Marco Civil da Internet a tutela da informação. Assim, no texto da presente norma encontra-se as garantias individuais dos internautas e os direitos e deveres para o uso da internet no Brasil. (BRASIL, 2014).

De acordo com Silva (2020) o Marco Civil da Internet desde a sua promulgação fora debatido. Apesar das discordâncias em alguns pontos da norma, fato é que ela trouxe importantes benefícios aos provedores, que deixou para os usuários a total responsabilidade por aquilo que produzem e consomem, com exceção dos conteúdos expostos em redes sociais. Em caso de retirada, se o provedor não o fizer, responderá em várias esferas judiciais.

Portanto, atualmente as leis citadas nesse tópico são as que regulamentam sobre os crimes virtuais no Brasil. Entretanto, ainda que seja necessária a sua existência, a sua eficácia tem tido pouco sucesso, em parte porque ela é vista como leis brandas. Nesse aspecto, Brandão (2021, p. 01) afirma que “o Brasil é um paraíso dos cibercriminosos, com penas brandas e procedimento processual penal ultrapassado”.

Soma-se a isso, o fato de que a pouca eficácia dessas leis acaba por também prejudicar a sua investigação, conforme se analisa no tópico a seguir.

5. DA INVESTIGAÇÃO POLICIAL DOS CRIMES VIRTUAIS

Inicialmente, para se obter resultados na investigação desses crimes ocorridos virtualmente, é essencial que se identifique qual forma o usuário utilizou, ou seja, quais ferramentas foram mecanismos para as práticas delituosas. Por isso a importância de compreender como funciona a internet e as formas maliciosas existentes nela.

Para se entender o grau de dificuldade existente na investigação policial nos crimes virtuais, cumpre ressaltar alguns aspectos básicos quanto aos procedimentos na execução dos crimes. Uma vez que na década de 1950, período no qual não existia internet, uma organização criminosa se dividia em funções para o cumprimento das práticas ilegais, uma delas envolvia o contato físico do criminoso com o cliente. Assim, a organização promoveria o encontro com o cliente-criminoso para a obtenção do "produto", efetivando o contato em local físico, consumando o crime. Caso a polícia não tomasse conhecimento, os membros da organização e o cliente se dispersariam na sociedade (BARRETO, 2017).

Porém, se a polícia conseguisse intervir, ela desmancharia parte da organização, identificaria alguns dos membros dela, seus meios de operação, algumas das práticas corriqueiras da organização, bem como os locais habituais de encontro e também o consumidor final. Agora, se esta mesma organização fosse formada atualmente, seria impossível que esta não se valesse dos recursos tecnológicos para efetivar a prática do crime. Utilizaria, por exemplo, a internet para comunicação interna entre os integrantes em diversos locais (BARRETO, 2017).

Ocorre também a facilitação da divulgação e compartilhamento de conteúdos ilícitos como vídeos sexuais através do meio virtual, uma vez que não se faria mais necessário à presença física do consumidor para a obtenção do material. Sem o local físico, a perspectiva de uma eventual apreensão dos produtos ilícitos, da identificação dos criminosos e dos consumidores, e até mesmo um possível resgate de vítimas é deteriorada.

Em uma análise feita por Soares (2013), as estatísticas criminais brasileiras indicam que o foco da repressão policial se concentra principalmente nas prisões em flagrante, as quais são mais fáceis de investigar. Porém, grande parte dos delitos não são sequer denunciados, por vários motivos como a opressão sócio-cultural ou os interesses particulares existentes no protecionismo político de esquemas criminosos sofisticados. Visto que esses crimes estão longe de serem de conhecimento público, é notório que a população e o Estado não possuem estatísticas que se aproximem à realidade fática criminosa. Uma vez que não são conhecidos, impossível criar mecanismos que solucionem esses problemas.

Outra grande dificuldade de se obter provas no mundo virtual é a instabilidade, ou seja, ela pode ser facilmente apagada, alterada, editada, excluída ou perdida. Isso se diferencia enormemente das investigações policiais em crimes do mundo real, uma vez que no mundo físico é muito mais difícil de exterminar por completo evidências das ações humanas (CUNHA, 2020).

Já no mundo virtual, com essa possibilidade, o acesso aos vestígios criminosos são impalpáveis e demandam mais esforço da análise criminal. Além disso, devido à globalização, se torna muito mais simples a prática dos crimes virtuais uma vez que se pode acessar a internet de qualquer lugar do mundo, o que torna o ato criminoso muito mais fácil e rápido do que a identificação dele.

Sobre isso, Gustavo Testa Corrêa (2018, p. 10) discorre:

> Enquanto no mundo real o dano causado à vítima é quase que imediato, no mundo virtual ela talvez demore muito tempo até perceber que seu computador foi infectado, ou suas informações roubadas, fazendo com que muitas das evidências relacionadas ao fato criminoso se percam. Até mesmo as grandes empresas, quando identificam a invasão em contas particulares de seus clientes, geralmente não informam a polícia a fim de inibir que se torne de conhecimento público a falha no sistema de segurança, colocando em situação delicada sua imagem perante os clientes. Dessa forma, é comum que os *crackers* se encaminhem em maior quantidade para esta finalidade.

As redes sociais também se tornaram alvos dos crimes virtuais conforme foram se tornando cada vez mais populares entre os brasileiros e ao redor do mundo, sendo utilizadas para buscar relacionamentos, diversão, passatempo, divulgar informações, anunciar produtos e serviços, além de muitas outras funções.

Visto a facilidade de criar perfis falsos nas redes sociais, acessando as contas virtuais por qualquer computador ou dispositivo em qualquer lugar, é muito difícil, para não dizer quase impossível que as autoridades consigam alcançar o autor da prática. Todas essas características tornam a identificação do agressor muito complexa, exige muito tempo da polícia, e ainda a incerteza de sucesso é muito grande (PRADO, 2020).

No entanto, algumas medidas tem sido implantadas para que os crimes cibernéticos não vinguem. A título de exemplo, no campo legislativo, há o Projeto de Lei nº 4554/20 que visa aumentar as penas pelos crimes de furto e estelionato realizados com o uso de dispositivos eletrônicos (celulares, computadores, tablets).

Em 2021 o presente projeto foi aprovado pelo Plenário da Câmara do Senado, se transformando posteriormente na Lei Ordinária 14.155/2021. Em seu texto, cria-se agravantes para os crimes acima mencionados. Como menção, cita-se:

> Art. 154-A. [...]
>
> § 4º-B. A pena é de reclusão de 4 (quatro) a 8 (oito) anos e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
>
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerando a relevância do resultado gravoso:
>
> I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
>
> II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.
>
> (BRASIL, 2020)

Com a presente norma, nota-se que o legislador buscou aumentar a pena como forma de coibir que os cibercriminosos venham a praticar qualquer ato contra terceiros por meio virtual. Também se preocupou em inserir aumento de pena quando o crime

for praticado contra idoso ou vulnerável, justamente pela facilidade que esses indivíduos possuem em “cair” nas armadilhas dos cibercriminosos.

Já a Lei Ordinária 14.155/2021 formalizou as mudanças trazidas pelo Projeto de Lei. A respeito das suas principais mudanças, cabe destacar:

Quadro 1 – Mudanças trazidas pela Lei Ordinária 14.155/2021

Redação original	Redação atual
Art. 154-A. Invadir dispositivo informático **alheio**, conectado ou não à rede de computadores, **mediante violação indevida de mecanismo de segurança** e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.	Art. 154-A. Invadir dispositivo informático **de uso alheio**, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou **de** instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.	§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
§ 3º (...) Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.	§ 3º (...) Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

Fonte: PROCÓPIO (2021).

Ao comentar sobre a norma, Brandão (2021, p. 02) afirma que ela busca dar maior visibilidade à efetividade do combate ao crime digital, aumentando a “abrangência dos tipos penais, aumentando as penas para esses crimes, assim como delimitando a regra de competência que visa facilitar o acesso da vítima às autoridades locais”.

No campo da investigação, algumas medidas também tem sido implantadas buscando diminuir a prática de crimes cibernéticos. Como exemplo, há no Brasil o inquérito eletrônico, que simplifica e dá maior rapidez ao cumprimento dos mandados, além de facilitar a instrução probatória (NETO; SANTOS; GIMENES, 2018).

Outro ponto muito importante nesse cenário é a identificação do autor. Nesses casos, é possível encontrar a autoria do crime cibernético por meio do número do IP (Internet Protocol) que é como uma identidade própria que cada máquina possui. Por meio do IP de um computador, por exemplo, é possível encontrar a identidade do cibercriminoso fazendo uso de registros de navegação, que mapeiam lugares acessados por ele e ainda quais os serviços que foram utilizados (NETO; SANTOS; GIMENES, 2018).

No entanto, em alguns casos, os cibercriminosos conseguem driblar esse sistema, se tornando impossível a sua identificação. Aqui, volta-se novamente a discussão sobre uma maior atenção à modernização do sistema de investigação da polícia relacionada à essa área.

Além da importância em se ter equipamentos mais modernos de investigação aos crimes virtuais, os processos jurídicos para esses crimes também devem acompanhar a rapidez dos avanços tecnológicos. Num cenário atual, muitos cibercriminosos ficam impunes devido a demora na investigação e punição.

Ao opinar sobre esse assunto, Wendt (2019, p. 44) defende que só haverá "melhoria nas investigações quando houver uma maior rapidez na expedição e cumprimento de mandados além da celeridade por parte da perícia, união entre as forças de Segurança Pública e aperfeiçoamento na legislação".

Dessa forma, finaliza-se esse estudo entendendo que de fato há empecilhos que dificultem a investigação dos crimes cibernéticos. No entanto, com a união de todos os poderes públicos, da sociedade e de um sistema mais ágil, pode-se vislumbrar uma melhoria no combate, punição e prevenção dos crimes virtuais no Brasil.

6. CONSIDERAÇÕES FINAIS

A tecnologia tem avançado no mundo de modo rápido e constante. Em que pese a sua importância e os benefícios dela advindos, o fato é que tem aumentado o número de crimes praticados na rede da internet. São os chamados de crimes cibernéticos ou crimes virtuais.

Diante dessa nova realidade, houve o surgimento de novas práticas ilícitas no contexto digital, o que torna necessária a intervenção do Direito Penal na evolução dessas tecnologias, a fim de garantir a aplicação das normas penais de forma eficaz, abrangendo todo o universo criminoso existente na sociedade da informação.

Conforme exposto no decorrer desse estudo, ficou claro observar que os crimes cibernéticos afetam toda a estrutura política, social e jurídica, trazendo prejuízos de toda ordem. Desse modo, não pode o Direito – enquanto ciência social – se afastar dessa realidade. O fato é que utilizar a internet como forma de prejuízo social e jurídico contra pessoas ou organizações ou até mesmo ao Estado é considerado crime.

Para além da criação de leis e outras normativas, o que se verificou é que a investigação aos crimes virtuais ainda é bastante limitada. Isso decorre pelo fato de que, mesmo com o avanço dos aparatos tecnológicos de identificação e busca de cibercriminosos, os investigadores encontram-se aparados por equipamentos ainda muito atrasados em relação aos já encontrados pelos cibercriminosos.

A identificação do criminoso nesse campo também é possível, mas ainda não é plenamente eficaz, uma vez que os cibercriminosos mais experientes tem conseguido driblar o sistema de segurança, impossibilitando a sua identificação.

Em que pese todos os problemas encontrados, é imperioso afirmar que já existe um movimento de todas as áreas para que os crimes virtuais não possam prosperar. Campanhas publicitárias informando os perigos da rede virtual são constantemente divulgados na mídia como forma de conscientização da sociedade, leis que ampliam a pena para crimes virtuais têm surgido com mais frequência nos

últimos anos (vide a Lei Ordinária 14.155/2021) e no campo jurídico, já há ferramentas que ajudem a agilizar o processo, como o citado inquérito policial.

Apesar disso, frisa-se novamente a urgência em se ter leis mais específicas que tratem desses crimes, uma vez que dados probabilísticos têm demonstrado um aumento na prática. Soma-se a isso, uma maior modernização dos equipamentos de investigação a esses crimes. Com isso, facilmente os crimes virtuais irão diminuir.

7. REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, Matheus de Araújo. **Crimes Digitais: análise da criminalidade digital sob a perspectiva do Direito Processual Penal e do Instituto da Prova**. 1º Edição. Editora: Dialética, 2020.

BARRETO, Alessandro Gonçalves. **Investigação Digital em fontes abertas**. Rio de Janeiro. Brasport, 2017.

BITTENCOURT, Rodolfo Pacheco Paula. **O anonimato, a liberdade, a publicidade e o direito eletrônico**. 2017. Disponível em: https://rodolfoppb.jusbrasil.com.br/artigos/371604693/o-anonimato-a-liberdade-a-publicidade-e-o-direito-eletronico> Acesso em: 24 ago. 2021.

BRANDÃO, Francisco. **Câmera aprova penas mais duras para crimes cibernéticos**. 2021. Disponível em: https://www.camara.leg.br/noticias/746980-camara-aprova-penas-mais-duras-para-crimes-ciberneticos/. Acesso em: 28 ago. 2021.

BRASIL. **Projeto de Lei nº 4554/2020**. Altera o Código Penal, para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Código de Processo Penal, para prever a competência dos crimes cometidos pela internet ou de forma eletrônica pelo lugar de domicílio ou residência da vítima. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0yz4x06etwvmhy7uqfwlk8iq74267515.node0?codteor=1947262&filename=PL+4554/2020. Acesso em: 28 ago. 2021.

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: 24 ago. 2021.

CIRIACO, Douglas. **Qual a diferença entre Internet e World Wide Web?** 2016. Disponível em: https://canaltech.com.br/entretenimento/qual-a-diferenca-entre-internet-e-world-wide-web/. Acesso em: 12 ago. 2021.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 8 ed. São Paulo, Saraiva, 2018.

CUNHA, Rogério Sanches**. Manual de direito penal: parte especial**. 12ª Ed. Salvador: Juspodivm, 2020.

D'URSO, Filizzola Luiz. **Em Tempos de Cibercrimes.** 2019. Disponível em: https://www.migalhas.com.br/dePeso/16,MI310551,31047Em+tempos+de+ciber crimes. Acesso em: 12 ago. 2021.

FERREIRA, Ivette Senise. **A Criminalidade Informática. Direito & Internet – Aspetos Jurídicos Relevantes.** Editora Edipro, 2018.

GIMENES, Emanuel Alberto S. Garcia. **Crimes Virtuais.** 2018. Disponível em: http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html. Acesso em: 12 ago. 2021.

GOMES, Luiz Flávio. **Crimes informáticos**. 2000. Disponível em: www.ibcrim.org.br. Acesso em: 17 mar. 2021.

GONÇALVES, Carlos Roberto. **Direito civil brasileiro: parte geral**. 15. ed. São Paulo: Saraiva, 2017.

GRECO, Rogério. **Curso de Direito Penal: parte especial**, volume III. Niterói: 2014.

MACHADO, Felipe e VIANNA, Túlio Lima. **Crimes Informáticos:** Conforme a Lei 12.737/2012. Belo Horizonte: Editora Fórum, 2013.

NETO, Mário Furlaneto Neto. SANTOS, José Eduardo Lourenço dos. GIMENES, Eron Veríssimo. **Crimes na internet e inquérito policial eletrônico**. 2. ed. Edipro, 2018.

PINHEIRO, Patrícia Peck. **Direito Digital.** 7ª Edição. São Paulo: Saraiva Jur, 2021.

PRADO, Luiz Régis. **Curso de direito penal brasileiro: parte geral e parte especial**. 18 ed. Rio de Janeiro: Forense, 2020.

PROCÓPIO. Michael. **Lei 14.155/20211: a fraude eletrônica e outras alterações no Código Penal**. 2021. Disponível em: https://www.estrategiaconcursos.com.br/blog/lei-14-155-2021-a-fraude-eletronica-e-outras-alteracoes-no-codigo-penal/. Acesso em: 25 ago. 2021.

ROSA, Fabrizio**. Crimes da Informática**. 2ª Ed. Campinas. Bookseller, 2016.

SARTÓRIO, Giovanna. **Crimes Virtuais: Entenda o que são e Saiba Como recorrer.** 2018. Disponível em: http://www.joaquimnabuco.edu.br/noticias/crimes-virtuais-entenda-o-que-sao-e-saiba-como-recorrer. Acesso em: 13 ago. 2021.

SILVA, Mazukyevicz Ramon Santos do Nascimento. **Crimes virtuais e o ordenamento jurídico Brasileiro: análise dogmática**. 1 ed. Editora: Clube dos Autores, 2020.

SOARES, Luís Eduardo. **PEC - 51: revolução na arquitetura institucional da segurança pública**. In: Boletim do IBCCrim, ano 21, nº 252, novembro de 2013.

TAVARES, Winicius Matias. **Estelionato Eletrônico e Necessidade de Tipificação Legal**. 2013. 58 f. Trabalho de conclusão de curso de Direito – Faculdade UNIRG, Gurupi – TO, 2013.

TRUZZI, Gisele. **Crimes Eletrônicos: A internet é uma terra sem leis?** Revista de Criminologia e Ciências Penitenciárias PROCRIM – SP. ISSN: 2238-1678. Ano 2 – nº. 04, Fevereiro, 2013.

WENDT, Emerson. **Direito E TI Cibercrimes**: Livraria do Advogado Editora, 2019.

WENDT, Emerson; NOGUEIRA JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: Ameaças e Procedimentos de Investigação**. 2º ed. Editora Braspot: 2017.