CRIMES CIBERNÉTICOS[1]

Alex Costa Pedroso

Emilly Rocha

Resumo

O presente trabalho teve como objeto de estudo os crimes cibernéticos. Com o avanço tecnológico, a sociedade experimentou diversas facilidades e avanços na vida pessoal, no trabalho, na educação etc., mas, também, ficou vulnerável a determinados riscos, como os crimes virtuais. Nesse vértice, a pesquisa se justificou na necessidade de aprofundamento teórico a respeito dos crimes cibernéticos. O objetivo geral consistiu em entender o que são os crimes cibernéticos. Por sua vez, os objetivos específicos consistiram em contextualizar a questão relativa aos crimes cibernéticos, abordando os crimes mais praticados no ambiente virtual; discorrer sobre a aplicação das leis que objetivam a proteção das pessoas em ambiente virtual, sobretudo a respeito de sua atividade, e necessidade de edição de novos mecanismos legislativos. O trabalho seguiu o método dedutivo, sendo a metodologia de pesquisa bibliográfica, com toda a fundamentação retirada de livros e artigos sobre o tema e/ou temas correlatos, e julgados que também tratam sobre a matéria.

Palavras-chave: Tecnologia. Crimes cibernéticos. Provas. Desafios.

1 Introdução

O presente trabalho tem como objeto de estudo os crimes cibernéticos. Na atualidade, em decorrência do avanço tecnológico, a sociedade se informatizou e as pessoas estão, cada vez mais, interligadas por dispositivos tecnológicos.

A internet, na atualidade, se tornou fundamental em vários seguimentos, como o trabalho, o estudo, e, até mesmo, relacionamentos interpessoais, sendo indispensável para o uso de celulares, computadores e similares. Ainda existem regiões mais pobres no Brasil em que o acesso à internet é dificultado, mas a maioria massiva da população a utiliza e faz dela uma funcionalidade indispensável no cotidiano.

A tecnologia teve o seu ponto alto de desenvolvimento com a Revolução Industrial, época em que a mão de obra passou a ser substituída pelas máquinas. Nesse período, reconheceu-se a importância da tecnologia nas formas de produção, surgindo, a partir daí, as grandes e modernas fábricas.

Nota-se que a tecnologia não se refere apenas ao surgimento de dispositivos eletrônicos mundialmente utilizados na atualidade, mas a toda uma profunda e complexa modificação dos meios de produção. A sociedade pós-moderna é veementemente

[1] Trabalho de Conclusão de Curso a ser apresentado ao Centro de Ensino Superior Una de Catalão como requisito parcial para a integralização do curso de Direito, sob orientação do professor Marcos de Oliveira Gonçalves Toledo.

influenciada por questões tecnológicas e atualizações digitais, que são desenvolvidas a todo tempo e são alvo de desejo de milhares de pessoas.

Além das facilidades ocasionadas pela evolução tecnológica, o meio informático também passou a ser um ambiente propenso ao cometimento de crimes. O crime é um fato social, portanto, onde há sociedade, há crime. Esse fenômeno se adequa aos novos moldes sociais, e não seria diferente com o ambiente virtual. Assim, como a sociedade direcionou parte de suas relações para a internet, com compras, movimentações financeiras e relacionamentos interpessoais, os criminosos viram uma oportunidade no ambiente virtual.

Existe a errônea percepção de que a internet é uma terra sem lei e que tudo que ali for praticado não ensejará nenhum tipo de responsabilização legal, tanto civil como penal. Em decorrência dessa percepção, as pessoas se excedem em suas condutas e cometem atos ilícitos, os chamados “crimes virtuais” ou “crimes cibernéticos”.

A internet não pode ser considerada terra sem lei porque o Direito Penal precisa interferir realizando a proteção dos bens jurídicos mais importantes, mas ainda é necessário que o Poder Legislativo destine parte do seu tempo na elaboração de mecanismos legais efetivos que versem sobre crimes digitais, para que a impunidade não seja garantida.

Os criminosos digitais são pessoas inteligentes, possuem conhecimento apurado a respeito do funcionamento das tecnologias, exemplo é o hacker, que possui conhecimento específico sobre programas e segurança. Assim, é comum que os crimes sejam cometidos sem que seja fácil identificar a autoria.

Por outro lado, sabe-se que existe uma deficiência investigativa por parte das autoridades policiais, que decorre da falta de especialização do pessoal, bem como da insuficiência de recursos e meios de investigação eficazes.

Nesse vértice, a pesquisa se justifica na necessidade de aprofundamento teórico a respeito dos crimes cibernéticos. A utilização segura da internet é necessária, tendo em vista que o ambiente virtual tem sido utilizado de forma frequente para a prática de diversos crimes, logo, estudar a fundo esse tema é necessário.

Em uma perspectiva social, os estudos científicos são utilizados como meio de informação e obtenção de conhecimento por parte da sociedade. É essencial que as pessoas não relacionem os crimes cibernéticos com a impunidade. Na atualidade, embora a obtenção de provas seja um desafio, é possível identificar o criminoso e responsabilizá-lo.

A pesquisa, além de propor um estudo ampliativo do tema, serve como meio de informação para a própria sociedade, como já destacado. O Estado deve se comprometer com o Direito, garantindo que o Processo Penal Brasileiro se adeque a essa nova realidade tecnológica e garanta um processo com resultados efetivos.

2 Crimes cibernéticos

Em decorrência do acelerado avanço tecnológico experimentado nas últimas décadas, a humanidade passou a utilizar a internet cotidianamente, acessando-a de diversos tipos de aparelhos eletrônicos. A internet, atualmente, é interessante em diversos cenários, sendo útil no trabalho e na vida social. É difícil pensar na sociedade atual sem acesso a essas facilidades contemporâneas.

Ocorre que, juntamente com as facilidades, a internet também apresenta perigo, crimes que sempre foram cometidos na "vida real", antes do advento da tecnologia, agora são cometidos em meio virtual, trazendo acentuada dificuldade na comprovação do fato e identificação do criminoso. Isso se deve, em grande parte, no fato de o Direito não acompanhar a evolução da sociedade frente à tecnologia, reforçando a ideia de que na internet não há o império da lei.

Pinheiro (2021) é clara ao afirmar que o Direito Digital traz a obrigação de atualização tecnológica para todos os operadores do Direito, como advogados, juízes, delegados, peritos, dentre outros. Essa mudança de postura é necessária para que se alcance uma realidade de sociedade digital segura.

Nesse tópico serão estudados três pontos importantes: o surgimento da tecnologia e da internet, a necessidade do Direito se adequar às novas configurações tecnológicas, e o cometimento de crimes pela via virtual.

2.1 A internet e a evolução tecnológica

O surgimento da internet e da tecnologia se relaciona com o desenvolvimento das técnicas, pois o homem sempre adotou procedimentos e técnicas diferenciadas para alcançar objetivos, como o desenvolvimento ou o aperfeiçoamento de algo socialmente útil. Assim, essa preocupação com as técnicas fez com que o homem realizasse uma revolução social, com o descobrimento e desenvolvimento de várias coisas (Veraszto, et. al., 2009).

Assim, a tecnologia é resultado da preocupação do homem com as técnicas: “É com o homem que as técnicas iniciam seu desenvolvimento, porque, este torna-se um prodigioso inventor de novos mecanismos, muito diferente daquilo que é concebido pela natureza” (Veraszto, et. al., 2009, p. 24).

O ponto alto do desenvolvimento tecnológico se deve à Revolução Industrial, momento em que a tecnologia passou a substituir o trabalho humano. Nesse período, as máquinas passaram a ser utilizadas em larga escala nas fábricas, em seu processo de produção, que, até então, era realizado pelo homem.

Chiavenato (2011) explica que, a partir de então, a tecnologia foi sendo desenvolvida em vários campos. Nos escritórios, surgiu a máquina de escrever, e o telefone surgiu no final do século XIX, permitindo a expansão de negócios e empresas. “O desenvolvimento tecnológico sempre constituiu a plataforma básica que impulsionou o desenvolvimento das organizações e permitiu a consolidação da globalização” (Chiavenato, 2011, p. 414).

A internet surgiu em 1969 por meio de uma operação chamada “ARPAnet” (Advanced Research Projects Agency Network) e podia ser acessada por 4 computadores que integravam a operação. Ela era utilizada como uma ferramenta de comunicação militar alternativa para facilitar a troca de informações e a elaboração de estratégias de guerra. O seu surgimento foi, então, ambientado na Guerra Fria. Foi na década de 90 que a popularidade da internet se expandiu, e, em 1995, a internet começou a se difundir no Brasil (Monteiro, 2001).

De acordo com Machado, et. al. (2018), a palavra “internet” deriva de *internetworking*, que se traduz em ligação entre redes. Mesmo ela sendo pensada como uma rede única, ela é o conjunto de todas as redes que usam protocolos TCP/IP. Assim, a “Internet emergiu como fruto de um processo de virtualização do computador, que o transformou de máquina em espaço de comunicação navegável e transparente” (Machado, et. al., 2018, p. 37).

Pinheiro (2021, p. 40) trabalha com um conceito completo de internet, como se vê:

> Tecnicamente, a Internet consiste na interligação de milhares de dispositivos do mundo inteiro, interconectados mediante protocolos (IP, abreviação de Internet Protocol). Ou seja, essa interligação é possível porque utiliza um mesmo padrão de transmissão de dados. A ligação é feita por meio de linhas telefônicas, fibra óptica, satélite, ondas de rádio ou infravermelho. A conexão do computador com a rede pode ser direta ou através de outro computador,

> conhecido como servidor. Este servidor pode ser próprio ou, no caso dos provedores de acesso, de terceiros. O usuário navega na Internet por meio de um browser, programa usado para visualizar páginas disponíveis na rede, que interpreta as informações do website indicado, exibindo na tela do usuário textos, sons e imagens. São browsers o MS Internet Explorer, da Microsoft, o Netscape Navigator, da Netscape, Mozilla, da The Mozilla Organization com cooperação da Netscape, entre outros.

Assim, como explicado pelo autor, a internet é complexa e se constrói a partir da interligação de milhares de dispositivo de todo o mundo, que se interligam por protocolos específicos. Por ser mundialmente utilizada, certamente, teria um sistema complexo de funcionamento.

Foi com a criação do World Wide Web (www), que a internet se popularizou a nível universal. Em uma perspectiva mais contemporânea, as redes sociais podem ser consideradas um segundo grande movimento de popularização da internet, depois do www (Machado, et, al., 2018).

A respeito disso, explica Pinheiro (2021, p. 40) que, na década de 90, o avanço que a internet experimentou foi extremamente evidente, e "seu rápido crescimento deve-se a vários de seus recursos e facilidades (...) que vão desde o correio eletrônico (e-mail) até o acesso a banco de dados e informações disponíveis na World Wide Web (WWW)".

No Brasil, o desenvolvimento da internet ocorreu juntamente com o desenvolvimento da pesquisa acadêmica e científica:

> A internet no Brasil se desenvolveu junto ao meio acadêmico e científico, e no seu início, o acesso era restrito a professores e funcionários de universidades e instituições de pesquisa. Somente no ano de 1995 a internet deixou de ser um privilégio das universidades para se tornar de acesso público. Desde então o número de provedores que oferecem o serviço e número de usuários que usam a internet aumentam a cada ano (Mancilla, 2014, p. 14).

Atualmente, a junção das tecnologias físicas, como celulares e computadores, com a internet proporciona a conectividade e a globalização para a sociedade. Inicialmente, a ideia da comunicação por meio da internet, embora fascinante, era desconhecida, causando temor para o homem comum, o que era coerente. Mas, com o tempo, foi se provando que a internet seria fundamental na sociedade (D'urso, 2017).

São milhares de websites e redes sociais existentes, o acesso a ferramentas gratuitas e pagas de criação de websites é facilitado, o mundo, de fato, passou a estar fortemente conectado por meio da internet e as pessoas passaram a poder criar relacionamentos interpessoais com pessoas de todos os países.

Nas palavras de Greco (2022, p. 1.111), o avanço tecnológico do século XXI é inacreditável:

> O século XXI está experimentando um avanço tecnológico inacreditável. Situações que, em um passado não muito distante, eram retratadas em filmes e desenhos infantis como sendo hipóteses futuristas, hoje estão presentes em nosso dia a dia. As conversas on-line, com visualização das imagens dos interlocutores, seja através de computadores, ou mesmo de smartphones, que pareciam incríveis no início da segunda metade do século XX, atualmente fazem parte da nossa realidade.

O autor supracitado explica que a internet, dentro de um mundo globalizado, se transformou em uma ferramenta essencial que o ser humano não pode abrir mão. As pesquisas são velozes, a localização de materiais e livros é facilitada, mas junto com toda essa modernidade necessária, a internet também traz os seus problemas (Greco, 2022).

Conforme lecionam Nucci e Teixeira (2019), a evolução social sofre o impacto das tecnologias disruptivas, que resultam no rompimento de padrões de comportamento social em decorrência do desenvolvimento da tecnologia. Assim, cabe ao Direito acompanhar as mudanças de comportamento com o uso da ciência, e, nesse cenário, algumas condutas, que antes não eram comuns, passam a exigir a atuação do Direito, sobretudo do Direito Penal.

Explica Machado, et. al. (2018, p. 39), que, mesmo que a internet e as redes sociais, bastante utilizadas na atualidade, sejam submetidas às leis, ainda se verifica a ocorrência de manifestações ilícitas:

> Apesar de estarem submetidas às leis, as redes sociais podem ser usadas como meio de divulgação de outros mecanismos de biopoderes, como campanhas, pesquisas e estatísticas, que visam controlar a vida humana, impondo ou desaconselhando uma postura, seja com o objetivo de obter rendimentos econômicos, seja com o fim de tentar eliminar supostas diferenças por concebê-las como inadequadas. Ao lado das posturas lícitas, também podem ocorrer manifestações ilícitas.

As pessoas que se utilizam da internet para o cometimento de crimes são os chamados cibercriminosos, são pessoas que, cada dia mais se especializam, obtendo conhecimento aprofundado a respeito do funcionamento das tecnologias e da própria internet.

Logo, nota-se que a sociedade digital tem evoluído com rapidez e o Direito deve acompanhar essas mudanças, sob pena de se tornar obsoleto, fazendo com que a falácia de que a internet é “terra” sem lei, se torne realidade.

2.2 Conceito e classificação dos crimes cibernéticos

O crime é um fato social estudado, recorrentemente, pela criminologia. Não há um conceito de crime na legislação brasileira, como havia nos Códigos de 1830 e 1890. A tarefa de definir crime passa a ser, então, da doutrina e não do legislador. Assim, as concepções doutrinárias de crime seguem dois pontos de vista: o material e o formal.

Sob o ponto de vista material, crime é a ação ou omissão que provoca lesão a interesse penalmente protegido. Logo, para a concepção material, o crime se relaciona com a proteção dos bens protegidos pela lei penal, correspondendo, então, à violação de um bem penalmente tutelado (Jesus, 2020).

Por sua vez, o conceito formal deságua no conceito analítico de crime. André Estefam (2021) explica que existem autores que definem o crime como fato típico, antijurídico, culpável e punível, mas que essa definição possui pouco prestígio na doutrina, pois a culpabilidade não deve ser considerada um elemento do crime, já que lhe é algo exterior. Existem, portanto, as teorias que conceituam o crime. A teoria clássica aponta que o crime é fato típico, ilícito e culpável, e a teoria finalista aponta que o crime é fato típico e ilícito. A doutrina majoritária brasileira segue a teoria finalista.

Nesse sentido, a doutrina é clara ao apontar que não existem dúvidas de que o crime é um fato típico e ilícito:

> O que se busca num conceito analítico é a identificação dos requisitos ou elementos constitutivos do crime, sob a ótica do nosso direito positivo. Sendo assim, não há dúvida de que o crime só pode ser considerado fato típico e ilícito, figurando a culpabilidade não como elemento do crime, mas como pressuposto de aplicação da pena (Estefam, 2021, p. 256).

Os crimes se dividem em diversas categorias/modalidades, como os crimes contra a vida, contra o patrimônio, contra à Administração Pública, dentre outros. Tais classificações estão presentes no próprio texto do Código Penal. Há também os crimes digitais ou cibercrimes que, muito embora não estejam na codificação penal, são também uma categoria.

De acordo com D'urso (2017), o termo "cibercrime" teria sido utilizado pela primeira vez no ano de 1990, em uma reunião do G-8, então composto pelos sete países mais desenvolvidos do mundo, mais a Rússia. O foco da discussão eram as práticas ilícitas cometidas por meio da internet e como combatê-las. Percebe-se que, no início da década

de 90, esse tipo de crime já era uma preocupação, mesmo que a tecnologia ainda não tivesse se expandido.

Os crimes cibernéticos, portanto, são "(...) qualquer conduta humana (omissiva ou comissiva) típica, antijurídica e culpável, em que a máquina computadorizada tenha sido utilizada e, de alguma forma, tenha facilitado de sobremodo a execução ou a consumação da figura delituosa" (Lima, 2012, p. 01).

Feliciano (2000, p. 42) também define a criminalidade informática como "o recente fenômeno histórico-sócio-cultural caracterizado pela elevada incidência de ilícitos penais quem por objeto material ou meio de execução o objeto tecnológico informático". O autor identifica o crime informático como um fenômeno histórico, social e cultural, o que evidencia a complexidade desse tipo de crime.

A doutrina alerta para a facilidade do cometimento de crimes em um ambiente virtual:

> Com a utilização da internet, delitos considerados como tradicionais, a exemplo do estelionato, podem ser praticados sem que a vítima conheça sequer o rosto do autor da infração penal. Nossa vida pessoal pode ser completamente devassada e colocada à disposição de milhões de pessoas. Nossa intimidade, enfim, estará disponível com apenas um toque no computador (Greco, 2022, p. 2.302).

Como citado, os crimes comumente cometidos no mundo real migraram para a internet, local que proporciona aos criminosos o anonimato. Indo mais além, a internet é o local que pode assegurar a impunidade, diante da dificuldade na produção de provas desse tipo de crime.

Teixeira (2022) explica que, além da popularização da internet, a pulverização do comércio eletrônico, com a movimentação de grandes quantias de dinheiro e informações pela internet, possibilitou a criação de um ambiente virtual muito visado pelos criminosos.

De acordo com Pinheiro (2021), a maioria dos crimes cometidos na rede ocorre também no mundo real, trata-se dos crimes informáticos impróprios, ou seja, a internet surge apenas como um facilitador para o cometimento de determinados crimes, principalmente pelo anonimato que ela proporciona ao sujeito ativo. Ou seja, a internet é uma extensão da sociedade, motivo pelo qual os crimes ocorrem de forma indiscriminada nesse meio.

Existem inúmeras dificuldades encontradas para punir os infratores virtuais, o que ocorre pela ausência de norma que caracteriza a conduta, a dificuldade na obtenção de

provas de autoria e materialidade, bem como a dificuldade na condução de uma investigação técnica especializada por parte da polícia (Duarte; Almeida, 2023).

Os crimes cibernéticos podem ser divididos em duas categorias diferentes. Essas categorias são denominadas de crimes digitais próprios e crimes digitais impróprios. Com relação a essa classificação, tem-se o entendimento de Crespo (2015, s/p) como se vê:

> Crimes digitais próprios ou puros (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático. São exemplos de crimes digitais próprios o acesso não autorizado (hacking), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas; e Crimes digitais impróprios ou mistos (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc). São exemplos de crimes digitais impróprios os contra a honra praticados na Internet, as condutas que envolvam trocas ou armazenamento de imagens com conteúdo de pornografia infantil, o estelionato e até mesmo o homicídio.

Teixeira (2022) também explica essa classificação e diz que vários tipos penais já existentes podem ser praticados pela internet, pois, via de regra, as características do tipo penal se referem à conduta, e não à maneira como se deu a conduta, exceto quando se trata de uma qualificadora.

Ato contínuo, os crimes informáticos impróprios são justamente os já existentes, mas que são praticados pela internet. Por sua vez, os crimes próprios são aqueles que apenas se referem a condutas praticadas no meio informático.

Ainda, cumpre ressaltar que os crimes cibernéticos não se relacionam apenas com práticas realizadas na internet, mas, também, com qualquer ação ou omissão que se utilize de sistemas informáticos, estejam eles ligados na internet ou não.

Por sua vez, Pinheiro (2021) ensina que o crime eletrônico, a princípio, é um crime de meio, ou seja, é utilizado o meio virtual para o seu cometimento. Não se trata de um crime fim por natureza, pois o crime fim só ocorre em ambiente virtual; a exceção são os crimes cometido por hackers. A maioria dos crimes cibernéticos também ocorre no mundo real, e a internet surge como uma facilitadora do seu cometimento.

3 Os crimes cibernéticos mais cometidos na atualidade

Os criminosos cibernéticos se diferem dos criminosos comuns pelo fato de possuírem uma maior inteligência e conhecimentos técnicos sobre o assunto. Os crimes são cometidos à distância, sem contato físico. Os hackers, por exemplo, possuem

conhecimentos profundos sobre programação e sistemas operacionais, conhecem as falhas de segurança nos sistemas e, geralmente, a sua grande motivação consiste em apenas demonstrar sua capacidade.

Os crimes digitais possuem roupagens distintas, ao mesmo tempo que é possível realizar a subsunção de um crime digital à uma norma já existente, também é necessária a atuação do Poder Legislativo na edição de novos tipos penais que se adaptem a essa nova realidade digital.

Pinheiro (2021, p. 223) opina: "Legislar sobre a matéria de crimes na era digital é extremamente difícil e delicado. Isso porque sem a devida redação do novo tipo penal corre-se o risco de se acabar punindo o inocente". Assim, trata-se de uma questão que deve ser encarada com cautela.

São vários os tipos de crimes cibernéticos passíveis de serem cometidos. É importante, portanto, compreender os principais tipos já existentes em que se enquadra uma conduta cometida virtualmente.

3.1 Crimes contra a honra

Os crimes contra honra são alguns dos crimes mais cometidos no meio virtual, pois os seus autores encaram a internet como território sem lei, onde pode haver o livre lançamento de ofensas sem que haja responsabilidade.

Ocorre que, a Constituição Federal, em seu art. 5º, X, dispõe que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988).

O Código Penal, em seus artigos 138, 139 e 140, traz a tipificação da calúnia, da difamação e da injúria:

> Calúnia
> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime [...]
>
> Difamação
> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação [...]
>
> Injúria
> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro (BRASIL, 1940).

Assim, de acordo com Greco (2022), a honra é um conceito que se constrói durante toda a vida, podendo, em virtude de uma única acusação leviana, ruir de forma imediata. Desta feita, muito embora a Constituição Federal aponte a possibilidade de indenização no campo cível, os Códigos Penais, de forma tradicional, têm evidenciado a importância de punir tais condutas, a partir da criação de figuras típicas que afetam a honra.

Sobre os crimes contra a honra no ambiente digital, destaca-se o seguinte entendimento:

> Os crimes contra honra em específico, são cometidos pelo meio de rede sociais como whatsapp, facebook e instagram. Normalmente tais crimes são cometidos por redes sociais, em comentários, postagens ou mensagens privadas. As consequências jurídicas dos crimes contra a honra por meio virtual têm início pela lesão do bem jurídico tutelado qual é a honra, visto que é um direito fundamental observado pela Constituição Federal de 1988 (Rodrigues; Lima; Freitas, 2020, p. 356).

No meio virtual há a constante troca de informações, desenvolvimento de diálogos, emissão de opiniões, críticas, dentre outras formas de manifestação do pensamento, que contribuíram para que os crimes contra a honra se difundissem de forma desproporcional. Assim, é possível encontrar com facilidade insultos contra pessoas ou grupos específicos, bem como o discurso de ódio.

Teixeira (2022) esclarece que crimes contra a honra, quando praticados no mundo virtual, podem provocar danos mais graves às vítimas, isso porque as informações postadas em rede alcançam um número ilimitado de pessoas, desrespeitando a dignidade da vítima, e podendo, inclusive, incitar o ódio contra ela ou grupo por ela pertencente.

Contudo, tudo que é expresso na internet deve ser avaliado e reavaliado pelo usuário, ainda mais se a opinião ou expressão for criminosa, pois a liberdade de expressão assegurada constitucionalmente, embora seja constantemente invocada na defesa de alguns crimes virtuais, não é um direito absoluto, podendo ser limitado (Soares, 2016).

3.2 Crimes contra o patrimônio

Os crimes contra o patrimônio figuram na lista das infrações penais mais cometidas na atualidade. A doutrina tenta encontrar um motivo para o grande cometimento desse tipo de crime:

> Estudos criminológicos já demonstraram que as infrações patrimoniais são praticadas em decorrência da ausência do Estado, melhor dizendo, da má administração da coisa pública, que gera a desigualdade social, criando bolsões de miséria, separando, cada vez mais, as classes sociais existentes (Greco, 2022, p. 1156).

Ocorre que, os crimes contra o patrimônio se difundiram tanto, que passaram a ser cometidos também pela internet, considerando, inclusive, que existem aplicativos e plataformas digitais bancárias por onde usuários fazem movimentações financeiras. Um dos crimes contra o patrimônio mais praticados é o furto. Ele está presente no artigo 155 do Código Penal, que traz a seguinte redação: "Subtrair, para si ou para outrem, coisa alheia móvel" (BRASL, 1940).

O furto pode ser praticado pela via virtual, a partir da violação de dispositivo informático, ou invasão de contas bancárias, por exemplo. Nessas situações, o agente tem acesso a informações ou valores que se encontram disponíveis em meio virtual e os furta.

A respeito desse tipo de crime, a doutrina explica:

> Um dos crimes contra o patrimônio de maior alcance é aquele em que, pela internet, os criminosos transferem quantia em dinheiro de contas de terceiros para suas próprias contas; ou de terceiros (ou mesmo contas fantasmas) e depois se apoderam das quantias. No sistema bancário, um dos golpes mais aplicados consiste basicamente nesse tipo de ação, que e é chamado salami slicing (fatias de salame), pois o criminoso transfere pequenas quantias de milhares de contas para a sua própria. Estes casos, no passado, muitas vezes, gozavam de algum fator interno da instituição financeira que colaborava para a execução do crime, geralmente envolvendo funcionários que subtraíam as senhas de correntistas e as compartilhavam com os criminosos. 273 Também podemos citar a facilidade com que se abre uma conta bancária no Brasil, com documentos de identificação e declarações de rendimentos falsos (Teixeira, 2022, p. 449).

Por outro lado, se assemelhando ao estelionato, há os agentes que se utilizam de meios enganosos para ter acesso a bens e valores das vítimas. O estelionato está previsto no artigo 171 do Código Penal, e tem a seguinte redação: "Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento" (BRASIL, 1940).

O estelionato virtual ou fraude eletrônica ocorre quando o criminoso engana a vítima por meio da internet, redes sociais, e-mail ou outro meio eletrônico que possibilite contato com ela, fazendo com que forneça algum dado confidencial, como senhas de acesso, por exemplo.

As fraudes de maior frequência, de acordo com Teixeira (2022), ocorrem em leilões, compra e venda de mercadoria, esquemas de pirâmide, utilização de senhas falsas ou alheias na conexão com provedores ou acesso a serviços on-line, dentre outros.

O crime de extorsão está previsto no artigo 158 do Código Penal, tendo a seguinte redação: "Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa" (BRASIL, 1940).

A extorsão também pode ser praticada em ambiente virtual, ocorrendo, frequentemente, por meio de invasões a dispositivos informáticos, com o fim de obter alguma informação sobre a vida da vítima, para, posteriormente, extorqui-la, com o fim de obter vantagem econômica. Foi o que ocorreu com a atriz Carolina Dieckmann, caso que será tratado em momento posterior.

O roubo é uma figura que pode ocorrer em meio virtual, embora possa ser facilmente confundido com a extorsão. Greco (2022) ensina que o crime de extorsão se assemelha muito com o delito de roubo, havendo, até mesmo, em alguns casos, dificuldade de diferenciar ambos os crimes. Trata-se de crime que pode ser cometido em ambiente virtual, mas que precisa da violência ou grave ameaça para a sua configuração.

3.3 Crimes sexuais

Outro exemplo de crime sexual cometido por meio da internet é a pornografia de vingança. Esse crime é caracterizado pela divulgação não consentida de material íntimo de conotação sexual por parte de uma pessoa que manteve relação íntima com a vítima e obteve, assim, o material. Gonçalves (2016, p. 10) conceitua: "consiste na divulgação, principalmente, na Internet, de qualquer material íntimo e privado, de conotação sexual, sem a sua devida autorização, seja ele foto, vídeo, montagem ou qualquer material sexualmente gráfico".

A pornografia de vingança foi inserida no Código Penal, em seu artigo 218-C, por meio da Lei n° 13.718/2018:

> Art. 218-C. 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, 1940).

A pornografia infantil também é contemplada pelo artigo 218-C do Código Penal. De acordo com Capez (2019), esse tipo penal tutela a intimidade sexual, notadamente no âmbito dos meios de comunicação, em especial o ambiente virtual. Por se tratar de vítima criança, a tutela é mais abrangente, visto os graves danos psicológicos e físicos que a criança sofreu para que esse conteúdo midiático fosse produzido.

De acordo com os ensinamentos de Pinheiro (2021), a pornografia infantil é o crime virtual mais cometido no Brasil, juntamente com o estelionato. Teixeira (2022, p. 452) explica como o crime pode ocorrer:

> Esta modalidade aparece na internet, em geral, em sites, redes sociais ou por mensagem eletrônica. Na primeira opção, os gerenciadores das páginas recebem uma quantia dos usuários (via depósito ou cartão de crédito), que dispõem de um acervo de fotos e vídeos.

Já na segunda, as redes sociais são mantidas e visitadas pelos pedófilos. Por sua vez, na última, o material é distribuído de um usuário a outro, diretamente, via transmissão de e-mails, torpedos etc.

Pauvels (2013) explica que a pornografia virtual é um crime extremamente praticado em todo o mundo, sendo mais avançado do que se pode imaginar. Ademais, a punição legal ainda é insuficiente, não apresentando a rigidez necessária, considerando a rapidez com a qual se dissemina o conteúdo de pornografia infantil na internet.

Esses crimes de divulgação de mídia pornográfica, seja ela adulta ou infantil, resulta em um dano irreparável à imagem, já que o que é colocado na internet, rapidamente chega em territórios inimagináveis, ultrapassando barreiras geográficas. Uma imagem divulgada na internet nunca mais será completamente excluída

Outro crime que pode ser abordado nessa classificação é o estupro virtual, pouco falado, mas possível de ser caracterizado. O estupro está tipificado no artigo 213 do Código Penal, que contém a seguinte redação: “Constranger alguém, mediante violência ou grave ameaça, a ter conjunção carnal ou a praticar ou permitir que com ele se pratique outro ato libidinoso: Pena - reclusão, de 6 (seis) a 10 (dez) anos” (BRASIL, 1940).

O tipo penal, muito embora pareça, não exige exclusivamente o estupro por contato físico. De acordo com a seguinte explicação doutrinária:

> Abre-se espaço, dessa forma, ao estupro virtual, praticado à distância, mediante a utilização de algum meio eletrônico de comunicação (Skype, Whatsapp, Facetime etc.). Pensemos na situação em que o sujeito, apontando uma arma de fogo para a cabeça do filho de uma mulher, exige que esta, em outra cidade, se automasturbe à frente da câmera do celular. Estão presentes as elementares típicas do art. 213, caput, do Código Penal: houve constrangimento da mulher, mediante grave ameaça, a praticar ato libidinoso diverso da conjunção carnal, razão pela qual ao agente deverá ser imputado o crime de estupro (Masson, 2018, p. 92).

De igual modo, Greco (2022) explica que não é essencialmente necessário o contato físico entre o criminoso e a vítima para a caracterização do crime de estupro, motivo pelo qual pode ser cometido à distância, ou por meio virtual, por exemplo. Trata-se de entendimento moderno e que deve ser considerado no caso concreto, já que os criminosos têm se aperfeiçoado cada vez mais e levado, para o mundo virtual, condutas que nem se pensaria ser possível praticar por esse meio.

3.4 Outros tipos de crimes

Outros crimes podem ser mencionados, como o cyberstalking. Esse crime consiste na perseguição no mundo virtual, por meio da internet. De acordo com os ensinamentos de Greco (2022), a todo momento surgem novos aplicativos e redes sociais que facilitam a interação entre pessoas, o que facilita, sobremaneira, a ocorrência do cyberstalking.

Os crimes de ódio também são cometidos na internet frequentemente. Discurso de ódio é o que incita o ódio, desprezo, violência e desrespeito contra uma minoria social. De acordo com Martins, et. al., (2011), para que se configure o discurso de ódio, assim como toda expressão discursiva, é necessária a transposição de ideias do plano mental (abstrato) para o plano fático (concreto). É muito comum que esse tipo de discurso seja encontrado na internet, em redes sociais, fóruns de discussão etc. Exemplo de grupos atingidos pelo discurso de ódio são os negros, as mulheres, a comunidade lgbtqia+, pessoas de uma região específica, dentre outros.

A falsidade ideológica é muito comum em ambiente virtual, onde uma pessoa se passa pela outra, valendo-se do uso de suas imagens, informações pessoais. Ressalta-se que, por meio desse perfil “fake” criado, o criminoso pode cometer outros tipos de crimes mais graves.

Teixeira (2022) trata da interceptação de correspondência e da violação de direitos autorais. O primeiro ocorre quando há a invasão de correios eletrônicos, os chamados e-

mails, e o segundo quando acontece o plágio seguido da publicação do conteúdo, por exemplo.

Há crimes cometidos especificamente em ambiente virtual sem que haja um tipo penal do mesmo crime cometido na vida real. Exemplo é a conduta praticada por hackers, que consiste em invadir sistemas, programas, sites, com a intenção de serem reconhecidos ou com a intenção de cometerem algum ilícito. Pinheiro (2021) exemplifica os ataques informáticos ocorridos, com certa frequência, em sites do governo brasileiro, deixando-os fora do ar.

Por fim, importante destacar o seguinte entendimento doutrinário que busca apontar o porquê do aumento de tantos crimes digitais na atualidade:

> Entendemos que há três razões para o aumento de crimes digitais: 1ª) Crescimento dos usuários de Internet e demais meios eletrônicos (celular, atm etc.) principalmente junto à baixa renda (classes C e D) e que se tornam vítimas fáceis, pois ainda não possuem cultura de uso mais seguro. 2ª) Quanto mais pessoas no meio digital, os bandidos profissionais (quadrilhas) também migram, e então há maior ocorrência de incidentes. 3ª) Falta de conscientização em segurança da informação, a maior parte das pessoas acha que nunca vai ocorrer com ela, empresta a senha, deixa o computador aberto e ligado, não se preocupa em usar as ferramentas de modo mais diligente, isso somado com uma dose de inocência potencializa as ocorrências (Pinheiro, 2021, p. 230).

Nota-se, portanto, que diversas são as possibilidades de um criminoso se valer do ambiente virtual no cometimento de crimes. A internet, como estudado, facilitou a vida de inúmeras pessoas, possibilitando acesso a informações inimagináveis, mas, ao mesmo tempo, abriu espaço para que infrações penais fossem cometidas.

4 Conclusão

Como estudado, nas últimas décadas o mundo tem presenciado uma grande evolução tecnológica. Nos últimos anos, as pessoas passaram a utilizar a internet e dispositivos eletrônicos para inúmeras atividades do cotidiano, como para conversar com outras pessoas, trabalhar, realizar compras, movimentações bancárias, dentre outras. Trata-se de uma facilidade que é realmente muito útil, mas a tecnologia não trouxe somente benefícios.

É como se o mundo experimentasse duas realidades e sociedades: a real e a virtual. Ocorre que, a noção de segurança não deve ser aplicada tão somente no mundo real, ou seja, na vida em sociedade, mas também no ambiente virtual. Mas, com o avanço

acelerado das tecnologias, o Direito foi tendo grandes dificuldade em acompanhar as mudanças. Várias situações jurídicas podem ser visualizadas com o uso da internet e uma delas é o crime, que é um fato social punido por uma ordem jurídica.

Os criminosos, em grande parte os mais especializados, migraram para o mundo virtual e passaram a praticar os chamados crimes cibernéticos. Várias são as maneiras de se cometer um crime em ambiente virtual, fala-se dos crimes cibernéticos próprios, que são aqueles cujo tipo descreve a prática de uma conduta que somente pode ocorrer pelo meio virtual, e fala-se dos crimes virtuais impróprios, que são aqueles cujas condutas são praticadas no mundo real e que também podem ser praticadas no ambiente virtual, como o estelionato, por exemplo.

Como estudado, existem os crimes mais comuns cometidos pela internet, exemplo são os crimes contra a honra, pornografia infantil, estelionatos, furtos. Ocorre que, os crimes cibernéticos próprios têm ficado cada vez mais sofisticados, em decorrência da inteligência dos seus autores, que são grandes conhecedores das tecnologias. O Direito Penal tem ficado parado diante dessas inovação, o que não é aceitável.

Atualmente, milhares de pessoas anônimas são vítimas dos criminosos cibernéticos e não há uma legislação consistente que preveja a conduta, criminalizando-a. Não está sendo afirmado que não existe legislação para crimes digitais no Brasil, pois existe, está sendo afirmado que elas são insuficientes e confirmam a falácia de que a internet é terra sem lei, dando abertura para a impunidade.

O presente estudo teve como foco especial a introdução a respeito dos crimes cibernéticos e das legislações aplicáveis atualmente no cenário brasileiro.

Muitos criminosos se valem do anonimato que a internet proporciona, tornando um desafio a identificação do criminoso, o que pode resultar em quebra dos dados pessoais dos usuários de uma determinada rede social, por exemplo. Outro ponto de destaque é que em grande parte dos casos, os crimes podem ser cometidos por meio de um perfil falso, com informações falsas, o que dificultaria ainda mais a identificação do criminoso.

O presente estudo não visou esgotar o assunto, mas sim contribuir para que novos estudos sobre o tema sejam realizados. Enquanto o Brasil não tiver normas substanciais sobre crimes cibernéticos, eles vão se sofisticar cada vez mais, dificultando mais ainda a obtenção de provas e eventual condenação. Espera-se que, em pouco tempo, esse cenário mude e navegar na internet possa ser algo seguro, e que condutas ilícitas cometidas nesse meio possam ser realmente punidas.

5 Referências

BRASIL, **Constituição Federal da República Federativa do Brasil**. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 30 set. 2023.

_____. **Decreto-lei n. 2.848, de 7 de dezembro de 1940**. Código Penal. Disponível: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em 30 set. 2023.

CAPEZ, Fernando. **Curso de direito penal.** Volume 3, parte especial: arts. 213 a 359-H. 17. ed. São Paulo: Saraiva Educação, 2019.

CHIAVENATO, Idalberto. **Introdução à teoria geral da administração**. 8. ed. Rio de Janeiro: Elsevier, 2011.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**: do que estamos falando? Disponível em: <http://canalcienciascriminais.com.br/ artigo/crimes-digitais-do-que-estamos-falando/>. Acesso em: 03 mai. 2023.

D'URSO, Luiz Augusto Filizzola. **Cibercrime**: perigo na internet. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/cibercrime-perigo-na-internet/>. Acesso em 07 out. 2020.

DUARTE, Samuel Victor; ALMEIDA, Tyciano Magno de Oliveira. Coagindo crimes cibernéticos: uma análise do arcabouço legal brasileiro para a segurança digital e comunicação. **Revista Altus Ciência**. Vol. 18, 2023. Disponível em: <http://revistas.fcjp.edu.br/ojs/index.php/altusciencia/article/view/148/115>. Acesso em 26 set. 2023.

ESTEFAM, André. **Direito penal parte geral**. 10. ed. São Paulo: Saraiva Educação, 2021.

FELICIANO, Guilherme Guimarães. Informática e criminalidade: parte 1: lineamentos e definições. **Boletim do Instituto Manoel Pedro Pimentel.** v. 13, n. 12. São Paulo, 2000, pp. 35-45.

GONÇALVES, Victor Hugo Pereira. M**arco Civil da Internet Comentado**. São Paulo: Editora Atlas, 2016.

GRECO, Rogério. **Curso de direito penal:** parte especial, artigos 121 a 212. 19. ed. Barueri: Atlas, 2022.

JESUS, Damásio. **Direito penal**. 37. ed. São Paulo: Saraiva Educação, 2020.

LIMA, Paulo Marco Ferreira. **Crimes de Computador**. 2012. Disponível em: <http://www.cartaforense.com.br/conteudo/entrevistas/crimes-de-computador/8112>. Acesso em 03 mai. 2023.

MACHADO, Vinicius Rocha Pinheiro; DIAS, Jefferson Aparecido; FERRER, Walkiria Martinez Heinrich. Biopolítica e novas tecnologias: o discurso do ódio na Internet como mecanismo de controle social. **Revista de Informação Legislativa**: RIL, v. 55, n. 220, p. 29-51, out./dez. 2018. Disponível em: <http://www12.senado.leg.br/ril/edicoes/55/220/ril_v55_n220_p29>. Acesso em 19 set. 2023.

MANCILLA, Omar Reyes. **A importância da Internet para o desenvolvimento das vendas no Brasil**. 2014. 29. Trabalho de Conclusão de Curso (Bacharelado em Administração) – Instituto Municipal de Ensino Superior de Assis, Fundação Educacional do Município de Assis. Assis, 2014.

MARTINS, Anna Clara Lehmann; SILVA, Rosana Leal da; NICHEL, Andressa; BORCHARDT, Carlise Kolbe. Discurso de ódio em redes sociais: jurisprudência brasileira. **Revista Direito GV**, São Paulo, pp. 445-468, 2011. Disponível em: <https://www.scielo.br/j/rdgv/a/QTnjBBhqY3r9m3Q4SqRnRwM/?format=pdf&lang=pt>. Acesso em 19 set. 2023.

MASSON, Cleber. **Direito penal**. Vol. 3. 8. ed. São Paulo: Forense, 2018.

MONTEIRO, Antonio Lopes. **Crimes hediondos**: texto, comentários e aspectos polêmicos. 7 ed. São Paulo: Saraiva, 2001.

NUCCI, Amanda Ferreira de Souza; TEIXEIRA, Leonardo de Aquino. Uma análise sobre *revenge porn* e a eficácia dos mecanismos jurídicos de repressão. **Consultor Jurídico**, São Paulo, 30 jul. 2019. Disponível em: <https://www.conjur.com.br/2019-jul-30/opiniao-revenge-porn-eficacia-mecanismos-repressao>. Acesso em: 03 mai. 2023.

PAUVELS, Carolina Maria. **Cibercrime sob o enfoque constitucional penal**: aspectos controvertidos da pornografia infantil e pedofilia. Seminário Internacional de Educação no Mercosul, 2013.

PINHEIRO, Patrícia Peck. **Direito digital**. 7. ed. São Paulo: Saraiva Educação, 2021.

RODRIGUES, Mariane; LIMA, Inayá Farias de; FREITAS, Rafael Silva de. FREITAS, Rafael Silva de. **Crimes Cibernéticos à luz dos crimes contra a honra**. Anais da 16° Mostra de Iniciação Científica, 2020, pp. 354-359. Disponível em: <http://revista.urcamp.edu.br/index.php/congregaanaismic/article/view/3929/2798>. Acesso em 25 set. 2023.

SOARES, Samuel Silva Basilio. **Os crimes contra a honra na perspectiva do ambiente virtual. 2016**. Disponível em: <https://semanaacademica.org.br/system/files/artigos/artigo_-_dos_crimes_virtuais_-_ambito_0.pdf>. Acesso em 25 set. 2023.

TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico**. 6. ed. São Paulo: SaraivaJur, 2022.

VERASZTO, Estéfano Vizconde; SILVA, Dirceu da; MIRANDA, Nonato Assis; SIMON, Fernanda Oliveira. Tecnologia: buscando uma definição para o conceito. **Prisma.Com**, São Paulo, p. 19-46, 2009. Disponível em: <https://ojs.letras.up.pt/ojs/index.php/prismacom/article/view/2065/1901>. Acesso em: 05 out. 2020.