ESCOLA SUPERIOR ASSOCIADA DE GOIÂNIA – ESUP

COORDENAÇÃO DO CURSO DE DIREITO

MARCIA FLAVIA TEIXEIRA BARROSO

O ALCANCE DA LEGISLAÇÃO BRASILEIRA NA RESPONSABILIZAÇÃO PENAL E OS OBSTÁCULOS PRESENTES NA INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS NA CIDADE DE GOIÂNIA-GO

GOIÂNIA

2022

MARCIA FLAVIA TEIXEIRA BARROSO

O ALCANCE DA LEGISLAÇÃO BRASILEIRA NA RESPONSABILIZAÇÃO PENAL E OS OBSTÁCULOS PRESENTES NA INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS NA CIDADE DE GOIÂNIA-GO

Artigo científico apresentado à Banca Examinadora do curso de Direito da Escola Superior Associada de Goiânia-ESUP, para Trabalho de Conclusão de Curso, requisito imprescindível à obtenção do grau de Bacharel em Direito.

Orientador: Professor Cristiano Moraes de Lemos

GOIÂNIA

2022

FACULDADE ESUP

ATA DA SESSÃO DE AVALIAÇÃO DE TCC

O trabalho final intitulado **"O ALCANCE DA LEGISLAÇÃO BRASILEIRA NA RESPONSABILIZAÇÃO PENAL E OS OBSTÁCULOS PRESENTES NA INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS DE GOIÂNIA - GO"**, elaborada pelo (a) aluno(a) **MARCIA FLAVIA TEIXEIRA BARROSO**, matrícula nº **1610ESDIRM012**, foi apresentado em sessão pública de avaliação, em **16** de **dezembro** de **2022**, às **09:00**, perante a Banca Examinadora, formada pelos membros que abaixo assinam, tendo obtido aprovação com nota 10,0 e sido julgada e aprovada para suprir a exigência parcial à obtenção de grau de Bacharel em **Direito**, em conformidade com a Resolução CNE/CES nº 9 e regulamento interno de TCC da Faculdade ESUP.

Goiânia (GO), **16 de dezembro de 2022**.

Prof.(a) **Cristiano Moraes de Lemos**, Esp.
Orientador(a)

Prof. (a) **Wanessa Silveira Costa**, Esp.
Membro da Banca

Prof. (a) **Danielle Oliveira e Souza**, Esp.
Membro da Banca

RESUMO

O presente trabalho irá discorrer sobre os Crimes Cibernéticos praticados âmbito mundial, os procedimentos adotados pelos órgãos de investigação criminal, os obstáculos enfrentados na busca dos infratores e a eficácia do ordenamento jurídico brasileiro no que se refere às punições dos atos ilícitos praticados pelos transgressores virtuais. Para tanto, será utilizado o método indutivo como metodologia de pesquisa, utilizando a observação e análise dos dados contidos em documentos e na legislação brasileira para, posteriormente, realizar a comprovação dos fatos estudados. Além disso, um questionário será elaborado e remetido aos órgãos de investigação na cidade de Goiânia para que se consiga efetuar o levantamento de dados quantitativos acerca dos principais crimes cibernéticos cometidos, e, em seguida, proceder à coleta e análise dos elementos apontados pela pesquisa. O referencial teórico a ser utilizado baseou-se na leitura de duas obras que abordam os tipos de fraudes cibernéticas, a maneira pela qual a legislação brasileira tipifica as infrações e de que forma os órgãos de investigação conduzem os procedimentos para apurar os fatos e punir os criminosos. Dessa maneira, será possível avaliar se a legislação brasileira é capaz de alcançar o avanço dos crimes cibernéticos, diante da celeridade tecnológica e do especializado conhecimento dos infratores do ambiente virtual.

PALAVRAS-CHAVE: Crimes Cibernéticos; Investigação Criminal; Legislação Brasileira.

ABSTRACT

The present work will discuss the Cyber Crimes practiced worldwide, the procedures adopted by the criminal investigation bodies, the obstacles faced in the search for offenders and the effectiveness of the Brazilian legal system with regard to the punishment of illicit acts practiced by virtual transgressors. Therefore, the inductive method will be used as a research methodology, using the observation and analysis of data contained in documents and Brazilian legislation to later carry out the verification of the facts studied. In addition, a questionnaire will be prepared and sent to the investigative bodies in the city of Goiânia so that it is possible to collect quantitative data about the main cyber crimes committed, and then proceed to the collection and analysis of the elements pointed out by the research. The theoretical framework to be used was based on the reading of two works that approach the types of cyber fraud, the way in which the Brazilian legislation typifies the infractions and how the investigative bodies conduct the procedures to investigate the facts and punish the criminals. In this way, it will be possible to assess whether Brazilian legislation is capable of achieving the advancement of cyber crimes, given the speed of technology and the specialized knowledge of offenders in the virtual environment.

Keywords: Ciber crimes; Criminal Investigation; Brazilian Law.

SUMÁRIO

INTRODUÇÃO

O século XXI caracteriza-se pela ampliação de diferentes formas de conexão entre pessoas e máquinas, utilizando de diferentes recursos tecnológicos, como redes sociais, aplicativos, chats e diversos outros meios de comunicação possíveis com o advento da internet. Não existem, atualmente, fronteiras fisicamente estabelecidas que consigam conter o fluxo de informações, serviços, mercadorias e pessoas, já que o avanço tecnológico veio com o propósito de diminuir a distância entre os indivíduos, permitir a comunicação de maneira célere e eficiente, por intermédio de diferentes plataformas de comunicação e facilitar a realização de atividades corriqueiras, com o emprego de dispositivos móveis, como *notebooks*, celulares e *tablets.*

As grandes transformações proporcionadas pela tecnologia trouxeram vários benefícios para toda a sociedade. Entretanto, há diversos aspectos negativos que vem ocasionar danos, às vezes, até irreversíveis para as pessoas, quando tratam de situações que envolvam a privacidade e intimidade. A internet afeta a mente, o pensamento, o comportamento, atitudes e valores dos indivíduos, despertando em alguns um sentimento maldoso, que levam a praticar as piores atrocidades.

Os crimes cibernéticos, cometidos utilizando-se de computadores ou dispositivos eletrônicos conectados pela internet, podem gerar danos terríveis aos indivíduos e a seus patrimônios. Tais crimes são realizados em toda parte do mundo e, com a popularização de equipamentos utilizados para acessar a rede mundial de computadores, novas ameaças se manifestam. A preocupação com a segurança torna-se cada vez maior, uma vez que computadores são invadidos, informações pessoais são obtidas para fins ilícitos e as pessoas tornam-se reféns dos infratores virtuais.

Nesse sentido, por se tratar de um tema novo e em evidência, houve a necessidade de se entender o procedimento de investigação dos delitos virtuais, os mecanismos pelos quais os indivíduos conseguem detectar que foram vítimas, e quais os crimes mais comuns praticados na cidade de Goiânia. Além disso, serão apresentados os obstáculos encontrados no procedimento de investigação dos crimes cibernéticos, os dispositivos infraconstitucionais existentes no ordenamento jurídico que cuidam do tema em tese, se tais instrumentos legais são suficientes e tem efeitos positivos no sentido de proteger os indivíduos e empresas que se encontram vulneráveis quanto a tais práticas delitivas.

Quanto ao referencial teórico utilizado, além da leitura de diversos artigos científicos, foram utilizadas duas obras principais que tratam dos tipos de fraudes cibernéticas. [1]

No que tange ao Capítulo 1, será discorrido sobre o surgimento da internet, quando foi disponibilizada no Brasil e como ocorreu sua evolução no decorrer dos anos. Será realizada uma abordagem conceitual de alguns termos mais utilizados na área da tecnologia da informação no que tange aos crimes cibernéticos, as diferentes formas pelas quais esses delitos são praticados e como essas condutas afetam a intimidade, a honra e a privacidade dos indivíduos.

O Capítulo 2 trará informações acerca da legislação adotada no Brasil para penalizar os responsáveis pelas práticas na internet. As normas tratadas são: a Lei nº 12.737/2012 (Lei Carolina Dieckman), que tem por finalidade a punição dos invasores de dispositivos informáticos, que obtém mídias e as divulgam na internet; a Lei nº 12.965/2014 (Marco Civil da Internet), que estabelece os princípios, os direitos e deveres para o uso da internet no Brasil e o Código Penal Brasileiro, norma maior no ordenamento jurídico, que contempla uma grande quantidade de regras sistemáticas de cunho punitivo.

O Capítulo 3 irá abordar os procedimentos de investigação adotados pelas autoridades policiais para identificar os responsáveis pelos atos ilícitos, analisar os principais tipos penais praticados na cidade de Goiânia, no que tange aos crimes cibernéticos, e mencionar os mecanismos realizados pelos órgãos de investigação para colher as provas e providenciar o envio das informações ao Poder Judiciário para que haja a devida punição aos infratores.

Pelo estudo realizado, foi verificado que os mecanismos de investigação dos crimes cibernéticos são eficazes, entretanto, a estrutura dos órgãos de Polícia precisa ser mais robusta para que haja mais celeridade na identificação dos infratores. As leis existentes no ordenamento jurídico brasileiro abarcam uma grande quantidade de crimes praticados e já contemplam sanções mais severas aos delitos cibernéticos.

[1] As publicações "Ameaças e procedimentos de investigação", dos autores Emerson Wendt e Higor Vinicius Nogueira Jorge, e 'O impacto da Tecnologia no Direito', de Pedro Augusto Zaniolo detalham os tipos de crimes virtuais comumente praticados no Brasil, abordam os métodos de investigação utilizados pelos delegados de polícia e peritos criminais, apontam alguns documentos utilizados pelas autoridades policiais para registrar e dar andamento ao processo dos delitos cibernéticos, além de indicar a legislação brasileira empregada na responsabilização dos transgressores.

1 ASPECTOS HISTÓRICOS E CONCEITUAIS DOS CRIMES CIBERNÉTICOS

1.1 HISTÓRICO E EVOLUÇÃO DA INTERNET

A revolução da conectividade no mundo iniciou a partir do lançamento do primeiro satélite artificial da história da humanidade realizado pela Rússia em outubro de 1.957– o Sputnik. Alguns meses depois, com o objetivo de reagir ao avanço tecnológico russo, o presidente americano Dwight S. Eisenhower anunciava a criação da Agência de Investigação de Projetos Avançados (ARPA – Advanced Research Project Agency), que tinha como propósito acelerar o desenvolvimento tecnológico do país e coordenar atividades relacionadas com o espaço e satélites (WENDT, 2021, p. 5).

Após alguns anos, houve a necessidade de se criar uma rede que fosse capaz de integrar computadores distantes uns dos outros e que, por meio desta integração, houvesse a comunicação de dados. Assim, "nascia" a ARPANET[2], a primeira rede de computadores construída entre a Universidade da Califórnia – Los Angeles e de Santa Bárbara, Universidade de Utah e Instituto de Pesquisa de Stanford, em Dezembro de 1969. Contudo, somente na década de 80 a ARPANET se disseminou pelos Estados Unidos, o que possibilitou a interligação de computadores entre as universidades, governo e órgãos militares norte-americanos. E, finalmente, em 1991 surgia o *World Wide Web*[3], um espaço que permite a troca de informações por meio da estrutura da internet. Deste modo, surgem os navegadores utilizados para que os usuários possam realizar buscas na no meio virtual.

A década de 1990 teve um papel fundamental para toda a sociedade mundial, já que foi possível o intercâmbio entre diferentes culturas e a "democratização da informação". O acesso à internet, inicialmente, era restrito a uma elite, já que poucas famílias podiam adquirir equipamentos e dispositivos eletrônicos nesta época, devido ao custo alto e por não conseguirem usar, já que não tinham conhecimento das ferramentas disponíveis.

No Brasil, em 1.965 foram criados o Serviço Federal de Processamento de Dados e a Empresa Brasileira de Telecomunicações – Embratel. Em 1.972 foi fabricado o primeiro computador brasileiro, mas somente no ano de 1.992 foi implementada a

[2] ARPANET: Rede da Agência de Pesquisas em Projetos Avançados - foi a primeira rede de computadores, construída em 1969 como um meio robusto para transmitir dados militares sigilosos e para interligar os departamentos de pesquisa por todo os Estados Unidos. (WENDT, 2021)

[3] World Wide Web: Termo também conhecido como www, é um serviço de informação que funciona sobre a Internet e assenta numa estrutura baseada em documentos hipertexto interligados. (NUNES, 2012)

primeira rede de computadores conectada à Internet. Nesta época, entretanto, não existia interface gráfica e somente em 1.995 foi disponibilizado o uso da internet no país.

1.2 ABORDAGEM CONCEITUAL DOS CRIMES CIBERNÉTICOS

A sociedade atualmente vive a "Era Digital", em que a liberação do acesso à internet, inicialmente restrita apenas à comunidade acadêmica, tornou-se uma ferramenta indispensável aos indivíduos. Até mesmo em lugares remotos, como em regiões de difícil acesso, é possível a utilização da internet.

A rede mundial de computadores transformou a sociedade, pois possibilitou o acesso rápido a diversos serviços, que no passado poderiam ser realizados apenas presencialmente, como atividades bancárias e serviços disponibilizados pelos órgãos do governo. Tornou-se espaço para comunicação, política, economia e democracia, local para a realização do homem e participação e interação cívica, além de ter trazido diversão, lazer, contatos pessoais, profissionais e o exercício de liberdade de expressão. (MORAES, 2007)

O avanço trazido pela tecnologia, entretanto, acarretou o surgimento dos crimes virtuais ou também denominados crimes cibernéticos ou ainda *cyber crimes*. Os crimes cibernéticos podem ser definidos como os delitos praticados por intermédio de dispositivos tecnológicos, como computadores, *notebooks*, *tablets*, celulares etc., conectados ou não à internet. (WENDT, 2021, p. 14)

É possível também a prática de crimes cibernéticos no ambiente de nuvem. O método de armazenamento de dados em nuvem consiste em depositar, ou manter um ou mais arquivos em um disco fora do computador, por meio da internet. Dessa maneira, utiliza-se de dispositivos informáticos com o intuito de acessar as informações nesse ambiente virtual. (WENDT, 2021, p. 14)

De acordo com Wendt (2021, p. 15), as condutas indevidas praticadas utilizando computadores e/ou dispositivos móveis" podem ser divididas em "crimes cibernéticos" e "ações prejudiciais atípicas". Estas ações podem causar algum transtorno e/ou prejuízo para a vítima, e lamentavelmente não se tratam de fatos típicos, ou seja, ainda não se encontram previstos como crime na legislação penal.

Para entender melhor o conceito de crimes cibernéticos, é necessário que se estabeleça a classificação em "crimes cibernéticos abertos" e "crimes exclusivamente cibernéticos". Os crimes cibernéticos considerados "abertos" são aqueles que podem ser praticados com a utilização de dispositivos tecnológicos ou sem o uso deles. Alguns tipos

penais que compreendem esta modalidade são os crimes contra a honra, ameaça, furto mediante fraude, estelionato, falsificação de documentos, identidade falsa, extorsão etc. (WENDT, 2021, p. 15).

Os crimes "exclusivamente cibernéticos", conforme Wendt (2021, p. 15), podem ser praticados somente com a utilização de dispositivos informáticos. Neste contexto, se enquadram os crimes de aliciamento de crianças, em que os infratores conseguem "encontrar" crianças em salas de bate-papo na internet; há também a conduta ilegal daqueles que utilizam fotos ou vídeos das vítimas e divulgam na internet. Os crimes que podem ser destacados nesta categoria são: divulgação de cena de estupro ou de cena de estupro de vulnerável; cena de sexo ou de pornografia; instigação ou indução ao suicídio ou automutilação ocorridos por meio da internet; registro não autorizado da intimidade sexual.

Os responsáveis pela prática dos crimes cibernéticos geralmente são pessoas altamente especializadas e com grau de conhecimento elevado na área da tecnologia, os *hackers*. Ao analisar o termo *hacker*, é necessário mencionar duas classificações ou significados. A primeira seria considerada uma pessoa do bem, que é dotada de grande conhecimento na área de informática, e a outra seria a de uma pessoa estudiosa e com habilidade na área tecnológica, mas que realizam invasões e são considerados vândalos digitais. (ROCHA, 2013)

De acordo com Rocha (2013), o *hacker* do bem e o *hacker* do mau são pessoas altamente especializadas no funcionamento de programas (softwares) ou dispositivos (hardwares), conseguindo identificar suas vulnerabilidades. O hacker do mau utiliza-se deste conhecimento para conseguir alterar o funcionamento dos programas ou dispositivos, e implementar ações que nem os projetistas originais conceberam. Desta maneira, conseguem desbloquear as "travas" de fábrica dos sistemas e invadir redes e sistemas de computadores. (ROCHA, 2013)

Alguns estudiosos da área da tecnologia defendem que os criminosos devem ser identificados como *crackers*, termo criado pela própria comunidade para sua distinção. Os *hackers* são pessoas da área da tecnologia, especializados na área da segurança da informação e suas ações são destinadas a construir coisas ou detectar falhas de segurança de sistemas de grandes empresas para que elas possam ser corrigidas, e não tem a intenção de atingir terceiros. Os *crackers*, de maneira inversa, burlam a segurança eletrônica com o intuito de obterem vantagem, ou seja, utilizam de suas habilidades para prejudicar pessoas ou atuam em benefício próprio, objetivando vantagem monetária ou apenas para

mostrar que são capazes de “quebrar” as chaves de proteção das pessoas físicas e/ou jurídicas.

As invasões realizadas em sites, e-mails e redes sociais são cometidas por *crackers*, assim como a inclusão de vírus nos ambientes de pessoas, empresas e órgãos de governo são realizadas pelos *crackers*. Eles conseguem descriptografar dados ou informações utilizadas para proteger o ambiente pessoal ou organizacional. A descriptografia é um processo que transforma dados que foram tornados ilegíveis por meio da criptografia. As senhas, por exemplo, são criadas por nós, simples usuários; contudo, internamente, há um método computacional que modifica as letras e/ou números informados para que aumente a dificuldade de os *crackers* obtê-la para invadir contas de e-mails, contas bancárias, bancos de dados de empresas etc.

Uma técnica utilizada frequentemente no ambiente virtual para o cometimento de crimes é a engenharia social. É empregada com a intenção de ludibriar a vítima, induzindo-as a fornecer dados confidenciais, bem como a abrir links para sites infectados com vírus. Conforme Wendt (2021, p. 16), “geralmente os criminosos simulam fazer parte de determinada instituição confiável, como bancos, sites de grandes lojas, órgãos de governo para que a vítima confie nos falsos dados apresentados, o que, na verdade, será a isca para que sejam fornecidas as referidas informações”.

Deste modo, percebe-se que, apesar da tentativa dos *hackers* na proteção das informações pessoais e patrimoniais de pessoas e empresas, a atuação dos *crackers* é mais efetiva e eficiente, pois encontram diversas formas de realizar delitos no ambiente cibernético, por se tratar de pessoas criativas e atacam desde as pessoas mais vulneráveis até sistemas complexos de processamento de dados.

2 A LEGISLAÇÃO BRASILEIRA E A RESPONSABILIZAÇÃO CRIMINAL QUANTO AOS CRIMES CIBERNÉTICOS

2.1 A LEI Nº 12.737/2012 (LEI CAROLINA DIECKMAN)

A Lei nº 12.737, também conhecida como Lei "Carolina Dieckman" foi criada no ano de 2012 após um *hacker* ter invadido o computador pessoal da atriz, tendo acesso a fotos pessoais de natureza íntima. Nesse sentido, após ter havido a exposição do conteúdo na mídia e gerado uma grande repercussão midiática, o que veio a causar profundos transtornos à vida de Carolina Dieckman e a sua família, o poder público se viu obrigado a dar uma resposta à sociedade para proporcionar mais segurança na internet quanto ao uso indevido de informações pessoais ligadas à intimidade das pessoas.

Após a criação da lei acima mencionada, foram acrescentados os artigos 154-A e 154-B e modificados os artigos 266 e 298 do Código Penal. O artigo 154-A trata do delito "Invasão de dispositivo informático" e traz o seguinte texto: "Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita". Para este tipo penal, a pena é de detenção de 3(três) meses a 1(um) ano e multa.

Por meio desse dispositivo, verifica-se que o bem jurídico tutelado é a inviolabilidade de dados, que tem por finalidade a proteção do sigilo e da privacidade das pessoas. A invasão a dispositivo informático diz respeito à falta de autorização do proprietário do equipamento no acesso às informações, sejam ela pessoais ou corporativas, realizadas por meio de violação de artefato de segurança, como antivírus e obtenção de senhas. Estes delitos são praticados por pessoas com amplo conhecimento em tecnologia, mais especificamente, na área da segurança da informação, os *hackers,* pessoas com qualificação técnica e inescrupulosas, capazes das maiores atrocidades no ambiente virtual.

Um ponto relevante que merece ser destacado diz respeito à instalação de *softwares* em dispositivo alheio. Este método tem como propósito a obtenção de vantagem ilícita de dados das vítimas, uma prática recorrente nos dias atuais. Os infratores conseguem introduzir fragilidades no equipamento alheio, como softwares maliciosos, que são capazes de capturar informações de login e senhas, como acesso a aplicativos

bancários, informações de empresas, causando prejuízos de valor econômico e violando a privacidade e intimidade das pessoas, por meio da obtenção de fotos, vídeos e, em muitos casos, efetuam a divulgação na internet.

O advento da Lei nº 12.737/12, portanto, trouxe mais segurança jurídica, no sentido em que permitiu às vítimas dos crimes cometidos no meio cibernético uma maior proteção, já que as punições são mais severas. Além disso, trouxe a possibilidade de o magistrado aplicar a lei com o uso de tipos penais específicos, ao invés de realizar interpretação e decidir por analogia, como ocorria anteriormente, em que os casos relativos aos delitos cometidos no âmbito da internet não eram tratados no Código Penal Brasileiro.

Deste modo, verifica-se que a Lei "Carolina Dieckman", quando entrou em vigor no sistema jurídico brasileiro, foi um marco que deu início aos mecanismos de proteção dos dados pessoais das pessoas contra os infratores virtuais. Entretanto, a norma necessita ainda de muito amadurecimento para conseguir abarcar diversas situações ainda não contempladas, para trazer mais clareza e eliminar dúvidas oriundas de sua interpretação.

2.2 LEI N º 12.965/2014 (MARCO CIVIL DA INTERNET)

O acesso à internet é um direito atribuído ao cidadão. Embora a Constituição Federal não abarque explicitamente o acesso à internet no art. 5º, inciso XIV, é possível realizar tal interpretação. Nesse sentido, a Lei nº 12.965 (Marco Civil da Internet), vigente a partir de 23.06.2014 regulamenta o uso e estabelece os princípios, os direitos e deveres para o uso da internet no Brasil e o respeito à liberdade de expressão.

A lei nº 12.965 dispõe que são assegurados os direitos à inviolabilidade da intimidade e da vida privada, assim como a do sigilo das comunicações, os procedimentos de guarda e fornecimento de dados de pessoas físicas e/ou jurídicas, além de determinar as sanções que poderão ser aplicadas aos infratores que utilizam o ambiente cibernético para cometer crimes.

No que tange à responsabilização pelos danos causados aos conteúdos disponibilizados nas redes sociais ou *sites*, determina o artigo 18, o §1º do art. 19, e o art. 21 da Lei do Marco da Internet que "O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros", a menos que uma ordem judicial específica tenha sido descumprida pelo provedor. Para exemplificar, podemos citar o fato de que o *Google* apenas exibe as informações

relacionadas ao material disponibilizado na internet, ou seja, ele não é responsável por elas, porque é impossível controlar o conteúdo criado e publicado pelos usuários da internet (ZANIOLO, p. 649).

Nos termos do §1º do artigo 19 da Lei 12.965/2014, em consonância com a jurisprudência do STJ, o provedor de conteúdo ou de hospedagem deverá ser notificado judicialmente para retirar uma determinada publicação de usuários que ofenda a imagem e à honra das pessoas atingidas. É indispensável, portanto, indicar a URL correspondente ao conteúdo divulgado com o objetivo de removê-lo do ambiente virtual, para que outras pessoas não consigam visualizá-lo. O intuito é proteger e garantir a integridade dos indivíduos que tiveram sua honra ou dignidade violados (ZANIOLO, p. 649).

O artigo 22 da presente lei diz "A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet". Dessa forma, a pessoa que sofreu violação em seus dados poderá requerer informações do provedor de internet dados para que consigam identificar o(s) responsável(is) pelo material disponibilizado.

Diante do que foi mencionado com relação à Lei do Marco Civil da Internet, é garantido a todos os indivíduos o direito ao acesso a sites, aplicações, redes sociais e todo dispositivo que permita o uso do ambiente virtual. Cabe ao poder público, entretanto, determinar as sanções aos provedores de conexão e de aplicações por danos decorrentes de material publicado indevidamente e sem autorização do interessado, com o intuito de resguardar a integridade das pessoas.

2.3 A PREVISÃO DOS CRIMES CIBERNÉTICOS NO CÓDIGO PENAL BRASILEIRO

O Código Penal (Decreto-lei nº 2.848/1940) trata-se de uma norma infraconstitucional presente no ordenamento jurídico brasileiro e é constituído de um conjunto de regras de caráter punitivo. A finalidade de tal dispositivo é aplicar sanções àqueles que praticam delitos contra a sociedade. Embora seja uma norma extensa, não abrange toda a matéria penal necessária, visto que houve poucas atualizações após sua criação e não consegue atender toda matéria penal existente, gerando insegurança jurídica.

As penas previstas no Código Penal, infelizmente, não têm o condão de reduzir o índice de delinquência e reincidência dos delitos praticados pelos infratores, tampouco conseguem garantir a ressocialização dos criminosos, após o cumprimento de suas penas. Isso se deve, em parte, aos diversos benefícios garantidos, tais como livramento condicional, progressão de regime, remição e unificação das penas. (BARRETO, 2013)

Embora haja a necessidade de reforma no Código Penal, pelo fato de não estar presente o termo "internet" na previsão legal, tal fato não impede o cumprimento das punições, possível mediante a aplicação do tipo penal existente pelo Poder Judiciário. O meio utilizado pelos infratores não é o fator mais importante, pois a sentença proferida pelo juiz será realizada pela prática ilícita, independentemente da ferramenta recorrida pelos criminosos.

Nesse sentido, é de extrema relevância citar alguns dispositivos elencados no Código Penal relacionados às práticas criminosas na internet, além de mencionar os critérios observados para realizar as sanções necessárias:

1) Estelionato: o estelionato é uma prática frequente na internet, pois com a utilização em massa de *sites* e redes sociais é possível obter informações pessoais dos usuários por meio do fornecimento de dados para o cadastro de senhas. Assim, no momento em que o acesso a determinadas lojas virtuais é liberado ou quando é realizada a criação de usuários em redes sociais e aplicativos de mensagens instantâneas, os *hackers* conseguem obter informações de usuário e senha, e as utilizam para praticar diferentes formas de delitos; um deles seria o estelionato.

O Código Penal realizou recentemente uma atualização para tratar do "estelionato virtual". O §2º-A do art. 171 trata da fraude eletrônica, quando o estelionato é cometido "com a utilização de informações fornecidas 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". Nota-se, contudo, que há uma maior dificuldade para se identificar os responsáveis pelas fraudes praticadas no ambiente cibernético, visto que os *hackers* dispõem de recursos tecnológicos que impossibilitam a identificação de equipamentos e/ou dispositivos utilizados para a prática dos crimes cometidos no ambiente virtual.

2) Crimes contra a honra. Dentre eles, podemos destacar os crimes de calúnia, injúria e difamação. Art. 138 – "Caluniar alguém, imputando-lhe falsamente fato definido como crime", art. 139 – "Difamar alguém, imputando-lhe fato ofensivo à sua reputação", Art. 140 – Injuriar alguém, ofendendo-lhe a dignidade ou o decoro". Nesse sentido,

quando alguém é ofendido por questão de sua raça, cor, religião, ou até mesmo por questão de idade ou deficiência física ou intelectual, ocorre o crime de injúria. A difamação e a calúnia ocorrem quando alguém diz algo falso sobre a pessoa, prejudicando sua reputação. Compreende-se, portanto, que, independentemente do meio utilizado para a discriminação ou ofensa, seja pela internet ou outros veículos, o dano é causado à pessoa.

3) Apologia a crime ou a fato criminoso: ocorre crime quando alguém pratica o disposto no art. 287 do Código Penal: "Fazer, publicamente, apologia de fato criminoso ou de autor de crime". Esse delito ocorre quando há a divulgação ou compartilhamento de vídeos, comentários, ou quando indivíduos que incitam ou reforçam o uso da violência. Esse compartilhamento pode ser feito de diferentes maneiras, pela divulgação em redes sociais, pelo envio de e-mails ou de aplicativos de mensagens instantâneas. Percebe-se, portanto, que, embora não haja o termo "internet" nos tipos penais acima mencionados, é possível utilizar-se dos mecanismos contidos na legislação penal para realizar as punições dos infratores.

4) Crime de falsa identidade: é muito comum a criação de perfis *fakes*, em que o infrator, sem autorização, se passa pelo proprietário da conta da rede social. Ele consegue obter os dados da conta, senha e fotos da pessoa, agindo como se fosse o real dono. E, consequentemente, pode acarretar danos à vítima, de cunho pessoal ou financeiro. Este crime virtual é punido como crime de falsa identidade, do art. 307 do Código Penal, que tem por conduta "atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem". (BRASIL, 1940)

5) Crimes de perseguição ou *stalking*: ocorre quando algum indivíduo é perseguido, reiteradamente, e tem sua integridade física ou psicológica atingida, além de ter sua capacidade de locomoção limitada ou sua liberdade e privacidade invadidas. Esse crime, incluído recentemente no Código Penal, encontra-se tipificado nos artigos 147-A e 147-B, e pode ser cometido presencialmente ou por meio da internet. Na maioria dos casos, acontece contra as mulheres, sendo a perseguição realizada por parceiros ou ex-parceiros.

Segundo a conceituação doutrinária, o termo em inglês *stalking* presume o fator medo, pois corresponde à prática de uma perseguição repetida, que ocasiona um sofrimento emocional à vítima, visto que restringe a liberdade individual e capacidade de locomoção da vítima, de maneira reiterada. Essa infração pode ocorrer em diversas

situações, seja por meio da internet ou de maneira presencial. Embora não exista expressamente a existência do “medo”, muitos doutrinadores acreditam que seria um fator necessário para que o delito seja configurado. (MINISTÉRIO PÚBLICO DO MATO GROSSO DO SUL, 2021).

Há que se ressaltar que em 28/05/2021 foi publicada a Lei nº 14.155, que aplicou penas mais severas aos crimes de violação a dispositivos informáticos, como furto, fraude e estelionato. O texto da referida lei altera os artigos 70, 154-A, 151 e 170 do Código Penal. Dessa forma, o crime de invasão a dispositivo conectado à internet passará a ser punido com pena de reclusão, podendo haver também aumento de pena no caso de resultar prejuízo econômico para o usuário ou se o crime é praticado por intermédio de servidor mantido fora do território nacional ou quando o delito é cometido contra idoso ou vulnerável.

Diante do exposto acima, percebe-se que mesmo com a falta de uma legislação ampla e específica que cuide dos crimes cibernéticos, os tribunais brasileiros, por intermédio de juízes e desembargadores, tratam alguns crimes virtuais de maneira análoga aos delitos comuns já tipificados na Legislação Penal. Essa adaptação realizada pelos órgãos da Justiça se faz necessária para que os infratores sejam penalizados de maneira eficaz, pois cabe à autoridade judiciária a aplicação da lei ao caso concreto, com o intuito de assegurar a justiça e garantir o cumprimento dos direitos individuais existentes nas relações sociais.

3 OS PROCEDIMENTOS DE INVESTIGAÇÃO CRIMINAL DOS CRIMES CIBERNÉTICOS

3.1. OS MECANISMOS DE INVESTIGAÇÃO CRIMINAL ADOTADOS NO BRASIL

Os crimes cibernéticos podem ser praticados de diferentes maneiras, em razão da tecnologia da informação ser uma área dinâmica e abrangente. Isso vem a dificultar o trabalho de investigação, pois o acesso aos dados pode ser complexo; em muitos casos, não são colhidos facilmente como em crimes comuns. Cabe, portanto, aos órgãos de investigação efetuar o rastreamento do acesso realizado pelos infratores via sistema operacional e logs do sistema, com o intuito de identificar o caminho percorrido para a prática do ato ilícito.

Os procedimentos adotados pelos órgãos de investigação compreendem duas fases, quais sejam, a fase técnica e a de campo. Na fase técnica, o objetivo é localizar o dispositivo utilizado para a atividade criminosa. De acordo com Wendt (2021, p. 40), podem-se destacar as seguintes ações:

a) Analisar as informações narradas pela vítima e os dados coletados em busca da compreensão do fato ocorrido;

b) Orientar a vítima a preservar o material que possa comprovar o delito;

c) Coletar as evidências no ambiente virtual e realizar a conferência do que foi informado pela vítima;

d) Formalizar o fato criminoso por meio de boletim de ocorrência, que poderá ocasionar a instauração de um procedimento policial;

e) Realizar a investigação de possíveis autores, verificar a origem de e-mails, a criação de perfis em redes sociais e registro e hospedagem de domínios;

f) Formalizar os dados coletados por meio de relatório, contendo evidências materiais que possam auxiliar na investigação;

g) Requisitar dados cadastrais junto aos provedores de conexão e de aplicações;

h) Representar perante o Poder Judiciário a expedição de autorização judicial para afastar o sigilo de dados. Assim, o acesso aos dados irá auxiliar na identificação dos criminosos;

i) Efetuar a análise das informações prestadas pelos provedores de aplicações ou de conexões.

Após realizar todas as ações acima descritas, é possível que seja identificado e localizado o computador ou dispositivo utilizado para acessar os dados da vítima. Assim, surge então a fase de campo, em que são realizadas diligências aos locais em que os equipamentos foram identificados pelos órgãos de investigação. Esta operação deverá acontecer de forma prudente; na maioria das vezes, é feita representação ao Poder Judiciário para que seja concedido um mandado de busca e apreensão ao local. (WENDT, 2021, p. 41)

Outra medida que pode ser adotada é a solicitação ao Poder Judiciário para que seja determinado ao administrador da rede do local identificado em que ocorrera a prática delituosa para prestar as devidas informações, com a finalidade de indicar o dispositivo utilizado para a realização da ação criminosa. Essa determinação pode ocorrer de duas formas: encaminhada ao administrador de redes para cumprimento ou entrega pessoal ou ainda por meio da autoridade policial ou oficial de justiça. O ideal é que, para ambas as medidas adotadas, haja a presença de um perito oficial ou de um profissional capacitado da tecnologia da informação; mais especificamente da área de redes ou de segurança da informação.

3.1.1. Formas de guarda de prova a ser utilizada em Inquérito Policial e Procedimento Judicial

Durante o processo investigativo, várias atividades são realizadas pela equipe da polícia, dentre elas, podemos citar os meios utilizados para realizar a guarda de provas das ações praticadas na Internet. Os métodos mais adequados são aqueles que trazem uma maior confiabilidade, como no caso do registro de Ata Notarial, que, de acordo com a Associação dos Notários e Registradores do Brasil, trata-se de "um instrumento público no qual o tabelião documenta, de forma imparcial, um fato, uma situação ou uma circunstância presenciada por ele, perpetuando-os no tempo. A ata notarial tem eficácia probatória, presumindo-se verdadeiros os fatos nela contidos. É um importante meio de prova na esfera judicial, conforme disposto no artigo 384 do Código de Processo Civil (Lei 13.105/2015)".

Confome relata Wendt:

> A ata Notarial pode ser utilizada como meio de prova em ambiente eletrônico (RODRIGUES, 2004), sobre páginas eletrônicas (sites) e documentos eletrônicos, fixando data e existência de arquivos em meio eletrônico, prova de fatos contendo imagens, vídeos, texto e logotipos, além de inúmeras outras funções. Portanto, pode a parte interessada imprimir o site relacionado ao

> delito e/ou seu interesse, procurar um tabelionato e registrar uma Ata Notarial. Ela pode ser utilizada para fins de prova em processo cível, criminal, eleitoral, administrativo, dentre outros (WENDT, 2021, p. 55).

A Ata Notarial tornou-se um importante mecanismo utilizado pelos órgãos de investigação e ainda houve uma inovação, com a possibilidade de se gerar este documento de forma eletrônica, sem a necessidade de se dirigir a um cartório. Para isso, o interessado deverá ter o Certificado Digital e-Notariado ou ICB-Brasil, documento de identidade eletrônico ou possuir ficha aberta no cartório.

No caso de pessoas físicas, há alternativas para realizar a validação de informações obtidas em sites, como *Whatsapp*, *Facebook*, *Instagram*, *Webmail* e outras. O Verifact (<https://www.verifact.com.br/>) e do HashCool (<https://www.hash.coll/>) são ferramentas gratuitas para pessoas físicas e possuem extensão no navegador *Chrome*.

Um outro mecanismo utilizado para comprovação de informações obtidas no ambiente virtual é a Certidão elaborada pela Polícia Civil. O agente policial, na condição de escrivão poderá acessar uma página da internet, realizar o *print* da página ou do local em que obteve o dado a ser comprovado, certificar a data em que realizou a consulta e documentar as informações coletadas, seguindo os procedimentos e regras de modo a evidenciar o fato.

A Certidão poderá ser emitida pelo Escrivão da Polícia Civil quando algum cidadão comunicar a existência de um fato criminoso por meio do Boletim de Ocorrência. No que tange aos crimes cibernéticos, recentemente há a orientação de que o policial, após o registro do Boletim de Ocorrência, também elaborasse o Auto de Materialização de Evidência Eletrônica. Trata-se de um instrumento que torna mais ágil e simplificado o registro das informações relatadas pelo interessado ou vítima e evita que a evidência seja apagada. Deste modo, irá servir de prova a ser utilizada no procedimento de Inquérito Policial e na Ação Penal promovida pelo Ministério Público.

O Auto de Materialização de Evidência Eletrônica é um meio utilizado para coletar materiais na forma digital para o procedimento de investigação. Com sua utilização, a Polícia Civil dará autenticidade ao conteúdo obtido no ambiente cibernético e irá conferir fidedignidade. Neste contexto, Wendt cita Nogueira Jorge:

> O Auto de Materialização de Evidência Eletrônica é um documento que tem a finalidade de descrever como se deu o acesso às evidências, bem como informar a data, horário e fuso horário do acesso e formalizar o conteúdo criminoso indicado pela vítima ou por outra pessoa que tenha permitido que o

fato criminoso fosse investigado. (Wendt, 2021, p. 57 apud Higor Vinicius Nogueira Jorge, 2018).

3.1.2 Procedimentos de investigação quanto aos crimes praticados por intermédio do Instagram, Facebook e Whatsapp

Em razão do avanço dos crimes cibernéticos, algumas mudanças nas leis foram necessárias para facilitar o procedimento investigativo da Polícia Civil. É possível, em uma instrução processual penal, requisitar o teor das comunicações realizadas pelo Facebook, desde que já encerradas e armazenadas, nos termos da Lei n.º 9.296/96 (Lei das Interceptações Telefônicas). Todavia, o acesso às comunicações armazenadas pelo aplicativo de mensagens instantâneas só é permitido mediante ordem judicial, na forma do inciso III do artigo 7º da Lei 12.965/2014 (Marco Civil da Internet).

O artigo 22 da Lei 12.965/2014 (MCI) dispõe que "a parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações da internet". Nestes casos, o juiz deverá requerer obrigatoriamente: 1) fundados indícios da ocorrência do ilícito; 2) justificativa contendo os motivos para se utilizar os registros solicitados com o objetivo de realizar a investigação ou instrução probatória; e 3) período ao qual se referem os registros. (Ministério Público do Estado do Ceará, 2016).

A autoridade policial ou o Ministério Público poderão requerer aos provedores de internet, por meio de medida cautelar, que os logs - registros de acesso às aplicações, sejam armazenados por um período superior aos seis meses – prazo imposto pelo artigo 15 da Lei 12.965/2014 (MCI), aos Provedores de Aplicações de Internet. Nessa hipótese, não se faz necessária a existência de ordem judicial para a guarda das informações armazenadas nos logs de acesso. Tal requerimento pode ser realizado na plataforma disponibilizada pelo Facebook, utilizando o formulário Law Enforcement Online Requests, acessível no endereço https://www.facebook.com.br/records.

Dentre as informações a serem inseridas no formulário on-line disponibilizado pelo Facebook, conforme documento do Ministério Público do Distrito Federal e Territórios, a indicação da URL de cada conteúdo danoso é determinante para que se consiga identificar cada post no Facebook.. Deverão também constar no pedido: nome, e-mail, data de nascimento, número de telefone celular do usuário; endereço IP da conexão

utilizada no ato do cadastro no Facebook; logs de acesso (registros de acesso) ao aplicativo Facebook; o período; além de outras informações pertinentes.

Há algumas exceções no que tange ao procedimento de requisição de dados ao Facebook. Nos casos de crimes que envolvam a postagem de imagens e vídeos que tenham como conteúdo cenas de nudez e de atos sexuais privados, a pessoa prejudicada poderá requerer que o material seja retirado da plataforma sem que haja necessidade de se recorrer ao Poder Judiciário. Trata-se, portanto, de uma proteção à intimidade da vida privada da vítima, propiciando maior agilidade no procedimento com a intenção de tentar atenuar os transtornos causados pela exposição de material de cunho íntimo.

3.2 A investigação dos crimes cibernéticos na cidade de Goiânia

Foi realizado um levantamento das informações relacionadas ao procedimento de investigação junto à Delegacia de Repressão aos Crimes Cibernéticos localizada na cidade de Goiânia. Dentre as informações coletadas, algumas dizem respeito às dificuldades encontradas pelos policiais civis na identificação dos responsáveis pelos delitos cometidos no âmbito da Internet, mais conhecidos como *hackers*, que utilizam de métodos sofisticados para dificultar a obtenção de provas que os incriminem. Há apuração de crimes, por exemplo, que podem durar mais de 1 (um) ano, devido a complexidade do caso estudado.

Outro grande problema encontrado pela equipe de policiais civis é quanto ao pequeno número de pessoas destinadas ao procedimento investigativo; atualmente, existem apenas 20 profissionais, dentre delegados, escrivães, policiais civis e 1 papiloscopista, que, em algumas situações, exerce papel de perito, visto que apenas a Polícia Técnico-Científica é provida de perito criminal. Esse pessoal é responsável por averiguar todos os detalhes das práticas delitivas cometidas considerando toda a população no Estado de Goiás.

De acordo com informações oriundas da equipe da Polícia Civil, quando se encontra alguma indicação de que o equipamento ou dispositivo informático foi utilizado para o cometimento do crime, ele é enviado ao Instituto de Criminalística para ser efetuada a avaliação das informações, como localização de arquivos, fotos, vídeos, e-mails e identificação de data/hora em que a ação foi realizada. Assim, a equipe emite um laudo e o encaminha para a instrução do Inquérito Policial, que irá compor o processo. Posteriormente, o processo é destinado ao juiz competente.

Se comprovada a manipulação do equipamento para cometer o crime, é realizado o depósito judicial, a pedido do juiz. Deste modo, não é realizada sua devolução ao investigado. A entrega só poderá ser efetivada quando não tenha sido identificado o envolvimento do investigado no delito.

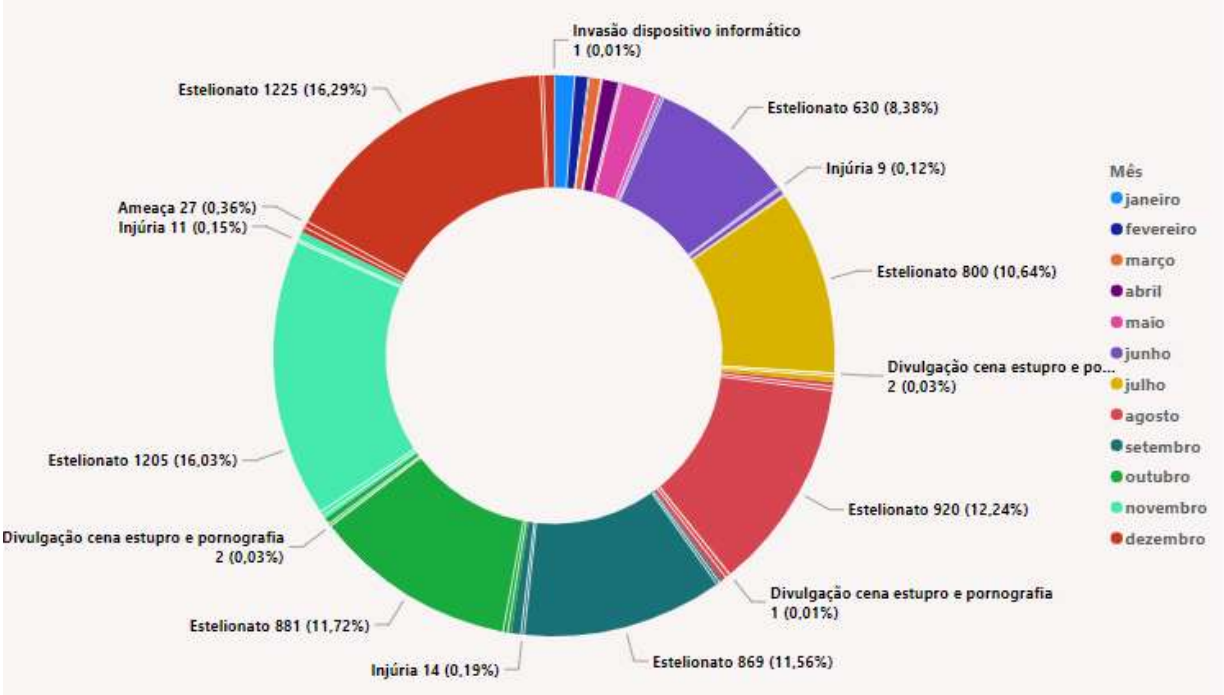
3.3 Indicadores de Crimes Cibernéticos praticados na Cidade de Goiânia (no período compreendido entre 2021 e 2022)

Um levantamento foi realizado juntamente aos órgãos vinculados à Secretaria de Segurança Pública, com a finalidade de obter dados quantitativos acerca dos principais crimes praticados na cidade de Goiânia e no Estado de Goiás no período compreendido entre 2021 e 2022. Conforme documento enviado pela Secretaria de Segurança Pública do Estado de Goiás, “a aferição foi realizada considerando todos os registros em que o tipo do local do fato informado foi " Ambiente Virtual (Internet)", tal opção de tipo de local foi inserida no sistema RAI - Registro de Atendimento Integrado, no final do ano de 2020, devido a isso o período utilizado foi de janeiro de 2021 a junho de 2022”.

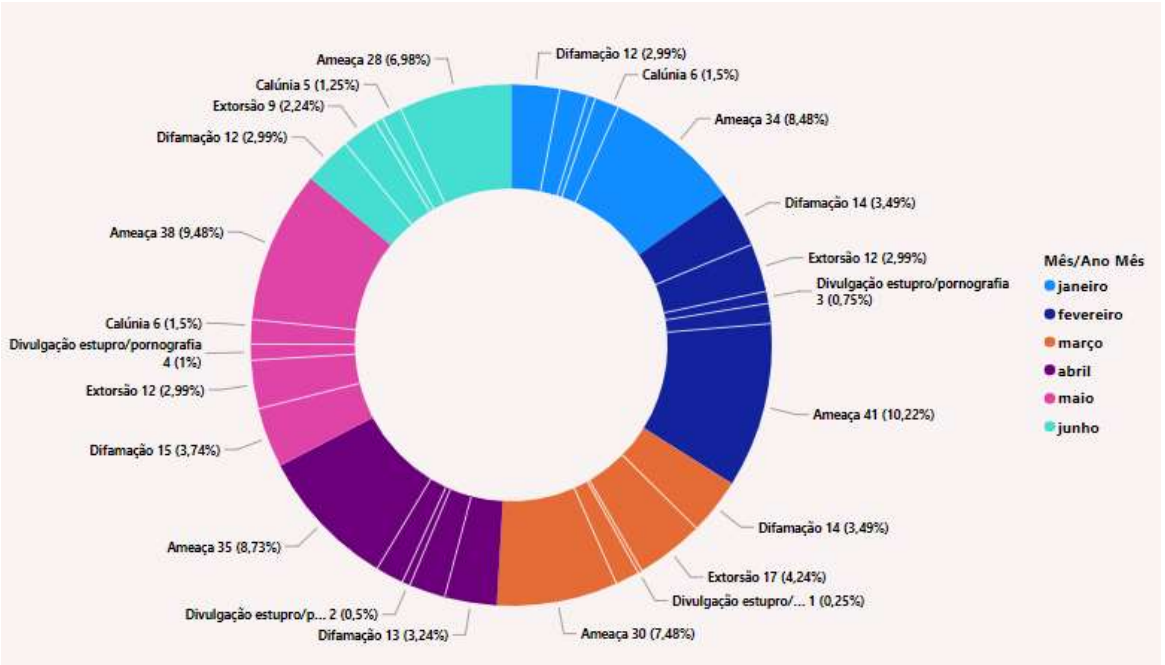
Cabe ressaltar que alguns tipos de crimes aferidos podem ser registrados por meio da Delegacia Virtual, em que a própria vítima realiza o registro da ocorrência, anexa fotos, documentos pessoais, provas de que houve a lesão. Caso as informações não sejam satisfatórias, haverá a reprovação da ocorrência e a consequente devolução para que sejam providenciadas as correções e reenvio. No prazo de 24h a partir do registro, o requerente irá receber informações por intermédio do e-mail cadastrado, bem como a indicação da Delegacia de Polícia responsável pelo caso. Isso porque, mesmo que se trate de um crime virtual, se houver envolvimento de idosos, crianças ou adolescentes, os autos serão encaminhados para as Delegacias especializadas para esse tipo de delito.

Após ter sido realizado o registro da ocorrência e iniciado o procedimento investigativo, as Delegacias Especializadas enviam os dados coletados à Secretaria de Segurança Pública do Estado de Goiás. Tais informações encontram-se pormenorizadas abaixo, utilizando o recurso de geração de indicadores:

Crimes cometidos na cidade de Goiânia – 2021



Crimes cometidos na cidade de Goiânia - 2022



Crimes cometidos na cidade de Goiânia (2021 e 2022)

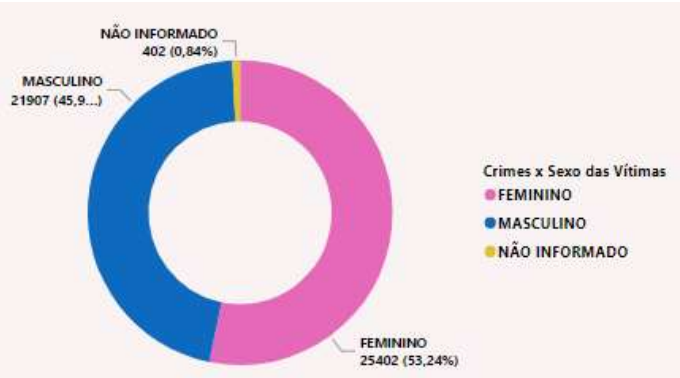
Ano	Adquirir fotografia/vídeo criança/adolescente	Perseguição	Difamação	Calúnia	Ameaça	Extorsão	Furto	Injúria	Falsificação de cartão	Divulgação estupro/pornografia	Falsa identidade	Estelionato
2021	15	15	57	26	127	66	237	96	12	6	37	6953
janeiro	0	0	3	0	0	2	0	0	0	0	0	87
fevereiro	0	0	0	0	1	0	2	0	0	0	0	58
março	0	0	0	0	1	1	3	0	0	1	2	51
abril	0	1	2	0	1	0	3	5	0	0	2	72
maio	0	0	0	1	4	2	13	0	1	0	0	155
junho	0	2	2	2	12	12	24	9	0	0	3	630
julho	0	2	5	3	8	10	24	12	1	2	1	800
agosto	0	4	5	5	18	8	33	20	0	1	3	920
setembro	12	2	12	4	14	8	39	14	1	0	4	869
outubro	1	1	12	3	20	8	26	11	1	2	7	881
novembro	0	1	8	5	21	8	36	11	3	0	8	1206
dezembro	2	2	11	3	27	7	45	14	5	0	8	1225
2022	0	32	80	35	206	66	219	120	10	14	83	7718
janeiro	0	5	12	6	34	7	26	13	1	2	17	1300
fevereiro	0	6	14	5	41	12	36	20	1	3	18	1128
março	0	5	14	6	30	17	33	21	6	1	14	1298
abril	0	7	13	7	35	9	39	19	0	2	12	1388
maio	0	5	15	6	38	12	48	22	0	4	2	1329
junho	0	4	12	5	28	9	40	25	2	3	20	1275
Total	15	47	137	61	333	132	456	216	22	20	120	14671

Como pode ser observado nos gráficos acima, o crime de estelionato é o que detém o mais alto índice de ocorrência na cidade de Goiânia e no Estado de Goiás. Provavelmente seja a maneira mais utilizada pelos infratores, visto que realizam diferentes métodos para manipular e enganar as pessoas com a intenção precípua de obter vantagem de cunho financeiro.

Os demais tipos penais aparecem com menor percentual, mas isso também se deve ao fato de que diversas pessoas não denunciam a prática criminosa, como nos casos de calúnia, difamação, invasão de dispositivo informático e falsificação de cartão. Também, conforme informado pela equipe da Delegacia de Crimes Cibernéticos, uma grande quantidade de pessoas não registra o fato pois muitas delas acreditam que o procedimento é moroso e que não serão aplicadas sanções aos infratores.

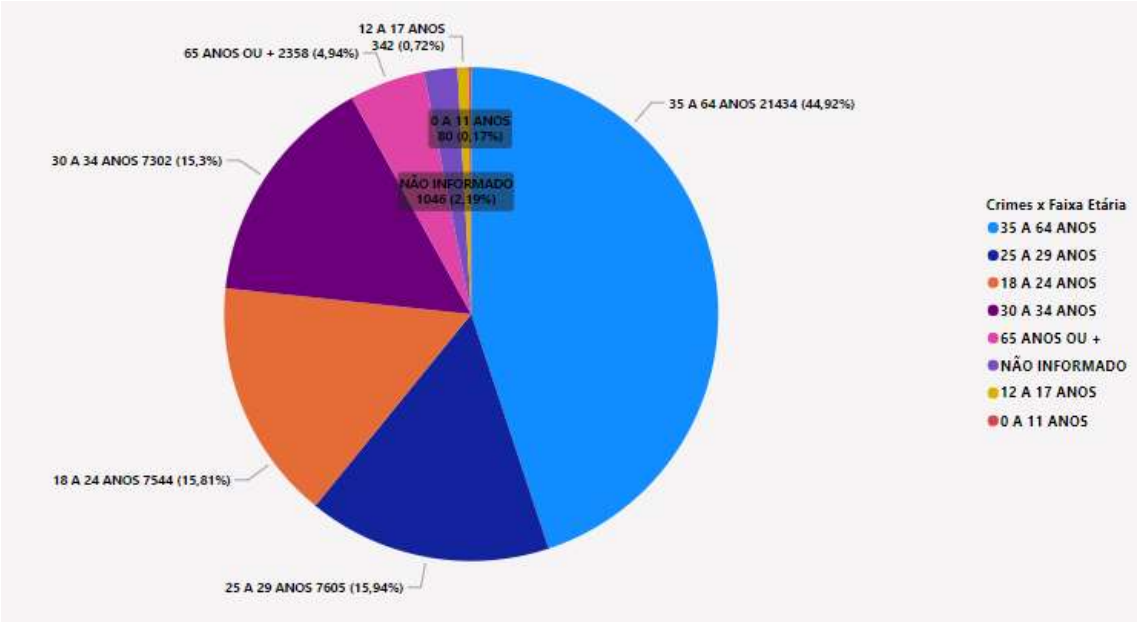
É nítido que os casos que envolvam criança e adolescente apresentam um índice muito pequeno em relação aos demais delitos. Contudo, não há meios de conhecer a quantidade real e se as famílias das vítimas denunciam todas as ocorrências. Muitas delas, por constrangimento, não reportam o fato às autoridades policiais.

Crimes x Sexo das Vítimas



No que tange aos indicadores de crimes praticados conforme o sexo, é muito próxima a quantidade de vítimas do sexo masculino e feminino; embora, o índice maior ocorra entre as mulheres.

Crimes x Faixa Etárias das Vítimas



Com relação à faixa etária das vítimas, há que se considerar que o maior percentual se encontra entre a idade de 35 e 64 anos. Mesmo que haja uma grande quantidade de crianças e adolescentes utilizando habitualmente a internet e os recursos disponíveis, como redes sociais, aplicativos de mensagens instantâneas, o índice na faixa etária entre 12 e 17 anos é bem reduzido; ele começa a aumentar após os 18 anos, já na fase adulta.

Deste modo, ao avaliar os dados coletados gerados por meio de gráficos, é possível realizar uma análise minuciosa quanto aos crimes cibernéticos praticados na Cidade de Goiânia. O procedimento de coleta foi rápido, visto que, atualmente, a Secretaria de Segurança Pública disponibiliza um canal (*site*) exclusivo para a população que necessita obter informações acerca de assuntos de interesse geral.

CONSIDERAÇÕES FINAIS

A evolução tecnológica possibilitou a realização de tarefas antes impraticáveis por pessoas, empresas e órgãos governamentais, tais como a comunicação por vídeo e áudio entre pessoas, o envio de mensagens instantâneas e o encaminhamento de e-mails para qualquer indivíduo, independentemente de sua localização física, e possibilitou o desenvolvimento de ferramentas essenciais para a realização do trabalho. Por outro lado, ocasionou o surgimento de situações maléficas para o ser humano e pessoas jurídicas, como a ocorrência dos crimes virtuais, que foi o objeto de estudo do presente trabalho.

Diante disso, houve a curiosidade em estudar o tema em questão e descobrir os problemas encontrados durante o procecimento de investigação dos crimes cibernéticos. Foi elaborado um questionário destinado à Delegacia de Crimes Cibernéticos na cidade de Goiânia, bem como foi efetuada a coleta dos dados. O resultado obtido foi que os infratores não atingem apenas um público-alvo específico, atingem faixas etárias diversas, mas a que tem um índice mais expressivo é entre 35 e 64 anos, e geralmente as vítimas com um maior percentual são as do sexo feminino.

No que diz respeito aos tipos de delitos cometidos, identificou-se que a maior quantidade trata-se do crime de estelionato. Por meio das redes sociais, os transgressores conseguem persuadir as vítimas de diferentes maneiras, utilizando de meio ardil, com o intuito de causar prejuíjos às pessoas. Eles conseguem obter informações de login e senha das vítimas, acessam *e-mails* e contas bancárias para cometer os delitos.

Quanto ao aspecto da análise da legislação penal atual do Brasil, verificou-se que há a aplicação das leis brasileiras na punição dos infratores do ambiente cibernético, mesmo que existam poucos dispositivos capazes de prever a gama de delitos cometidos, como a Lei 12.737/2012, também conhecida por “Lei Carolina Dieckman” e o Marco Civil da Internet. Ainda foi observado que o Código Penal utiliza a tipificação dos crimes já existentes para associá-los com os crimes cometidos na internet, já que a única diferença diz respeito o meio praticado.

Neste sentido, os objetivos propostos para o estudo dos obstáculos encontrados nos procedimentos de investigação e a eficácia da legislação brasileira na responsabilização dos criminosos da internet foram cumpridos. Foram obtidos resultados concretos após a realização do levantamento dos dados junto à Delegacia de Crimes Cibernéticos e Secretaria de Segurança Pública do Estado de Goiás, que retratam um certo avanço nos mecanismos utilizados pelos órgãos investigativos; todavia, há necessidade

de contratação de pessoal para que os procedimentos de investigação sejam realizados com maior agilidade e possibilitem um retorno mais rápido à sociedade afetada.

Também foi constatado que as leis atualmente em vigor no Brasil são eficazes para proteger as vítimas e punir os infratores, pois a maioria dos delitos está prevista na legislação penal. Entretanto, a necessidade de atualização periódica se faz necessária diante da criatividade do ser humano em agir com o intuito de atingir e prejudicar as pessoas, afetando-as tanto no aspecto financeiro quanto no psicológico.

Dessa forma, foi observado durante a realização deste estudo que os procedimentos de investigação criminal são eficientes, mas não há quantidade de pessoal capaz de solucionar os casos com celeridade. Apesar de serem realizados treinamentos com frequência, é muito grande o volume de casos tratados pela Polícia Civil, e, como consequência, as vítimas não recebem respostas rápidas dos órgãos de investigação, após ter sido efetuado o registro da ocorrência da infração cometida.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, J. M. F. **Breve história da Internet**. Disponível em: https://repositorium.sdum.uminho.pt/bitstream/1822/3396/1/INTERNET.pdf. Acesso em: 04 mai. 2022 às 07:22h.

ANOREG-BR (Associação dos Notários e Registradores do Brasil)**. Ata Notarial.** Disponível em: https://www.anoreg.org.br/site/atos-extrajudiciais/tabelionato-de-notas/atasnotariais/#:~:text=O%20que%20%C3%A9%3F,verdadeiros%20os%20fatos%20nela%20contidos. Acesso em: 31 out. 2022 às 07:09h.

BAPTISTA, Rodrigo. **Lei com penas mais duras contra crimes cibernéticos é sancionada**. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada. Acesso em: 25 jul. 2022 às 21:12 h.

BARRETO, Paula Leite. **A necessidade da atualização do Código Penal**. Disponível em: https://www.campograndenews.com.br/artigos/a-necessidade-da-atualizacao-do-codigo-penal. Acesso em: 29 ago. 2022 às 16:58h.

BRASIL. Decreto-Lei nº 2.848, de 07 de Dezembro de 1940. Código Penal. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 20 ago. 2022 às 07:30h.

BRASIL. Lei nº 12.737, de 30 de Novembro de 2012. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 17 ago. 2022 às 07:15h.

BRASIL. Lei nº 12.965, de 23 de Abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 ago. 2022 às 06:35h.

BRASIL. Lei nº 13.105, de 16 de Março de 2015. Código de Processo Civil. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 30 out. 2022 às 07:18h.

BRASIL**.** LEI Nº 14.155, de 27 de Maio de 2021**.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 20 out. 2022 às 07:43h.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A TRAJETÓRIA DA INTERNET NO BRASIL: DO SURGIMENTO DAS REDES DE COMPUTADORES À. INSTITUIÇÃO DOS MECANISMOS DE GOVERNANÇA**. Disponível em: https://www.researchgate.net/profile/Marcelo-Carvalho-13/publication/268809917_A_TRAJETORIA_DA_INTERNET_NO_BRASIL_DO_SURGIMENTO_DAS_REDES_DE_COMPUTADORES_A_INSTITUICAO_DOS_MECANISMOS_DE_GOVERNANCA/links/54774a430cf2a961e4825bd4/A-TRAJETORIA-DA-INTERNET-NO-BRASIL-DO-SURGIMENTO-DAS-REDES-DE-COMPUTADORES-A-INSTITUICAO-DOS-MECANISMOS-DE-GOVERNANCA.pdf. Acesso em: 04 mai. 2022 às 08:05h.

CRUZ, Diego e RODRIGUES, Juliana. **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 30 ago. 2022 às 09:40h

Ministério Público do Estado do Ceará. **REQUISIÇÃO JUDICIAL DE DADOS E DE PRESERVAÇÃO EXTRAJUDICIAL DE REGISTROS DO FACEBOOK**. Disponível em: http://www.mpce.mp.br/wp-content/uploads/2015/12/Boletim-Caopel-02-requisi%C3%A7%C3%A3o-judicial-facebook.pdf. Acesso em: 31 Out. 2022 às 18:35h.

Ministério Público do Distrito Federal e Territórios – MPDFT. **Facebook: Requisição Judicial de Dados e Pedido de Preservação Extrajudicial de Pedidos**. Dispoível em: https://www.mpdft.mp.br/portal/pdf/imprensa/cartilhas/Cartilha_Facebook_Requisicao_Judicial_Dados.pdf. Acesso em: 31 Out. 2022 às 19:09h.

Ministério Público do Mato Grosso do Sul. **O novo crime de Stalking e algumas de suas implicações**. Disponível em: https://www.mpms.mp.br/noticias/2021/04/o-novo-crime-de-stalking-e-algumas-de-suas-implicacoes#. Acesso em: 16 set. 2022 às 07:12h.

MORAES, Claudia. O impacto das novas tecnologias na sociedade: conceitos e características da Sociedade da Informação e da Sociedade Digital. Disponível em: https://www.researchgate.net/profile/Claudia-Moraes-2/publication/238065799_O_impacto_das_novas_tecnologias_na_sociedade_conceitos_e_caracteristicas_da_Sociedade_da_Informacao_e_da_Sociedade_Digital1/links/58f409060f7e9b6f82e7c45c/O-impacto-das-novas-tecnologias-na-sociedade-conceitos-e-caracteristicas-da-Sociedade-da-Informacao-e-da-Sociedade-Digital1.pdf. Acesso em: 04 mai. 2022 às 17:54h.

MOREIRA, Paulo Roberto Silvério. **Estelionato praticado por meio da internet: Uma visão acerca dos crimes digitais**. Disponível em: https://www.migalhas.com.br/depeso/359821/estelionato-praticado-por-meio-da-internet. Acesso em: 31 ago. 2022 às 06:54h.

NUNES. Sergio. **World Wide Web**. Disponível em: https://web.fe.up.pt/~ssn/teach/cdi/slides/04-web.pdf. Acesso em: 11 out. 2022 07:57h.

PADOVEZ, Rafael Silva e PRADO, Florestan Rodrigo do. **O Direito Penal Brasileiro no contexto dos crimes cibernéticos**. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7962/67648763. Acesso em: 15 ago. 2022 às 07:45h.

Redação. BBC News Mundo. **Google: a nova função para ocultar seus dados pessoais das buscas**. Disponível em: https://www.bbc.com/portuguese/geral-61315133. Acesso em: 05 mai. 2022 às 08:16h.

ROCHA, Carolina Borges. **A evolução criminológica do Direito Penal: aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012**. Disponível em: https://jus.com.br/artigos/25120/a-evolucao-criminologica-do-direito-penal-aspectos-gerais-sobre-os-crimes-ciberneticos-e-a-lei-12-737-2012. Acesso em: 14 mai. 2000 às 08:10h.

ROCHA, Juliano vieira da. **HACKERS e suas características**. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/50168678/Hackers_e_suas_caracteristicas-with-cover-page-v2.pdf?Expires=1652617962&Signature=OWGU1zIKcQWx7FFV~uJz4s1nQj-6~jJQXVl3bcUMh57FPaKhM~XUhiie5zE36uzjn77tUC9HBptid48iRU4wf-F7przjmXOOJ7hSw6Cgn~qmZlEWrDzD9lmMB9MO34EAizaxxepZ4vMMRGF9TtFBK4q-zBaFyu9~xIkiPIaX2i5K6ANyhY4AoZiMgI13QbeyFR7S6QOte~cDF5UDZbychUSEySCtH4KwfzJuaq2BYwSCUlAgFdfivKw5eWnGlNE54Dw1QFLWYP1NOCGivgUj1~pDy0Mx1V9J9pqeHJHEnAYYqiCpHVDpoGrT54PvPdMYVPLGp9ORkpOXoU~pf~jUcg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Acesso em: 14 mai. 2022 às 08:34h.

SANTOS, Cristiane. A Internet como meio de comunicação: possibilidades e limitações. nternet_como_meio_comunicacao-with-cover-page-v2.pdf. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/57799090/Internet_como_meio_comunicacao-with-cover-page-v2.pdf?Expires=1651686940&Signature=RPUMdzhQ1JFRDlSjbliy1l9DjRDXiDlnnnhi6IMbIhHYF9azREo7DKZAwWrCjv3HetuGU0Gac7Grt4E4NU9-5iE6SMSMlG-5~j3eG-TF4P6Nt4vGu9Rh6WEqLaIdLS1rjG7heUvC59sy7AllRdFGB0es98hE0EUxjRk12iQ7fueB0xojhsgZKHT9nccOZe9vptlwTS3iedDc~GUO2fWb~gOsXjAsJz-yeAzanwoePaqu54Kn1FhC-7l0PcnXYeFIOYuc7qoun3Uiqk4ljRll0-DdJ3iPiJOjnsf6m1KmSGBMz03puMV~B-0Co1VG9VDb~Z1sbU7LIFzytCJp9XcOnw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Acesso em: 04 mai. 2022 às 10:00h

WENDT, Emerson e JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos. Ameaças e procedimentos de investigação**. 3ª Edição Rio de Janeiro, 2021 Editora Brasport.

ZANIOLO, Pedro Augusto. **Crimes Modernos. O Impacto da Tecnologia no Direito**. 4ª Edição S Editora JusPODIVM .