EUROPEAN ACADEMIC RESEARCH
Vol. IX, Issue 7/ October 2021

Impact Factor: 3.4546 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

Crimes Cibernéticos: A insuficiência das leis brasileiras para punição de tais crimes

CÉSAR AUGUSTO BORGES DE ANDRADE[1]
JOÃO PAULO ABREU MARANHÃO[2]
RAFAEL T. DE SOUSA Jr.[3]

Resumo

Este artigo pretende realizar um estudo dos principais crimes cibernéticos, visando identificar as características que os tornam tão difíceis de serem tipificados criminalmente, como o anonimato e a dificuldade em localizar o infrator. Também é objetivo deste estudo analisar a evolução das leis brasileiras que abordam o assunto e demonstrar as dificuldades que os legisladores encontram em acompanhar a evolução desses crimes. Por fim, aborda-se as lacunas ainda existentes no ordenamento jurídico brasileiro.

Palavras Chaves: Crimes Cibernético, Legislação, Tipificação

[1] **César Augusto Borges de Andrade** received his bachelor degree in data processing in 1997 from the Mackenzie Presbiterian University, São Paulo, Brazil, and his M.Sc. degree in systems and computing in 2013 from the Military Institute of Engineering (IME), Rio de Janeiro, Brazil. Currently, he is a Ph.D. student at the Graduate Program in Electrical Engineering at the University of Brasilia (UnB), Brazil, researching on machine learning applied to malicious software detection systems.

[2] **João Paulo Abreu Maranhão** received his bachelor degree in telecommunications engineering in 2003 and his M.Sc. degree in systems and computing in 2014 both from the Military Institute of Engineering (IME), Rio de Janeiro, Brazil. Currently, he is a Ph.D. in Electrical Engineering at the University of Brasilia (UnB), Brazil, researching on multidimensional signal processing and machine learning applied to network intrusion detection systems.

[3] **Rafael T. de Sousa Jr.** (Senior Member, IEEE) received the bachelor's degree in electrical engineering from the Federal University of Paraíba (UFPB), Campina Grande, Brazil, in 1984, the master's degree in computing and information systems from the Ecole Supérieure d'Electricité–Supélec, Rennes, France, in 1985, and the Ph.D. degree in telecommunications and signal processing from the University of Rennes 1, Rennes, in 1988. He was a Visiting Researcher with the Group for Security of Information Systems and Networks (SSIR), Ecole Supérieure d'Electricité–Supélec, from 2006 to 2007. He has worked in the private sector from 1988 to 1996. Since 1996, he has been a Network Engineering Associate Professor with the Electrical Engineering Department, University of Brasília (UnB), Brazil, where he is currently the Coordinator of the Professional Post-Graduate Program on Electrical Engineering–Cybersecurity (PPEE) and supervises the Decision Technologies Laboratory (LATITUDE). He is Chair of the IEEE VTS Centro-Norte Brasil Chapter (IEEE VTS Chapter of the Year 2019) and of the IEEE Centro-Norte Brasil Blockchain Group. He is currently a Researcher with the Productivity Fellowship Level 2 (PQ-2) granted by the Brazilian National Council for Scientific and Technological Development (CNPq). His professional experience includes research projects with Dell Computers, HP, IBM, Cisco, and Siemens. He has coordinated research, development, and technology transfer projects with the Brazilian Ministries of Planning, Economy, and Justice, as well as with the Institutional Security Office of the Presidency of Brazil, the Administrative Council for Economic Defense, the General Attorney of the Union and the Brazilian Union Public Defender. He has received research grants from the Brazilian research and innovation agencies CNPq, CAPES, FINEP, RNP, and FAPDF. He has developed research in cyber, information and network security, distributed data services and machine learning for intrusion and fraud detection, as well as signal processing, energy harvesting and security at the physical layer.

Abstract

This article intends to carry out a study of the main cyber crimes, in order to identify the characteristics that make them so difficult to be criminally criminalized, such as anonymity and the difficulty to locate the offender. It is also the objective of this study to analyze the evolution of the Brazilian laws that approach the subject and to demonstrate the difficulties that legislators find in monitoring the evolution of these crimes. Finally, it addresses the gaps still existing in the Brazilian legal system.

Keywords: Cyber Crimes, Legislation, Typification

1. INTRODUÇÃO

É inegável que a internet trouxe inúmeros benefícios para a nossa sociedade, tanto em relação aos relacionamentos pessoais, quanto na área educacional e corporativa, porém ela também possibilitou o surgimento de novos crimes e amplificou os meios para a prática de crimes já existentes, principalmente pela facilidade e pela sensação de impunidade que a internet propicia.

Há vários tipos de crimes cibernéticos, sendo difícil precisar quando houve a primeira ocorrência, entretanto, há um consenso entre os autores de que os crimes virtuais têm origem na década de 60, segundo afirma Ivete Senise Ferreira (2005):

> Ulrich Sieber, professor da Universidade de Würzburg e grande especialista no assunto, afirma que o surgimento dessa espécie de criminalidade remonta à década de 1960, época em que aparecem na imprensa e na literatura científica os primeiros casos de uso do computador para a prática de delitos, constituídos, sobretudo por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas, denunciados, sobretudo em matérias jornalísticas. (FERREIRA, 2005)

Tendo origem na década de 60, os crimes cibernéticos se tornaram um grande problema mundial, devido aos avanços tecnológicos, às facilidades que se tem em cometer tal crime, junto com a dificuldade em definir a autoria do crime e ainda devido às leis ineficazes.

A primeira prisão de um criminoso virtual ocorreu apenas em dois de novembro de 1988, quando o estudante Robert Tappan Morris Junior, foi condenado a cinco anos de prisão por ter transmitido um *worm* que contaminou cerca 6.000 computadores que usavam sistema operacional *Unix*.

Os Crimes Cibernéticos são considerados pelos juristas pátrios como alguns dos crimes de mais difícil punição, justamente pela ausência de tipificação de alguns crimes e pelas lacunas encontradas nas leis existentes. Tipificar as infrações virtuais é de suma importância, haja vista que uma condutada não tipificada em lei, não é considerada como crime, pois segundo o Código Penal brasileiro no seu artigo 1º, "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal".

Os crimes tradicionais previstos na legislação brasileira não são suficientes para abranger a maioria dos crimes cibernéticos. O nosso Código Penal é de 1940 e embora ele possa ser aplicado em alguns crimes cometidos por meios digitais, se faz necessário a criações de leis específicas que englobem o maior número possível de delitos digitais.

A falta de normas específicas é um empecilho para o combate à criminalidade digital, ela propicia impunidade e acaba incentivando a prática de tais crimes. Embora o ordenamento jurídico brasileiro esteja atrasado em relação aos países desenvolvidos, algumas leis que tipificam crimes virtuais estão sendo criadas, como é caso da Lei Nº 12.737 de 30 de novembro de 2012, apelidada como lei Carolina Dieckmann e a Lei Nº 12.965 de 23 de abril de 2014, conhecida como Marco Civil da Internet, porém ainda há muitas lacunas na legislação brasileira.

Quando falamos de leis sobre Cibercrimes no mundo, nos deparamos com a Convenção sobre Cibercrime do Conselho da Europa também conhecida como Convenção de Budapeste, que é um documento de direito internacional público e foi elaborada por um comitê de peritos nacionais, congregados no Conselho Europa e teve a participação de vários outros países como os Estados Unidos da América, Canadá, Japão e África do Sul.

Também é importante destacar as dificuldades de identificação do autor ou autores dos crimes cibernéticos, seja pela indispensabilidade de autorização judicial para identificação do

endereço IP (*Internet Protocol*) de onde pode ter partido a ação e também pela necessidade de identificação daquele que efetivamente utilizou o dispositivo informático para a prática de um delito.

Dessa forma, o presente artigo visa demonstrar as principais características dos crimes cibernéticos e das leis brasileiras que abrangem tais crimes, disponibilizando um maior entendimento acerca do assunto, além de apontar as lacunas encontradas no ordenamento jurídico e identificar os crimes cibernéticos que ainda não são tipificados criminalmente, assim como mostrar os mecanismos que podem ser utilizados em caso de ausência de tipificação penal.

O texto deste trabalho está organizado da seguinte maneira: as seções 2 e 3 apresentam alguns conceitos básicos e discute trabalhos relacionados. As seções 4 a 7 detalham as características e os sujeitos dos principais crimes cibernéticos, assim como descrevem os principais motivos para a impunidade de algumas infrações virtuais e, apresentam mecanismos que os aplicadores da lei podem utilizar em caso de inexistência de lei que tipifica o crime julgado. As seções 8 e 9 trazem os crimes tipificados no ordenamento jurídico brasileiro e as lacunas encontradas em determinadas leis. A seção 10 apresenta as principais características da Convenção Internacional Sobre Cibercrime (Convenção de Budapeste), enquanto a seção 11 conclui o trabalho.

2. CONCEITOS BÁSICOS

Esta seção tem como objetivo apresentar as definições dos principais termos utilizados no artigo e facilitar o entendimento dos conceitos apresentados no trabalho.

2.1. Crimes Cibernéticos

Segundo Abdurrahmani (2014), crimes cibernéticos, *cibercrimes*, crimes informáticos ou crimes virtuais são termos utilizados para se referir a toda atividade na qual um computador ou uma rede de computadores é utilizada como meio para a prática de algum crime.

Crespo (2016) define duas categorias para os crimes cibernéticos: crimes digitais próprios (ou puros) e crimes digitais impróprios (ou mistos):

> 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.

2.2. Tipificação de crime

Tipificar significa tornar uma conduta em crime. Para isso é necessário descrever com precisão a conduta e atribuir uma pena. A tipificação penal decorre do princípio da legalidade, previsto no artigo 1º, do Código Penal brasileiro: "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal".

2.3. Ransomware

A Cartilha de Segurança para Internet (CERT.BR, 2018) define *Ransomware* como "um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário".

3. TRABALHOS RELACIONADOS

Esta seção apresenta uma análise de alguns trabalhos sobre crimes cibernéticos e as leis brasileiras que contemplam esses crimes.

Siqueira, et al (2017) tratam sobre a realidade dos crimes cibernéticos no Brasil e de que forma eles são ancorados pelo ordenamento jurídico. Nesse contexto, eles analisaram a história da internet desde os tempos primórdios até os dias atuais, ressaltando sua importância na sociedade da era informática, dando maior atenção ao surgimento da criminalidade virtual e explicitando os tipos

de crimes mais comuns. Por fim, os autores abordam a regulamentação existente para estas condutas ilícitas.

O artigo tem uma abordagem abrangente sobre os principais crimes cibernéticos, porém faz uma análise muito superficial sobre a lei Carolina Dieckmann e o Marco Civil da Internet. Também não aborda as leis mais recentes e não apresenta as falhas das leis analisadas.

No trabalho de Sanches e Ângelo (2018), os autores relacionam a evolução histórica de internet com o surgimento dos crimes cibernéticos. Para eles, as leis brasileiras são insuficientes para punir as infrações virtuais e assim acabam por permitir que até pessoas comuns causem danos consideráveis, como a pedofilia, publicação de informações pessoais e crimes contra honra. O artigo também explica a importância da criação de leis competentes para o combate de delitos informáticos. Os autores abordam detalhadamente a Lei Carolina Dieckmann, porém deixam de fora o Marco Civil da Internet, bem como alguns crimes previstos em outras leis, como o Código Penal.

Caiado e Caiado (2018) abordam como a evolução tecnológica facilitou a criação de vários crimes cibernéticos, em especial a pornografia infantil. No artigo o autor explica que as leis estão desatualizadas e que há a necessidade de maiores investimentos em pesquisas e técnicas de combates às infrações virtuais. As principais leis que tipificam os crimes virtuais são abordadas no artigo, porém o autor não aborda as brechas encontradas nessas leis e também focam apenas na pornografia infantil, deixando de lado outros tipos de crimes.

Panazzolo (2018) explora aspectos dos crimes cibernéticos, em especial o crime de racismo praticado pela internet, em comunhão com os princípios da terceira dimensão de direitos fundamentais e a proteção dos bens jurídicos inerentes aos direitos dessa dimensão. O trabalho começa analisando os crimes cibernéticos, notadamente a sua conceituação. Depois, analisa o crime de racismo. Em seguida, adentra no exame da teoria das dimensões dos direitos fundamentais. Por fim, explora a junção dos direitos da terceira dimensão e o racismo praticado no campo cibernético, sempre em apreço aos direitos humanos e fundamentais, abordando a

jurisprudência, a doutrina e a legislação vigentes no Brasil, bem como os tratados internacionais.

4. PRINCIPAIS CRIMES CIBERNÉTICOS

A evolução tecnológica, em especial da internet, possibilitou o surgimento de novos crimes, assim como criou novos meios para a prática de crimes já existentes, como por exemplo, a pedofilia e o racismo. Esta seção traz as características dos principais crimes cibernéticos.

4.1. Calúnia, Difamação e Injúria

A calúnia é a conduta na qual imputa-se a uma pessoa um crime sem que este o tenha realmente cometido. O Código Penal em seu artigo 138 define calúnia como o ato de "caluniar alguém, imputando-lhe falsamente fato definido como crime". A calúnia é comum em redes sociais, onde uma pessoa compartilha a foto de um indivíduo e o acusa injustamente de ter cometido um crime.

A difamação ocorre quando há ofensa à reputação de uma pessoa perante a sociedade. Diferentemente da calúnia, neste caso não é necessário que a ofensa se refira a um crime. Um exemplo é o de um sujeito que acusa injustamente um vendedor de não entregar o produto vendido. Assim, há a difamação da imagem do vendedor.

Por fim, a injúria é a ofensa a dignidade ou o decoro de uma pessoa. Como exemplo de injúria cometida na internet, temos comentários do tipo "ladrão", "burro", feitos em fotos publicadas em redes sociais.

4.2. Pornografia e Pedofilia

O Código Penal define pornografia como:

> 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. (BRASIL, 1940)

Já a pedofilia é caracterizada como um desvio sexual, no qual um indivíduo adulto sente-se sexualmente atraído por crianças. A pedofilia torna-se um crime de informática quando os pedófilos trocam entre si materiais pornográficos através de e-mails, redes sociais e outras ferramentas da internet.

Segundo artigo 241-A da Lei nº. 8.069, de 13 de julho de 1990, também conhecida como Estatuto da Criança e do Adolescente (ECA), pedofilia é

> oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. (BRASIL, 1990)

O Estatuto da Criança e do Adolescente sofreu no ano de 2008 uma atualização dada pela Lei nº. 11.829, de 25 de novembro de 2008, com objetivo de "aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet", adequando o ECA à dinâmica da internet.

4.3. Racismo

Existem diferentes formas de discriminação racial e a internet com certeza é uma das ferramentas mais eficazes para se praticar um crime de racismo, graças às redes sociais, *e-mails*, *chat* entre outros.

A Constituição da República Federativa do Brasil no seu artigo XLII prevê que a "prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei".

Apesar de todas as previsões legais os crimes de discriminação racial ainda são comuns na nossa sociedade e a difícil identificação do autor de um crime praticado através da internet faz com que alguns criminosos saiam impunes.

4.4. Divulgação de conteúdo sem autorização

Consiste na divulgação não autorizada de conteúdo após a invasão de um dispositivo informático. Tivemos dois casos emblemáticos deste crime: o da atriz Carolina Dieckmann, que sofreu uma invasão em seu

computador de uso pessoal e teve fotos íntimas divulgadas em redes sociais. Este caso deu origem à lei 12.737, de 30 de novembro de 2012 que foi batizada de lei Carolina Dieckmann. Mais recentemente, tivemos o caso do ator Stênio Garcia, que teve fotos íntimas com sua esposa, divulgadas na internet.

4.5. Furto de dados

O crime de furto de dados virtual pode ocorrer de duas formas: através da invasão de dispositivo informático alheio, na qual o criminoso obtém de forma ilícita dados ou informações da vítima, ou através de sites falsos que prometem prêmios ou simulam sites de empresas confiáveis, neste caso a própria vítima insere os dados que são capturados pelo criminoso.

4.6. Violação dos Direitos Autorais

Copiar, reproduzir ou utilizar indevidamente obras sem a expressa autorização do(s) autor(es) configura violação dos direitos autorais, também conhecido como pirataria. Vários sites como os de gerenciamento de arquivos e de downloads violam indiscriminadamente os direitos autorais.

A pirataria virtual é crime previsto em lei, porém ainda divide opiniões em relação a sua configuração, para alguns autores o fato de simplesmente disponibilizar arquivos sem a expressa autorização do autor confira um crime de pirataria, mas para outros autores é necessário que haja a intenção de se obter lucro com a disponibilização dos arquivos.

Independentemente da configuração de um ato como pirataria virtual, a punição para quem pratica tal crime é difícil de ser aplicada, pois milhares de pessoas disponibilizam arquivos para download e milhões baixam esses arquivos, sendo muito difícil identificar quem disponibilizou o arquivo e praticamente impossível identificar todas as pessoas que baixaram.

4.7. C*iberbullying*

É um tipo *bullying* praticado através de meios de comunicação virtual. Segundo Bari e Abbas (2016), praticar *ciberbullying* significa usar o espaço virtual para hostilizar uma pessoa por motivos supérfluos.

Diferentemente do *bullying* convencional, o *ciberbullying* é mais fácil de ser cometidos, pois pode ser feito de forma anônima nas diversas redes sociais, através de e-mails ou mensagens de texto.

Os ataques de *ciberbullying* são geralmente direcionados a características pessoais da vítima e são feitos em meio público, denegrindo a imagem da pessoa e afetando a sua autoestima.

Uma pesquisa realizada pela revista FORBES em 2018, com pais de 28 países, constatou que quase um em cada cinco pais diz que seu filho sofreu *ciberbullying* pela menos uma vez. Entre os países presentes na pesquisa, o Brasil aparece em segundo lugar, no qual 29% dos pais afirmam que o seu filho já sofreu *bullying* online, sendo que a Índia aparece em primeiro lugar com 37% dos casos.

Curiosamente, o fenômeno parece ser praticamente inexistente na Rússia onde não houve pais citando casos de *ciberbullying*, sendo que no estudo de 2016 a taxa era de 0%, conforme pode ser visto na figura 1.

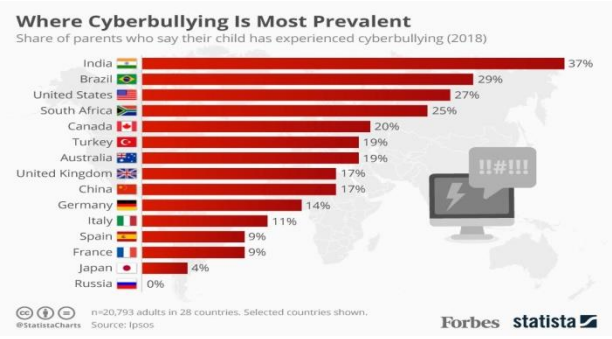

Figura 1 – Casos de *Ciberbullying* em alguns países
Fonte: (McCARTHY, 2018)

5. SUJEITOS DO CRIME CIBERNÉTICO

Em relação aos sujeitos do crime cibernético, temos as figuras do sujeito ativo e do sujeito passivo. O sujeito ativo é quem pratica o crime, podendo ser uma pessoa com amplo conhecimento técnico ou um indivíduo comum. Já o sujeito passivo, é quem sofre os danos causados pela ação criminosa do sujeito ativo.

5.1. Sujeito Ativo

Ao contrário do que muita gente pensa os criminosos da informática não são os *hackers*. Os profissionais de informática e os doutrinadores preferem chamar esses criminosos de *crackers*.

Assim como os *crakers*, os *hackers* também detêm um amplo conhecimento de informática, porém diferentemente dos *crakers*, eles não usam esse conheci mento para danificar sistemas e nem para prejudicar as pessoas. Normalmente os *hakers* são contratados por empresas que pretendem encontrar alguma falha de segurança nos seus sistemas. Também conhecidos como "*White Hat*", os *hakers* não praticam nenhum crime, assim como afirma Assunção (2008):

> *Hacker White-Hat*: Seria o "*hacker* do bem", chamado de "*hacker* chapéu branco". É aquela pessoa que se destaca nas empresas e instituições por ter um conhecimento mais elevado que seus colegas, devido ao autodidatismo e à paixão pelo que faz. Não chega a invadir sistemas e causar estragos, exceto ao realizar teste de intrusão. Resumindo: tem um vasto conhecimento, mas não o usa de forma banal e irresponsável.

Os *crakers* são os criminosos que usam seu vasto conhecimento para invadir sistemas, para roubar dados ou causar danos a terceiros. Ao contrário dos *hakers* que são conhecidos como "*White Hat*", os *crakers* são conhecidos como "*Black Hat*", conforme Assunção (2008):

> *Hacker Black-Hat*: "*hacker* do Mal" ou "chapéu negro". Esse, sim usa seus conhecimentos para roubar senhas, documentos, causar danos ou mesmo realizar espionagem industrial. Geralmente tem seus alvos bem definidos e podem passar semanas antes de conseguir acesso onde deseja, se o sistema for bem protegido.

É comum as pessoas trocarem os termos, associando o criminoso ao termo *hacker*, entretanto o termo mais adequado é *craker*, sendo *hacker* aquela pessoa que detém um vasto conhecimento de informática, mas não prejudica ninguém.

5.2. Sujeito Passivo

Qualquer pessoa que tenha ou não acesso à internet pode ser vítima de um crime cibernético. Os sujeitos passivos são as pessoas que utilizam qualquer tecnologia informática (computadores, *smartphones*, *tablets* etc).

6. MOTIVOS DA IMPUNIDADE

Os motivos que implicam na impunidade de quem pratica um crime cibernético são: Inexistência de lei tipificadora, difícil identificação do autor do crime, falta de conhecimento técnico dos magistrados e também as facilidades encontradas para praticar tais crimes.

6.1. Princípio da legalidade e Inexistência de lei tipificadora

O princípio da legalidade traz que caso não haja uma lei que tipifica uma conduta, então ninguém será obrigado praticar ou deixar de praticar tal conduta, é o que diz o artigo 5º, inciso II da Constituição Federal, "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei", em outras palavras, mesmo que a conduta seja imoral ou antiética, ninguém poderá ser punido por praticá-la, caso a mesma não esteja enquadrada em alguma lei.

A Constituição Federal e o Código Penal brasileiro definem sem eu artigo 5º, inciso XXXIX e artigo 1º, respectivamente, que "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal". Tais artigos são exemplos do princípio constitucional da legalidade e deixam bem claro o grande problema da impunidade dos crimes cibernéticos – como em sua maioria eles não são tipificados por nenhuma lei, então nem crimes eles são, e se não são crimes, não pode haver punição para quem praticá-los.

Nesse contexto Castro (2012) afirma que

> O problema surge em relação aos crimes cometidos contra o sistema de informática, atingindo bens não tutelados pelo legislador, como dados, informações, hardware, sites, home *pages*, *e-mail* etc... São condutas novas que se desenvolveram junto com nossa sociedade razão pela qual o legislador de 1940, época do Código Penal, não pôde prever tais tipos penais.

Tal princípio se justifica para limitar o poder arbitrário do Estado, protegendo os direitos dos cidadãos e limitando a atuação do Estado à lei. Porém, acaba por beneficiar o agente do crime cibernético, já que não existe lei para a maioria desses crimes.

Para os magistrados pátrios a maior dificuldade em punir quem pratica um crime virtual está relacionada à dificuldade de enquadrar tais crimes na nossa legislação comum, opinião

compartilhada por Prieto e Gahyva (2012), como não há um regramento legal específico que componha um microssistema que trate do tema, muitas condutas danosas acabam sem punição, pois nem sempre se faz possível à aplicação da legislação penal comum.

Ainda segundo Prieto e Gahyva (2012),

> [...] as infrações penais e abusos que constantemente ocorrem são de toda a ordem: racismo; pornografia infantil; apologia ao crime; difamação; estelionato; pirataria; espionagem clandestina; crimes contra a economia popular; ameaça; violação de correspondência; furto; e, até mesmo prática de terrorismo.

Diante da amplitude dos Crimes Cibernéticos é necessário que se crie uma lei que tipifique os crimes da informática com urgência, é o que defende Silva (2012),

> É extremamente necessário e urgente, buscar a tipificação dos crimes de informática e condutas criminosas que são efetuadas através da Rede Mundial de Computadores, sob o risco da própria sociedade como um todo entrar em uma área ainda por muitos desconhecida, onde não há território delimitado e muito menos um ordenamento jurídico de controle social.

A dificuldade em criar tal lei fica mais evidente quando o crime ocorre fora do território brasileiro, pois o Brasil adota o princípio geral da territorialidade, onde as leis ficam limitadas ao seu território.

Em sua obra Roque (2007) explana que,

> [...] a questão que sucinta maiores dúvidas é a dos crimes à distância como nos casos dos delitos praticados através da internet quando a ação é executada em um país e seus efeitos ocorrem no Brasil. Como resolver, então, estes problemas: a solução estaria na celebração de tratados internacionais, mas para isso ser possível há necessidade da existência, primeiramente, da dupla incriminação, ou seja, que as condutas constituam crime em ambos os países.

Prieto e Gahyva (2012) concluem que não resta outra solução para o direito senão acompanhar essa evolução, buscando ampliar a regulamentação de tais comportamentos, reconhecendo sempre que o combate a tal espécie de criminalidade representa um enorme e diário desafio para todos os componentes do sistema penal.

6.2. Difícil identificação do autor

Para acessar a internet não é necessário na maioria dos casos nenhum tipo de identificação pessoal, qualquer pessoa pode acessá-la praticamente de qualquer lugar e sem nenhum controle.
A maior falha de segurança da internet é que não é necessária a identificação do usuário através de um documento oficial. Hoje a identificação de um usuário é feita através do IP da máquina.

É através do protocolo IP que é feito a identificação com exatidão de onde o criminoso praticou o crime, o problema é que o protocolo identifica apenas o computador e não o usuário, o que prejudica a identificação de uma pessoa em específico.

A identificação do autor do crime se torna mais difícil quando o criminoso utiliza uma rede sem fio livre, como as encontradas em faculdades por exemplo. Essas redes são utilizadas por várias pessoas e identificar um usuário em específico é praticamente impossível. As *Lan Houses* também são utilizadas por criminosos que se aproveitam do fato de que grande parte delas não cobram a apresentação de um documento para liberar o acesso à internet.

Outro fator que prejudica a identificação do autor do crime é que é necessária uma autorização judicial para a identificação do IP.

6.3. Falta de conhecimento técnico dos magistrados

Para a maioria dos autores um dos grandes problemas em se julgar um crime de informática é a falta de conhecimento técnico de juízes e advogados.

Alguns julgamentos como o da apresentadora de TV Daniela Cicarelli e seu namorado, Tato Malzoni, que tiveram um vídeo com cenas íntimas divulgado num site de compartilhamento de vídeos, Segundo Porfírio (2006). Na ocasião, o desembargador de São Paulo Ênio Santarelli Zuliani determinou o bloqueio da transmissão de dados entre a web brasileira e o site de compartilhamento de vídeo.

Segundo a Associação dos Magistrados Brasileiros (2007), a decisão equivocada do desembargador afetou milhões de usuários da internet que ficaram sem acesso ao site durante três dias. Provavelmente por falta de conhecimento da área, o desembargador tomou uma decisão que prejudicou várias pessoas, sendo que apenas uma intimação para que o site retirasse o vídeo do ar, seria suficiente.

6.4. Facilidade em cometer tais crimes

Com crescimento das redes sociais as pessoas passaram a expor cada vez mais a sua vida na internet, inclusive as crianças e os adolescentes, o que aumentou o interesse de pedófilos, que criam perfis falsos para atrair as vítimas e assim pôr em pratica os seus crimes.

Assim como a pedofilia, o crescimento da internet e das redes sociais possibilitou o surgimento de vários crimes cibernéticos próprios e a intensificação de outros crimes já existentes, como a pirataria virtual de músicas, vídeos e livros, que podem ser encontrados facilmente com uma simples pesquisa.

Atualmente não é necessário que uma pessoa detenha grandes conhecimentos em informática para praticar um crime, pois há vários fóruns na internet que ensinam quem quiser a ser um *craker*, são vários tópicos que contém passo a passo o que deve ser feito para capturar senhas de mensageiros instantâneos.

Além dos fóruns, há vários sites que disponibilizam vírus que podem ser facilmente programados e espalhados pela internet. Esses criminosos aproveitam da inocência de grande parte dos usuários da internet, para disseminar vírus e assim obterem informações pessoais.

7. OUTROS MECANISMOS PARA PUNIÇÃO DE CRIMES CIBERNÉTICOS

Mesmo com as lacunas encontradas nas leis existentes, os magistrados contam com algumas opções para condenar um réu. Essas alternativas estão elencadas no artigo 4º do Decreto-Lei nº. 4.657, de 4 de setembro de 1942: "Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia".

A fundamentação é essencial na sentença, pois é nela que o juiz menciona seus motivos, e essas alternativas permitem aos juízes fundamentarem as suas decisões mesmo quando a lei for omissa ou lacunosa. O juiz pode ser afastado da carreira de magistrado se não utilizar os costumes, analogia, caso a lei seja omissa.

7.1. Analogia

A analogia consiste em aplicar uma lei que regule um caso semelhante a casos não previstos por lei. Portanto quando um magistrado recorre

à analogia ele está estendendo a um caso semelhante à resposta dada a um caso particular.

> Segundo Reale (2012) analogia é um processo pelo qual:
> Estendemos a um caso não previsto aquilo que o legislador previu para outro semelhante, em igualdade de razões. Se o sistema do Direito é um todo que obedece a certas finalidades fundamentais, é de se pressupor que, havendo identidade de razão jurídica, haja identidade de disposição nos casos análogos, segundo um antigo e sempre novo ensinamento: *ubi eadem, ibi eadem juris* dispositivo (onde há a mesma razão deve haver a mesma disposição de direito). (REALE, 2012)

Mesmo a analogia sendo permita no Direito Civil, o seu uso deve ser feito com muita cautela, pois existem casos que aparentam ser completamente iguais, mas pode existir um detalhe em um deles que altere totalmente a sua essência jurídica, tornando-o diferente e assim inadequado compará-lo ao outro.

Há alguns requisitos necessários para o uso da analogia, que são os seguintes: a ausência de norma que regule um caso concreto, a similaridade entre o caso não regulado por lei e aquele amparado expressamente por uma norma e a existência de uma razão jurídica que permita a extensão normativa expressa ao caso não contemplado na lei, no caso do Direito Civil o Decreto-Lei nº. 4.657/42 no seu artigo 4º permite o uso de analogia nos casos em que a lei for omissa.

7.2. Costumes

A palavra costume deriva do latim *consuetudo*, e significa tudo que se estabelece por força do uso e do hábito. O costume ocupa um plano secundário em relação à lei e só pode ser usado depois que o juiz esgotar todas as possibilidades de uso da analogia para suprir as lacunas da lei. Há três tipos de costumes, quando comparados à lei, *secudum legem*, *praeter legeme contra legem*.

O costume amparado por lei é o *secudum legem*, que pode ser observado no art. 1.297, § 1º, do Código Civil e no artigo100, inciso III, do Código Tributário Nacional. *Praeter legem* é o costume não amparado por lei, mas que completa o sistema legislativo e por fim *contra legem* que é o costume contrário a lei, onde as normas costumeiras contrariam a lei e implicitamente revogam-nas, por resultar na não aplicação da lei em virtude de desuso.

8. TIPIFICAÇÃO DE CRIMES CIBERNÉTICOS COMUNS

Apesar da demora, o ordenamento jurídico brasileiro teve alguns avanços em relação a tipificação de alguns crimes virtuais impróprios. Leis mais antigas como o Código Penal (CP) e o Estatuto da Criança e do Adolescente (ECA), já previam ou foram modificados para abarcar determinados crimes virtuais como a pornografia infantojuvenil, pedofilia, estelionato e furto eletrônico, falsificação e supressão de dados etc.

Mesmo com várias leis tratando do assunto, a legislação brasileira ainda é muito incipiente na tipificação de crimes cibernéticos, pois ela não consegue acompanhar na mesma velocidade a evolução e o surgimento de novos delitos digitais, mesmo as leis existentes possuem algumas lacunas e por isso sofrem duras críticas de peritos em informática e advogados especialistas em direito digital.

A tabela 1 traz uma lista de crimes cibernéticos, com as suas respectivas tipificações:

Tabela 1: Tipificação de crimes cibernéticos comuns

Crime	Tipificação
Estelionato e furto eletrônicos (fraudes bancárias)	Artigos 155, 3° e 4°, II e 171 do Código Penal
Invasão de dispositivo informático e furto de dados	Artigo 154-A do Código Penal
Falsificação e supressão de dados	Artigos 155, 297, 298, 299, 313-A e 313-B do Código Penal
Armazenamento; produção; troca; publicação de vídeos e imagens contendo pornografia infantojuvenil	Artigos 241 e 241-A do Estatuto da Criança e do Adolescente (ECA)
Assédio e aliciamento de crianças	Artigo 241-D do ECA
Ameaça	Artigo 147 do Código Penal
Cyberbullying	Artigos 138, 139 e 140 do Código Penal
Interrupção de serviço	Artigo 266, parágrafo 1° do Código Penal
Incitação e Apologia de crime	Artigos 286 e 287 do Código Penal
Prática ou incitação de discriminação ou preconceito de raça, cor, etnia, religião	Artigo 20 da Lei n° 7.716/1989
Crimes contra a propriedade intelectual artística e de programa de computador	Artigo 184 do Código Penal
Venda ilegal de medicamentos	Artigo 273 do Código Penal

Fonte: Próprio autor.

9. TIPIFICAÇÃO DE CRIMES CIBERNÉTICOS PRÓPRIOS

Temos na legislação brasileira duas leis que tratam especificamente dos crimes cibernéticos próprios (aqueles que em que o sistema

informático do sujeito passivo é o objeto e o meio do crime). São elas: A Lei 12.737, de 30 de novembro de 2012 e a Lei Nº 12.965, de 23 de Abril de 2014.

9.1. Lei 12.737, de 30 de novembro de 2012 – Lei Carolina Dieckmann

A lei 12.373/12 veio tipificar o crime de invasão de dispositivo informático, para isso ela acrescentou ao código penal os artigos 154-A e 154B. O primeiro parágrafo trouxe a descrição dos crimes de invasão de dispositivo informático e os casos de agravamento da pena quando esses crimes são cometidos contra pessoas específicas, já o segundo parágrafo trata da ação penal.

> Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.
> Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
> "Invasão de dispositivo informático
> 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.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 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 a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;

> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."
> "Ação penal
> Art. 154-B.Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos." (BRASIL, 2012)

A lei também altera a redação dos artigos 266 - dobrando a pena quando o crime é praticado em ocasião de calamidade pública -, e 298 - equiparando cartão de débito ou crédito aos documentos particulares.

> Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:
> "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública
> Art. 266.
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública."
> Art. 298
> Falsificação de cartão
> Parágrafo único. Para fins do disposto no caput , equipara-se a documento particular o cartão de crédito ou débito." (BRASIL, 2012)

A Lei traz penas inexpressivas, em completa discrepância em relação aos danos que podem ser causados através de invasão de dispositivos informáticos. Em 2017, por exemplo, o *ransomware Wannacry* afetou mais de duzentos mil sistemas, em 150 países. A montadora Renault fechou sua maior fábrica na França e os hospitais do Reino Unido tiveram de rejeitar pacientes. Já no Brasil, o ataque causou a interrupção do atendimento do Instituo Nacional de Seguro Social, além de afetar empresas e órgãos públicos de quatorze Estados mais o Distrito Federal.

Para advogados especialistas em direito eletrônico, se o autor do crime não tiver precedentes, no máximo, deverá cumprir alguma pena alternativa como a doação de cestas básicas. Se a pena máxima

desses crimes fosse maior, haveria maior flexibilidade para, eventualmente, conforme a gravidade do crime, um juiz mandar esses criminosos para a cadeia.

O artigo 154-A define invasão de dispositivo informático como "invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança [...]", ou seja, caso o equipamento não tenha nenhum tipo de mecanismo de segurança, então uma invasão a este equipamento não pode ser enquadrada na lei 12.737.

Além disso, a lei também sofreu várias críticas de advogados criminalistas, principalmente em relação a ausência de definição de termos técnicos e pela aparente falta de suporte técnico-jurídico aos legisladores dos dispositivos. Um exemplo, é a utilização do termo "dispositivo informático", este termo deixa de fora dispositivos que não são considerados aparelhos informáticos, como as *Smart* TVs e os *smartphones*. O mais adequado seria utilizar o termo "dispositivo eletrônico" justamente para abranger a maior quantidade possível de equipamentos.

9.2. Lei Nº 12.965, de 23 de Abril de 2014 - Marco Civil da Internet

O Marco Civil da Internet (MCI), oriundo do Projeto de Lei nº 2.126, de 2011, uma elaboração interministerial que envolveu representantes do Ministério da Justiça, Ministério do Planejamento, Ministério da Ciência e Tecnologia e Ministério das Comunicações, representa a atuação conjunta de setores do Executivo, do Legislativo e da sociedade civil.

A Lei 12.965/14 é dividida em cinco capítulos e estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

O capítulo primeiro, das disposições preliminares, aponta os objetivos (Art. 4), fundamentos (Art. 2) e princípios (Art. 3) da Lei. Além disso, traz diversas definições para termos técnicos (definições ausentes na Lei 12.373/12):

> I - *internet*: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a

> finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;
> II - terminal: o computador ou qualquer dispositivo que se conecte à internet;
> III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;
> IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;
> V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;
> VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
> VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
> VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP. (BRASIL, 2014)

O segundo capítulo, dos direitos e garantias dos usuários, define o acesso à internet como essencial ao exercício da cidadania e assegura ao usuário o direito a inviolabilidade da intimidade e da vida privada, a manutenção da qualidade contratada da conexão à internet e a garantia do direito à liberdade de expressão.

Aspecto relevante, a neutralidade da rede, foi tratada no terceiro capítulo, art. 9, que define que "o responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação".

A ideia é que se possa acessar indistintamente uma página de internet, enviar um e-mail ou assistir a um filme ou conversar por videoconferência, sem prejuízo da velocidade de transmissão dos dados. Ademais, a discriminação dos dados deve abster-se de causar

danos às pessoas, assim como deve ser feita com proporcionalidade, transparência e isonomia, informando-se previamente, com transparência e clareza os critérios de gerenciamento e mitigação de tráfego adotadas, inclusive quando relacionadas à segurança da rede. Também a discriminação de dados não pode implicar oferecimento de serviços em condições comerciais discriminatórias nem resultar em práticas anticoncorrenciais.

O terceiro capítulo também define requisitos de proteção aos registros e aos dados pessoais, que devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes envolvidas. Define ainda a guarda de registros de conexão pelo prazo de um ano e que estes devem ser disponibilizados somente mediante autorização judicial.

A atuação do poder público é tratada no capítulo cinco, ele define as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios e estabelece que estes entes devem criar mecanismos transparentes, colaborativos e democráticos, envolvendo o governo, o setor empresarial e a sociedade civil, visando o desenvolvimento da internet no Brasil.

O último capítulo, das disposições finais, aborda o respeito aos direitos autorais, a defesa dos direitos relacionados ao uso da internet e o cuidado com o acesso aos conteúdos postados, principalmente em relação aos menores de idade, respeitando os princípios do Estatuto da Criança e do Adolescente.

Os provedores de internet receberam tratamento especial no Marco Civil da Internet. Eles são responsáveis pela guarda e disponibilização dos registros de conexão, sendo que o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial. O MCI também prevê a responsabilidade civil dos provedores.

Conforme Filho (2016):

> O legislador tratou da responsabilidade civil dos provedores de internet por ofensa aos direitos da personalidade das pessoas, como honra, imagem, vida privada e intimidade das pessoas. O art.18 reconheceu a irresponsabilidade civil do provedor de acesso por danos causados pelos usuários. Por outro lado, o art.19 regulamentou especificamente a responsabilidade civil dos provedores de conteúdo, por exemplo os armazenadores de arquivos fotográficos e musicais, bem como de páginas da internet, entre eles, os blogs. Estabeleceu-se,

> nesse caso, a responsabilidade subsidiária entre o usuário da internet que praticou o ato ilícito civil e o provedor de conteúdo. Dessa maneira, a responsabilidade primária é do usuário da internet e o provedor de conteúdo somente responde conjuntamente com o causador do dano quando descumprir ordem judicial para que tornasse indisponível o conteúdo ofensivo.
>
> Ainda segundo Filho (2016):
>
> Em se tratando de imagens, vídeos ou outros materiais que contenham cenas de nudez ou de atos sexuais de caráter privado, o provedor de aplicações de internet responderá subsidiariamente com o divulgador, quando, após notificação, deixar de tornar indisponível o acesso a esse conteúdo. Aqui a diferença é que não se requer ordem judicial para a solicitação da indisponibilidade do conteúdo, podendo ser feita pelo próprio interessado mediante notificação.

A criação do MCI possibilitou o surgimento de novas delegacias especializadas em crimes cibernéticos, sendo que atualmente 15 estados possuem uma dessas delegacias.

A tabela 2 traz uma lista desses estados e de suas respectivas delegacias especializadas:

Tabela 2 – Relação de Delegacias Especializadas em Crimes Cibernéticos.

Estado	Cidade	Delegacia Especializada
Bahia	Salvador	Grupo Especializado de Repressão aos Crimes Eletrônicos
Distrito Federal	Brasília	Delegacia de Repressão aos Crimes Cibernéticos
Espírito Santo	Vitória	Delegacia de Repressão aos Crimes Eletrônicos
Maranhão	São Luiz	Departamento de Combate aos Crimes Tecnológicos
Minas Gerais	Belo Horizonte	Delegacia Especializada de Investigação de Crimes Cibernéticos
Mato Grosso	Cuiabá	Gerência Especializada de Crime de Alta Tecnologia
Pará	Belém	Delegacia de Repressão aos Crimes Tecnológicos
Pernambuco	Recife	Delegacia de Polícia de Repressão aos Crimes Cibernéticos
Piauí	Teresina	Delegacia Especializada de Repressão aos Crimes de Alta Tecnologia
Paraná	Curitiba	Núcleo de Combate aos Cibercrimes
Rio de Janeiro	Rio de Janeiro	Delegacia de Repressão aos Crimes de Informática
Rio Grande do Sul	Porto Alegre	Delegacia de Repressão aos Crimes Informáticos
Sergipe	Aracajú	Delegacia de Repressão a Crimes Cibernéticos
São Paulo	São Paulo	Delegacia de Delitos Cometidos por Meios Eletrônicos
Tocantins	Palmas	Divisão de Repressão a Crimes Cibernéticos.

Fonte: Próprio Autor.

10. LEGISLAÇÃO INTERNACIONAL - CONVENÇÃO DE BUDAPESTE

Enquanto o Brasil apenas engatinha com a tipificação de crimes cibernéticos, alguns países já estão bem avançados nesse quesito, principalmente os que aderiram a Convenção sobre o Cibercrime, ou Convenção de Budapeste. Em 2008, o Brasil até que tentou participar da Convenção através do senador Eduardo Azeredo (PSDB-MG), mas o país só poderia se tornar signatário do tratado se fosse convidado pelo Comitê de Ministros do Conselho Europeu, o que não aconteceu. Segundo a Câmara dos Deputados (2021), em 2019, o Brasil foi convidado a aderi à Convenção de Budapeste. O PDL 255/2021, Projeto de Decreto Legislativo de Acordos, tratados ou atos internacionais, está aguardando deliberação no plenário (PLEN) em Regime de Tramitação de Urgência.

A Convenção sobre Cibercrime do Conselho da Europa é o primeiro trabalho internacional de fundo sobre crime no ciberespaço. Foi elaborado por um comitê de peritos nacionais, congregados no Conselho da Europa e consiste num documento de direito internacional público. Embora tenham na sua origem, sobretudo, países membros do Conselho da Europa, tem vocação universal. Na sua elaboração participaram vários outros países (Estados Unidos da América, Canadá, Japão e África do Sul) e pretende-se que venha a ser aceite pela generalidade dos países do globo.

A Convenção sobre Cibercrime (2001) prioriza "uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional" e reconhece "a necessidade de uma cooperação entre os Estados e a indústria privada".

O tratado traz quatro capítulos (Terminologia, Medidas a Tomar a Nível Nacional, Cooperação Internacional e Disposições Finais) e define os cibercrimes, tipificando os como: infrações contra sistemas e dados informáticos; infrações relacionadas com computadores; infrações relacionadas com o conteúdo, pornografia infantil e infrações relacionadas com a violação de direitos autorais.

O capítulo 1 da convenção traz as terminologias necessárias para a compreensão do tratado, as definições são as seguintes:

a)Sistemas informáticos "significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou

mais entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados";

b) Dados informáticos são "qualquer representação de fato, de informações ou de conceitos sob uma forma suscetível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função";

c) Fornecedor de serviço é:

- "Qualquer entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático e"
- * "Qualquer outra entidade que processe ou armazene dados informáticos em nome do referido serviço de comunicação ou dos utilizadores desse serviço".

Já o capítulo 2 tece sobre as medidas que cada país membro deverá adotar em relação aos seguintes assuntos:

- Acesso ilegítimo – "cada país adotará as medidas legislativas e outras que se sejam necessárias para estabelecer como infração penal, no seu direito interno, o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático".
- Interceptação ilegítima – "cada parte adotará as medidas legislativas e outras que se revelarem necessárias para estabelecer como infração penal, no seu direito interno a interceptação intencional e ilegítima de dados informáticos, efetuadas por meios técnicos, em transmissões não públicas, para dentro de um sistema informático, incluindo emissões eletromagnéticas provenientes de um sistema informático que veicule esses dados".
- Interferência em dados – "cada país adotará as medidas legislativas e outras que se revelarem necessárias para estabelecer como infração penal, no seu direito interno, o ato de intencionalmente e ilegitimamente danificar, apagar, deteriora, alterar ou eliminar dados".
- Interferência em sistemas – "cada parte adotará as medidas legislativas e outras que se revelarem necessárias para estabelecer como infração penal, no seu direito interno, a obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, através de introdução, transmissão,

danificação, eliminação, deterioração ou supressão de dados informáticos".

- * Uso abusivo de dispositivos – "cada país adotará as medidas legislativas e outras que se revelarem necessárias para estabelecer como infração penal a produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de disponibilização de:

i) Dispositivos, inclusive programas informáticos, concebido ou adaptado para permitir a prática de um crime.
ii) Um código de acesso que permitam acessar em todo, ou em parte um sistema informático.

- Falsidade informática – "cada país adotará as medidas legislativas necessária para estabelecer como infração e introdução, a alteração, a eliminação ou a supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que estes sejam ou não diretamente legíveis".
- Burla informática – "cada parte adotará as medidas legislativas que se revelem necessárias para estabelecer com infração penal, o ato intencional e ilegítimo, que origine a perda de bens a terceiros através da introdução, da alteração, da eliminação ou da supressão de dados informáticos".
- Pedofilia – "Cada país tomará medidas legislativas para estabelecer como crime as seguintes condutas, quando cometidas de forma intencional e ilegítima:

a) Produzir pornografia infantil com o objetivo da sua difusão através de um sistema informático;
b) Oferecer ou disponibilizar pornografia infantil através de um sistema informático;
c) Oferecer ou transmitir pornografia infantil através de um sistema informático;
d) Obter pornografia infantil através de um sistema informático para si próprio ou para terceiros;
e) Possuir pornografia infantil num sistema informático ou num meio de armazenamento de dados informáticos;

- Violação dos direitos do autor - Cada parte adotará as medidas necessárias para estabelecer como crime a violação do direito do

> autor, relacionada com a interpretação, execução, com exceção de qualquer direito moral conferido por essa convenção, quando esses atos forem praticados intencionalmente, a uma escala comercial e por meio de um sistema informático.

O tratado traz ainda em seu texto regras de cooperação internacional onde é fixado o limite mínimo de um ano de prisão, para que seja admissível a extradição, sendo necessária a dupla incriminação. Porém, o texto prevê a possibilidade de haver extradição para crimes de pena inferior em caso de existir um tratado bilateral entre os dois estados envolvidos e nesse tratado se prever um limite inferior. Segundo o artigo 24º da convenção um país signatário pode recusar a extradição caso o crime cometido seja considerado de ordem política ou relacionado com a mesma, ou ainda que esteja em causa a soberania, a segurança, a ordem pública ou outros interesses essenciais do Estado.

Em relação à cooperação mútua a Convenção de Budapeste em seu artigo 26º prevê a possibilidade de um país encaminhar informações a outro Estado caso essas informações sejam úteis ou necessárias ao início ou ao desenvolvimento de uma investigação de um crime enquadrado na Convenção. A remessa de informação para outro país signatário deve observar a confidencialidade dos dados.

O ingresso do Brasil no tratado será de suma importância para o combate aos crimes cibernéticos, pois se o país se tornará membro da convenção, ele adentrará num regime internacional de combate ao cibercrime, facilitando, assim, uma cooperação maior com outros países que sofrem das mesmas práticas ilícitas, mas que possuem leis diferentes.

11. CONSIDERAÇÕES FINAIS

Esta pesquisa se propôs, como objetivo geral, apresentar ao leitor um estudo sobre os crimes cibernéticos e as dificuldades encontradas para punir quem comete tais crimes. Essas dificuldades advêm principalmente das características das infrações digitais – que diferem e muito dos crimes comuns –, e das lacunas encontradas na legislação brasileira.

Esse trabalho foi baseado na análise de alguns trabalhos relacionados, bem como nas características dos principais crimes cibernéticos, trazendo para o leitor os principais motivos para impunidade de algumas infrações digitais, assim como os mecanismos que podem ser utilizados pelos juristas brasileiros, nos casos em que a lei seja omissa na tipificação de alguma conduta criminosa.

Foi feito também, um levantamento dos crimes já previstos nas leis atuais, como o Código Penal e o Estatuto da Criança e do Adolescente, e também uma análise detalhada das duas principais leis que tratam de crimes cibernéticos – Lei 12.737, de 30 de novembro de 2012 e a Lei Nº 12.965, de 23 de Abril de 2014. A legislação internacional também foi abordada na pesquisa, através da análise da Convenção sobre Cibercrime do Conselho da Europa.

O crime cibernético pertence a um ramo extremamente novo do direito brasileiro, e os nossos legisladores ainda são muito inexperientes em relação a complexidade e a dinâmica desses crimes, fato que pode ser observado nas defasadas leis brasileiras, como o Código Penal, e nas lacunas existentes nas leis que tratam especificamente de crimes cibernéticos.

Apesar de o ordenamento jurídico brasileiro ainda estar se adaptando a essa nova modalidade de crime, citando, por exemplo, a criação da Lei Carolina Dieckmann e do Marco Civil da Internet, pode-se afirmar que o Brasil ainda está em processo de crescimento em relação a tipificação de crimes cibernéticos, pois mesmo essas leis, necessitam de adequações quanto a termos técnicos e penas mais pertinentes ao dano gerado à vítima.

Portanto, faz-se necessário a adequação da legislação existente e a criação de novas leis que versem sobre crimes cibernéticos, uma vez que esses crimes trazem prejuízos que vão além do campo virtual e que muitas vezes, atingem a vida íntima da vítima e causam até problemas psicológicos. A punição proporcional ao dano, é uma forma de coibir a prática destes delitos, dado que, ao saber que poderá responder criminalmente, o *cracker*, ou até mesmo uma pessoa comum, se policiará em seus atos. Nesse sentido, recentemente, um importante passo foi dado com a aprovação da Lei nº 14.155, de 27 de maio de 2021, que 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.

Por fim, cabe ressaltar que o presente artigo não tem a finalidade de exaurir a matéria de tipificação de crimes cibernéticos. O objetivo foi possibilitar um maior entendimento sobre o assunto e demonstrar a importância de leis mais eficazes no combate a infrações digitais.

REFERÊNCIAS

ABDURRAHMANI, Bledar, Cybercrime in Albania: A Discourse on Law, Policy and Practice. **EUROPEAN ACADEMIC RESEARCH**. Vol. II, Issue 1/ April2014.

AMB – Associação dos Magistrados Brasileiros. **Desembargador do TJ-SP manda desbloquear YouTube.** 2007. Disponível em: <https://www.amb.com.br/desembargador-do-tj-sp-manda-desbloquear-youtube/>. Acesso em: 04 out. 2021.

BARI, Shumaila, ABBAS, Furrakh. Online Harassment - A Study of its Sources, Intensity and Psychological Impact on Students. **EUROPEAN ACADEMIC RESEARCH**. Vol. IV, Issue 5/ August 2016.

BRASIL. Código Penal. **Decreto-Lei nº 2.848**, de 7 de dezembro de 1940. Disponível em:<http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm> Acesso em: 25 mar. 2019.

BRASIL. **Constituição Federal de 1988**. Promulgada em 5 de outubro de 1988. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm> Acesso em: 25 mar. 2019.

BRASIL. Lei de Introdução às normas do Direito Brasileiro. **Decreto-Lei n 4.657**, de 4 de setembro de 1942. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657.htm>. Acesso em: 27 de mar. de 2019.

BRASIL. **Lei Ordinária nº 7.716**, de 5 de janeiro de 1989. Define os crimes resultantes de preconceito de raça ou de cor. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l7716.htm>. Acesso em: 02 de abr. de 2019.

BRASIL. **Lei Ordinária nº 8.069**, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 27 de mar. de 2019.

BRASIL. **Lei Ordinária 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: 16 abr. 2019.

BRASIL. **Lei Ordinária nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 27 abr. 2019.

CAIADO, Felipe B, CAIADO, Marcelo. **Combate à Pornografia Infanto juvenil com aperfeiçoamento na identificação de suspeito e na detecção de arquivos de interesse**. 2018. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos>. Acesso em: 04 out. 2021.

CÂMARA DOS DEPUTADOS. **Deputados e especialistas defendem adesão do Brasil a convenção sobre crimes cibernéticos.** 2021. Disponível em: <https://www.camara.leg.br/noticias/772464-deputados-e-especialistas-defendem-adesao-do-brasil-a-convencao-sobre-crimes-ciberneticos/>. Acesso em: 04 out. 2021.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**. Rio de Janeiro: Lumen Juris, 2012.

CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança No Brasil. **Ransomware**. Disponível em: <https://cartilha.cert.br/ransomware/>. Acesso em: 14 de maio 2021.

CONVENÇÃO SOBRE O CIBERCRIME. 2001. Budapeste. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf>. Acesso em: 06 de jun. 2021.

CRESPO, Marcelo. **Crimes Digitais: do que estamos falando?**. 2016. Disponível em: <http://canalcienciascriminais.com.br/artigo/crimes-digitais-do-que-estamos-falando/>. Acesso em: 06 jun. 2021.

FERREIRA, Ivette Senise. A Criminalidade Informática. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet:** Aspectos Jurídicos Relevantes. 2. ed. São Paulo: Quartier Latin, 2005. p. 239.

FERREIRA, Giovana. **O dilema entre a garantia da liberdade de expressão e o direito à privacidade no marco civil da internet**. 2014. Disponível em: <https://jus.com.br/artigos/37886/o-dilema-entre-a-garantia-da-liberdade-de-expressao-e-o-direito-a-privacidade-no-marco-civil-da-internet>. Acesso em 06 mai. 2021.

FILHO, Eduardo Tomasevicius. **Marco Civil da Internet: uma lei sem conteúdo normativo**. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142016000100269. Acesso em 27 abr. 2019.

McCARTHY, Niall. New Report: Cyberbullying Is Most Prevalent In India [Infographic]. **Forbes.** 2018. Disponível em: <https://www.forbes.com/sites/niallmccarthy/2018/10/29/new-report-cyberbullying-is-most-prevalent-in-india-infographic/?sh=1d2adbe87537>. Acesso em: 10 de jun. 2019.

PANAZZOLO, Pedro de Vilhena. **Racismo Cibernético e os Direitos da Terceira Dimensão**. 2018. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos>. Acesso em: 04 de out. 2021.

PORTÍRIO, Fernando. **O namoro do ano:** Justiça confirma veto ao vídeo de Cicarelli na internet. 2006. Disponível em: <https://www.conjur.com.br/2006-set-28/justica_confirma_veto_video_cicarelli_internet>. Acesso em: 04 out. 2021.

PRIETO, André Luiz; GAHYVA, Hercules da Silva. **Crimes cibernéticos e a legislação brasileira**. 2012 Disponível em: <https://lfg.jusbrasil.com.br/noticias/2224740/crimes-cib>. Acesso em: 22 de mai. 2021.

REALE, Miguel. **Lições preliminares de direito**. São Paulo: Saraiva, 27a ed., 2012.

ROQUE, Sérgio Marques. **Criminalidade Informática – Crimes e Criminosos do Computador**. 1 ed. São Paulo: ADPESP Cultural, 2007.

SANCHES, Ademir Gasques, ANGELO, Ana Elisa. Insuficiência das leis em relação aos crimes cibernéticos no Brasil. 2018. **Revista Jus Navigandi.** Disponível em: <https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil>. Acesso em: 04 out. 2021.

SILVA, Jacimar Oliveira da. **Tipificação de crimes efetuados pela internet**. 2012. Disponível em: <www.pc.ms.gov.br/>. Acesso em: Acesso em: 22 de mai.2019

SIQUEIRA, M. S. OLIVEIRA, N. OLIVEIRA, B. M. MATTOS, K. R. **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: 17 abr. 2021. . Acesso em: 04 abr. 2021.