FACULDADE CIDADE DE JOÃO PINHEIRO – FCJP
CURSO DE GRADUAÇÃO EM DIREITO

SAMUEL VICTOR DUARTE

CRIMES CIBERNÉTICOS.

JOÃO PINHEIRO/MG
2022

SAMUEL VICTOR DUARTE

CRIMES CIBERNÉTICOS.

Artigo científico apresentado à Faculdade Cidade de João Pinheiro, com requisito parcial de avaliação da disciplina de Trabalho de Curso.

Orientador: Prof. Esp. Tyciano Magno de Oliveira Almeida

JOÃO PINHEIRO/MG
2022

Ficha Catalográfica - Biblioteca - FCJP
Faculdade Cidade de João Pinheiro

FOLHA DE APROVAÇÃO

SAMUEL VICTOR DUARTE

CRIMES CIBERNÉTICOS.

Trabalho de conclusão de curso apresentado junto à Faculdade Cidade de João Pinheiro, em ____/____/_____, para obtenção do título de bacharel em Direito.

Aprovada em ____/____/____

Banca examinadora

_____

Orientador(a):

_____

1° Examinador(a):

_____

2° Examinador(a):

JOÃO PINHEIRO/MG

2022

TERMO DE RESPONSABILIDADE DO ALUNO EM RELAÇÃO ÀS NORMAS DE TRABALHO DE CONCLUSÃO DE CURSO

Curso de Direito

Professor (a) de TCC _____

Aluno: _____

Tema: _____

O aluno abaixo assinado declara conhecer as normas de TCC descritas em manual próprio dessa instituição estando ciente da responsabilidade de realizar o seu trabalho com fidelidade às obras utilizadas. Tendo plena consciência das penalidades relacionadas ao plágio comprovado que impedem a conclusão do curso e exigem que curse novamente a disciplina de TCC.

João Pinheiro, _____ de _____ de 20_____

_____

Assinatura do(a) aluno(a)

AGRADECIMENTOS

A Deus pela minha vida, e por me ajudar a passar por cima de todos os obstáculos encontrados ao longo do curso e da minha vida. Agradeço aos meus familiares, que me incentivaram desde o primeiro momento. Por fim, aos professores, pelas correções e ensinamentos que me permitiram apresentar um melhor desempenho .

CRIMES CIBERNÉTICOS

Samuel Victor Duarte [1]
Tyciano Magno de Oliveira Almeida [2]

RESUMO: A comunicação no mundo sofreu grandes modificações ao longo do tempo, sobretudo com o advento da internet e dos meios de comunicação tecnológicos, elevando a rapidez na troca de informações entre as pessoas, estando elas próximas ou distantes, e com isso, também, evoluíram as práticas criminosas, que antes eram realizadas apenas de forma física, passando, para também, para a forma virtual. O presente trabalho, portanto, investida se o regramento legal brasileiro atual é suficientemente eficiente para a coerção de crimes cibernéticos, e realizar alguns apontamentos sobre possíveis melhorias no arcabouço legal afeto ao tema, a fim de que se possa obter ações mais contundentes contra este tipo de crime. Espera-se concluir que o país possa avançar, rumo ao atendimento das necessidades das pessoas no sentido da proteção de dados e patrimônio, trabalho pelo qual o legislador pátrio deve primar a fim de que seja possível utilizar-se dos meios digitais com segurança, praticidade e sossego.

PALAVRAS CHAVE: Comunicação. Crime. Cibernético. Legislação. Virtual. Segurança.

[1] Acadêmico(a) do oitavo período do curso de Direito da Faculdade Cidade de João Pinheiro– FCJP.
[2] Orientador(a) e docente do curso de Direito da FCJP. Graduado em Direito pela UFMG em 2006. Especialista em Direito Público. Especialista em Direito Tributário. Especialista em Direito Administrativo. Oficial de Apoio do Tribunal de Justiça de Minas Gerais (2006 a 2008). Analista do Ministério Público do Estado de Minas Gerais.

ABSTRACT: Communication in the world has undergone major changes over time, especially with the advent of the internet and technological means of communication, increasing the speed in the exchange of information between people, whether they are close or distant, and with that, too, the criminal practices, which were previously carried out only in a physical form, now also taking on a virtual form. The present work, therefore, investigates if the current Brazilian legal regulation is efficient enough for the coercion of cyber crimes, and makes some notes on possible improvements in the legal framework related to the subject, in order to obtain more forceful actions against this type. of crime. It is expected to conclude that the country can move forward, towards meeting the needs of people in the sense of protecting data and assets, a work for which the national legislator must excel so that it is possible to use digital media with safety, practicality and quiet.
KEYWORDS: Communication. Crime. cybernetic. Legislation. Virtual. Safety.

1 INTRODUÇÃO

A comunicação global transformou drasticamente desde o advento da internet e dos meios tecnológicos, hoje existe uma grande rapidez na troca de dados entre pessoas que estão próximas ou muito distantes, o que não havia há cerca de duas décadas atrás onde a comunicação era mais lenta, feita por meio de cartas ou através de e-mails repassados através de um sistema de internet ainda arcaico e que não era tão democrático quanto os dias atuais.

É notório a grande evolução dos computadores nas últimas décadas, o que antes eram máquinas gigantes que preenchiam o ambiente de uma sala de estar, hoje são portáteis e podem ser levados até mesmo no bolso de uma calça para qualquer lugar por qualquer pessoa, conectando-se à rede mundial de comunicações, a internet, estabelecendo uma conexão completa graças à rede sem fio.

Ocorre que, com o grande avanço das tecnologias, também surgiram novas modalidades de crimes cibernéticos, os quais podem se classificar em diversas categorias, como sendo, invasão cibernética, fraude, roubo de identidade, pirataria, pornografia cibernética e ciber-violência. Sempre com o objetivo de tirar algum tipo de vantagem sobre pessoas físicas e jurídicas, na maioria das vezes, por dinheiro. Infelizmente, na maioria dos países não é possível estimar a quantidade de crimes virtuais que acontecem, pois apesar da realidade, ainda não existe uma legislação mais dura aplicada ao tema. [3]

Os crimes cibernéticos são um contraponto moderno ao crime antigo, pois, antes da era da tecnologia os criminosos assaltavam as casas, usando a comunicação verbal para garantir o sucesso de seu intento, com o advento da internet, os criminosos usam a internet e comunicação online para cometer seus crimes.[4]

No Brasil, a primeira lei que trata dos crimes virtuais foi promulgada em 2012, e se preocupou apenas em observar o aspecto físico dos crimes virtuais, ou seja, é necessário que haja a violação de um direito da vítima como a invasão de um

[3] BORTOT, Jéssica Fadundes. Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. Ano 2017. VirtuaJus, Belo Horizonte, v. 2. ISSN 1678-3425, p. 141.

[4] ALVES, Marco Antônio. DINIZ, Thiago Dias de Matos. CASTRO, Viviane Vidigal de. Criminologia e cybercrimes. RECAJ – UFMG – Belo Horizonte, 2020. Livro Digital. Disponível em: https://www.conpedi.org.br/wp-content/uploads/2020/12/Livro-8-Criminologia.pdf. Acesso em 08 de setembro de 2022, às 22h00min.

dispositivo de informática, a falsificação de documento particular, falsificação de cartão e/ou interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.[5]

Apesar de recentemente o Brasil ter sido convidado a participar da Convenção do Conselho da Europa contra a Criminalidade Cibernética, que tem o objetivo de reforçar a proteção de dados e da dignidade da pessoa humana, ainda existe uma certa leniência com relação aos crimes virtuais.

Posteriormente, no ano de 2021, foi sancionada a Lei 14155/2021, que alterou o Código Penal, tornando mais rigorosa a punição para os crimes de violação de dispositivo informático, furto e estelionato cometidos pela internet ou por meio de dispositivos eletrônicos. As alterações de acordo com a nova lei, buscam atualizar o Código Penal mediante as mudanças que ocorrem no mundo, principalmente sobre os crimes relacionados ao ambiente digital, incluindo uma responsabilização penal mais gravosa para quem cometer delitos específicos. Além disso, o texto incrementa um aumento de pena que, antes, eram excessivamente brandas.

Pretende-se, portanto, investigar se a legislação brasileira atual tem sido suficiente para a apuração, condenação e coação de crimes cibernéticos. Apontando quais seriam as possíveis melhorias a serem feitas no regramento legal brasileiro, que resultariam em ações mais contundentes contra este tipo de crime. Ressaltando ainda os obstáculos encontrados pela polícia judiciária para apuração do delito em apreço.

Em tempo, tendo em vista o crescente número de ataques criminosos na internet, o trabalho acadêmico poderá ser de grande importância. Podendo cientificar desde aqueles que não possuem conhecimento no meio ambiente virtual, quanto aqueles que tem um certo nível de conhecimento, pois diante da realidade atual, dos novos crimes que estão surgindo, é imprescindível uma busca constante por um conhecimento maior, a fim de diminuir o alto número de vítimas dessa modalidade de delitos.

Ademais, a pesquisa foi inicialmente bibliográfica, buscando em livros, artigos, periódicos, na legislação brasileira e publicações de revistas de cunho jurídico, buscando informações que sejam o suficiente para embasar a teoria proposta na

[5] BRASIL, Lei n° 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 20 de abril de 2022, às 19h30min.

presente pesquisa. A pesquisa bibliográfica é desenvolvida com base em material que já foi elaborado, e que é constituído principalmente por livros e artigos científicos.[6]

Consideramos também que a pesquisa explicativa tem como preocupação central identificar os fatores que são determinantes para que determinados fatos ocorram. Trilha-se também por este caminho com vistas a conhecer mais profundamente a realidade do tema proposto, encaminhando-se para a razão o porquê de ainda não haver uma legislação que puna com rigidez os crimes praticados no meio virtual.[7]

Optou-se ainda pelo método dedutivo que se trata de um processo de análise de informação que propicia uma conclusão, de forma que os pesquisadores se valem da dedução para encontrar um resultado final que satisfaça o seu intento. Quis-se com esta opção, permitir que a pesquisa tenha um ponto onde o pesquisador possa também sugerir e demonstrar a partir da observação realizada com a pesquisa, possíveis ações que possibilitem melhora no tema querido.[8]

2 CONCEITOS GERAIS DE CRIME CIBERNÉTICO

Para que se inicie a discussão é necessário compreender o que é crime cibernético, portanto, neste tópico serão abordados os principais conceitos e onde essa modalidade de delito se encaixa no nosso ordenamento jurídico.

2.1 Conceito de crimes cibernéticos na legislação brasileira

Inicialmente, faz-se necessário recorrer à Lei de Introdução ao Código Penal Brasileiro, que em seu artigo 1° define crime como a infração penal que a lei comina pena de reclusão ou de detenção, isolada, alternativa ou cumulativamente com pena de multa. Também se considera crime a contravenção ou infração penal a que a lei comina, isoladamente a pena de prisão simples ou de multa, ou as duas, de maneira alternativa ou cumulativa.

---

[6] GIL, Antônio Carlos. Como elaborar projetos de pesquisa. São Paulo: Atlas, 2008, p. 81.

[7] GIL, Antônio Carlos. Como elaborar projetos de pesquisa. São Paulo: Atlas, 2008, p. 81.

[8] MENEZES, Pedro. Método Dedutivo. Ano 2020. Disponível em: https://www.todamateria.com.br/metodo-dedutivo/. Acessado em 01 de outubro de 2022, às 18h15min.

Em suma, crime é toda conduta típica, antijurídica e culpável, ou seja, é tudo aquilo que contraria ao que está disposto na lei e no ordenamento jurídico de um país. De maneira que os crimes virtuais, ou cibernéticos, são atividades ilegais realizadas valendo-se da tecnologia, com o objetivo de acessar ou comprometer sistemas computacionais.[9]

Portanto, crimes cibernéticos são condutas ilegais que são praticadas por criminosos a partir de um equipamento eletrônico, que pode ser um computador, uma rede de computadores ou celulares. Ações estas que incluem a disseminação de vírus, e que visem derrubar a infraestrutura de rede ou sites, ou ainda, que queiram dar espaço para a prática de condutas criminosas.[10]

A partir de um conceito analítico, crime cibernético é toda espécie de ação típica, antijurídica e culpável, cometida contra ou pela utilização do processamento analítico de dados ou transmissão.[11]

É importante destacar a partir desta conceituação, que os crimes que são cometidos no ambiente virtual, ou contra dados e sistemas de funcionamento de uma máquina informatizada, são consequência direta da evolução dos equipamentos de comunicação e da internet.

A maior parte dos autores jurídicos brasileiros ainda não construiu um conceito estabelecido do que é o crime cibernético, e ainda há uma certa confusão a respeito de quem seriam as vítimas dos crimes cibernéticos, como por exemplo, se acreditar que o crime seja contra a máquina, que não possui personalidade jurídica.

Para tanto, os crimes cibernéticos podem ser divididos em duas vertentes, como sendo os crimes cibernéticos puros ou próprios e os crimes cibernéticos impuros ou impróprios.

Os crimes cibernéticos são classificados como puros ou próprios e impróprios, o primeiro são aqueles praticados por computador e se realizam ou se consomem também em meio eletrônico. Neste tipo de crime, a informática, não em si, mas a

---

[9] NUCCI, Guilherme de Souza. Manual de Direito Penal. 11. ed. Rio de Janeiro, Forense, 2015, p. 210.

[10] BORTOT, Jéssica Fadundes. Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. Ano 2017. VirtuaJus, Belo Horizonte, v. 2. ISSN 1678-3425.

[11] BRASIL, Lei 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm, acessado 20 de novembro de 2022, às 00h14min.

segurança dos sistemas, a titularidade das informações, a integridade de dados, da máquina e dos periféricos, é que está sob a proteção legal.

São, portanto, crimes nos quais é necessário que o agente criminoso precise imprescindivelmente de um computador para realizar os ataques de maneira remota ou direta. Assim sendo, pode-se dizer que não estão envolvidas apenas a invasão e a captura dos dados salvos em massa, mas também a intenção ruidosa de modificar, adulterar ou destruir dados existentes no computador.[12]

Por outro lado, os crimes cibernéticos impróprios ou impuros, sabe-se que são aqueles praticados com o uso do computador, utilizando o computador como um mero instrumento para a realização do crime.

Destarte, são modalidades de delito em que o agente se utilizando-se do meio virtual, produz um resultado naturalístico, que venha a ofender o mundo físico ou o espaço real, ameaçando ou lesando outros bens, não computacionais ou diversos da informática.[13]

Em relação a conceituação dos crimes cibernéticos, levando em consideração que podem abranger a interferência no uso legal de um computador, a divulgação de material ofensivo, como por exemplo pornografia, pornografia infantil, jogos, apostas e conteúdos racistas. Também ameaçar comunicações, extorsão, falsificação, roubo de identidade, fraudes financeiras, roubo de internet e serviços telefônicos e vendas diretas, interceptação ilegal de comunicações, espionagem e lavagem de dinheiro.[14]

Diante do exposto, crimes cibernéticos são todos aqueles atos ruidosos que estão intrinsecamente ligados ao uso de dados em rede, valendo-se de computadores ou qualquer outro meio tecnológico que tenha acesso à rede mundial de computadores, visando algum malefício a outrem ou ao coletivo.

---

[12] CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. Âmbito Jurídico, Rio Grande, XV, n.99, abr. 2012. Disponível em: <http//www.ambitojuridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo _id=11529&revista_caderno=17>. Acesso em: 22 nov. 2022.

[13] CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. Âmbito Jurídico, Rio Grande, XV, n.99, abr. 2012. Disponível em: <http//www.ambitojuridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo _id=11529&revista_caderno=17>. Acesso em: 22 nov. 2022.

[14] CABETTE, Eduardo Luiz Santos. Primeiras impressões sobre a Lei nº 12.735 e o crime de invasão de dispositivo informático, 2013. Disponível em: <https://jus.com.br/artigos/23522/primeiras-impressoes-sobre-a-lei-n-12-737-12-e-o-crime-deinvasao-de-dispositivo-informátic. > Acesso em 22 de outubro de 2022.

2.2 A legislação brasileira e o sistema de proteção de dados

O Código Penal Brasileiro foi criado em 1940, quando ainda não havia a influência do advento da internet, que se deu em média trinta anos depois, e evoluiu, no Brasil particularmente, a partir da década de 90. Não havia, portanto, nenhuma lei que tipificasse ou previsse punição para os crimes virtuais. Até que em 2012, a Lei nº 12.737, trazendo a forma pela qual os crimes virtuais são cometidos e quais são as penas aplicadas aos mesmos.[15]

Destarte, a Lei nº 12.737/2012, mais conhecida como "Lei Carolina Dieckmann", tendo como estopim para a aprovação da lei o vazamento de fotos íntimas da atriz Carolina Dieckmann, que após mais de 10 anos de discussão, trouxe consigo quatro novos artigos para o ordenamento jurídico criminal. Sendo os mais relevantes a adequação do artigo 154 do Código Penal para tratar do crime de invasão digital, acrescentando consigo o artigo 154-A e 154-B e modificando os artigos 266 e 298 do Código Penal.

De frente ao estudo do presente dispositivo é notável observar que o núcleo do tipo é invadir, todavia a base do tipo penal é a conduta humana, e invadir é um verbo de conduta real, não conduta informática. O verbo mais lógico seria acessar, ou ter acesso.

Ademais, outro aspecto conveniente que deve ser observado consiste na condicionante de modo, já que a invasão deve ser mediante violação indevida de mecanismo de segurança. Portanto, é perceptível a imprecisão do legislador, que possibilita a realização do tipo penal com a violação de senha de bloqueio de tela, por exemplo, de um celular. Esse tipo penal tem dolo específico, já que o agente ao invadir tem que ter como vontade específica obter, adulterar ou destruir dados ou informações ou instalar vulnerabilidade para obter vantagem indevida.[16]

---

[15] ALVES, Marco Antônio. DINIZ, Thiago Dias de Matos. CASTRO, Viviane Vidigal de. Criminologia e cybercrimes. RECAJ – UFMG – Belo Horizonte, 2020. Livro Digital. Disponível em: https://www.conpedi.org.br/wp-content/uploads/2020/12/Livro-8-Criminologia.pdf. Acesso em 08 de setembro de 2022.

[16] NUCCI, Guilherme de Souza. Código penal comentado. 14. ed. Rio de Janeiro: Forense, 2014. p. 814.

Em 2014, foi criado o marco civil da internet que trouxe as conceituações do mundo virtual, suas formas legais de uso e estabeleceu as garantias e direitos à privacidade cibernética, que são as condições para o pleno exercício de acesso ao mundo virtual.[17]

A Lei 12.965 de 2014, mais conhecida como Marco Civil da Internet, afirma que o acesso à internet é essencial para o exercício da cidadania, e, desta maneira, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. A MCI, foi criada com intuito de suprir as lacunas no sistema jurídico em relação aos crimes cometidos no âmbito virtual.[18]

Contudo, isto ainda não basta para que crimes que atingem a dignidade da pessoa humana e causam danos patrimoniais às pessoas todos os anos sejam coibidos de maneira exemplar e tornem a não ocorrer. Há a necessidade de se debruçar sobre as possibilidades legislativas, buscando a formação de um arcabouço legal que seja capaz de movimentar o setor de informação, bem como promover uma ampla e irrestrita tipificação dos crimes, o que facilitará as condenações e persecuções penais.

Diante disto, apesar de ser o acesso à internet é uma condição de cidadania, não são todas as pessoas que têm acesso a este meio, bem como, não são todas as pessoas que possuem esses direitos assegurados de forma plena, como a garantia da inviolabilidade dos dados, sigilo do fluxo de suas comunicações e mantendo seguras também a intimidade e a vida privada, ainda mais quando se trata de investigação e punição de crimes virtuais.

Historicamente, o Brasil recebeu o advento da internet a partir de 1988, inicialmente em São Paulo e no Rio de Janeiro. Desde sua concepção tiveram algumas leis citadas no primeiro capítulo como a Constituição Federal de 1988 que trata a respeito das proteções dos dados e ainda anterior a constituição federal, como forma de prevenção a lei 7.232/84, que dispõe sobre a Política Nacional de Informática e outras providências.

---

[17] ALVES, Marco Antônio. DINIZ, Thiago Dias de Matos. CASTRO, Viviane Vidigal de. Criminologia e cybercrimes. RECAJ – UFMG – Belo Horizonte, 2020. Livro Digital. Disponível em: https://www.conpedi.org.br/wp-content/uploads/2020/12/Livro-8-Criminologia.pdf. Acesso em 08 de setembro de 2022.

[18] OLIVEIRA, Bruna Machado et al. **Cri**mes 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: <https://core.ac.uk/download/pdf/229767447.pdf>. Acessado em: 22 novembro 2022.

Em 2012 foram promulgadas as leis n° 12.735 e 12.737, que alteram o Código Penal e o Código Penal Militar e a Lei de Preconceitos, tipificando crimes no uso de sistemas eletrônicos e digitais e também os crimes contra sistemas informatizados.

Da primeira, quisemos colecionar os seguintes excertos, que indicam que deverão ser criados meios de combate a este tipo de crime pelos órgãos da polícia judiciária.

Pode-se perceber pelos excertos colacionados acima que o Poder Legislativo não se preocupou com os crimes cibernéticos em si, mas sim com um momento pelo qual o país passava, quando uma pessoa de renomada fama teve suas imagens íntimas expostas, e também visando assegurar as pessoas que se encontrarem nos cargos de poder nomeados no §5º da lei colacionada anteriormente. Os crimes praticados na internet cotidianamente continuam sendo julgados tendo como base apenas o dano causado pelos infratores.

Em suma, pode-se dizer que o problema maior relacionado aos crimes virtuais não está exatamente na ausência de uma lei que os venha punir, mas em questões técnicas, que sejam capazes de desvendar os infratores, e de quem seria a competência julgadora, tendo em vista o espaço onde o crime fora cometido.

2.3 Lei 14.155/2021

O advento da pandemia da Covid-19 obrigatoriamente tornou as pessoas mais ativas na internet, com muitos se adaptando ao meio virtual. Por efeito da doença, o isolamento social era a medida determinada, tornando a internet o principal meio de comunicação, ocorrendo assim a virtualização. Um exemplo disso é a educação a distância, estudantes que antes frequentavam as aulas presencialmente começaram a enfrentar as “aulas remotas”, do mesmo modo, muitos trabalhadores passaram a trabalhar em “*home office*”, alargando drasticamente o tempo em que ficam no ambiente virtual.

Conforme foi aumentando os usuários no meio virtual, ocorreu também um crescimento bastante expressivo de crimes virtuais, como mostra o relatório da Fortinet, (NASDAQ: FTNT), líder global em soluções amplas, integradas e automatizadas de segurança cibernética, o Brasil sofreu mais de 88,5 bilhões de

tentativas de ataques cibernéticos em 2021, que comparado ao ano anterior, houve um aumento de mais de 950%, em relação ao ano de 2020 (com 8,5 bi).[19]

Consoante com os dados levantados pelo FortiGuard Labs, laboratório de inteligência de ameaças da empresa, o Brasil ocupou o segundo lugar em número de ataques na América Latina e Caribe, atrás apenas do México (com 156 bi).

Tabela 1 – Quantitativo dos ataques de crimes cibernéticos nos países da LATAN no ano de 2021.

México	156,000,000,000
Brasil	88,500,000,000
Peru	11,500,000,000
Colômbia	11,200,000,000
Chile	9,400,000,000
Argentina	3,200,000,000
Panamá	3,200,000,000
Costa Rica	2,500,000,000
República Dominicana	2,200,000,000
Porto Rico	926,000,000
LATAM	**289,000,000,000**

Fonte: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021. Acesso em: 22 nov. 2022.

[19] Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021. Fortinet, São Paulo, 08 fev. 2022. Disponível em: <https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021>. Acesso em: 22 nov. 2022.

Desta vista, diante do exacerbado aumento de fraudes virtuais, o legislador brasileiro precisou fazer algo para dar uma freada nos crimes cometidos, a Lei n° 14.155/21 foi positivada no dia 28 de maio de 2021, por via da qual foram promovidas diversas modificações no Código Penal e, também, no Código de Processo Penal, visando reprimir os crimes de maneira mais eficaz, sendo que tais condutais são recorrentes atualmente, portanto a mencionada lei traz uma série de normas que proporcionam sanções mais graves a condutas delituosas praticadas no âmbito virtual.[20]

A nova lei corrigiu o artigo 154-A do Código Penal, excluindo a necessidade de a invasão ser fruto de “violação indevida de mecanismo de segurança”.[21]

Isto posto, caso o dispositivo, alvo da invasão, seja acessado de forma que não necessite da quebra de segurança, estará amparado pela lei, um exemplo seria o usuário deixa seu dispositivo ligado e, enquanto está ausente alguém aproveita a sua ausência e invade as informações sem a devida autorização do proprietário estaria cometendo o ilícito descrito no artigo em apreço, vale ressaltar que a consumação sucede com a efetiva invasão do dispositivo, ou seja, mesmo se o invasor não obter, adulterar ou destruir os dados da máquina.[22]

Além das regras acima explanadas, a Lei 14.155/2021 designou mais uma modalidade qualificada de furto, a qual se entende por denominar de furto qualificado pela fraude eletrônica. Isso ocorreu pela inserção do art. 155, § 4º-B no Código Penal.

Deveras, esta norma traz uma interessante hipótese de qualificadora da qualificadora. O artigo 155, § 4º, inciso II do Código Penal qualifica o furto com emprego de fraude, prevendo uma pena, para este comportamento, de 02 (dois) a 08 (oito) anos de reclusão. Por sua vez, o artigo 155, § 4º-B prevê uma pena de 04 (quatro) a 08 (oito) anos de reclusão para os furtos realizados mediante fraude eletrônica, ou seja, cometida por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de

---

[20] LAI, Sauvei; MOURÃO, Pedro Borgues. Lei 14.155/2021 dos crimes cibernéticos. 2021. Disponível em: <https://www.conamp.org.br/publicacoes/artigos-juridicos/8468-lei-14-155-2021-dos-crimes-ciberneticos.html>. Acesso em: 22 nov. 2022.

[21] PINHEIRO, Patrícia Peck. Direito Digital. Patrícia Peck Pinheiro, 2010. p. 46. 4. ed. São Paulo: Saraiva.

[22] PINHEIRO, Patrícia Peck. Direito Digital. Patrícia Peck Pinheiro, 2010. p. 46. 4. ed. São Paulo: Saraiva.

segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.[23]

Sincronicamente, a Lei n° 14.155/21 hasteou nova modalidade de estelionato, caso a fraude seja cometida com o emprego de informações concebidas pela vítima ou por terceiro induzido a erro através de redes sociais, contatos telefônicos ou envio de correio eletrônico, ou outro meio fraudulento semelhante, qualificando as penas, se comparado ao estelionato previsto no *caput* do artigo 171.[24]

Por instrumento do novel artigo 171, § 2º-A, a pena do estelionato é sobrelevada, quando a fraude empregada pelo criminoso é cometida com a utilização de informações providas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

Ulteriormente, a Lei 14.155/2021 inseriu importante modificação com relação à competência para apreciação do estelionato eletrônico, inserindo, no artigo 70 do Código de Processo Penal, o § 4º.

Em vista disso, à luz do artigo 70, § 4º do Código de Processo Penal, nos casos de estelionato por meio do ambiente virtual, a competência será determinada pelo local do domicílio da vítima, e, em casos de pluralidade de vítimas, pela prevenção.

3 COMPARATIVO DA LEGISLAÇÃO CONTRA A PRÁTICA DE CRIMES VIRTUAIS NO MUNDO COM A O NOSSO ORDENAMENTO JURÍDICO

É de conhecimento geral que os crimes cibernéticos têm afetado todo o mundo, portanto, neste capítulo será levantado uma comparação da nossa legislação brasileira com as legislações dos outros países.

3.1 Medidas impostas pelo brasil para evitar crimes virtuais

[23] BRASIL, Lei 14.155, de 27 de maio de 2021. Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm#art1, acessado 20 de abril de 2022, às 19h50min.

[24] BRASIL, Lei 14.155, de 27 de maio de 2021. Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm#art1, acessado 20 de abril de 2022, às 19h50min.

O crime virtual, apesar de na atualidade ser algo “usual” ainda é uma novidade para os meios de proteção existentes tanto no Brasil quanto no mundo, e apenas recentemente tem sido criado meios específicos de registrar este tipo de crime. A criação de uma legislação específica, criada para lidar com a relação de computadores e processos conexos a estes deve ser feita conjuntamente com um processo de conscientização da sociedade, onde estão as vítimas dos crimes virtuais, como também aumentar a proteção ao consumidor, que está cada vez mais inseguro e relutante de adquirir produtos na internet, por exemplo, pelo receio de ter seus dados financeiros expostos de maneira inadequada.[25]

O Brasil criou o Marco Civil da Internet (Lei n° 12.965/2014) que regula determinados princípios e garantias legais para quem se utiliza da internet, e que podem servir de base para a criação de relatórios estatísticos sobre crimes que tenham sido denunciados e apurados, aumentando a capacidade da polícia de buscar compreender melhor sobre a extensão desta corrente criminosa, o que tem acontecido de maneira mais acentuada nas últimas duas décadas.[26]

Com a promulgação da Lei Geral de Proteção de Dados o Brasil se inseriu num contexto planetário de países que estão se adequando melhor no que tange à proteção de dados e da privacidade dos usuários da internet, bem como das formas de utilização destes dados que de uma forma ou de outra estão expostos na rede mundial de computadores.

Na fase anterior a promulgação da LGPD, o dispositivo aplicado a proteção dos dados pessoais encontrava-se de maneira esparsa em nossa CF e em leis como Código Civil em seus artigos 20 e 21, no Código de Processo Penal (art. 201 § 6) e no Marco Civil da Internet (Lei n° 12 965/2014). Por sua vez, a introdução da LPGD estreou no país um sistema normativo protetivo de dados pessoais, pois esta norma constitui princípios que norteiam os direitos dos titulares de dados pessoas, fundamentos e obrigações.[27]

---

[25] CASTRO, Suelen. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em 01 de outubro de 2022.

[26] BRASIL, Lei 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm, acessado 20 de novembro de 2022, às 00h14min.

[27] VASCONCELOS CONI JUNIOR, Vicente; PAMPLONA FILHO, Rodolfo. A lei geral de proteção de dados e seus reflexos nas relações jurídicas trabalhistas. *In*: MIZIARA, Raphael; MOLLICONE, Bianca;

3.2 Medidas impostas pela união europeia para evitar crimes virtuais

Tendo em vista o crescimento dos crimes virtuais, a União Europeia tem adotado diversos sistemas de proteção a fim de coibir o aumento e facilitar as investigações para chegar nas organizações criminosas.

É de suma importância ressaltar a criação da Convenção de Budapeste, essa que consiste em um ordenamento desenvolvido pelo Conselho da Europa em 2002, em que seu intuito girava em torno da proteção da sociedade contra a criminalidade no ciberespaço. De início, a Convenção de Budapeste promovia a escolha de uma legislação comum que objetivasse uma maior cooperação entre os Estados da União Europeia, contudo atualmente encontra-se aberta à assinatura por qualquer país que a deseja, tendo em vista que os crimes cibernéticos atingem todos os territórios do mundo.[28]

No âmbito do Direito Internacional, existe o a modalidade Uniforme, a qual é utilizada por quase todos os países do mundo, que ocorre quando coincidem os direitos primários entre ordenamentos, seja ela por ter a mesma origem, ou por sofrerem influências análogas, ou, ainda, quando países adotam sistemas jurídicos clássicos total ou parcialmente, de outros Estados.[29]

Por outro lado, há uma proposição a favor da segurança jurídica do Direito Brasileiro em vista da tipificação dos crimes cibernéticos, configura-se no fato do Brasil abraçar a Convenção de Budapeste, tendo em vista que, o conteúdo dos projetos de leis, que se encontram há anos sob o julgamento do Congresso Nacional, é semelhante aos tratados pela referida Convenção.[30]

Não obstante, mesmo que existam convenções e tratados internacionais que se destinam exclusivamente a coibir redes criminosas já bem estabelecidas, ou

---

PESSOA, André. Reflexos da LGPD no direito e no processo do trabalho. 1. ed. São Paulo: Thomson Reuters, 2020. cap. 4, p. 82.

[28] FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. REVISTA DA FACULDADE DE DIREITO DA UFMG, 2013, 2013.62: 139-178.

[29] FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. REVISTA DA FACULDADE DE DIREITO DA UFMG, 2013, 2013.62: 139-178.

[30] FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. REVISTA DA FACULDADE DE DIREITO DA UFMG, 2013, 2013.62: 139-178.

mesmo criminosos independentes que estejam agindo através das fronteiras entre os países, estes dispositivos de coação não têm conseguido impetrar o patamar que estes crimes têm conseguido alcançar, dada a sua larga escala de atuação e pelo fato de não haver distância física que os distancie das pessoas.

É dizer que pela velocidade em que os crimes acontecem, a legislação aplicada ainda caminha a passos lentos, o que deveria ser o contrário, a legislação deveria se adiantar ao criminoso, não lhe dando espaço de atuação como acontece atualmente.

Ordinariamente, o papel das agências multinacionais como a INTERPOL, nunca foi tão necessário, uma vez que a atuação de muitos países, inclusive o Brasil, não tem conseguido acompanhar a evolução dos crimes cibernéticos. São necessários acordos internacionais bilaterais, onde os países deverão cooperar para manter a internet como um ambiente mais hostil para os criminosos. [31]

Destarte, a compatibilidade de atividade criminosa com essas mudanças globais é ilustrada pela expansão e convergência dos negócios rentáveis do contrabando de seres humanos e pornografia, com o desenvolvimento da comunicação e do comércio ilícito.[32]

De modo que no mesmo ambiente virtual caminham dois mundos opostos, sendo eles a globalização cada vez mais pungente, que movimento um comércio multimilionário de bens e serviços, como também um ambiente hostil no qual as pessoas de bem se sentem temerosas pelas práticas criminosas que ali acontecem.

4 DA INVESTIGAÇÃO

As investigações dos crimes virtuais são realizadas por meio de uma análise técnica, na qual irá verificar tanto a autoria quanto a materialidade dos crimes perpetrados por meio de uma rede que interliga os computadores. Entretanto, ao analisarmos casos de crimes cibernéticos, fica nítido a dificuldade de concluir de fato, o agente que praticou o delito em tela, tendo em vista que os crimes praticados no

[31] RODRIGUES, Juliana. CRUZ, Diego. Crimes cibernéticos e a falsa sensação de impunidade**.** Disponível em: http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso em 18 de novembro de 2022.

[32] SILVA, Eduardo Soares da. BARAKAT, Najah Jamal Daakour. **Crimes Cibernéticos**. Disponível em: https://www.conpedi.org.br/wp-content/uploads/2020/12/Livro-8-Criminologia.pdf. Acesso em 18 de novembro de 2022.

espaço cibernético não deixam rastros, facilitando assim, o anonimato do agente que pratica tal ato, além de que a proporção que algo pode atingir na rede de internet é ilimitada.

4.1 Identificação da autoria delitiva

Para a identificação do agente que perpetra os delitos no ambiente virtual, são utilizadas das mais diversas ferramentas na investigação, dentre elas as análises de Logs (registros de login) e servidores, interceptação de correspondência eletrônica, análise de pacotes de dados, entre outros.

Concernente aos meios de produção de provas deve esclarecer que os crimes cibernéticos no ordenamento jurídico brasileiro, admite que estas sejam produzidas por todos meios lícitos, o que é importante descrever que podem ser utilizadas provas documentais, prova testemunhal, prova pericial. Todas estas hipóteses podem ser admitidas e utilizadas para a caracterização da materialidade e autoria dos crimes cibernéticos, contudo, em se tratando da modalidade cibernética merece especial atenção a prova pericial.[33]

Especialmente, nas investigações sobre os crimes virtuais, em decorrência da facilidade da adulteração dos dados, as provas necessitarão passar por perícias técnicas rigorosas para serem aceitas nos processos, de forma a garantir a validade e integridade da materialidade. Esse é o objetivo da computação forense, o de provar os fatos ocorridos de forma mais sucinta o possível.

A computação forense é um tipo de perícia qualificada pela inspeção cientifica e sistemática em computadores, modo que através da coleta de provas digitais, busca chegar a conclusões sobre o fato investigado, devendo ser feita uma reconstituição dos eventos encontrados, possibilitando determinar se a aparelho eletrônico analisado foi utilizado para a realização ou não de condutas ilícitas.

Alguns dos exemplos de indícios que podem auxiliar na fase investigatória dos crimes virtuais, são os arquivos de imagem de pornografia infantil, mensagens eletrônicas com ameaças e chantagens, arquivos com informações incriminatórias ou dados subtraídos.[34]

---

[33] VIANNA, Túlio; MACHADO, Felipe. Crimes informáticos. Belo Horizonte: Fórum, 2013. p. 74.

[34] PINHEIRO, Patrícia Peck. Direito Digital. 5. ed. rev. atual. São Paulo: Saraiva, 2013, p. 38.

Os cibercrimes proporcionam dificuldades assombrosas para sua comprovação, se por um lado há uma enorme facilidade na prática do delito por meio virtual, por outro lado, a verificação dos vestígios exige uma qualificação técnica específica, que nem sempre está disponível em todos os lugares de consumação dos crimes.

Perante a escassez de técnica e recursos humanos nas polícias judiciárias no que diz respeito à investigação e punição do criminoso cibernético, os exames periciais transformam-se em uma ferramenta eficiente na produção de prova no crime cibernético.[35]

Assim sendo, o principal desígnio do processo de investigação é localizar dados úteis, necessários e pontuais, e auxiliar o investigador a não perder tempo com o que está disponível, usufruindo das fontes abertas e fontes fechadas.

As fontes abertas são aquelas que não possuem entraves, ou seja, que estão disponíveis ao público em geral e não exige nenhuma espécie de restrição de acesso. Os dados ou informações de acesso livre podem ser encontrados nos mais variados meios de comunicação, redes sociais, livros, softwares e, principalmente, intensificados pela internet.

Destarte, as fontes Abertas, são dados ou informações acessíveis a qualquer pessoa, ou seja, livres de sigilo, que podem auxiliar a atuação do policial que realizará a investigação criminal ou o agente de inteligência que produzirá um determinado tipo de conhecimento, de modo que, a utilização de fontes abertas para na persecução penal deve ser incitada, uma vez que permite extrair, de forma célere, informações que estejam disponíveis sobre alvos da investigação.[36]

O emprego de fontes abertas tem sido exitoso em diversas ocasiões, dentre elas, informações disponíveis em perfis de redes sociais do delituoso e da vítima, sobretudo em casos de homicídio, softwares e aplicações de internet gratuitas que auxiliam na premeditação de operações policiais, consultas aos sites de tribunais sobre dados úteis a respeito do investigado e uso de alertas para localizar foragidos em outros estados.

---

[35] MALAQUIAS, Roberto Antônio Darós. Crime Cibernético e Prova: a investigação criminal em busca da verdade. Curitiba: Juruá, 2012, p. 72.

[36] JORGE, Higor Vinícius Nogueira. Tratado de Investigação Criminal Tecnológica. São Paulo: JusPodivm, 2020. p. 153.

Por sua vez, as fontes fechadas são aquelas que estão protegidas e, muitas vezes, exigem permissão do poder judiciário, para serem acessadas. Comumente possuem, sigilo constitucional, limitação ao exercício do poder punitivo do Estado, garantias do cidadão e direitos fundamentais, restrição de acesso e relativização dos direitos fundamentais do investigado, além da autorização judicial, à luz do artigo 5°, inciso XII, CF.

4.2 Dificuldades encontradas na investigação de crimes virtuais

Primeiramente, para a análise das etapas da investigação dos crimes da modalidade virtuais, é necessário haver uma denúncia de tal tipo penal, para que em seguida possa ser iniciado e rastreado o meio utilizado para a prática do delito, pois para cada tipo há um caminho diferente a ser seguido.

As proeminências no mundo virtual são consideradas provas da ocorrência de um crime e são associadas com o lugar onde o crime teria sido praticado (nesse caso, na internet). Alguns dos exemplos de evidências digitais, são os logs (registros de login), amostras de registros de sessões e registros de navegação da internet.[37]

Posto isso, são inúmeras as dificuldades que os órgãos do Ministério Público, da Polícia e do Judiciário Brasileiro encontram para punir os agentes cibercriminosos. Uma dessas dificuldades encontradas para punir os infratores dos crimes praticados no ambiente virtual, ocorre pela ausência de norma que caracteriza os crimes e os classifica em uma ordem, além de fundamental a comprovação da autoria e da materialidade, ou a existência de fortes indícios de que o sujeito praticou o crime, assim como também a falta de tecnologia e de mão de obra especializada para o combate aos cibercrimes.

Outro fato que dificulta a investigação dos crimes cibernéticos, em razão que a polícia ao realizar as investigações criminais, em primeiro instante identifica a forma que o crime aconteceu, o local que ocorreu, em segundo momento busca localizar o endereço de IP (número que identifica o dispositivo na rede), após a identificação do IP do infrator, o setor de investigação da polícia entra em contato com a empresa responsável que disponibiliza o número na rede, e só assim identifica o criminoso.

[37] WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos: ameaças e procedimentos de investigação. 2 ed. Rio de Janeiro: Brasport, 2013. p. 130.

Entretanto, não se pode olvidar que algumas empresas de informação, até mesmo com a autorização da justiça, se recusam a prestar informações quanto aos usuários investigados, o que faz retardar e perder provas essenciais no processo de investigação.

Ademais, quando informado, os problemas de identificação de autoria não dizem respeito apenas à identificação do computador de onde se originou o fato ilícito ou do responsável por tal computador, mas passa a ser à identificação da pessoa que agiu com a intenção de praticar o ato ilícito ou que contribui para prática de tal conduta.

Outrossim, para ter a obtenção dos dados de identificação do IP, se faz necessário a autorização do Juiz para realizar as investigações e comunicações com as empresas que armazenam informações da localização dos criminosos, tendo em vista que elas têm o respaldo que protege a privacidade e os dados dos usuários, ocasionando uma maior demora para a obtenção de provas.

Conseguinte, a identificação do agente é ainda mais dificultada, pois quando se considera que a localização através do endereço IP permite a identificação de um computador e não, efetivamente, do autor do delito. Na realidade, a grande dificuldade decorrente da identificação da autoria está em correlacionar o computador e o sujeito que o opera em determinado espaço de tempo.

Em vista disto, as informações providas pelos provedores são de grande valia, levando em conta que quando ocorre a conexão de um computador ou aparelho similar a Internet lhe é atribuído um número de IP (Internet Protocol), cujo qual é exclusivo para aquele usuário e permite sua identificação e localização.[38]

Sobretudo, há de se ressaltar o pouco efetivo de profissionais especializados para agilizar nas investigações, empresas de informação que não colaboram com o judiciário, como dito acima, leis fundamentais no nosso ordenamento jurídico brasileiro, apesar de ter evoluído nas duas últimas décadas, ainda encontra-se algumas lacunas sob ótica dos crimes virtuais.

5 CONCLUSÃO

[38] WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos: ameaças e procedimentos de investigação**.** 2 ed. Rio de Janeiro: Brasport, 2013. p. 54.

Muito se fala dos crimes praticados na internet, mas pouco se estuda sobre os mesmos a fim de se traçar um parâmetro ideal de suas implicações jurídicas e da forma que estes crimes assumem perante o ordenamento jurídico brasileiro e internacional, bem como, de que maneira são investigados, tratados e punidos pelas autoridades legais do país.

Sabe-se que o conceito de crime cibernético ainda está em construção, mas de uma maneira ou de outra, ainda se é possível estabelecer meios ideais para a proteção de dados e de pessoas que estão continuamente utilizando a internet como meio de diversão, negócio ou educação.

Pelo fato de a legislação brasileira ainda estar sendo construída nesse sentido, é que ainda existe uma sensação de impunidade para os criminosos que praticam este tipo de crime. Todavia, isto não se deve apenas ao fato de inexistir um arcabouço legal acerca da temática, mas também pela dificuldade da polícia e do poder judiciário em encontrar o criminoso, identificando a autoria e a materialidade dos crimes.

Há que se dizer, que o Código Penal brasileiro já abarca algumas tipificações e punições de crimes que venham a ser cometidos contra pessoas ou patrimônio de outrem por via da internet. As leis que foram aprovadas nos últimos dez anos não fizeram tanto efeito no ordenamento jurídico, uma vez que não possuem a profundidade que se esperava das leis que regem um assunto tão complexo como os cibercrimes.

Faz-se necessário, portanto, a utilização da interpretação extensiva que, ao contrário da analogia, busca a verdadeira finalidade da norma de forma que a lei alcance os casos advindos dos crimes cibernéticos, como por exemplo, utilizar-se dos artigos que tratam dos crimes de furto, dano e estelionato, visando a proteção de danos a dados informáticos.

Em suma, deve-se considerar que a intenção do legislador é de proteger o utilizador da internet e buscar a punição dos infratores, todavia, é necessário que se façam as adequações necessárias, inserindo na norma termos técnicos específicos, como também dirimir melhor quais podem ser os danos gerados às vítimas.

Deve ainda considerar agregar estratégias de soluções no combate aos crimes cibernéticos seria a elaboração de termos de cooperação para suprir as lacunas da lei, como a criação de canais de denúncias e banco de dados únicos para o recebimento das comunicações, criação de delegacias especializadas com maior capacitação, efetivo e estrutura, concepção de grupos especializados nas unidades

das Procuradorias da República e por fim, treinamento e capacitação dos setores periciais.

Dessa forma, há uma necessidade de conscientização dos usuários da internet para que menos pessoas caiam nos golpes dos criminosos, lecionando sobre como se proteger dos ataques virtuais. Grandes partes da população podem até conhecer a internet e desfrutar de suas mil funcionalidades, no entanto não entendem a proporção dos riscos que pode estar sofrendo ao receber um simples e-mail ou acessar um link para um site.[39]

Por fim, foi concluído que as maiores parábolas no processo de investigação para os crimes na internet decorrem da falta de equipamentos e softwares atualizados para esse tipo de atividade e pessoas capacitadas e especializadas para rastrear os fatos, e um contato mais direto com o poder judiciário para a concessão rápida das autorizações investigatórias, contribuindo assim para o início do procedimento penal e se chegar a uma sanção para os indivíduos que cometem o cibercrime. Além do mais, tamanha ausência do Estado em repor o efetivo dos agentes de segurança nas polícias judiciárias, bem como treinar os que lá estão.

[39] WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos: ameaças e procedimentos de investigação**.** 2 ed. Rio de Janeiro: Brasport, 2013. p. 209.

REFERÊNCIAS

ALVES, Marco Antônio. DINIZ, Thiago Dias de Matos. CASTRO, Viviane Vidigal de. Criminologia e cybercrimes. RECAJ – UFMG – Belo Horizonte, 2020. Livro Digital. Disponível em: https://www.conpedi.org.br/wp-content/uploads/2020/12/Livro-8-Criminologia.pdf. Acesso em 08 de setembro de 2022, às 22h00min.

BORTOT, Jéssica Fadundes. Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. Ano 2017. VirtuaJus, Belo Horizonte, v. 2. ISSN 1678-3425, p. 141.

BRASIL, Ministério das Relações Internacionais. Brasil é convidado a aderir à Convenção do Conselho da Europa contra a criminalidade cibernética. Disponível em: https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica. Acesso em 08 de setembro de 2022, às 22h15min.

BRASIL, Lei n° 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 20 de abril de 2022, às 19h30min.

BRASIL, Lei 14.155, de 27 de maio de 2021. Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm#art1, acessado 20 de abril de 2022, às 19h50min.

GIL, Antônio Carlos. Como elaborar projetos de pesquisa. São Paulo: Atlas, 2008, p. 81.

NUCCI, Guilherme de Souza. Manual de Direito Penal. 11. ed. Rio de Janeiro, Forense, 2015, p. 210.

NUCCI, Guilherme de Souza. Código penal comentado. 14. ed. Rio de Janeiro: Forense, 2014. p. 814.

SILVA, Eduardo Soares da. BARAKAT, Najah Jamal Daakour. Crimes Cibernéticos. Disponível em: https://www.conpedi.org.br/wp-content/uploads/2020/12/Livro-8-Criminologia.pdf. Acesso em 01 de outubro de 2022, às 00h10min.

CABETTE, Eduardo Luiz Santos. Primeiras impressões sobre a Lei nº 12.735 e o crime de invasão de dispositivo informático, 2013. Disponível em: https://jus.com.br/artigos/23522/primeiras-impressoes-sobre-a-lei-n-12-737-12-e-o-crime-deinvasao-de-dispositivo-informátic. Acesso em 01 de outubro de 2022, às 19h21min.

CASTRO, Suelen. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em 01 de outubro de 2022, às 20h10min.

MENEZES, Pedro. Método Dedutivo. Ano 2020. Disponível em: https://www.todamateria.com.br/metodo-dedutivo/. Acesso em 01 de outubro de 2022, às 21h30min.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. Âmbito Jurídico, Rio Grande, XV, n.99, abr. 2012. Disponível em: http//www.ambitojuridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17>. Acesso em: 22 nov. 2022, ás 21h00min.

BRASIL, Lei 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm, acessado 20 de novembro de 2022, às 00h14min.

OLIVEIRA, Bruna Machado et al. Crimes virtuais e a legislação brasileira. (Re) Pensando o Direito - Rev. Do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13 (2017). Disponível em: <https://core.ac.uk/download/pdf/229767447.pdf>. Acessado em: 22 novembro 2022.

Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021. Fortinet, São Paulo, 08 fev. 2022. Disponível em: <https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021>. Acesso em: 22 novembro de 2022.

LAI, Sauvei; MOURÃO, Pedro Borgues. Lei 14.155/2021 dos crimes cibernéticos. 2021. Disponível em: <https://www.conamp.org.br/publicacoes/artigos-juridicos/8468-lei-14-155-2021-dos-crimes-ciberneticos.html>. Acesso em: 22 nov. 2022.

PINHEIRO, Patrícia Peck. Direito Digital. Patrícia Peck Pinheiro, 2010. p. 46. 4. ed. São Paulo: Saraiva.

VASCONCELOS CONI JUNIOR, Vicente; PAMPLONA FILHO, Rodolfo. A lei geral de proteção de dados e seus reflexos nas relações jurídicas trabalhistas. *In*: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. Reflexos da LGPD no direito e no processo do trabalho. 1. ed. São Paulo: Thomson Reuters, 2020. cap. 4, p. 82.

FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. REVISTA DA FACULDADE DE DIREITO DA UFMG, 2013, 2013.62: 139-178.

RODRIGUES, Juliana. CRUZ, Diego. Crimes cibernéticos e a falsa sensação de impunidade**.** Disponível em: http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso em 18 de novembro de 2022.

VIANNA, Túlio; MACHADO, Felipe. Crimes informáticos. Belo Horizonte: Fórum, 2013. p. 74.

PINHEIRO, Patrícia Peck. Direito Digital. 5. ed. rev. atual. São Paulo: Saraiva, 2013, p. 38.

MALAQUIAS, Roberto Antônio Darós. Crime Cibernético e Prova: a investigação criminal em busca da verdade. Curitiba: Juruá, 2012, p. 72.

JORGE, Higor Vinícius Nogueira. Tratado de Investigação Criminal Tecnológica. São Paulo: JusPodivm, 2020. p. 153.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos: ameaças e procedimentos de investigação. 2 ed. Rio de Janeiro: Brasport, 2013. p. 130.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos: ameaças e procedimentos de investigação**.** 2 ed. Rio de Janeiro: Brasport, 2013. p. 54.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos: ameaças e procedimentos de investigação**.** 2 ed. Rio de Janeiro: Brasport, 2013. p. 209.

- Os crimes cibernéticos são condutas ilícitas tipificadas em lei como crime, tendo como característica essencial o emprego da internet como meio de serem praticadas. A maior parte dos autores jurídicos brasileiros ainda não construiu um conceito estabelecido do que é o crime cibernético, alguns deles os classificam em duas vertentes: