Revista Multidisciplinar do Nordeste Mineiro, v.10, 2024
ISSN 2178-6925

O PERFIL DO CRIMINOSO NOS CRIMES CIBERNÉTICOS: COMPORTAMENTOS, MOTIVAÇÕES E TÁTICAS

CRIMINAL PROFILE IN CYBERCRIMES: BEHAVIORS, MOTIVATIONS AND TACTICS

Thaís Gomes Domingos

Graduanda em Direito, Faculdade de Ensino Superior de Linhares, Brasil

E-mail: thaisgomesdomingod@gmail.com

Alexandre Jacob

Mestre, Faculdade de Ensino Superior de Linhares, Brasil

E-mail: alexandre.jacob10@gmail.com

Resumo:

O presente artigo tem como objetivo realizar um estudo sobre os comportamentos, motivações e táticas dos cibercriminoso. A metodologia utilizada baseou-se em pesquisas teóricas e documentais, com consultas à doutrina, jurisprudências, teses, dissertações, além de fontes confiáveis, tanto governamentais quanto não governamentais. O estudo busca responder ao seguinte questionamento como a identificação dos tipos de perfil dos criminosos cibernéticos pode contribuir para o combate, prevenção e criação/aperfeiçoamento da legislação brasileira atual? O presente artigo tem como objetivos estudar sobre a parte histórica da internet e suas subdivisões, além de analisar o modus operandi dos criminosos digitais, assim como compreender a legislação brasileira sobre o tema e entender o perfil dos cibercriminoso. Os crimes cibernéticos estão se tornando uma ameaça crescente no ambiente digital, afetando empresas, governos e indivíduos em escala global. Com o avanço da tecnologia, os métodos utilizados pelos infratores virtuais se tornam mais sofisticados e difíceis de combater.

Palavras-chave: Direito penal. Política criminal. Crimes virtuais. Ciberespaço. Perfil criminoso.

Abstract:

This article aims to conduct a study on the behaviors, motivations and tactics of cybercriminals. The methodology used based on theoretical and documentary research, with consultations of doctrine, case law, theses, dissertations, as well as reliable sources, both governmental and non-governmental. The study seeks to answer the following question: how can the identification of the types of profiles of cybercriminals contribute to the fight, prevention and creation/improvement of current Brazilian legislation? This article aims to study the historical part of the Internet and its subdivisions, in addition to analyzing the modus operandi of digital criminals, as well as understanding Brazilian legislation on the subject and understanding the profile of cybercriminals.

Cybercrimes are becoming a growing threat in the digital environment, affecting companies, governments and individuals on a global scale. With the advancement of technology, the methods used by virtual offenders become more sophisticated and difficult to combat.

Keywords: Criminal law. Criminal policy. Cybercrimes. Cyberspace. Criminal profiling.

1. Introdução

Os crimes cibernéticos vêm se consolidando como uma ameaça crescente no ambiente digital, impactando empresas, governos e pessoas em nível global. Com o avanço da tecnologia, os métodos empregados por infratores virtuais tornam-se cada vez mais complexos e difíceis de conter. Entender o perfil dos indivíduos que realizam essas atividades ilícitas é essencial para desenvolver estratégias de prevenção e combate a esses crimes.

Desse modo, o presente artigo tem como objeto estudo as formas possíveis de prevenção e combate dos crimes virtuais com base na análise dos indivíduos envolvidos neste ilícito penal. A metodologia aplicada neste artigo embasou-se em pesquisas teóricas e documentais, relacionadas ao presente tema com consultas a doutrina, jurisprudências, teses, dissertações e em site confiáveis governamentais e não governamentais, tendo a pesquisa o seguinte questionamento, como a identificação dos tipos de perfil dos criminosos cibernéticos pode contribuir para o combate, prevenção e criação/aperfeiçoamento da legislação brasileira atual?

Infelizmente, está cada vez mais comum na atualidade brasileira as constantes notícias na mídia sobre o aumento incessante dos crimes cometidos através do ambiente virtual, principalmente de estelionatos, os quais geram grandes prejuízos as vítimas. A frequência e a gravidade desses delitos não só acarretam prejuízos financeiros indiretos, mas também prejudicam a economia de todo um país, devido à falta de confiança das vítimas nas plataformas digitais de venda e nas autoridades governamentais responsáveis pela segurança online.

Portanto, é fundamental que tanto as autoridades quanto os setores privados e públicos trabalhem em conjunto para aprimorar as ferramentas de prevenção e resposta a esses crimes. Investir em educação digital, fortalecer as

leis existentes e promover a colaboração entre diferentes entidades pode ajudar a mitigar os impactos negativos e proteger as vítimas.

2. Breve Contexto Histórico da Internet

Para entender o perfil dos criminosos cibernéticos e outras características destes, é essencial compreender a linha do tempo histórica da internet. Ambiente onde essas atividades ilegais se consumam, principalmente por conta da alta possibilidade de camuflagem dos indivíduos:

> Ao operador do Direito, pode parecer estranha a necessidade de conhecer, ainda que superficialmente, alguns aspectos técnicos relacionados à Internet. Afinal, em outras áreas, esse conhecimento técnico dificilmente é necessário: não é preciso saber o que mantém uma aeronave no ar, por exemplo, para pleitear reparação de danos decorrentes de um desastre aéreo, ainda que tal conhecimento possa ser útil (Leonardi, 2019).

A internet se originou através da criação da Advanced Research Projects Agency Network (ARPANET), uma rede de comunicação de dados desenvolvida para fins militares. Sua primeira conexão ocorreu em 29 de outubro de 1969, quando foi planejado um link entre a Universidade da Califórnia e o Instituto de Pesquisa de Stanford, marcando o envio do primeiro e-mail do mundo (Oliveira, 2011).

A ARPANET foi projetada para garantir a comunicação entre militares e cientistas, mesmo em caso de bombardeios, com a intenção de manter a funcionalidade da rede, mesmo que alguns pontos ficassem danificados. Esse contexto é relevante, considerando que a época foi marcada pela Guerra Fria, quando o risco de ataques com bombas e outros armamentos foi significativo (Kleina, 2018).

Com o decorrer dos anos, especialmente a partir de 1982, o uso da ARPANET foi expandido, inicialmente no meio acadêmico, e a rede começou a se estender para outros países como Holanda, Dinamarca e Suécia, passando a ser conhecido como Internet e alterando o antigo nome ARPANET. No entanto, o acesso ainda era restrito às universidades.

Apenas em 1987 foi autorizado o comércio de internet nos Estados Unidos, e os primeiros provedores de internet surgiram em 1992, oferecendo acesso à

população em geral. No mesmo ano, Tim Berners-Lee, cientista, físico e professor britânico, inventou o navegador World Wide Web (WWW), com o objetivo de tornar qualquer informação acessível aos usuários.

Em solo brasileiro a internet chegou de forma experimental somente no ano de 1988 onde houve a conexão entre o Laboratório Nacional de Computação Cientifica, situado no estado do Rio de Janeiro e a Universidade de Maryland, situado nos Estados Unidos, entretanto não havia muitos recursos disponíveis para ser utilizado com a internet, era possível apenas trocar e-mails e compartilhar arquivos, vale ressaltar que as conexões eram feitas via cabo telefônico que eram ligados de ponto a ponto.

Somente no final do ano de 1994 a internet foi lançada de maneira experimental para comercialização por meio da empresa denominada Embratel – Empresa Brasileira de Telecomunicação até então era uma empresa de economia mista a qual foi criada ainda na ditadura militar. Apenas cinco mil usuários foram escolhidos para participar dos testes da internet (Oliveira, 2011).

Após 1995, a internet no Brasil experimentou um crescimento exponencial, alcançando impressionantes 134 milhões de usuários em todo o território nacional. Com essa expansão, as interações virtuais passaram a superar as pessoais na vida de muitas pessoas, principalmente após a pandemia de Covid-19, levando ao surgimento de comportamentos específicos no ambiente digital. Isso gerou uma necessidade urgente de regulamentação desses comportamentos através de leis específicas, que antes eram impensáveis, mas tornaram-se essenciais com o avanço da internet, sendo de extrema importância estudar tais comportamentos.

É importante notar que, além da internet convencional, conhecida como surface web ou “internet da superfície”, acessível por meio de navegadores como Google Chrome e Edge, existe a deep web (internet profunda) e a dark web (internet escura). Estas últimas áreas não são acessíveis pelos métodos tradicionais, necessitando de ferramentas ou conhecimentos especiais para o acesso nesta rede (Fassanaro, 2007).

3. Como os Criminosos Operam no Mundo Digital

No mundo digital, os criminosos utilizam uma variedade de técnicas sofisticadas para explorar vulnerabilidades em sistemas e usuários. Por meio de ataques cibernéticos, como *phishing*, *ransomware* e *malwares*, eles conseguem roubar dados pessoais, bancários e informações corporativas sensíveis.

Além disso, aproveitam-se do anonimato da internet e de criptomoedas para ocultar suas identidades e movimentações financeiras, dificultando a rastreabilidade. Com o avanço tecnológico, esses criminosos estão se tornando cada vez mais habilidosos, exigindo medidas de segurança robustas e constante vigilância por parte de indivíduos e organizações.

É necessário também entender o funcionamento da internet para ser possível entender o modo de operação dos criminosos em ambiente virtual. Como citado anteriormente, existem dois lados da internet, o visível conhecida como aberta ou internet da superfície, onde todos os indivíduos com dispositivos seja computador ou celular acessam livremente, podendo efetuar pesquisas em sites como Google, Yahoo, Bing, entre outros.

Já a outra parte da internet é denominada como *deep web*, traduzida como internet profunda, parte que não é visível. Esta parte é restrita, devido estar armazenado dados como senhas, dados pessoais, conta de redes sociais, e-mails funcionais, entre outros, além de estar presentes as intranets de empresas, governamentais e comunicações (Lima *et al.*, 2019).

A *deep web* possui uma subdivisão denominada como *dark web*, traduzindo diretamente como internet obscura. Para acesso a essa parte da internet são necessários conhecimentos e programas específicos com o navegador Tor. Na *dark web* são praticados diversos ilícitos penais, como venda de dados de pessoas físicas e jurídicas, venda de drogas, armas, materiais que exploram a pornografia infantil, entre outros crimes, tais praticadas se dão devido principalmente a dificuldade de rastreabilidade e consequente identificação dos responsáveis por estes ilícitos penais (Lima *et al.*, 2019).

A obtenção de dados de pessoas físicas ou jurídica se principalmente através da aplicação do método phishing, que segundo Instituto de Tecnologia da Informação e Comunicação do Estado do Espírito Santo:

> Mesmo que você não saiba o que é phishing, já deve ter recebido um e-mail com o título “Atualize seus dados” ou “Você acaba de se tornar o mais novo milionário”. Essas mensagens são extremamente comuns e se configuram em um cibercrime conhecido como *phishing* (Prodest, 2024).

Através do phishing, enviados por e-mail e mensagens de texto na maior parte das vezes disparados em massa, os criminosos conseguem convencer as vítimas a clicarem no link em anexo, momento em que um aplicativo ou programa denominado como malware, é instalado no computador ou celular, e imediatamente inicia-se a captura de diversos dados, por exemplo senhas bancárias. Os criminosos que praticam este tipo de estelionato estão cada vez mais se aperfeiçoando na aplicação do phishing, recentemente um indivíduo foi preso no estado de São Paulo com equipamentos integrados que disparavam mensagens de texto para celulares da região que circulava, sempre por bairros tidos como nobres (Tomaz *et al.*, 2024).

Com esses dados em mãos, os criminosos vendem estes através da dark web para outros indivíduos que utilizam os dados pessoais como informações bancárias para efetuar outras fraudes com objetivo de obter quantias significativas. Esta prática tem sido cada vez mais comum, somente entre os anos de 2021 e 2022, foram detectadas 134 milhões de tentativa de phishing no Brasil.

Além de vender os dados obtidos de maneira fraudulenta, os criminosos podem ter acesso a aplicativos de bancos instalado por exemplo no celular da vítima, dessa forma efetuam transferência de todo o valor presente nas contas bancária para outras contas bancárias, e em seguida os valores são trocados por moedas virtuais. O que torna difícil a rastreabilidade visto que as moedas virtuais não dependem de intermédio por exemplo de um banco para que seja efetuada a transferência para outro indivíduo, devido utilizar a tecnologia conhecida como blockchain, em tradução denominado cadeia de blocos:

> O surgimento da tecnologia blockchain está intrinsicamente associado à criação da primeira moeda virtual, o Bitcoin, em 2009 – e não por acaso. Isso porque é a referida tecnologia, desenvolvida por seu preceptor, Satoshi Nakamoto, a que assegura a veracidade das criptografias que caracterizam as moedas virtuais e garante a validade das transações feitas entre uma parte e outra, sem a intervenção de uma autoridade central estatal (Schiavon, 2020).

A evolução do mundo digital proporcionou aos criminosos um vasto campo de atuação, permitindo que suas operações sejam realizadas de forma cada vez

mais sofisticada e difícil de rastrear. O surgimento de moedas virtuais também contribui com o modus operandi deste tipo de criminoso, visto que garantem além do anonimato, também uma forma de manter as quantias inacessíveis.

4. A Legislação Brasileira no Combate aos Crimes Virtuais

A primeira Lei Federal a tratar dos direitos vinculados ao uso da internet foi a Lei nº. 12.965 de 2014, conhecida como Marco Civil da Internet (Brasil, 2014). Antes disso, não havia uma legislação específica sobre o assunto. Vale mencionar que a internet começou a ser amplamente comercializada no Brasil em 1995, com a criação da Portaria Interministerial nº. 147, que distribuía o Comitê Gestor da Internet no Brasil. Entretanto, a formação desse comitê foi tardia, já que o uso civil da internet era possível.

A Portaria Interministerial nº. 147/1995, sofreu mudanças significativas a partir do Decreto nº. 4.829/2003, principalmente sobre o regulamento de questões técnicas aprofundadas como a utilização de domínios, por exemplo “.br”. Apesar de apenas em 2014 ter sido promulgada a chamada "Constituição da Internet", a Lei nº. 12.965/2014, conhecida como Marco Civil da Internet, que trata de artigos essenciais, observa-se um atraso significativo em comparação a outros países, como Portugal, que desde 1976 incluiu em sua constituição disposições sobre o uso da internet.

Esse atraso revela uma lacuna na legislação brasileira da época, pois direitos fundamentais dos usuários da internet já deveriam estar previstos na constituição vigente. O Marco Civil da Internet estabeleceu regras claras para o uso da rede, o que era necessário, já que, para muitos brasileiros, a internet era vista como uma "terra sem lei". Isso se justificava pelo princípio da legalidade, previsto no art. 5º, II da Constituição da República de 1988 e no art. 1º do Código Penal brasileiro, que determina que não há crime sem lei anterior que o defina:

> O Marco Civil é considerado uma vitória da sociedade brasileira. Uma reclamação da sociedade civil, em 2009, que repudiou as iniciativas no sentido de criminalizar condutas na Internet, exigindo, antes, que o Congresso desse uma carta de direitos dos internautas (Kleina, 2018).

No ano de 2018, foi proposto o projeto de lei complementar nº. 53/2018, projeto este que deu origem a Lei nº. 13.709/2018, denominada como Lei Geral

de Proteção de Dados Pessoais. Mesmo após promulgação está lei só entrou em vigor no ano de 2021, ou seja, aproximadamente três anos depois de sua promulgação:

> A norma protege de forma ampla os dados pessoais, cria direitos do titular, enumera as hipóteses autorizadas para tratamento, além de prever responsabilidades e sanções de ordem administrativa e pecuniária de ressarcimento de danos por vazamentos (Lima *et al*., 2019).

A legislação penal brasileira, assim como as legislações destacadas anteriormente, levou muito tempo para serem promulgadas. A primeira lei brasileira que tipificou penalmente as condutas realizadas em ambiente virtual foi a Lei nº. 12.735/2012, a referida lei teve origem do Projeto de Lei nº. 84 de 1999, sendo o autor o Deputado Federal Luiz Piauhylino, incrivelmente o referido Projeto de Lei se transformou em Lei somente treze anos depois de sua criação.

No ano de 2012 foi promulgada a Lei nº. 12.737/2012 a qual tipificou criminalmente os delitos informáticos, está lei ficou conhecida como Lei Carolina Dieckmann. Esta lei foi recebeu o nome da atriz, devido a um fato que ocorreu com a atriz muito conhecida a época Carolina Dieckmann, a qual teve seu computador invadido e em seguida o criminoso exigiu a quantia de R$10.000,00 para não divulgar as 36 fotos intimas, entretanto, a atriz não cedeu, com isso teve as fotos divulgadas, ganhando muito repercussão a época na mídia (Fachini, 2023).

A Lei nº. 12.737 de 2012 acrescentou diversos artigos ao Código Penal brasileiro de 1940, incluindo alguns que representam um importante avanço na legislação brasileira no campo da informática. Um deles é o artigo 154-A, que trata da invasão de dispositivo informático e apresenta a seguinte redação inicial:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena. Detenção, de 3 (três) meses a 1 (um) ano, e multa.
> §1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> §2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> §3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

> Pena. Reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> §4º Na hipótese do §3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> §5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I – Presidente da República, governadores e prefeitos;
> II – Presidente do Supremo Tribunal Federal;
> III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV – Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal (Brasil, 1940).

Em 2021, foi aprovada a Lei nº. 14.155, que aumentou a pena para o crime de invasão de dispositivo informático previsto no art. 154-A do Código Penal brasileiro. A pena, que antes era de detenção de 3 meses a 1 ano, e multa, passou a ser de reclusão de 1 a 4 anos. Além disso, houve um aumento nas causas de majoração de pena previstas no §2º do mesmo artigo, que passou de um sexto a um terço para um terço a dois terços.

A Lei nº. 14.155 também inovou em incluir o §4º-B ao art. 155 do CP que incluiu como furto qualificado o crime de furto mediante fraude que é cometido por meio de eletrônico ou informático, tendo como pena reclusão de 4 (quatro) a 8 (oito) anos, além do mais adicionou o §2º-A e §2º-B ao art. 171 que dispõe sobre a fraude eletrônica nos casos de estelionato tendo como pena reclusão de 04 (quatro) a 08 (oito) anos, contando ainda com causa de aumento de pena dependendo do resultado da conduta com aumento de um terço a dois terços da pena.

Está tramitando, atualmente na Câmara dos Deputados o Projeto de Lei nº. 583/20 que tem como objetivo atualizar a Lei nº. 12.737/2012, a Lei Carolina Dieckmann. Uma das propostas do projeto de lei é obrigar os fabricantes de aparelhos celulares ou qualquer outro tipo de aparelho fotográficos terão que emitir sons como câmeras antigas, a fim de dificultar que os criminosos utilizem tais aparelhos para fotografar sem permissão (Fachini, 2023). Outro Projeto de lei, que está em andamento também na câmara dos Deputados é o Projeto de Lei nº. 537/24, este tem o objetivo fortalecer as ações repressivas contra crimes cibernéticos, assim como fortalecer a atividade de inteligência policial a qual é de suma importância para o combate desses ilícitos penais (Júnior; Becker, 2024).

5. O Perfil do Criminoso Virtual

O perfil do criminoso virtual é marcado pela sua capacidade de explorar vulnerabilidades tecnológicas, agindo de maneira sofisticada e, muitas vezes, invisível. Diferente dos criminosos tradicionais, esses indivíduos utilizam o conhecimento avançado em tecnologia e redes de computadores para cometer uma ampla variedade de delitos, desde fraudes financeiras até a invasão de sistemas sigilosos.

O anonimato proporcionado pela internet e a constante evolução dos meios digitais tornam esses crimes complexos e desafiadores para as autoridades, que muitas vezes enfrentam dificuldades em rastrear e punir os responsáveis.

Sobre o perfil do criminoso digital:

> O perfil do criminoso, baseado em pesquisa empírica, indica jovens, inteligentes, educados, com idade entre 16 e 32 anos, do sexo masculino, magros, caucasianos, audaciosos e aventureiros, com inteligência bem acima da média e movidos pelo desafio da superação do conhecimento, além do sentimento de anonimato, que bloqueia seus parâmetros de entendimento para avaliar sua conduta como ilegal, sempre alegando ignorância do crime e, simplesmente, “uma brincadeira” (Silva, 2000).

O criminoso digital, cujo perfil difere daquele que usa armas para intimidar ou cometer assaltos. Geralmente, é uma pessoa jovem, extremamente inteligente, que opera confortavelmente atrás de um computador. Com paciência e algumas teclas digitadas, esse indivíduo pode realizar fraudes milionárias em bancos, roubar dados de cartões de crédito de cidadãos inocentes, compartilhar suas patologias sexuais com outros ou até mesmo causar apagões em um estado inteiro (Fassanaro, 2007).

Com base no perfil apresentado, fica claro que o criminoso digital foge dos estereótipos tradicionais de criminalidade. Suas ações são frequentemente impulsionadas por uma sensação de impunidade e anonimato proporcionados pelo ambiente virtual. Além disso, o desafio intelectual de ultrapassar barreiras tecnológicas serve de estímulo para esses indivíduos, que enxergam o crime como uma forma de testar suas habilidades, sem levar em conta as implicações legais ou éticas de seus atos.

A complexidade desses crimes torna sua investigação especialmente desafiadora para as autoridades. São necessárias habilidades técnicas avançadas e ferramentas especializadas de rastreamento digital, além de uma colaboração internacional eficaz, dado que muitos crimes cibernéticos ocorrem em escala global. A rápida evolução tecnológica também coloca à prova as legislações vigentes, que frequentemente se mostram inadequadas e desatualizadas para acompanhar o ritmo do avanço da criminalidade digital.

Assim, o combate e a prevenção ao crime cibernético exigem não só a modernização das leis e a capacitação dos órgãos de segurança, mas também a conscientização da população sobre os perigos envolvidos. A educação digital e a adoção de boas práticas de segurança online são essenciais para reduzir as brechas exploradas por esses criminosos, que se beneficiam tanto de falhas tecnológicas quanto da negligência dos usuários na proteção de suas informações.

6. Conclusão

O direito penal brasileiro caminha em passos lentos quanto as evoluções tecnológicas no mundo, diante da crescente sofisticação dos crimes cibernéticos e das dificuldades enfrentadas pelas autoridades para identificar e punir os responsáveis, fica evidente a urgência de uma abordagem mais integrada e proativa no combate a essas atividades ilícitas. O avanço da tecnologia trouxe tanto benefícios quanto riscos, sendo essencial que governos, empresas e indivíduos invistam na conscientização e na implementação de medidas robustas de segurança.

O perfil do criminoso digital apresentado no artigo aponta para um padrão específico que deve ser levado em conta no desenvolvimento de políticas públicas e de estratégias de prevenção. Por fim, a educação digital da população, a adoção de boas práticas de segurança e o fomento à cultura da proteção de dados são fatores determinantes para minimizar o impacto dos crimes cibernéticos, promovendo um ambiente virtual mais seguro e confiável para todos.

A modernização contínua das legislações, como as já discutidas no âmbito brasileiro, é vital para garantir a proteção de direitos no ambiente digital, além de fortalecer a punição e dissuasão de crimes virtuais. No entanto, a legislação por si só não basta. É preciso que ocorra uma capacitação efetiva das forças policiais e judiciais para lidar com o caráter global e muitas vezes anônimo desses delitos, assim como uma cooperação internacional sólida para enfrentar crimes que ultrapassam fronteiras.

Assim, o direito penal brasileiro ainda não conseguiu acompanhar as evoluções tecnologias, com isso, a criminalização e responsabilização dos indivíduos que utilizam as redes de computadores para praticar crimes é extremamente difícil de acontecer.

7. Referências

BRASIL. **Decreto-lei nº. 2.848 de 07 de dezembro de 1940**. Código penal. Rio de Janeiro: Catete, 1940. Disponível em: https://tinyurl.com/4t8n6dw6. Acesso em: 15 set. 2024.

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: Senado, 2014. Disponível em: https://tinyurl.com/47cw98p9. Acesso em: 15 set. 2024.

BRASIL. **Lei nº. 13.709 de 14 de agosto de 2018**. Lei geral de proteção de dados. Brasília-DF: Senado, 2018. Disponível em: https://tinyurl.com/mtcea948. Acesso em: 15 set. 2024.

FACHINI, Tiago. Lei Carolina Dieckmann: tudo o que você precisa saber sobre. **Projuris**, 05 set. 2023. Disponível em: https://tinyurl.com/zwvu4tdn. Acesso em: 15 set. 2024.

FASSANARO, Mariella de Lima. **Crimes na internet**: o perfil do novo criminoso e a dificuldade de tipificação do delito. 2007, 58 f. Monografia (Graduação em Direito) – Universidade Federal do Ceará, Fortaleza, 2007.

JÚNIOR, Janary; BECKER, Marcia. Projeto prevê medidas para fortalecer investigação de crimes cibernéticos. **Câmara dos Deputados Notícias**, 21 mar. 2024. Disponível em: https://tinyurl.com/3bppra7z. Acesso em: 06 out. 2024.

KLEINA, Nilton. Como tudo começou: a história da internet no Brasil. **TecMundo**, 01 maio 2018. Disponível em: https://tinyurl.com/4r8rhjx8. Acesso em: 19 set. 2024.

LEONARDI, Marcel. **Fundamentos de direito digital**. São Paulo: Revista dos Tribunais, 2019.

LIMA, Ana; HISSA, Carmina; SALDANHA, Paloma. **Direito digital**: debates contemporâneos. São Paulo: Revista dos Tribunais, 2019.

OLIVEIRA, Marcos. Nasce a internet: os passos científicos e tecnológicos que fizeram a grande rede mundial de computadores. **Pesquisa Fapesp**, n. 180, 2011. Disponível em: https://tinyurl.com/y4ehu5hr. Acesso em: 19 set. 2024.

PRODEST. Instituto de Tecnologia da Informação e Comunicação do Espírito Santo. **Entenda o que é phishing e adote medidas para evitá-lo**. 2024. Disponível em: https://tinyurl.com/mrxrvwju. Acesso em: 06 out. 2024.

SCHIAVON, Thaís. O blockchain no âmbito internacional: de “vilão” a mocinho e os desafios restantes. *In*: FALCÃO, Cintia; CARNEIRO, Tayná. **Direito exponencial**: como as novas tecnologias redefinirão o jurídico do futuro. São Paulo: Revista dos Tribunais, 2020.

SILVA, Mauro Marcelo de Lima. Os crimes digitais hoje: especialista dá o perfil do crime e do criminoso na Internet. **Consultor Jurídico**, 02 set. 2000. Disponível em: https://tinyurl.com/348ybh73. Acesso em: 06 out. 2024.

TOMAZ, Kleber; PEREZ, Alfredo; FERREIRA, Dalton. Motorista é preso com 'carro do golpe'; veículo equipado disparava falsos anúncios bancários para roubar dados de vítimas em SP. **G1 São Paulo**, 29 jul. 2024. Disponível em: https://tinyurl.com/e7sbbtx8. Acesso em: 19 set. 2024.