Pontifícia Universidade Católica de São Paulo

PUC-SP

VITOR TAVEIRA MACHADO

A EVOLUÇÃO LEGISLATIVA DOS CRIMES CIBERNÉTICOS NO ORDENAMENTO JURÍDICO BRASILEIRO

São Paulo

2023

Vitor Taveira Machado

A EVOLUÇÃO LEGISLATIVA DOS CRIMES CIBERNÉTICOS NO ORDENAMENTO JURÍDICO BRASILEIRO

Trabalho apresentado a Pontifícia Universidade Católica de São Paulo, PUC-SP, como requisito para obtenção do título de bacharel em Direito.

Orientador: Prof. Dr. Motauri Ciocchetti de Souza

Pontifícia Universidade Católica de São Paulo

PUC-SP

SÃO PAULO

2023

DEDICATÓRIA

Dedico essa pesquisa aos meus pais que foram os principais incentivadores para eu finalizar e concluir minha graduação em Direito.

Dedico também a todos os meus amigos de escola, faculdade e trabalho por sempre me ajudarem e proporcionarem dias mais felizes em minha vida.

AGRADECIMENTOS

Gostaria de agradecer primeiramente a Deus por me proporcionar forças, sabedoria e dedicação para finalizar minha primeira graduação.

Agradecer as pessoas mais importantes da minha vida: meus pais Marcelo e Marcia, minha irmã Laís e a minha namorada Rafaela. Sem eles eu não seria nada e não teria todo o incentivo e ajuda que recebi e recebo todos os dias para realizar meus sonhos.

Não posso deixar de citar meu melhor amigo Enrico, que também sempre me ajudou, me motivando, me ouvindo e me aconselhando nos momentos de alegrias e crises durante o período de graduação.

Agradeço também aos meus professores da Pontifícia Universidade Católica de São Paulo por me ensinarem tanto e me ajudarem em tudo o que foi preciso. Quero agradecer o professor Dr. Motauri Ciocchetti de Souza por aceitar, acompanhar e auxiliar no desenvolvimento do presente trabalho.

Por fim, gostaria de agradecer aos meus amigos da faculdade que foram especiais em todas as histórias, estágios, provas e trabalhos que vivi durante o curso de Direito.

Vitor Taveira Machado

“No que diz respeito ao empenho, ao compromisso, ao esforço, à dedicação, não existe meio termo. Ou você faz uma coisa bem feita ou não faz”. - Ayrton Senna

RESUMO

A internet cumpre papel essencial na sociedade atual, com presença e relevância nas diversas áreas da vida. Assim, com o aumento massivo do número de usuários conectados à rede, a prática de condutas ilícitas também está em constante crescimento. O estudo do presente trabalho tem por objeto a abordagem dos crimes cibernéticos com análise das principais práticas delitivas. Posteriormente, cabe a análise da forma encontrada pelo legislador brasileiro para coibir as práticas de crimes cibernéticos, bem como os direitos e formas de proteção dos usuários. Por fim, em decorrência de novas práticas delitivas é necessária a adequação da legislação, sendo analisados os principais projetos de lei referentes aos crimes cibernéticos.

Palavras-chave: Internet. Crime Cibernético. Evolução Legislativa

ABSTRACT

The internet has an essential role in today's society, with presence and relevance in different areas of life. With the massive increase in the number of users connected to the network, the practice of illicit conduct is also constantly growing. The study of this work aims to approach cybercrimes with an analysis of the main criminal practices. Subsequently, it is necessary to analyze the way found by the brazilian legislator to curb cybercrime practices, as well as the rights and method of protection of users. Finally, as a result of new criminal practices, it is necessary to adapt legislation, analyzing the draft law relating to cybercrimes.

Keywords: Internet. Cyber crime. Legislative Developments

SUMÁRIO

INTRODUÇÃO

A sociedade passou por grandes transformações devido ao desenvolvimento de tecnologias. A internet é uma das principais tecnologias criadas nos últimos séculos, sendo um meio para a transmissão de informações, dados, imagens, entre outros arquivos. Os tipos de atividades possíveis de serem realizados na internet são os mais diversos, desde os mais básicos como o e-mail para a troca de correspondências online entre usuários de qualquer parte do mundo, o acesso à informação por meio de arquivos informativos, técnicos, programas ou softwares fornecidos por provedores da rede, até as atividades mais complexas como o uso para comunicações militares.

Outra forma de utilização que vem ganhando maior espaço na atualidade é o uso para jogos e lazer, neste prisma os jogos recreativos vêm expandindo o seu público todos os anos e outras atividades como a prática de jogos de azar também vem ganhando espaço, por meio de casas de apostas, tal atividade que se encontra em constante crescimento, movimentando bilhões de dólares anualmente.

Com a expansão da rede, na sociedade outro meio que foi revolucionado é o do comércio, por meio da internet é possível a venda de produtos para pessoas de qualquer nacionalidade. As grandes empresas, tanto nacionais quanto as multinacionais, possuem um domínio na internet para que os usuários tenham acesso a seus produtos e serviços.

A conexão com a internet apresenta benefícios em virtude da gama de serviços prestados e passou a ser a base tecnológica para a forma de organização da Era da Informação.

Sendo assim, o presente trabalho tem por objetivo a análise do contexto histórico da internet com a sua evolução, junto a análise dos crimes cibernéticos, inclusive quanto à classificação, os sujeitos e o local do crime, bem como será explorada a legislação brasileira e os projetos de lei no âmbito dos crimes cibernéticos.

No primeiro capítulo, será abordado o antecedente histórico da internet, destacando o momento histórico da criação, os objetivos iniciais para a utilização da

rede, a forma com que foi projetada e a respectiva evolução para o estado atual da rede.

No segundo capítulo será apresentada a consequência negativa da evolução tecnológica que é a disseminação dos crimes cibernéticos. Para a compreensão dos crimes cibernéticos será apresentada a definição do termo, a classificação doutrinária internacional e nacional que subdivide em crimes cibernéticos próprios e impróprios, os sujeitos ativos e passivos dos delitos informáticos e o aspecto de grande relevância para a persecução penal que é o local do crime.

Ainda, no terceiro capítulo será analisada a investigação dos crimes cibernéticos, com os meios utilizados para efetivar a responsabilização do criminoso cibernético, bem como será analisada a dificuldade de investigação dos crimes cibernéticos.

Outrossim, no Brasil foram editadas diversas leis e regulamentações que buscam coibir os crimes cibernéticos, promovendo a segurança digital dos usuários. Dessa forma, no quarto capítulo será apresentada a evolução legislativa brasileira, com a discussão acerca das seguintes leis: Lei nº 12.015 de 2009; Lei nº 12.737/2012; Lei nº 12.965/2014 de 23 de abril de 2014; Lei nº 13.709 de 2018.

Por fim, no quinto capítulo serão analisados os projetos de lei no âmbito dos crimes cibernéticos, uma vez que na sociedade interconectada, surgem diariamente novas problemáticas e práticas delitivas, sendo de extrema importância o papel do legislador. Assim, caberá o estudo de projetos de lei, o primeiro que será objeto de estudo visa a responsabilização dos provedores de aplicações de internet, outro projeto de lei objetiva o combate as fake News e o último projeto que será objeto de análise de grande relevância será o projeto de lei nº 2.699/2021 que objetiva o combate ao cyberbullying.

1 HISTÓRICO

A internet é uma grande rede utilizada para interligar dispositivos informáticos independente da região, ou país em que está instalada, permitindo a comunicação e troca de dados entre estes dispositivos, sendo um marco histórico na forma como a humanidade se comunica, interage e compartilha informações. A partir da criação da internet, que teve origens modestas, até a transformação em um alicerce indispensável da sociedade, a internet passou por um crescimento exponencial que trouxe consigo uma série de desafios e oportunidades.

Assim, quanto a origem da internet, em seu momento de criação tinha objetivos e formatos diversos do atual. O surgimento da internet é decorrente do trabalho de peritos militares, no período da guerra fria. Dessa forma, durante a guerra fria, em resposta ao lançamento do Sputnik, satélite espacial russo, em 1957 o presidente dos Estados Unidos da América, criou a Agência de Investigação de Projetos Avançados (ARPA).

No ano de 1962, segundo Turner, a Força Armada dos Estados Unidos encomendou um estudo com objetivo de avaliar como as linhas de comunicação poderiam ser formadas para que mesmo no caso de um ataque nuclear, continuassem funcionais ou que pudessem ao menos ser recuperadas celeremente[1].

A solução encontrada foi construir uma rede de comunicação independente da central, sendo invulnerável a qualquer tentativa de destruição ou controle por parte de outras nações, surgindo, assim, a ARPANET (Advanced Research Projects Agency Network – Rede da Agência de Pesquisas em Projetos Avançados). Como vantagem da ARPANET, cabe destaque o correio eletrônico, por meio do e-mail foi possível a comunicação direta, sem ter a necessidade da presença simultânea do emissor e receptor.

Contudo, conforme leciona Crespo, apesar do crescimento da ARPANET, a internet foi consolidada com a implementação do protocolo de controle de transferência (TCP/IP25), sendo responsável pela interligação de múltiplos computadores[2].

---

[1] TURNER, David; MUNOZ, Jesus. Para os filhos dos filhos de nossos filhos: uma visão da sociedade de internet. São Paulo: Summus, 1999.p.29.
[2] CRESPO, Marcelo Xavier de Freitas. Crimes Digitais – São Paulo: Editora Saraiva, 2011. p. 12.

Assim, com os avanços tecnológicos, criou-se uma rede sem fronteiras espaciais ou territoriais, sendo de grande importância para a globalização e para o aparecimento da “Sociedade Digital”. Conforme lições de Vera Marques Dias: “Com o aparecimento da cibernética, da digitalização e sobretudo de uma comunidade com uma cibercultura e ciberespaço próprio deu-se a evolução para a Sociedade Digital”[3].

Outrossim, a evolução da internet ao longo do tempo foi marcada por avanços tecnológicos significativos, como a elaboração de protocolos de comunicação mais eficientes, o aumento da velocidade das conexões, a expansão da infraestrutura de rede e a proliferação de dispositivos eletrônicos conectados, como smartphones, computadores e outros dispositivos informáticos.

A capacidade proporcionada pela internet de circulação de informação, bem como a facilidade de comunicação, aliadas ao baixo custo expandiu a rede. Segundo dados do estudo digital 2022: *Global Overview Report,* o número de usuários que acessam a internet atingiu a marca de 5 bilhões de pessoas, o que representa quase 64% da população mundial. O estudo em questão, reporta ainda que nos últimos dez anos, o número de usuários no mundo dobrou, demonstrando que é um serviço essencial e que cresce cada vez mais.

O serviço disponível na internet é essencial para os países, nos mais diversos meios, como na comunicação de forma global, uma vez que a internet suprimiu as barreiras geográficas, proporcionando que pessoas de diferentes partes do mundo possam se conectar de forma instantânea por meio de redes sociais, e-mails, chamadas de vídeo entre outras. A facilidade na comunicação fez com que as relações interpessoais sejam mais fluidas, constantes e diretas.

Ademais, a internet democratizou o acesso à informação, permitindo que pessoas estudem, e realizem pesquisas aprofundadas sobre os mais diversos temas, sendo o conteúdo, em sua maioria, disponibilizado de forma gratuita. Outro benefício impactante na sociedade é no âmbito empresarial, pois, revolucionou a forma com que as empresas operam, permitindo a venda de produtos online que segundo dados da ABComm (Associação Brasileira de Comércio Eletrônico) as vendas totais online

[3] DIAS, Vera Marques. A problemática da investigação do cibercrime. 2012. Disponível em: <https://da-tavenia.pt/ficheiros/pdf/datavenia01.pdf#page=63>

atingiram só no Brasil, a marca de 169,6 bilhões de reais no ano de 2022 e para o ano de 2023 a projeção é de crescimento, podendo atingir 186 bilhões de reais.

Contudo, apesar das vantagens acima expostas, com a ampliação da utilização da internet, aumentaram as condutas lesivas e ilícitas praticadas na rede. Aliada ao anonimato da rede, parte dos usuários praticam condutas ilícitas, acreditando que o aparente anonimato promove a impunidade, o que torna cada vez mais comum a prática de cibercrimes, demonstrando a necessidade do desenvolvimento de tecnologias de segurança que promovam a proteção dos dados dos usuários e a identificação daqueles que se utilizam da rede para prática de infrações penais.

2 DOS CRIMES CIBERNÉTICOS

Preliminarmente, cabe destacar que segundo Dias, a prática de crimes na internet possui diversas nomenclaturas como crimes cibernéticos, crime digital, crime informático, crime informático-digital, sendo todos sinônimos para a mesma conduta[4].

Os crimes cibernéticos, aqueles praticados na internet, se concretizam em ambientes digitais, porém, trazem efeitos para o mundo real. A definição dada ao crime cibernético é a seguinte:

> "a conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade"[5].

No âmbito internacional, em 2001 durante a Convenção de Budapeste, os crimes cibernéticos foram definidos como "os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados"[6].

---

[4] DIAS, Vera Marques. A problemática da investigação do cibercrime. 2012. Disponível em: <https://da-tavenia.pt/ficheiros/pdf/datavenia01.pdf#page=63>. Aceso em 07/08/2023

[5] BARRETO, Alesandro Gonçalves. BRASIL, Beatriz Silveira. Manual de Investigação Cibernética à Luz do Marco Civil da Internet. Editora Brasport. Rio de Janeiro. 2016 p. 36.

[6] BARRETO, Alesandro Gonçalves. BRASIL, Beatriz Silveira. Manual de Investigação Cibernética à Luz do Marco Civil da Internet. Editora Brasport. Rio de Janeiro. 2016 p. 36.

2.1 CLASSIFICAÇÃO

A doutrina e a legislação internacional divergem acerca da forma de classificação, a Comissão Europeia divide os crimes cibernéticos em três categorias. A primeira categoria são os crimes tradicionais cometidos com o auxílio do computador e redes informáticas, a segunda categoria são os crimes relacionados com o conteúdo, ou seja, a publicação de conteúdos ilícitos por meio eletrônicos, e a terceira categoria são os crimes exclusivos das redes eletrônicas[7].

Já parte da doutrina brasileira, classifica os crimes cibernéticos em próprios ou impróprios. Os crimes cibernéticos próprios são aqueles em que o sistema é atacado por *hackers* maliciosos, que identificam vulnerabilidades no sistema para obter vantagem. Nesse caso, o que é alvo dos *hackers maliciosos* são em geral os dispositivos informáticos ou os conteúdos armazenados neles.

Para Carneiro, os crimes considerados próprios podem ser definidos como "aqueles que o sujeito se utiliza necessariamente do computador o sistema informático do sujeito passivo, no qual o computador como sistema tecnológico é usado como objeto e meio para execução do crime nessa categoria de crimes"[8].

A título de exemplificação, pode ser destacado o ataque que a empresa *Sony Pictures Entertainment* sofreu no ano de 2014, data em que os criminosos invadiram o sistema da Sony, obtendo acesso aos e-mails corporativos e ao roteiro do filme "007-Spectre". Assim, o caso se enquadra em crime cibernético próprio, sendo que na legislação brasileira, a conduta dos criminosos está tipificada no art. 154-A caput e §3º, do Código Penal Brasileiro, que estabelece:

> "Art. 154-A., Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> (...)
> § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações

[7] Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM:l14560>. Acesso em: 07/08/2023

[8] CARNEIRO, Adenele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema tipificação. 2012. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/

> sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa”[9]

Por sua vez, os crimes cibernéticos impróprios são aqueles onde utiliza-se da internet como meio para a prática do delito, provocando a execução ou o resultado. Como principal diferença do crime próprio, temos que no crime cibernético impróprio para a prática do crime a tecnologia é o veículo utilizado.

Para elucidar o crime cibernético impróprio, pode ser destacado o “Jogo da Baleia Azul”, que ganhou repercussão no ano de 2017, caso em que crianças eram incentivadas por terceiros na internet a praticar suicídios, além de autolesões. Sendo assim, os responsáveis praticaram crime cibernético impróprio, uma vez que se utilizam da internet como meio para a prática do deligo de induzir alguém a suicidar-se.

Cabe salientar que no caso do “Jogo da Baleia Azul” a conduta dos criminosos está tipificada no art. 122 do Código Penal que estabelece *in verbis*:

> “Art. 122. Induzir ou instigar alguém a suicidar-se ou a praticar automutilação ou prestar-lhe auxílio material para que o faça: (Redação dada pela Lei nº 13.968, de 2019)
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos.”[10]

Por fim, apesar da divergência quanto a classificação, esta demonstra maior relevância apenas para fins didáticos, sendo que a classificação adotada pela doutrina pátria, separando apenas em crimes cibernéticos próprios e impróprios, demonstra-se adequada.

2.2 OS SUJEITOS ATIVOS E PASSIVOS DOS DELITOS INFORMÁTICOS

O sujeito ativo é a pessoa responsável pela emissão do comando que provoca a leitura, escrita ou execução de dados para os quais não tinha autorização. A prática do delito informático é cometida, em geral por hackers maliciosos, denominados de *crackers* que são sujeitos que detém conhecimentos amplos de

[9] Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 20.08.2023.

[10] Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 20.08.2023.

informática, eletrônica e redes de computadores, que se utilizam dos computadores e da internet para a prática de delitos.

Cabe destacar que o termo *hacker*, por diversas vezes é utilizada de forma equivocada, atribuindo sentido pejorativo a palavra, sendo que os hackers se dedicam a modificação de softwares, desenvolvendo novas funcionalidades, encontrando falhas em sistemas para empresas, ajudando a corrigi-las, ou sejam, utiliza de seus conhecimentos para aprimorar a segurança.

Para Plantullo, o hacker é caracterizado como:

> "uma pessoa física que detém, como objeto, a investigação da integridade e da segurança de um sistema qualquer de computador. Utilizasse de técnicas avançadas para invadir sistemas e detectar suas respectivas falhas. Todavia, não os destrói ou prejudica."[11]

Apesar dos hackers e dos crackers possuírem vastos conhecimentos em informática, a principal diferença entre eles reside no fato de que as atividades dos hackers não são crimes, mas sim atividades positivas para a sociedade. Por sua vez as atividades dos crackers são criminosas, agindo com objetivo criminoso de obter vantagem ilícita.

Por definição os crackers são:

> "São pessoas que possuem um grande conhecimento de programação e de segurança em sistemas de computação. Tais pessoas utilizam esse conhecimento para tirar vantagens pessoais, como destruição de sistemas por mero vandalismo ou aplicação de condutas para diversos fins ilícitos, como o estelionato eletrônico"[12].

Os crackers são os usuários mais perigosos da internet. Parte da doutrina, como Auriney Brito, utiliza de nomenclaturas diferentes atribuindo o nome de *phreakers*, para os especialistas em telefonia e eletrônica; os *carders*, especialistas em fraudes com cartões de crédito; os *wardrivers* ou *warchalkers*, especialistas em invasão de redes wireless e os *insiders,* que representam a maior ameaça, conforme estudos dirigido pelo FBI (*Federal Bureau of Investigation*), serviço de inteligência americana, os insiders são em regra funcionários ou ex-funcionários, que, por motivos vários, utilizando-se da confiança que possuem para adquirir informações sigilosas de empresas, tornando-as mais vulneráveis[13].

---

[11] PLANTULLO, V. L. Estelionato Eletrônico. Curitiba: Juruá, 2002. Disponível em: <http://www.egov.ufsc.br:8080/portal/conteudo/estelionato-eletr%C3%B4nico-e-seusagentes>. Acesso em: 20.08.2023.

[12] CARLI, Daniel Michelon. Crimes virtuais no Brasil: uma análise jurídica. 2006. Disponível em: <http://www-usr.inf.ufsm.br/~dcarli/elc1020/artigo-elc1020.pdf>. Acesso em: 20.08.2023

[13] BRITO, Auriney. Direito Penal Informático, Editora Saraiva. São Paulo. 2013. P. 50

Já o sujeito passivo, como lecionado por Barreto, é qualquer pessoa que acaba sendo vítima de crimes cibernéticos, atingindo milhares de usuários da rede, uma vez que os criminosos utilizam técnicas cada vez mais apuradas de engenharia social, aliadas às novas tecnologias[14].

Outrossim, o sujeito passivo pode ser qualquer pessoa lesada seja física ou jurídica, individual ou coletiva ou ainda uma entidade titular seja pública ou privada titular do bem jurídico tutelado.

O papel individual de vigilância e proteção da rede, é de suma importância, pois há evidências de que grande parte dos delitos informáticos hoje só é possível graças à participação efetiva e direta da vítima, por meio de técnicas de engenharia social utilizadas pelos *crackers*.

A título de demonstração da vulnerabilidade e do elevado índice de crimes, no Brasil o número de tentativas de ataques cibernéticos a empresas chegou a 31,5 bilhões no primeiro semestre de 2022, conforme estudo realizado pelo laboratório de inteligência e ameaças, *FortiGuard Labs*. A marca de 31,5 bilhões de tentativas de ataques reflete o baixo investimento em cibersegurança no Brasil, ocasionando o maior número de vítimas[15].

Outrossim, o número de tentativas de invasão multiplicou exponencialmente em decorrência da pandemia de Covid-19, uma vez que o isolamento social provocou o aumento do uso da internet, se tornando essencial para estudo, trabalho e lazer. Segundo dados da *Fortinet Threat Intelligence Insider Latin America,* o aumento foi de mais de 950% no ano de 2021 em comparação ao ano anterior[16].

2.3 LOCAL DO CRIME

[14] BARRETO, Alesandro Gonçalves. BRASIL, Beatriz Silveira. Manual de Investigação Cibernética à Luz do Marco Civil da Internet. Editora Brasport. Rio de Janeiro. 2016 p. 45.

[15] OLIVEIRA, Ingrid. Levantamento mostra que ataque cibernéticos no Brasil cresceram 94%. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/>. Acesso em: 17/08/2023

[16] Crimes digitais crescem pós-pandemia e provocam corrida por ciberseguros. Disponível em: <https://valor.globo.com/patrocinado/dino/noticia/2022/06/27/crimes-digitais-crescem-pos-pandemia-e-provocam-corrida-por-ciberseguros.ghtml>. Acesso em: 17/08/2023

Sobre o local do crime o Código Penal estabelece em seu art. 6º que “considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado”[17].

Conforme o célebre doutrinador Guilherme de Souza Nucci, no Brasil “adota-se a teoria mista, reputando-se cometida a infração penal no lugar onde se desenvolveu a ação ou omissão ou onde ocorreu o resultado”[18].

A identificação do local do crime é de suma importância para que haja a aplicação da lei penal. Contudo, como o espaço virtual transpõe barreiras geográficos, a identificação do local do crime é dificultada, inclusive parte significativa dos delitos informáticos ocorre com a transição entre países.

A teoria mista soluciona parte da problemática da identificação do local do crime. Seguindo a teoria adotada pelo legislador brasileiro, se o delito tiver sua conduta no Brasil ou mesmo o resultado real ou potencial projetado para dentro do território nacional, considera-se o delito praticado no Brasil.

No entanto, a aplicação da teoria mista não é simples como aparenta. O legislador, por impossibilidade histórica, não levou em consideração algumas hipóteses, como no caso da utilização de programas fora do domínio territorial para prática de conduta penalmente relevante, ficando apenas a ação humana aparente. Outra hipótese apresentada pelo célebre doutrinador Sydow, é de que na informática o local da conduta pode estar fora do país, bem como no ambiente virtual há possibilidade de obter resultado fora do domínio territorial com certa tranquilidade, mesmo que se busque ideologicamente ofender um bem jurídico brasileiro[19].

Destarte, o conceito de ação ou omissão deve ser alargado, segundo definição de Spencer Toth a conduta informática é:

> “toda ação ou omissão, direta ou indiretamente executada por um usuário ação ou omissão, direta ou indiretamente executada por um usuário, praticada por um ou mais usuários ou programada para ser automaticamente executada por um programa ou inteligência artificial, dirigida a um fim específico

[17] Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 20.08.2023.
[18] NUCCI, Guilherme de Souza. Manual de Direito Penal, Editora Forense. Rio de Janeiro. 2019. P. 165

[19] SYDOW, Spencer Toth. Curso de Direito Penal Informático Parte Geral e Especial, Editora JusPODIVM. São Paulo. 2022. P. 321

> e demonstrável, e que faz com que um evento normativo seja atingido, seja ele um resultado ou uma tentativa”[20].

O local informático, segundo entendimento do doutrinador supracitado, deve ser considerado o território principal em que a conduta surte ou deveria surtir o efeito, pois, é possível que o resultado ocorra dentro de uma nuvem ou sistema similar que opera fora do território nacional, sem que haja qualquer lógica de se considerar o delito praticado no exterior.

3 INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

A investigação dos crimes cibernéticos busca seguir o caminho oposto ao seguido pelos criminosos, assim a investigação segue da seguinte forma: crime; aplicações de internet; conexão à internet; provedor de conexão; terminal e indivíduo.

Na fase de investigação há a fase inicial que é técnica, e uma fase consequencial ou de campo, em que é realizada a investigação policial propriamente dita. Preliminarmente, na fase técnica, são realizadas e analisadas as informações com o único propósito de identificar o equipamento utilizado para cometer o crime, são as seguintes tarefas e informações analisadas:

> “análise das informações narradas pela vítima e compreensão do fato ocorrido na internet;
> orientações à vítima com o intuito de preservar o material comprobatório do delito e a sua proteção virtual;
> coleta inicial de provas em ambiente virtual;
> formalização do fato criminoso por intermédio de um registro ou boletim de ocorrência, com a consequente instauração do feito;
> investigação inicial referente aos dados disponíveis na rede mundial de computadores sobre prováveis autores, origem de e-mails, registro e hospedagem de domínios;
> formalização de relatório ou certidão das provas coletadas e apuração preliminar;
> representação perante o Poder Judiciário para expedição de autorização judicial para quebra de dados, conexão ou acesso. Também poderão ser solicitados os dados cadastrais para os provedores de conteúdo.
> análise das informações prestadas pelos provedores de conexão e/ou provedores de conteúdo.”[21]

---

[20] SYDOW, Spencer Toth. Curso de Direito Penal Informático Parte Geral e Especial, Editora JusPODIVM. São Paulo. 2022. P. 322

[21] WENDT, Emerson. JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos Ameaças e Procedimentos de Investigação, Editora Brasport. São Paulo. 2013. P. 52-53

Após análise das informações repassadas pelo provedor, pode ser necessário a solicitação ao Poder Judiciário para requerer novos dados para complementar as demais provas produzidas.

Importante ressaltar que cada dispositivo informático ao se conectar com a rede, possui uma numeração única, chamada de IP ou *Internet Protocol.* Apesar de parecer simples a tarefa de identificação, os cibercriminosos sabem que há tal identificação e tentam camuflar o número de identificação IP.

A fase de campo tem como marco inicial a identificação com a respectiva localização do computador que realizou a conexão e o acesso criminoso na internet, em tal fase é necessário que agentes policiais se desloquem para a prática de diligência reconhecendo o local de operação.

Ademais, após a análise dos documentos pode ser necessário a depender do caso concreto, o requerimento ao Poder Judiciário para solicitar ao administrador da rede os dados técnicos que permitam a correta identificação do dispositivo que efetuou o delito. No geral, tal circunstância ocorre em delitos praticados dentro de redes corporativas, sendo que a determinação judicial deve ser enviada ao administrador de redes para cumprimento, mas também pode ser entregue por autoridade policial.

3.1 DIFICULDADES DE INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

A dificuldade na investigação do cibercrime é consequência das características da rede como o anonimato, acesso remoto e a automatização. O anonimato por meio de uso de identidades falsas, ou ferramentas que mascarem o IP é a característica principal para o início da prática criminosa. Ainda, outra característica é o acesso remoto que gera deslocalização, ou seja, uma vez identificada atividade ilícita ou conteúdos ilícitos em determinado domínio na internet, o servidor que hospeda o conteúdo é bloqueado ou encerrado, mas os infratores podem simplesmente transferir a atividade ou conteúdo para o domínio ou servidor de outro país.

Outra característica da rede que gera aumento dos crimes cibernéticos é a possibilidade de automatização, dentro da rede é possível que sejam programados atos repetitivos, o que provoca a multiplicação do delito atingindo um número indeterminado de vítimas.

A tais dificuldades soma-se que faltam recursos humanos e técnicos para a investigação de crimes cibernéticos, uma vez que cabe a análise de inúmeros conteúdos disponibilizados na rede.

Ademais, a transnacionalidade é outro grave problema, conforme Vera Marques Dias:

> "a transnacionalidade que leva a que a cena do crime se estenda por todo o globo, sendo extremamente complexo deslindar o *cibertrail* ou rasto cibernético que se pode alastrar pelos cinco continentes. O *inter criminis* de um cibercrime é muito enleado e elaborado, pois em regra os atos digitais são praticados em diversos pontos, o que envolve vários países e consequentemente diferentes jurisdições"[22]

Para a validade da prova digital no processo, é necessário que o acesso obtenha e converse a prova, bem como o acesso deve ser realizado seguindo formas específicas de maneira segura e legal, preservando a autenticidade e integridade da prova, sendo importante tarefa para a validade da investigação

Por fim, além da necessidade da validade da prova digital, há o problema da identificação e investigação dos crimes cibernéticos, pois falta legislação apropriada, também, conforme destacado por Vera Marques Dias, "falta de metodologia no tratamento da especificidade deste crime, a interoperatividade dos sistemas, e a lentidão da cooperação e falta de partilha de informações tanto entre entidades nacionais diferentes como ao nível internacional"[23].

4 LEGISLAÇÃO BRASILEIRA

A evolução legislativa brasileira no que diz respeito aos crimes cibernéticos apresenta crescente relevância junto ao constante desenvolvimento da tecnologia na sociedade moderna. O Brasil teve que desenvolver novas leis para enfrentar os desafios trazidos pelo mundo digital, na medida em que a internet e as tecnologias digitais se tornaram parte integrante da vida cotidiana.

---

[22] DIAS, Vera Marques. A problemática da investigação do cibercrime. 2012. Disponível em: <https://datavenia.pt/ficheiros/pdf/datavenia01.pdf#page=63>. Acessado em 10/08/2023

[23] DIAS, Vera Marques. A problemática da investigação do cibercrime. 2012. Disponível em: <https://datavenia.pt/ficheiros/pdf/datavenia01.pdf#page=74>. Acessado em 10/08/2023

Sendo assim, conforme exposto a seguir, no Brasil foi promulgado uma série de leis e regulamentações que visam o combate aos crimes cibernéticos e a proteção da segurança digital dos cidadãos e das instituições.

Na década de 1980 os legisladores brasileiros voltaram a atenção ao desenvolvimento de leis para regular a informática. Em maio de 1995, o Ministério das Comunicações e o Ministério da Ciência e Tecnologia ao perceber a necessidade de participação da regulamentação da internet criou o Comitê Gestor da Internet (CGI.br) por meio da Portaria Interministerial nº 147, de 1995.

O Comitê Gestor da Internet tem como atribuições: acompanhar a disponibilização de serviços Internet no país; estabelecer recomendações relativas a: estratégia de implantação e interconexão de redes, análise e seleção de opções tecnológicas, e papéis funcionais de empresas, instituições de educação, pesquisa e desenvolvimento (IEPD); emitir parecer sobre a aplicabilidade de tarifa especial de telecomunicações nos circuitos por linha dedicada, solicitados por IEPDs qualificados; recomendar padrões, procedimentos técnicos e operacionais e código de ética de uso, para todos os serviços Internet no Brasil; coordenar a atribuição de endereços IP (Internet Protocol) e o registro de nomes de domínios; recomendar procedimentos operacionais de gerência de redes; coletar, organizar e disseminar informações sobre o serviço Internet no Brasil; e deliberar sobre quaisquer questões a ele encaminhadas.

No entanto, somente a criação do Comitê Gestor da Internet não é suficiente para a regulação. No ano de 2008 com o advento da Lei 11.829, o legislador brasileiro buscou o combate à pornografia infantil, criminalizando “a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet”[24]. Outrossim, estabelece que também incorrem na pena aqueles que asseguram os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de pedofilia, bem como aqueles que asseguram, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de pedofilia, conforme disciplina o parágrafo primeiro, incisos I e II do art. 241-A da lei 11.829/2008.

[24] Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm>, Acesso em: 08/09/2023

Logo em sequência, no ano de 2009 foi publicada a Lei 12.015 que instituiu a pena de reclusão de 1 a 4 anos para aqueles que se relacionarem com menores de 18 anos em salas de bate-papo na internet, como disposto *in verbis:*

> "Art. 244-B. Corromper ou facilitar a corrupção de menor de 18 (dezoito) anos, com ele praticando infração penal ou induzindo-o a praticá-la:
> Pena - reclusão, de 1 (um) a 4 (quatro) anos.
> § 1º Incorre nas penas previstas no caput deste artigo quem pratica as condutas ali tipificadas utilizando-se de quaisquer meios eletrônicos, inclusive salas de bate-papo da internet.
> § 2º As penas previstas no caput deste artigo são aumentadas de um terço no caso de a infração cometida ou induzida estar incluída no rol do art. 1o da Lei no 8.072, de 25 de julho de 1990." – grifo nosso[25]

Após 3 anos da publicação da Lei 12.015, em 30 de novembro de 2012 a lei nº 12.737/2012, apelidada de Lei Carolina Dieckemann, foi sancionado. A lei surgiu após crackers invadirem o computador da atriz Carolina Dieckman a chantageando para evitar a exposição de imagens íntimas, que teve como fim a divulgação das respectivas imagens nas redes sociais.

A criação da lei se deu em virtude do caso da atriz, pois, a época Carolina Dieckman não tinha amparo na legislação para a penalização dos criminosos. O texto prevê a inclusão dos artigos 154-A e 154-B do Código Penal, acrescentando a tipificação de crimes virtuais e delitos informáticos, como a invasão de dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o objeto de obter, adulterar ou destruir dados, ou informações sem autorização expressa, ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Apesar da importância do texto legal, a redação original do dispositivo tinha problemas, conforme será estudado no capítulo seguinte, sendo alterado em 2021 mediante a lei nº 14.155, de 27 de maio de 2021.

De grande relevância, o Marco Civil da Internet mediante Lei nº 12.965/2014 de 23 de abril de 2014, apresentou inúmeras inovações, a fim de estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil.

Sendo assim, o Marco Civil da Internet é norma específica que visa a regulação das relações no ambiente virtual, apresentando os fundamentos da disciplina

---

[25] Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12015.htm>, Acesso em: 08/09/2023

do uso da internet no Brasil. A base para o desenvolvimento dos fundamentos é a Constituição Federal, colocando-se como ideias centrais a preservação e o respeito à liberdade de expressão, previstos no art. 5º e 220 ambos da Constituição.

Finalmente, no ano de 2018, foi publicada a Lei nº 13.709 de 2018, chamada de Lei Geral de Proteção de Dados. A Lei nº 13.709 tem como objetivo a proteção dos direitos fundamentais de liberdade, privacidade nos meios digitais e o livre desenvolvimento da personalidade da pessoa natural, bem como visa a criação de um cenário de segurança jurídica, com a padronização de regulamentos e práticas para promover a proteção aos dados pessoais de todo cidadão que esteja no Brasil, conforme os parâmetros internacionais existentes.

4.1 LEI CAROLINA DIECKMAMM – LEI Nº 12.737/2012 E LEI 14.155/2021

Para o defensor público Aldemar Monteiro, supervisor das Defensorias Criminais em Fortaleza, a Lei Carolina Dieckmann é considerada a principal ferramenta legal para a segurança virtual dos brasileiros. Explica o defensor público que "A lei trouxe uma ferramenta a mais para punição dos crimes informáticos, porque antes o [mecanismo] que tínhamos tratava-os apenas como atos preparatórios. Antes, só o fato de você ter acesso ao dispositivo não era considerado crime. Com o advento da lei, isso passou a ser crime"[26].

Porém, a lei causou controvérsias e sofreu críticas, sendo uma delas em relação ao quantitativo mínimo da pena aplicada, abaixo de 1 (um) ano, possibilitando a aplicação dos procedimentos dos Juizados Especiais. A pena mínima permite a suspensão condicional do processo, desde que, o autor não tenha condenação ou processo por outro crime, conforme art. 89 da Lei dos Juizados Especiais Cíveis e Criminais. Seguindo parte da doutrina, em decorrência da pena branda, estas são pouco inibidoras para prática de um crime que pode gerar sérios danos na vida das vítimas.

A tendência internacional é contrária a pena imposta pela lei nº 12.737/2012, alguns países como os Estados Unidos estabelecem penas mais graves

[26] Disponível em: <https://www.defensoria.ce.def.br/noticia/lei-carolina-dieckmann-10-anos-da-lei-que-protege-a-privacidade-dos-brasileiros-no-ambiente-virtual/>. Acesso em 01/09/2023

para tais crimes. Assim, no caso do cracker acusado de roubar fotos de celebridades nuas em 2011, este foi condenado pela justiça do Estado da Califórnia a dez anos de prisão e multa.

Além disso, a lei restringe a tipificação da conduta para os casos em que há violação indevida de mecanismos de segurança. Assim, a lei não define o que são “dispositivos informáticos” e não define os “mecanismos de segurança”, só a falta de definição já é um problema, no entanto, podemos observar outro problema mais grave que é o fato de o dispositivo legal só amparar os indivíduos que sabem instalar os mecanismos de segurança, aqueles sem conhecimentos de formas de proteção do dispositivo, como a implementação de senhas, antivírus ou outros meios não possuem amparo legal.

Outro ponto criticado é o emprego do termo “invadir”. Como já abordado no presente trabalho, o número de invasões tem aumentado e na maioria a própria vítima contribui sem saber para a invasão, nos casos em que os criminosos utilizam de técnicas de engenharia social. Portanto, nesse caso que os criminosos utilizam de engenharia social, o indivíduo que tiver seus dados roubados não possui proteção legal.

Ainda, a parte final do artigo 154-A, seguindo a redação da lei nº 12.737/2012, falha ao não contemplar o caso da invasão dispositivo informático com o intuito de observar os dados, informações e a vida de outra pessoa sem causar danos.

Conforme exposto a redação original do dispositivo continha problemas e foi alterada, tendo sua redação aprimorada. Dessa forma, em 2021 mediante a lei nº 14.155, de 27 de maio de 2021 passa a vigorar o art. 154-A do Código Penal com a seguinte redação:

> “Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021)
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
> § 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. (Incluído pela Lei nº 12.737, de 2012) Vigência

> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. (Redação dada pela Lei nº 14.155, de 2021)
> § 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: (Incluído pela Lei nº 12.737, de 2012) Vigência
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
> § 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. (Incluído pela Lei nº 12.737, de 2012) Vigência
> § 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra: (Incluído pela Lei nº 12.737, de 2012) Vigência
> I - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012) Vigência
> II - Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012) Vigência
> 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 (Incluído pela Lei nº 12.737, de 2012) Vigência
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Incluído pela Lei nº 12.737, de 2012) Vigência
> Ação penal (Incluído pela Lei nº 12.737, de 2012) Vigência
> 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. (Incluído pela Lei nº 12.737, de 2012) Vigência"[27]

A nova redação conferida ao art. 154-A e art. 154-B solucionou alguns dos problemas encontrados na redação antiga. Com a nova redação, a pena que foi amplamente criticada, foi majorada para um a quatro anos de reclusão e multa na sua forma básica, presente no caput do art. 154-A, também majorou os limites da causa de aumento de pena presente no §2º e majorou a pena da qualificadora do §3º ambos do art. 154-A do Código Penal.

Nesse prisma, cabe análise dos elementos objetivos do art. 154-A sob a ótica da lei de 2021. O primeiro elemento objetivo do tipo é invadir e representa a entrada à força em lugar alheio, a conduta no caso não é a simples entrada em dispositivo informático, mas sim acessar lugar não permitido. O objeto da conduta é o dispositivo informático que pode ser entendido como dispositivo que armazene informação por meio de computador ou outro similar, sendo que o dispositivo deve ser alheio.

---

[27] Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>, Acesso em: 08/09/2023

Na redação anterior à Lei 14.155/2021, o legislador instituía que para a tipificação era necessária que ocorresse “mediante violação indevida de mecanismo de segurança”, com a nova redação esse requisito foi retirado. Para o importante doutrinador Guilherme de Souza Nucci, fez bem o legislador ao retirar a necessidade de utilização de mecanismo de segurança, uma vez que era empecilho desnecessário inserido no tipo penal. A proteção demonstrava que havia proteção só para aqueles dispositivos informáticos que tivessem um sistema de proteção instalado[28].

A expressão sem autorização expressa ou tácita do usuário do dispositivo contém o elemento do injusto, foi escolha do legislador apesar de desnecessária, reforçar que a conduta é atípica caso haja autorização. O legislador teve a cautela de delimitar que a autorização pode ser expressa, ou seja por meio escrito ou falado ou tácito, aquele deduzido da ação.

Ademais, o acréscimo decorrente da lei 14.155/2021, introduziu o §2º-A do art. 171 do Código Penal que trata da fraude eletrônica, com pena de reclusão de quatro a oito anos e multa. A fraude eletrônica, conforme redação do art. 171, §2º-A, ocorre “se a fraude é cometida com a utilização de informações fornecidas pela vítima induza por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento ou outros meios análogos”[29].

No caso de estelionato, o número de casos em que os criminosos enganam a vítima para obter informações e consequente vantagem tornou-se comum, a engenharia social por trás dos crimes é sofisticada, sendo um acerto do legislador ao tipificar como qualificadora do crime de estelionato, visando coibir tais práticas.

4.2 MARCO CIVIL DA INTERNET - LEI N.º 12.695/2014

O projeto do Marco Civil da Internet teve início com a parceria da Secretaria de Assuntos Legislativos do Ministério da Justiça junto a Fundação Getúlio Vargas, por meio do Centro de Tecnologia e Sociedade da Escola de Direito.

---

[28] NUCCI, Guilherme de Souza. Manual de Direito Penal Volume Único, Editora Forense. Rio de Janeiro. 2023. P. 1168

[29] Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>, Acesso em: 08/09/2023

Já no início do projeto, o objetivo era a garantia de direitos e não a restrição de liberdades. Conforme Borbot, durante a elaboração do Marco Civil, foi realizada consulta pública, dividida em duas fases: a primeira contou com a participação da sociedade civil e diversas empresas, tanto nacionais quanto internacionais do ramo digital que apresentaram suas opiniões sobre o tema, já a segunda fase contou com participação popular, mas discutindo cada dispositivo proposto na primeira fase[30].

Com base no extenso debate sobre o tema, a Câmara dos Deputados através da Mensagem nº 326 de 2011, encaminhou o projeto de Lei nº 126 de 2011, tendo como relator o deputado Alessandro Molon.

Assim, no dia 23 de junho de 2014 a lei nº 12.695/2014 denominada de Marco Civil da Internet, entrou em vigor, após sessenta dias de *vacatio legis*. A lei em questão apresentou conceitos e procedimentos, que visam suprir a ausência de disciplina legal no ciberespaço, regulando os direitos civis do cidadão brasileiro no espaço digital. Sobre o tema, cabe destacar os ensinamentos de Ronaldo Lemos que leciona:

> "A situação pré-Marco Civil era de completa ausência de regulamentação civil da internet no país. Ao contrário do que alguns entusiastas libertários poderiam achar, a ausência de leis nesse âmbito não representa a vitória da liberdade e do laissez-faire. Ao contrário, gera uma grande insegurança jurídica. Uma das razões é que juízes e tribunais, sem um padrão legal para a tomada de decisões sobre a rede, acabam decidindo de acordo com regras muitas vezes criadas ad hoc, ou de acordo com as suas próprias convicções, resultando em inúmeras decisões judiciais contraditórias"[31]

O art. 2º do Marco Civil da Internet estabelece como fundamento o respeito à liberdade de expressão, bem como: "o reconhecimento da escala mundial da rede; os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; a pluralidade e a diversidade; a abertura e a colaboração; a livre iniciativa, a livre concorrência e a defesa do consumidor; e a finalidade social da rede".

---

[30] BORBOT, Jessica Fagundes. Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com Base nas Legislações Brasileira e Internacional. Disponível em: <http://periodicos.pucminas.br/index.php/virtuajus/article/view/15745>. Acesso em 05/09/2023

[31] LEMOS, Ronaldo. O Marco Civil Como Símbolo do Desejo por Inovação no Brasil. In: LEITE, George Salomão; LEMOS, Ronaldo. Marco Civil da Internet. Parte 1. São Paulo: Atlas, 2014 p. 10

O legislador busca a preservação dos direitos fundamentais e garantias individuais, especialmente sobre a proteção da privacidade e ao direito de imagem, bem como a liberdade de expressão. Cabe destacar que tais direitos já possuem proteção constitucional, a proteção à privacidade e ao direito de imagem estão previstos no art. 5º inc. X da CF e a liberdade de expressão prevista no art. 5º, inc. IX da CF.

No Art. 3º do Marco Civil da Internet, os princípios estão expressos, não excluindo outros princípios decorrentes do regime democrático, sendo que a disciplina do uso da internet no Brasil segue os princípios da: "garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; proteção da privacidade; proteção dos dados pessoais, na forma da lei; preservação e garantia da neutralidade de rede; preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; responsabilização dos agentes de acordo com suas atividades, nos termos da lei; preservação da natureza participativa da rede; liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei"[32].

Na Lei nº 12.695/2014 em seu art. 3º, inciso II, o legislador estabelece como princípio da disciplina do uso da internet no Brasil a proteção da privacidade. Assim como previsto na Constituição, o legislador assegura novamente no art. 7º, inciso I o direito a "inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação". No art. 8º é garantido o direito à privacidade e à liberdade de expressão nas comunicações. Finalmente, sobre a privacidade o legislador no art. 10º estabelece que "conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas".

A intenção do legislador de proteger a privacidade e a liberdade de expressão é clara, ao abordar o mesmo tema em diversos artigos. Para possibilitar a efetiva proteção à privacidade e imagem dos usuários da rede, o art. 19 institui em seu caput que "o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial

[32] Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>, Acesso em: 08/09/2023

específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente".

O legislador, estabelece como exceção ao artigo supracitado, o caso de conteúdos que violem a intimidade decorrente da divulgação sem autorização de cenas de nudez ou atos sexuais, conforme previsto no caput do art. 21:

> "Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.
>
> Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido."[33]

Não obstante, caso não haja relação entre a divulgação da imagem e a liberdade de expressão, subsiste apenas a evidente violação ao direito de imagem, à intimidade e à privacidade, tanto daquele que foi retratado, quanto de sua família.

Sobre o tema, insta salientar que apesar do Marco Civil tutelar preliminarmente os direitos civis na internet, também tem aplicação no Direito Penal e Processual Penal, pois estabelece conceitos fundamentais e determina a forma de obtenção de provas quanto à materialidade e à identificação da autoria delitiva.

4.3 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

A Lei Geral de Proteção de Dados Pessoais, publicada em 2018, inicialmente tinha como vigência prevista para o dia 16 de fevereiro de 2020, em decorrência da Medida Provisória nº 869/18, o prazo para vigência foi prorrogado por mais seis meses, passando para agosto de 2018, já as sanções impostas pela lei passaram a vigorar a partir de agosto de 2021.

---

[33] Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>, Acesso em: 08/09/2023

A LGPD tem os seguintes objetivos:

> “A lei busca um equilíbrio entre os novos modelos de negócio baseados no uso de dados pessoais e a proteção à privacidade, valor cada vez mais na pauta dos cidadãos a partir da divulgação cada vez maior de casos de uso indevido de tais informações.”[34]

Além disto, a Lei Geral de Proteção de Dados Pessoais apresenta em seu artigo segundo os fundamentos para a proteção de dados pessoais, sendo eles: “o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais”[35].

A lei estabelece que devem ser observados a boa-fé e outros dez princípios, como: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança: prevenção: não discriminação; responsabilização e prestação de contas.

Importante frisar que a LGPD deve ser aplicada em toda operação de tratamento realizadas por pessoa natural ou por pessoa jurídica de direito público ou privado no Brasil que tenham por objetivo a oferta de bens, serviços ou que trate dos dados de indivíduos que residam no Brasil, ou aqueles dados que tenham sido coletados no território nacional, conforme previsão no art. 3º da lei em questão.

A lei trouxe outro ponto importante que é o consentimento para ocorrer o tratamento dos dados pessoais, conforme art. 7º inc. I. Conforme definição dada pela lei no art. 5º, inc. XII, o consentimento é “manifestação livre, informada e inequívoca

---

[34] MACIEL, Rafael Fernandes. Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18). RM Digital Education. 1ª Edição. Goiânia – GO. 2019. P. 17

[35] Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>, Acesso em: 08/09/2023

pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Para a validade do consentimento, este deve ser livre, informado e inequívoco, sendo fornecido por escrito ou outro meio que demonstre a manifestação da vontade do titular, em cláusula destacada, sem vício de consentimento e referir-se a finalidades determinadas, sendo que as autorizações genéricas serão consideradas nulas, bem como caixas de seleção pré-selecionadas também são consideradas não legítimas, invalidando o consentimento. Sobre o consentimento, o controlador deve adotar formas para que possa provar o consentimento, uma vez que cabe ao controlador o ônus da prova de que o consentimento foi obtido, conforme art. 8º, §2º da lei nº 13.709/2018.

No Brasil, o órgão responsável pela proteção dos dados pessoais, também responsável pela elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade e pela fiscalização e aplicação das sanções em caso de tratamento de dados realizado em descumprimento à legislação, dentre outras atribuições é a Autoridade Nacional de Proteção de Dados. A Autoridade Nacional de Proteção de Dados (ANPD) é autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio, conforme art. 55-A da LGPD.

Os agentes de tratamento estão sujeitos à responsabilização civil pelo tratamento ilícito dos dados pessoais e sem prejuízo podem ser aplicadas sanções administrativas, como multa simples de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 por infração, dentre outras sanções administrativas previstas no art. 52 da lei nº 13.709/2018.

5 PROJETOS DE LEI NO ÂMBITO DOS CRIMES CIBERNÉTICOS

Na sociedade cada vez mais interconectada, surgem novas problemáticas e demandas para a regulamentação do espaço digital. Assim, o legislador desempenha papel fulcral na sociedade ao regular temas inovadores e que se encontram em constante mudança.

Nesse prisma, os projetos de lei no âmbito dos crimes cibernéticos que serão analisados no presente capítulo, são uma parte primordial da estratégia para combate as ameaças digitais na sociedade cada vez mais interconectada. A legislação tem o papel não apenas de definir o que é ilegal, mas também estabelece a base para a proteção dos indivíduos e a promoção de um ambiente online seguro e confiável o que garante a eficácia das leis, sendo fundamental que as leis sejam elaboradas com cuidado e se adaptem às mudanças tecnológicas.

5.1 PROJETO DE LEI Nº 2.237, DE 2015

Apesar do Marco Civil em seu art. 21, responsabilizar o provedor de aplicações de internet que disponibilizem conteúdo sem autorização de seus participantes, de imagens ou outros materiais contendo cenas de nudez ou de atos sexuais, a lei não regula sobre a divulgação e a venda de conteúdos de pessoas mortas.

Dessa forma, surgem casos como o do cantor Cristiano Araújo que demonstram a necessidade de regulamentação sobre a divulgação ou venda de conteúdos com imagens de pessoas mortas. No caso do cantor, falecido em junho de 2015 em decorrência de um acidente de carro, este teve imagens do seu procedimento de preparação do corpo e procedimento de embalsamamento, filmado e publicado nas redes sociais.

A conduta de divulgar imagem, vídeo que contenha cadáver ou parte dele não é punível, pois, atualmente pelo Código Penal só é punível a conduta de coletar a imagem. Nesse sentido, para coibir a prática de divulgação de imagens ou vídeos que exponham a memória do ente falecido, é necessária a criação de uma lei.

Sobre o tema podemos destacar o projeto de lei nº 2.237, de 2015 que visa alterar o art. 212 do Código Penal, criando o parágrafo único com a seguinte redação: “Parágrafo único. É punível quem reproduz acintosamente, em qualquer meio de comunicação, foto, vídeo ou outro material que contenha imagens ou cenas aviltantes de cadáver ou parte dele”.[36]

[36] Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=1554077>. Acesso em: 05/09/2023

Conforme já mencionado a inclusão do parágrafo único ao art. 212 é de grande relevância, a divulgação indesejada das imagens de mortes e cadáveres, multiplica a dor daqueles que perderam seu familiar, expondo a imagem de maneira insensível. Atualmente o projeto de lei está apensado ao PL2175/2015, que se encontra pronto para pauta no plenário.

5.2 PROJETO DE LEI 2.630 DE 2020

As notícias falsas, também chamadas de “fake news” têm um impacto significativo na sociedade contemporânea, deturpando a realidade dos fatos, abalando os alicerces da informação confiável, prejudicando a democracia e a confiança pública. A desinformação provocada pela “fake News” vem gerando impactos até na saúde da população, o movimento antivacina ganhou força por meio de notícias falsas, como exemplo recente, com o surgimento da vacina para Covid-19, foram circuladas notícias falsas nas mais diversas redes sociais, de que a vacina contra a Covid-19 continha um chip produzido pela China, também foi falado que as vacinas poderiam causar Alzheimer.

As informações falsas, sem embasamento científico ou legal, provocaram diminuição no número de vacinados no Brasil. Segundo dados da OMS, o índice aceitável de vacinação da população seria de 80%, contudo somente 55% dos brasileiros foram imunizados[37].

Assim, com a redução do número de vacinados doenças como o sarampo, por exemplo, que não tinham mais casos desde 2016, em 2018 voltou a oferecer risco à população e conforme dados da OMS há chance de novo surto da doença no país[38].

Além do impacto na saúde, outra área afetada pela “fake News” é a área política, o que gera prejuízos à democracia. Os eleitores, quando mal-informados, mediante notícias falsas podem decidir e votar baseados em informações incorretas, comprometendo a integridade das eleições e a legitimidade dos governos.

---

[37] Disponível em: <https://summitsaude.estadao.com.br/desafios-no-brasil/vacinas-e-fake-news-o-impacto-de-noticias-falsas-sobre-a-vacinacao-no-brasil/>. Acesso em: 08/09/2023

[38] Disponível em: <https://summitsaude.estadao.com.br/desafios-no-brasil/vacinas-e-fake-news-o-impacto-de-noticias-falsas-sobre-a-vacinacao-no-brasil/>. Acesso em: 08/09/2023

A democracia brasileira no ano de 2023 sentiu reflexos das “fake News”. No decorrer das eleições inúmeras “fake News” circularam pelas redes sociais, descredibilizando o sistema eleitoral e a confiabilidade das urnas. Dessa forma, após a derrota nas urnas do candidato Jair Messias Bolsonaro, no dia 08 de janeiro de 2023, surgiu o movimento liderado por bolsonaristas radicais que não aceitaram o resultado das urnas eletrônicas e acabaram atacando e depredando o Congresso Nacional, o Supremo Tribunal Federal e o Palácio do Planalto.

Diante do atual cenário, a importância de uma regulamentação e de responsabilização pela divulgação de “fake News” demonstra-se de extrema importância, mas cabe destacar a dificuldade de legislar sobre o tema, uma vez presente o embate entre a censura e a liberdade de imprensa.

Nesse âmbito, no Brasil está sendo debatido o projeto de Lei 2.630 de 2020, que trata da liberdade, responsabilidade e transparência na internet. O projeto de lei em análise determina normas sobre a transparência nas redes sociais, aplicativos de troca de mensagens, especialmente em relação à responsabilidade dos provedores pelo combate à desinformação, reforçando a transparência na rede, com o fim de garantir a segurança e ampla liberdade de expressão.

O projeto de lei tem os seguintes objetivos:

> “Art. 4º Esta Lei tem como objetivos: I – o fortalecimento do processo democrático por meio do combate ao comportamento inautêntico e às redes de distribuição artificial de conteúdo e do fomento ao acesso à diversidade de informações na internet no Brasil; II – a defesa da liberdade de expressão e o impedimento da censura no ambiente online; III – a busca por maior transparência das práticas de moderação de conteúdos postados por terceiros em redes sociais, com a garantia do contraditório e da ampla defesa; e IV – a adoção de mecanismos e ferramentas de informação sobre conteúdos impulsionados e publicitários disponibilizados para o usuário.”

Como solução para o combate a desinformação, a proteção da liberdade de expressão e o acesso à informação, o legislador estabelece que os provedores da internet devem adotar medidas que impeçam a utilização de contas inautênticas, vedando a utilização de contas automatizadas não identificadas, bem como devem ser identificados os conteúdos impulsionados presentes na rede.

O art. 32 do projeto de lei estabelece que os provedores tanto de redes sociais quanto de serviços de mensagem devem ter sede e nomear representantes no Brasil. Caso o projeto de lei seja aprovado com a atual redação, aplicativos como Telegram, que não possuem sede no país, devem se adequar.

Portanto, apesar da dificuldade de regulamentação e do cumprimento do projeto de lei, devido ao vasto número de usuários e de conteúdos disponibilizados na rede, a regulamentação é de grande importância, sendo um avanço significativo para a sociedade e para o sistema democrático.

5.3 PROJETO DE LEI 2.699/2021

O avanço tecnológico apresentou benefícios, mas junto aos benefícios a internet também trouxe desafios significativos, sendo um deles o *cyberbullying*. O cyberbullying é a prática de utilizar a tecnologia, principalmente as redes sociais, para praticar ataques que atingem a esfera moral de determinada pessoa, por meio de assédio, ameaça, difamação ou humilhação de outra pessoa.

A característica do cyberbullying é a natureza insidiosa, pois como é praticada em ambiente virtual e na maior parcela dos casos de forma anônima, é mais fácil para os agressores atacarem suas vítimas sem enfrentar as consequências diretas de suas ações.

As vítimas do *cyberbullying* enfrentam efeitos no âmbito emocional, psicológico e até físico. Em casos extremos as vítimas podem desenvolver quadros de estresse, ansiedade e depressão, provocando até o suicídio.

Esta prática em ambientes virtuais, ocasionou a morte do jovem Lucas Santos, filho da cantora Walkyria Santos. Após a publicação e repercussão negativa do vídeo do jovem simulando beijar um amigo, o jovem sofreu grandes críticas de *haters* com comentários maldosos, o que agravou o quadro de depressão e ocasionou o suicídio de Lucas[39].

[39] Disponível em: <https://fmp.edu.br/caso-lucas-santos-lei-cria-programa-de-combate-ao-cyberbullying-na-paraiba/>. Acesso em 08/09/2023

Devido à grande repercussão do caso, de forma célere foi publicada no ano de 2021 a Lei 12.031/2021, dando início ao programa Estadual de Combate ao Cyberbullying Lucas Santos, que consiste na promoção de ações educativas direcionadas ao público escolar.

Contudo, é evidente que a promoção de medidas educativas não é suficiente, sendo necessária uma regulamentação com punições para aqueles que praticam o *cyberbulling.*

Nesse sentido, o projeto de lei 2699/2021 trata sobre a criminalização da prática de *haters* na internet. Seguindo o art. 1º do projeto de lei em análise, comete o crime de *haters* "aquele que usa a rede mundial de computadores, seja em redes sociais ou quaisquer meios de facilite sua propagação, para disseminar ódio ou proferir comentários discriminatórios de qualquer natureza, que cause danos a integridade psíquica da criança e do adolescente"[40]. Ainda, o projeto de lei atribui responsabilidade civil e criminal para aqueles que cometam o crime de haters.

Logo, ao analisar o aumento da utilização das redes sociais, atrelado ao aumento do número de doenças mentais, demonstra-se necessário e importante uma regulamentação com punições para aqueles que pratiquem o chamado *hate* na internet.

6 CONSIDERAÇÕES FINAIS

Conforme já exposto, a internet teve origem no período da guerra fria, devido à necessidade de uma comunicação que não fosse afetada mesmo em casos de ataque nuclear, com a formação de uma rede de comunicação independente da central. Após a criação, o seu desenvolvimento ocorreu de forma célere, surgindo uma rede de comunicação e circulação de informações em massa.

Contudo, a ferramenta que deveria ser utilizada com o fim de beneficiar a sociedade de forma geral, é utilizada por parte dos usuários como ferramenta para lesar e praticar atividades ilícitas. A alta lucratividade da atividade ilícita, o relativo

[40] Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2053707&filename=PL%202699/2021>. Acessado em: 08/09/2023

anonimato da rede, aliada à possibilidade da prática ilícita ser cometida de qualquer lugar, inclusive de dentro de penitenciárias, faz com que a taxa de crimes virtuais aumente expressivamente.

Para um ambiente virtual mais seguro, é necessário o desenvolvimento de tecnologias de segurança que protejam os dados dos usuários e que promovam a identificação dos criminosos. Ademais, como em muitos casos a vítima acaba por colaborar para a efetivação da invasão, uma vez que os criminosos utilizam de técnicas avançadas de engenharia social, cabe ao Estado promover a educação por meio de propagandas que informem os usuários de métodos eficazes para a proteção, evitando que a prática do delito se efetive.

Outrossim, apesar da existência de algumas leis esparsas no ordenamento jurídico brasileiro que regulam sobre o uso da rede, tais leis não conseguem acompanhar o avanço das práticas delitivas. O fato de ser extremamente complexo a identificação do usuário que praticou o delito, faz com que os criminosos cibernéticos pratiquem reiteradamente o delito sem uma punição por parte do Estado.

Portanto, há necessidade de investimentos na área da segurança digital, efetivando a proteção do usuário, bem como cabe ao poder legislativo a elaboração de leis mais eficazes que regulamentem os mais diversos tipos de crimes cibernéticos.

REFERÊNCIAS

BRITO, Auriney. Direito Penal Informático, Editora Saraiva. São Paulo. 2013.

BARRETO, Alesandro Gonçalves. BRASIL, Beatriz Silveira. Manual de Investigação Cibernética à Luz do Marco Civil da Internet. Editora Brasport. Rio de Janeiro. 2016

BORBOT, Jessica Fagundes. Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com Base nas Legislações Brasileira e Internacional. Disponível em: <http://periodicos.pucminas.br/index.php/virtuajus/article/view/15745>. Acesso em 05/09/2023

CARLI, Daniel Michelon. Crimes virtuais no Brasil: uma análise jurídica. 2006. Disponível em: http://www-usr.inf.ufsm.br/~dcarli/elc1020/artigo-elc1020.pdf

CARNEIRO, Adenele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema tipificação. 2012. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/

CRESPO, Marcelo Xavier de Freitas. Crimes Digitais – São Paulo: Editora Saraiva, 2011.

DIAS, Vera Marques. A problemática da investigação do cibercrime. 2012. Disponível em: https://datavenia.pt/ficheiros/pdf/datavenia01.pdf#page=63

LEMOS, Ronaldo. O Marco Civil Como Símbolo do Desejo por Inovação no Brasil. In: LEITE, George Salomão; LEMOS, Ronaldo. Marco Civil da Internet. Parte 1. São Paulo: Atlas, 2014

MACIEL, Rafael Fernandes. Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18). RM Digital Education. 1ª Edição. Goiânia – GO. 2019.

NUCCI, Guilherme de Souza. Manual de Direito Penal Volume Único, Editora Forense. Rio de Janeiro. 2023.

PLANTULLO, V. L. Estelionato eletrônico. Curitiba: Juruá, 2003.

SYDOW, Spencer Toth. Curso de Direito Penal Informático Parte Geral e Especial, Editora JusPODIVM. São Paulo. 2022.

TURNER, David; MUNOZ, Jesus. Para os filhos dos filhos de nossos filhos: uma visão da sociedade de internet. São Paulo: Summus, 1999

WENDT, Emerson. JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos Ameaças e Procedimentos de Investigação, Editora Brasport. São Paulo. 2013.

https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM:l14560

http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l14560_pt.htm

https://entretenimento.r7.com/pop/roteiro-do-novo-filme-de-james-bond-foi-roubado-em-ataque-hacker-aos-arquivos-da-sony-01042023

https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-cibernetico-s-no-brasil-cresceram-94/

https://valor.globo.com/patrocinado/dino/noticia/2022/06/27/crimes-digitais-crescem-pos-pandemia-e-provocam-corrida-por-ciberseguros.ghtml

https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm

https://www.cgi.br/portarias/numero/147/

https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm

https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12015.htm

https://www.defensoria.ce.def.br/noticia/lei-carolina-dieckmann-10-anos-da-lei-que-protege-a-privacidade-dos-brasileiros-no-ambiente-virtual/

http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm

https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=1554077

https://www.camara.leg.br/propostas-legislativas/2256735

https://summitsaude.estadao.com.br/desafios-no-brasil/vacinas-e-fake-news-o-impacto-de-noticias-falsas-sobre-a-vacinacao-no-brasil/

https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2292364

https://fmp.edu.br/caso-lucas-santos-lei-cria-programa-de-combate-ao-cyberbullying-na-paraiba/