doi.org/10.51891/rease.v10i5.14073

ESTUDO SOBRE CRIMES VIRTUAIS E SUAS IMPLICAÇÕES LEGAIS NA SOCIEDADE MODERNA

Agnaldo Adriano Ferreira Filho[1]
Leonardo Guimaraes Torres[2]

RESUMO: Com o advento da era digital houve o avanço positivo em diversos campos, contudo a maior liberdade também teve consequências, os crimes virtuais tornaram-se um problema significativo na sociedade moderna, diante disto houve a necessidade de atualizações legislativas para a devida adequação a estas novas tipificações criminais. Diante disto, visa-se responder a seguinte problemática: O que são crimes virtuais e quais as legislações concernentes a estes? Esta investigação tem como objetivo definir estes crimes informáticos em seus diferentes aspectos e denominar a legislação e os métodos de classificação associados aos crimes virtuais, explorando os seus diversos sintomas e os recursos legais disponíveis para os resolver. A investigação emprega uma abordagem bibliográfica, em que os dados serão analisados qualitativamente. A análise destes cibercrimes e das suas consequências jurídicas fornecem informações essenciais para a promoção da segurança digital e o desenvolvimento de políticas eficazes de segurança cibernética.

Palavras-chave: Crimes Virtuais. Legislação. Consequências jurídicas. Segurança cibernética.

ABSTRACT: With the advent of the digital era there was positive progress in several fields, however greater freedom also had consequences, virtual crimes became a significant problem in modern society, given this there was a need for legislative updates to properly adapt to these new criminal classifications. In view of this, the aim is to answer the following problem: What are virtual crimes and what are the laws concerning them? This investigation aims to define these computer crimes in their different aspects and name the legislation and classification methods associated with virtual crimes, exploring their different symptoms and the legal resources available to solve them. The investigation employs a bibliographical approach, in which the data will be analyzed qualitatively. The analysis of these cybercrimes and their legal consequences provides essential information for promoting digital security and developing effective cybersecurity policies.

Keywords: Virtual Crimes. Legislation. Legal consequences. Cyber security.

[1]Graduando em Direito pela Universidade de Gurupi-UNIRG.
[2]Professor especialista em Direito Tributário e Direito Contratual.

INTRODUÇÃO

É evidente que a internet é a principal ferramenta da comunicação atual, é a maior defensora da agilidade na transmissão de informações, pois permite que pessoas de diferentes locais se comuniquem e aprendam sobre coisas em tempo real. Facilita a pesquisa e o acesso a novas informações, altera a velha realidade e cria um novo mundo para hoje.

Carvalho (2018) afirma que o mundo virtual é antes de tudo um espaço sem regulamentações. Saindo da função do mundo real que a tecnologia e a Internet proporcionam, o mundo virtual é expansivo e os usuários viajam livremente. Neste sentido, é crucial reconhecer que mais leis devem ser promulgadas e especialmente a aplicação de sanções penais para crimes cibernéticos, isto servirá para evitar que aqueles que violam as regras tenham que pagar um preço e servirá para evitar ou regular o crescimento de novos crimes.

Hoje, os crimes virtuais tornaram-se uma ameaça significativa à segurança digital, esta ameaça não se limita às empresas ou instituições, afeta também os indivíduos durante as suas atividades diárias online. A rápida evolução da tecnologia e a natureza global das comunicações facilitaram a proliferação de crimes cibernéticos, incluindo o roubo de dados e a fraude financeira, bem como a distribuição de conteúdo ilegais na Internet. Imposta a esta realidade, existe uma necessidade premente de compreender e abordar as questões associadas aos crimes virtuais.

Diante disto, visa-se responder a seguinte problemática: O que são crimes virtuais e quais as legislações concernentes a estes? Por meio de uma pesquisa bibliográfica, em que os dados foram analisados qualitativamente, tem como objetivo identificar e diferenciar os diversos tipos de crimes virtuais, bem como apresentar a legislação vigente relacionada a esses delitos.

Esta pesquisa justifica-se pela crescente importância dos crimes virtuais na sociedade moderna. Compreender e diferenciar esses delitos, bem como estudar as legislações vigentes, é fundamental para a formação de profissionais e estudantes da área. A investigação do crime cibernético e dos seus efeitos jurídicos fornece informações importantes sobre a proteção digital e a criação de políticas eficazes de segurança cibernética.

1. CRIMES VIRTUAIS

Os crimes de virtuais aumentam a um ritmo acelerado, principalmente porque a Internet é facilmente acessível e proporciona uma forma rápida de acesso à informação. O meio é cada vez mais popular e as pessoas dependem dele para compartilhar informações de diversas formas.

A rápida evolução tecnológica também permite o acesso a computadores, o que possibilita a prática de crimes virtuais por indivíduos que se aproveitam da vulnerabilidade das informações para receber benefícios fraudulentos em detrimento de terceiros. (Bastos, 2016).

O crime virtual é considerado um ato típico e contraproducente, perpetrado através de tecnologia relacionada à troca de informações em geral, ou contra um computador, um sistema ou uma rede. Na atualidade, é possível afirmar que, no crime informático, a tecnologia da informação ou é o alvo do crime ou o meio pelo qual o alvo já está protegido pelo Direito Penal (Jesus; Milagre, 2016).

Além disso, é importante reconhecer que existem múltiplas definições de crimes relacionados com as novas tecnologias: crimes informáticos, crimes cibernéticos, crimes virtuais, crimes eletrônicos, cibercrimes e crimes digitais. Verifica-se que, apesar de nomes diferentes, acabam por ter o mesmo significado (Jesus; Milagre, 2016).

O ambiente cibernético é complexo e evolui rapidamente, muitas vezes da noite para o dia. Nesse contexto, observa-se que o espaço geográfico, assim como a presença física, não é mais necessário para a prática de crimes (Malaquias, 2015).

Como resultado, os crimes digitais são um fenômeno recentemente observado e intrínseco ao desenvolvimento da sociedade da informação e aos avanços tecnológicos. Com a rápida evolução da tecnologia prejudicial aos crimes, lidar com crimes virtuais tornou-se uma dificuldade, porque o Código Penal Brasileiro é baseado no rádio e carece de qualquer referência aos crimes cibernéticos, situações em que a tecnologia deveria ser protegida por lei. Criminoso (Jesus; Milagre, 2016).

Entre os crimes virtuais mais comuns, o site Safernet realizou uma pesquisa que publicou um artigo sobre eles: pornografia infantil, pirataria, fraudes e golpes, vandalismo informático, difamação, calúnia, insulto, dano, peculato, crimes financeiros, ameaças e crimes ilegais, captura de dados no tráfego através de serviços de telecomunicações. Esses são apenas alguns dos muitos crimes virtuais que são cometidos (Martins, 2017).

Neste contexto, é importante considerar o princípio da legitimidade no contexto do direito penal, isto é amparado pelo artigo Art. 5º, XXXIX da Constituição Federal, que diz: "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal". Como resultado, a reserva legal é considerada uma restrição ao poder de punir do Estado e uma garantia fundamental dos direitos humanos, que impede que a punição ocorra até que um crime seja

cometido. Como resultado, acredita-se que haverá apenas crimes nos cenários hipotéticos que estão explicitamente cobertos pela lei penal (Capez, 2013).

Conforme descreve Malaquias (2015), diversos comportamentos dos criminosos cibernéticos ainda são considerados atípicos, o que impede o uso de analogias para beneficiar o acusado (na parte malam), o que não é aceitável no Direito Penal. Dito isto, vale ressaltar que no Brasil alguns comportamentos são amparados pela legislação vigente, especificamente aqueles comportamentos que envolvem a internet como meio de aplicação do crime.

Contudo, verifica-se que o Código Penal de 1940 é eficaz no que diz respeito aos crimes comuns cometidos online, pois representa inúmeros crimes que já foram reconhecidos pela sociedade e são comumente praticados no mundo virtual, como a fraude e exploração sexual infantil. Com isso, nesta modalidade já existem crimes reconhecidos e tipificados na legislação penal, mas o ambiente virtual é utilizado como meio para cometê-los.

De acordo com Jesus e Milagre (2016, p. 49), "o crime virtual pode ser um crime-meio, mas vem se desenvolvendo como crime-fim, o que demandou, aliás, a tipificação de alguns crimes informáticos próprios, com a edição das Leis n. 12.735/2012 e n. 12.737/2012".

No entanto, os crimes de peculato e pornografia infantil, mencionados anteriormente, são considerados crime, pois podem ser cometidos tanto no mundo virtual como na realidade, sendo utilizados apenas como meio para cometer o crime. Por outro lado, a violação da segurança de um computador pelo criminoso, que foi formalizada na legislação brasileira pela Lei nº 12.1737/2012, é considerada um crime que termina, porque o recurso legal salvaguardado é a segurança dos computadores e dos dados (Jesus; Milagre, 2016).

Segundo Malaquias (2015) a conduta no crime cibernético em muitos tipos penais emergentes é multifacetada, via de regra, afeta negativamente diversos bens jurídicos protegidos, como, por exemplo, a violação de sistema de computador de outra pessoa, o que pode levar a perdas financeiras ou expor a vítima a detalhes pessoais e íntimos. Este é o exemplo comum de crime formal que envolve o primeiro ato, independentemente das consequências ou resultados seguintes, que, em regra, violam múltiplos interesses jurídicos protegidos pelo direito penal.

Dentre as inúmeras classificações de crimes utilizadas para descrever crimes virtuais, a mais relevante é aquela que diferencia entre crimes cibernéticos que utilizam novas tecnologias como meio para cometer crimes antigos, tradicionalmente descritos pelo Direito Penal, e crimes cibernéticos que são a própria tecnologia da informação como sua posse legal protegida (Jesus; Milagre, 2016).

Nucci (2017) afirma que o participante ativo (autor ou agente) é o indivíduo que pratica a conduta descrita pelo tipo criminoso. Em última análise, é o indivíduo quem executa o crime ou ação típica, intencional ou acidental. Somente humanos podem participar de comportamento ativo, e não animais ou objetos.

O participante passivo do crime, segundo Nucci (2017), é o proprietário do bem jurídico que está sendo protegido pelo tipo penal que é incriminador, lesado ou em perigo de ser ferido. Indivíduos ou grupos de indivíduos, mesmo aqueles que são incapazes de agir, podem aparecer como participantes passivos - vítimas, aqueles que são ofendidos, ou o Estado ou a comunidade internacional, todos estes podem ser considerados como tal.

2. CLASSIFICAÇÃO DOS CIBERCRIMES

Várias são as classificações concernentes aos crimes virtuais são categorizadas. Distinguem-se dois tipos de crimes: crimes digitais próprios ou puros e crimes digitais inadequados ou mistos. Como resultado, é essencial distinguir a diferença entre crimes virtuais próprios e impróprios.

Crimes digitais próprios ou puros são ações, condutas passíveis de punição criminal e que tenham como alvo computadores e dados, eles também são conhecidos como crimes relacionados a informática. Exemplos de crimes digitais específicos incluem o acesso ilegal (hacking), a transmissão de vírus e a obstrução de funcionalidades. Exemplos de crimes digitais impróprios são crimes contra a honra baseados na internet, condutas que envolvam troca ou armazenamento de imagens com conteúdo infantil, peculato e até homicídio (Crespo, 2015).

Exemplos de crimes virtuais próprios incluem hackear e-mails, redes sociais, sites e instalar arquivos enganosos (como “Cavalo de Tróia”), entre outros. Barreto e Brasil (2016) definem crimes virtuais como aqueles que envolvem o uso de computadores, smartphones ou tablets, todos considerados criminosos virtuais. Esses dispositivos são alvo de criminosos, que normalmente identificam suas vulnerabilidades por meio do uso de software malicioso ou engenharia social (golpistas que enganam a vítima para que compartilhe informações pessoais com ela).

Por outro lado, crimes virtuais impróprios são aqueles cometidos através do computador, esta é a plataforma para a realização de atividades criminosas e são violados bens jurídicos já protegidos. Conforme demonstrado por Caiado e Caiado (2018), ocorre por meio do estelionato e furtos eletrônicos e fraude no banco, hacking informático e perda de dados, falsificação e

supressão de dados, armazenamento, produção e publicação de vídeos e imagens que contenham pornografia infantil (art. 241 e 241-A, do ECA - Lei nº 8.069/1990).

Além disso, há os casos de abuso e negligência infantil (art. 241-D, do ECA - Lei nº 8.069/1990, ameaça, cyberbullying (publicação de crimes em na Internet e em comunidades virtuais), incitação e tolerância a comportamentos criminosos, prática ou incitação à discriminação ou preconceito com base na raça, cor, etnia, religião ou origem nacional, vendas ilegais de produtos farmacêuticos (Caiado; Caiado, 2018).

Para Albuquerque (2006, p.168), os crimes virtuais que são impróprios envolvem o uso de computadores para cometer crimes, o objetivo é proteger bens jurídicos que já são de natureza existencial. Na sociedade digital, a frequência das ações criminosas é aumentada pela presença de objetos tecnológicos ou meios de execução que estão associados ao mundo digital: hardware, software, redes, etc.

Outra categorização de crimes envolve a diferenciação entre três tipos: crime exclusivamente virtual, crime virtual misto e crime virtual comum. Fiorillo (2013), afirma que o crime virtual puro significaria comportamento ilegal visando um sistema computacional, violando o hardware e seus componentes, incluindo dados e sistemas (software, hardware e suportes de dados);

São considerados crimes virtuais mistos aqueles em que a utilização de meios computacionais é condição necessária para a prática de um ato, embora o bem jurídico pretendido seja outro que não o informático. E, por último, os crimes virtuais comuns corresponderiam aos crimes em que a Internet é utilizada como ferramenta para a prática de um delito já definido na legislação penal (como os crimes contra a honra e a distribuição de pornografia infantil) (Fiorillo, 2013).

Independentemente da classificação da doutrina, quando o computador for empregado como meio para a prática de um crime, este será considerado cometido independentemente da existência de lei específica que puna esse comportamento em espaço virtual, seja com a intenção de concretizar atos que tenham consequências jurídicas associadas à própria tecnologia da informação ou outros crimes protegidos por lei.

3. LEGISLAÇÃO VIGENTE

O principal objetivo da legislação sobre crimes virtuais, também conhecidos como crimes cibernéticos, é combater e punir as atividades ilegais que ocorrem no ambiente digital. Estas leis

destinam-se a abranger uma vasta gama de crimes, desde a pirataria informática e roubo de dados até fraudes electrónicas e crimes contra a honra cometidos online.

A Lei nº 12.737/2012, lançada em dezembro de 2012, é comumente conhecida como "Lei Carolina Dieckmann", em homenagem à atriz que teve suas fotos divulgadas indevidamente. A norma incluía punições no Código Penal. 154-A e 154-B, o que acarreta violação da segurança do computador e altera os arts. 266 e 298, do mesmo tipo (Crespo, 2013).

A alteração do artigo 154 do Código Penal Brasileiro, que foi denominado "invasão de dispositivo de computador", teve como objetivo punir prioritariamente as ações do hacker, pois a figura incorporada ao artigo 154-A representava a invasão de dispositivo de computador com o objetivo de adquirir, alterar ou destruir informações de outras pessoas ou instalar software vulnerável para tirar vantagem.

Em arte. 154-B afirma que, tipicamente, a representação é necessária para a conduta criminosa descrita no art. 154, salvo se o crime for cometido contra liderança direta ou indireta de qualquer dos poderes da União, dos estados, do Distrito Federal ou do município, ou de empresas prestadoras de serviços públicos (Brasil, 1940).

A referida Lei também 12.737/2012, alterou o artigo 298 do Código Penal em que foi acrescentado ao seu parágrafo único: Para fins de prática criminosa, considera-se documento particular a falsificação de cartão de crédito ou de débito.

A inovação legislativa provocada pela Lei 12.737/2012, que foi incorporada ao Código Penal no âmbito da modalidade Invasão de Dispositivos Informáticos, art 5º-A do Código Penal Brasileiro, caracteriza-se pelos comportamentos elencados a seguir: Violar a privacidade do computador de outra pessoa, esteja ou não conectado à Internet, através da perspectiva de um criminoso, ele irá: adquirir, possuir ou destruir dados ou informações sem a permissão expressa ou tácita do proprietário ou instalar vulnerabilidades para tomar um vantagem ilegal.

O tipo penal mencionado anteriormente era punido com pena de reclusão de três meses a um ano, além de multa. Isso também faz com que a pena seja aumentada em uma seção caso a invasão resulte em prejuízo financeiro (Brasil, 2012).

Adicionalmente, o parágrafo 3º do referido tipo penal aumenta a pena caso a invasão envolva conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações confidenciais (Brasil, 2012), neste caso, o indivíduo está sujeito a uma pena de prisão de seis meses a dois anos e, no caso de crimes contra o Presidente, a pena é aumentada em um terço.

Além disso, foi feita uma atualização ao artigo 266 do Código Penal, esta versão passou a referir-se a quem interromper ou inutilizar serviços telegráficos, telefónicos, informáticos ou qualquer forma de utilidade pública, e à falsificação de documento privado (BRASIL, 2012).

De acordo com Siqueira (2017) importante ressaltar que a polêmica em torno da tramitação do tema da Lei 12.737/2012 fez com que projetos de lei com o mesmo assunto tramitassem por mais de 10 anos sem produção legislativa final, isso se deu pela dificuldade de compreensão e conclusão da legislação.

As regulamentações sobre crimes informáticos (Leis 12.735/2012 e 12.737/2012) entraram em vigor em 2 de abril de 2013, essas leis também alteraram o Código Penal para tratar de crimes cibernéticos. Depois de surgir como substituta da Lei Azeredo, que foi criticada pelo medo de impactar negativamente a liberdade virtual dos internautas, a lei apenas exigia que os órgãos judiciais se estruturassem, para buscar atividades criminosas no mundo virtual. Essa mesma legislação é transitou no Congresso desde 1999 (Crespo, 2013).

Seu conteúdo original era bastante extenso e discutível quanto à responsabilidade dos provedores de internet, mas após seu processamento foi reduzido a quatro artigos, dois dos quais foram posteriormente retirados pelo Presidente da República através de veto.

Em maio de 2014, foi iniciado o Decreto Federal nº 7.962/13 com o intuito de preencher as lacunas do Código de Defesa do Consumidor no que diz respeito ao comércio online, ou comércio eletrônico, uma vez que atualmente não existe legislação específica quanto ao processo de comprar ou vender pela internet. Com as novas regulamentações, as empresas que atuam no comércio eletrônico terão que revelar informações sobre seus sites sobre produtos, fornecedores, serviços e melhor atendimento ao cliente (Cassanti, 2014).

Com a edição do Marco Civil da Internet em 11 de maio de 2016, a preocupação de aplicar as leis brasileiras aos crimes na Internet já cometidos tornou-se mais significativa, principalmente devido às dificuldades associadas à obtenção de dados e evidências da Internet prestadores de serviços que atuam no Brasil (Brant, 2014).

Após a promulgação do Marco dos Direitos Civis para a Internet, houve um aumento significativo no compromisso do governo em regular o comportamento da sociedade civil no domínio digital. Esses são exemplos da tentativa de presença do poder estatal no combate e prevenção de crimes virtuais que ainda não foram formalmente classificados (Brant, 2014).

O Marco Civil da Internet regulamenta a proteção de dados na internet, é concedida proteção aos internautas, e afirma que as comunicações em princípio são impermeáveis, caso isso ocorra, só poderão ser retiradas mediante ordem judicial (Cassanti, 2014).

A salvaguarda dos dados pessoais é importante devido à natureza específica de algumas informações. Para evitar o excesso de zelo ou o uso indevido dessas informações, foi implementada a Lei 12.965/2014. Essas informações, conforme mencionado no artigo 4º da Lei 12.527/2011, são de propriedade do usuário, e não do site que armazena essas informações. Como resultado, o site que contém informações pessoais não tem autoridade sobre ele, por isso o legislador procurou evitar que o usuário fosse abusado.

A lei também concede às vítimas indenização por danos financeiros ou morais causados pela violação da privacidade, da vida pessoal e do sigilo das comunicações, exceto aqueles causados por ordem judicial formal e fundamentada (Brasil, 2002).

Na ausência de legislação específica, quem pratica crimes informáticos deve ser avaliado pelo próprio Código Penal, mantidas as distinções necessárias. Se, por exemplo, um determinado indivíduo participasse do ato de destruição, inutilização ou destruição de propriedade alheia, o indivíduo estaria sujeito a multa ou prisão de um a seis meses. Além disso, teriam que responder pelo crime de violação do artigo 163 do Código Penal, que é "destruir, inutilizar ou deteriorar coisa alheia: detenção, de um a seis meses ou multa".

Este artigo descreve como a pornografia infantil pode ser categorizada em dois tipos de comportamento: o primeiro é a prática de tirar ou publicar fotos ou vídeos que retratam crianças e adolescentes fazendo sexo, comportamento considerado explícito. O Estatuto da Criança e do Adolescente 8.69/90, determina que qualquer conteúdo da Internet que contenha imagens de crianças ou adolescentes em situações sexuais será considerado pornografia infantil. A pena base de 1 (um) a 4 (quatro) 28 anos de reclusão foi aumentada para 2 (dois) a 6 (seis) anos por esta conduta:

> Art. 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente. § 1º Incorre na mesma pena quem: I – agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação de criança ou adolescente em produção referida neste artigo; II – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do caput deste artigo; III – assegura, por qualquer meio, o acesso, na rede mundial de computadores ou Internet, das fotografias, cenas ou imagens produzidas na forma do caput deste artigo (BRASIL, 1940).

E se o agente que comete o crime de pornografia infantil utilizando seu cargo ou função; ou ainda, se o agente cometer o crime com o objetivo de obter vantagem financeira para si ou

para outrem, será qualificado nos termos do art. 4º § 2º, aumentando a pena base de 2 (dois) para 3 (três) anos de reclusão.

Estas disposições visam proteger os direitos e a integridade das crianças e dos jovens, criminalizando condutas que exploram ou violam a sua dignidade e desenvolvimento. Além disso, ao prever a classificação de crimes em determinadas circunstâncias, a lei visa aumentar as penas para aqueles que abusam do seu poder ou procuram lucrar com a exploração sexual de menores.

Por outro lado, a Calúnia, injúria e difamação são todas abordadas nos arts. 138 a 140 para que os crimes de calúnia e difamação sejam caracterizados via internet, o delito deve ser encaminhado ao público em geral, e não apenas à vítima. Como o dano ocorre, a mensagem deve ser enviada ao público como um todo, e não apenas à vítima. Nas instâncias citadas, o crime será honrar o objetivo e na segunda, desobedecer ao sujeito (Martins, 2017)

Ainda, a Lei nº 13.718/18 alterou a forma como são tratados os crimes de conteúdo sexual. A partir deste grau legal, a agressão sexual e a distribuição de cenas de estupro ou estupro de indivíduo vulnerável, sexo ou pornografia tornaram-se ações ilegais. Além disso, expõe as causas do aumento das penas criminais para esses crimes. Esta lei revelou um novo tipo penal através do artigo 218-C do Código Penal, que é o seguinte:

> Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio – inclusive por meio de comunicação de massa ou sistema de informática ou telemática –, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia: Pena – reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave (BRASIL, 2018).

Masson (2020) descreve o bem jurídico como sendo de natureza sexual e tendo uma contrapartida material: fotografia, vídeo ou outras gravações audiovisuais. Nesse sentido, o autor também enfoca as características centrais desse tipo criminoso, que são oferecer, trocar, disponibilizar, transmitir, vender, expor à venda, distribuir e publicar.

O participante ou espectador pode ser qualquer pessoa. No entanto, o primeiro parágrafo do artigo 218-C do Código Penal, que descreve a pornografia de vingança, estipula que o legislador aumentará a pena para o agente "que manteve ou mantém relação amorosa com a vítima" de um terço para dois terços.

Nesse sentido, apesar de se assemelhar aos artigos 241 e 241-A do ECA, a referida classificação distinguiu a inovação das demais classes, mas reconheceu ampla punição para a divulgação de imagens de crianças e adolescentes em cenas sexuais, bem como para qualquer

gravação que contenha cenas de estupro ou de tolerância ou indução ao estupro; sexo, nudez ou representação de pessoa que não esteve envolvida na conduta criminosa do artigo 218-C (Gilaberte, 2018).

Por último, a punição para quem cometia o crime de peculato virtual foi a prevista no início do artigo 171 do Código Penal, normalmente envolveria encarceramento por um a cinco anos, além de multa. Porém, esta situação foi alterada com a implementação da Lei nº 14.155, ocorrida em 27 de maio de 2021, esta lei adicionou o conceito de fraude eletrônica ao rol de crimes.

Agora, de acordo com o segundo parágrafo do artigo 171, quem cometer um crime de forma não presencial, envolvendo meios eletrônicos como redes sociais, chamadas telefónicas falsas ou envio de e-mails prejudiciais ou métodos semelhantes, será punido com 4-8 anos de reclusão.

Com a nova regra que permite aumento de pena em até 1/3, se os acusados vitimarem idosos. Trata-se de uma alteração legislativa positiva, conhecida como *novatio legis in mellius*, que permite a aplicação de leis retroativas a casos de fraude de idosos ocorridos antes da promulgação da Lei nº 14.155/2021. (Castro, 2021). Além disso, em casos onde vulneráveis são atingidos, a legislação também tem sua pena aumentada.

As leis sobre crimes virtuais e a proteção da privacidade online são essenciais para manter as pessoas seguras no ambiente digital. O objetivo de leis como a Lei nº 12.965/2014 e o Código Penal Brasileiro não é apenas punir os criminosos, mas também proteger os direitos individuais dos internautas. Além disso, recentes alterações legislativas, como a Lei nº 13.718/18, demonstram esforços contínuos para adaptar a regulamentação às novas realidades e desafios que o mundo virtual enfrenta.

CONSIDERAÇÕES FINAIS

Diante das informações acima mencionadas, compreende-se que o rápido crescimento da tecnologia digital levou a novas oportunidades para atividades criminosas, o que representou um desafio à eficácia das leis existentes na monitorização destas alterações. A variedade de crimes virtuais, desde invasões de sistemas e transmissão de malwares, até a exploração de crianças e adolescentes, mostra a complexidade e gravidade do fenômeno. Estas práticas não são apenas prejudiciais à segurança e à privacidade das pessoas, mas também têm o potencial de causar danos emocionais, financeiros e sociais significativos.

A legislação vigente serve como quadro jurídico para lidar com muitos aspectos do crime cibernético, no entanto, a sua aplicação ainda é um problema. A complexidade do ambiente digital e a natureza transfronteiriça destes crimes dificultam frequentemente a investigação e a punição dos criminosos.

Nesta perspectiva, torna-se crucial que a legislação continue a ser revista e modificada para enfrentar os novos desafios técnicos colocados pelo avanço da tecnologia. Além disso, a cooperação internacional é crucial para combater eficazmente o crime cibernético, uma vez que frequentemente atravessa fronteiras nacionais.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. Os objetos intangíveis na era da criminalidade informática. **Espaço Jurídico, Jornal of Law**, v.7, n.2, p.165-178, 2006.

BARBOSA, Adriana Silva et al. Relações Humanas e Privacidade na Internet: implicações Bioéticas. **Rev. Bioética y Derecho**, Barcelona, n. 30, p. 109- 124, 2014.

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à luz do Marco Civil na Internet**. Rio de Janeiro: Brasport, 2016.

BASTOS, J. T. **Crime Cibernético E O Estelionato Virtual.** Erechim, 2016. Trabalho de Conclusão de Curso (Bacharelado em Direito) –Universidade Regional Integrada do Alto Uruguai e das Missões –Campus Erechim. 2016. Disponível em: https://www.uricer.edu.br/cursos/arq_trabalhos_usuario/4259.pdf. Acesso em: 08 de maio de 2024.

BRASIL. **Lei nº 14.155**, de 27 de maio de 2021. Brasília, 27 de maio de 2021; 200º da Independência e 133º da República. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acessoem: 08 de maio de 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Brasília. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2014/lei/l12965.htm. Acesso em: 08 de maio de 2024.

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: 08 de maio de 2024.

BRASIL. Código Penal. **Código Penal Brasileiro.** Brasília, DF: Senado Federal, 1940.

BRANT, Cássio Augusto Barros. **Marco Civil da Internet:** comentários sobre a Lei 12.965/2014. Belo Horizonte: D´Placido, 2014.

CAIADO, Felipe B.; CAIADO, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. In: DOMINGOS, Fernanda Teixeira Souza et al. **Crimes cibernéticos:** coletânea de artigos. Brasília: MPF (Ministério Público Federal), 2018. Cap. 1. p. 8- 25. Disponível em: https://memorial.mpf.mp.br/nacional/vitrinevirtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 08 de maio de 2024.

CAPEZ, Fernando. **Curso de Direito Penal**. 17. ed. São Paulo: Saraiva, 2013.

CARVALHO, G. C. Crimes cibernéticos. **Rev. Conteúdo Jurídico**. 2018. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/51878/crimes-ciberneticos Acesso em 08 de maio de 2024.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.

CASTRO, Leandro. **Direito pena l:** parte geral. Leonardo Castro. - 1. ed - São Paulo: Rideel. 2021

CRESPO, Marcelo. **Crimes digitais:** do que estamos falando? 2015. Disponível em: https://canalcienciascriminais.jusbrasil.com.br/noticias/199340959/crimes-digitais-doque-estamos-falando. Acesso em: 08 de maio de 2024.

CRESPO, Marcelo Xavier de Freitas. Marcelo Xavier de Freitas. Os crimes digitais e as Leis 12.735/2012 e 12.737/2012. **Boletim IBCCRIM**, ano 21, n. 244, 2013.

FIORILLO, Celso Antônio Pacheco. **Crimes no meio ambiente digital**. São Paulo: Saraiva, 2013.

GILABERTO, Bruno. **Lei nº 13.718/2018:** importunação sexual e pornografia de vingança. Jusbrasil. Online, 2019. Disponível em: https://canalcienciascriminais.jusbrasil.com.br/artigos/629753885/lei-n13718-2018-importunacao-sexual-e-pornografia-de-vinganca. Acesso em: 08 de maio de 2024.

JESUS, D. D.; MILAGRE, J. A. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016.

MALAQUIAS, Roberto Antônio Darós. **Crime Cibernético e Prova:** a investigação criminal em busca da verdade. 2. ed. Curitiba: Juruá, 2015.

MARTINS, A. B. da S. **Crimes virtuais**. Curso de Direito da Faculdade de Sabará. 2017. Disponível em:<http://faculdadesabara.com.br/media/attachments/monografias/Monografia_Crim es-Virtuais_Aluno-Aislan.pdf> Acesso em 08 de maio de 2024.

MASSON, Cleber. **Direito penal:** parte especial - (arts. 213 a 359-H). São Paulo: Método, 2020.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**. 13 ed. Rio de Janeiro: Forense, 2017.

SIQUEIRA, Marcela Scheuer et al. Crimes virtuais e a legislação brasileira. (**Re)Pensando o Direito** – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13, 2017. Disponível em http://local.cnecsan.edu.br/revista/index.php/direito/article/view/468. Acesso em: 08 de maio de 2024.