Revista Nativa Americana de Ciências, Tecnologia & Inovação, v.4, n.1, 2023
ISSN: 2764-1295
Centro Universitário São Lucas Ji-Paraná – JPR

Instruções preventivas contra crimes *cybernéticos* e orientações da perícia forense computacional

Kewry Mariobo Franck[1*], Romario Vitorino Ferreira[2]

[1]Graduanda em Sistemas de Informação, Centro Universitário São Lucas Ji-Paraná (JPR), Ji-Paraná, RO, Brasil. E-mail: kewryfranck@gmail.com.
[2]Especialista e Professor do Curso de Bacharelado em Sistemas de Informação, Centro Universitário São Lucas Ji-Paraná (JPR), Ji-Paraná, RO, Brasil. E-mail: romariovitorio@hotmail.com.

***Autor correspondente:** Kewry Mariobo Franck. Centro Universitário São Lucas Ji-Paraná (JPR), Câmpus Ji-Paraná. Av. Engenheiro Manfredo Barata, Bairro Aurélio Bernardes, Ji-Paraná, RO, Brasil. E-mail: kewryfranck@gmail.com.
Recebido: 18/06/2023 **Aceito:** 25/07/2023.

Resumo
Os crimes *cybernéticos* são atividades criminosas que tem como alvo ou faz uso de um computador, uma rede de computadores ou ainda um dispositivo conectado em rede. A perícia Forense Computacional investiga *cybercrimes*, por isso desenvolve importante trabalho de segurança para a sociedade. O objetivo desse estudo foi realizar um levantamento de dados com a finalidade de divulgar instruções preventivas contra crimes *cybernéticos* e propor orientações da perícia forense computacional, à qual se baseia na legislação penal brasileira. Trata-se de uma pesquisa quali-quantitativa sobre a segurança da informação. O estudo tem caráter exploratório descritivo, objetivando analisar, sistematizar, comparar e cruzar dados entre diferentes literaturas científicas. Foi realizada a análise bibliométrica para divulgar e organizar um conjunto de instruções e normativas, para orientação na defesa contra *cybercrimes*, assim como a divulgação do trabalho dos profissionais de perícia forense computacional. Esse estudo disponibiliza informações na forma de instruções preventivas contra crimes *cybernéticos*. Isso através da conscientização dos procedimentos orientados pela Perícia Forense Computacional. Foram explicitadas as evidências e as categorizações dos crimes digitais, assim como as principais instruções de como evitá-las e inibi-las. Foi possível compreender as atualizações da legislação brasileira e da atuação dos peritos forenses computacionais. É preciso combater os crimes *cybernéticos* principalmente nas redes sociais e foi apresentado também o acolhimento de ideias para manter o bem-estar dos usuários, seja pessoa física ou jurídica. Foram descritos os processos de desenvolvimento do combate aos cybercriminosos para dispositivos móveis ou plataforma *Web*.
Palavras-chave: Análise forense de redes. legislação penal brasileira. *Cybercrimes*. Segurança da informação. Soluções digitais.

Abstract
Cybercrimes are criminal activities that target or use a computer, a computer network or a networked device. Computational Forensic expertise investigates cybercrimes, which is why it develops important security work for society. The aimed of this study was to carry out a data survey in order to disseminate preventive instructions against cybercrimes and to propose guidelines for computer forensic expertise, which is based on Brazilian criminal law. This is a quali-quantitative research on information security. The study has a descriptive exploratory character, aiming to analyze, systematize, compare and cross data between different scientific literatures. Bibliometric analysis was carried out to disseminate and organize a set of instructions and regulations, for guidance in the defense against cybercrimes, as well as the dissemination of the work of computer forensics professionals. This study provides information in the form of preventive instructions against cybercrimes. This is done by raising awareness of procedures guided by Computational Forensic Expertise. The evidence and categorization of digital crimes were explained, as well as the main instructions on how to avoid and inhibit them. It was possible to understand the updates of Brazilian legislation and the performance of computer forensic experts. It is necessary to combat cybercrimes mainly on social networks and the reception of ideas to maintain the well-being of users, whether individuals or companies, was also showed. The development processes for combating cybercriminals for mobile devices or the Web platform were described.
Keywords: Brazilian criminal law. Cybercrimes. Digital solutions. Forensic analysis of networks. Information security.

1. Introdução

Os crimes *cybernéticos* ou *cybercrimes* são atividades criminosas que tem como alvo ou faz uso de um computador, uma rede de computadores ou ainda um dispositivo conectado em rede (LIMA; SOARES, 2022). Mais especificamente, a maioria dos *cybercrimes* são cometidas por *cybercriminosos* ou *hackers* que querem ganhar dinheiro à custas dos usuários. Enquanto a perícia forense computacional, a área cuja função é a investigação de crimes digitais, investigação de seus fatos e a coleta dos dados para evidenciar o *cybercrime*. Os peritos dessa área de conhecimento empregam procedimentos para detectar o crime e identificar o criminoso, para que a evidência não seja comprometida ou perdida (PEREIRA; OLIVEIRA, 2019). Diante disso, a

perícia forense computacional define-se como a qualidade de perícia criada para contraditar e combater os crimes digitais, adotando análises e métodos apropriados para detectar e coletar evidências suficientes para identificar os *cybercriminosos*. Então, de acordo com Peixoto (2012, p.42), para a perícia criminal da polícia, a computação forense envolve o trabalho investigativo e toda função pericial, para desvendar cybercrimes. Essa função pode ser empregada para fins legais de investigação de espionagem industrial, assim como as ações disciplinares internas, por exemplo, o emprego indevido de recursos de uma pessoa jurídica.

Atualmente, com o desenvolvimento do conhecimento em tecnologia da informação, houve a introdução do conceito de computação em nuvem móvel (CNM)), em que os dados são armazenados e os aplicativos são processados em nuvens computacionais. O NCM é empregado para inibir problemas relacionados à duração da bateria, poder computacional, capacidade de memória e atrasos de processamento em dispositivos *smartphones* (SHIRAZ *et al.*, 2013). Especificamente, aplicativos computacionalmente intensivos são descarregados para a nuvem, que executa e retorna os resultados de volta para o dispositivo smartphone (SHIRAZ; GANI, 2014). Esses aplicativos são executados em recursos remotos, como máquinas físicas e virtuais, fornecidos por provedores de serviços em nuvem. Os usuários desconhecem o local onde os aplicativos descarregados são executados. Esta condição implica que a execução das aplicações seja transparente devido ao conceito de virtualização no CNM (TZANAKAKI et al., 2013). No entanto, nenhum processo no CNM é possível sem links de rede que conectam recursos dentro e fora da nuvem. Esses *links* de comunicação de rede no MCC são chamados de "posicionamento de rede" (DINH *et al*., 2011). Todas as posições de rede no CNM estão sujeitas a *cyberataques* de rede que afetam vários *hosts*, servidores e *data centers*. Os invasores acessam *links* de rede e executam ações maliciosas em pacotes de rede para propagar efeitos adversos aos recursos da nuvem. São exemplos de *cyberataques*, espionagem, modificação de dados, falsificação de endereço IP, DoS, DDoS, *man-in-the-middle* e modificação de conteúdo de pacote (HANSMAN; HUNT, 2005). Foram vários os pesquisadores que propuseram estruturas forenses de rede (EFRs) para explorar evidências digitais e identificar a origem dos *cyberataques* (JEONG; LEE, 2014), detectar códigos maliciosos (KIM *et al*., 2013) e monitorar as atividades dos invasores em redes tradicionais (KHAN *et al*., 2014). No entanto, as redes CNM carecem de EFRs, que são necessários devido ao número de *cyberataques* que ocorrem nas redes CNM.

Os *cybercriminosos* acessam os recursos da nuvem por meio de redes de acesso à nuvem e realizam ações maliciosas dentro da nuvem (GUPTA *et al*., 2013). É necessária uma abordagem abrangente para investigar esse comportamento malicioso, extraindo evidências legais de vários dispositivos de rede e posições de rede no CNM, o que só é possível quando uma investigação forense de rede tem acesso às redes do CNM. A investigação forense tem acesso apenas à rede de acesso à nuvem e não ao data center e às redes *intercloud* no CNM (ZAWOAD; HASAN, 2013). Essa limitação restringe a capacidade da investigação forense detectar *cyberataques* e identificar evidências encontradas nas redes dentro da nuvem. Para resolver esse problema, os serviços em nuvem devem realizar sua própria análise forense de rede e identificar evidências legais. Essa abordagem forneceria análise forense como um serviço para usuários CNM (RUSSO, 2019). Vários EFRs atuais podem ajudar os PSNs a se adaptarem às redes CNM para identificar vulnerabilidades e a origem dos cyberataques (CHEN et al., 2013; WANG et al., 2013). No entanto, estudos abrangentes sobre a adaptabilidade dos EFRs atuais para redes CNM são bem pouco disponíveis. Por isso, é necessário abordar sobre os *cyberataques* e a falta de EFRs para redes CNM, assim como divulgar instruções preventivas e acatar as recomendações de solução da perícia forense computacional, à qual se

baseia na legislação brasileira no combate a *cybercrimes*. Diante desse contexto, como é possível estender esse conhecimento à sociedade? Como levar as instruções legais para inibir *cyberataques* às instituições? Talvez tornar disponível à mão a legislação penal vigente e divulgar sugestões de atualizações e melhorias a essa legislação. Assim como, maior divulgação de informações sobre *cybercrimes* e a existência da perícia forense computacional. Além disso, elevar o nível de seguimento e bom uso das tecnologias da informação por parte dos usuários. Com a utilização cada dia mais frequente dos dispositivos móveis, computadores e emprego da computação em nuvem, os usuários pessoas físicas e jurídica devem ter mais cuidados com relação aos riscos de má utilização desses recursos.

A perícia forense computacional investiga *cybercrimes*, portanto desenvolve importante trabalho para a sociedade que talvez desconheça sua existência e sequer conhece um conjunto de instruções e normativas vigentes informadas para orientação na defesa contra *cybercrimes*. Mediante ao cenário apresentado é necessário criar meios de divulgação das informações de *cybercrimes* e também desenvolver meios de recomendar instruções preventivas. Por isso, o objetivo geral desse estudo foi realizar um levantamento de dados com a finalidade de divulgar instruções preventivas contra crimes *cybernéticos* e propor orientações da perícia forense computacional, à qual se baseia na legislação penal brasileira.

2. Metodologia

Trata-se de uma pesquisa quali-quantitativa onde tende a enfatizar os aspectos dinâmicos, holísticos e individuais da experiência humana com a segurança da tecnologia da informação. Dessa forma, para apreender a totalidade do conhecimento daqueles que vivenciam o fenômeno abordado. Essa pesquisa envolve o pensamento positivista lógico, procurando enfatizar o raciocínio dedutivo, as regras da lógica e os atributos mensuráveis da experiência humana com a regulação de ações nas redes de computadores. Portanto, o estudo tem caráter exploratório descritivo, objetivando analisar, sistematizar, comparar e cruzar dados entre diferentes literaturas científicas relacionadas ao tema. As buscas na *Web*, armazenamento e análise de dados foram realizadas de junho a dezembro de 2022.

O estudo aborda sobre as atribuições da perícia forense computacional, sua importância e seu papel na segurança digital da sociedade. Como também, esclarecer sobre suas funções e o grau de conhecimento sobre essa área de conhecimento para combater *cybercrimes*. Primeiramente, dados foram levantados de artigos científicos em bases bibliográficas reconhecidas, por isso foi empregado o *software Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA), para identificar, triar e analisar os documentos publicados nas bases Google Acadêmico, Hindawi e Scielo. E também, foram realizadas buscas de trabalhos (livros, capítulos de livros, monografias, dissertações de mestrado e teses de doutorado) em repositórios de Universidades públicas e privadas.

Os descritores utilizados foram análise forense de redes, estruturas forenses em rede, legislação penal brasileira, redes de computadores, *cybercrimes*, computação em nuvem móvel, e outras. As buscas foram realizadas nas línguas portuguesa e inglesa, com palavras e termos separados pelos operadores booleanos 'AND' e 'OR' de acordo com os objetivos de busca em cada tópico abordado nos resultados. Por fim, foi realizada a análise bibliométrica de pesquisas para divulgar e organizar um conjunto de instruções e normativas vigentes, para orientação na defesa contra *cybercrimes* assim como a divulgação do trabalho dos profissionais da área de perícia forense computacional. O programa utilizado para armazenamento dos dados foi o *Dropbox*^{TM} (versão 3.3, 2019). Os dados armazenados, depois de transformados em informação, foram

sistematizados e interpretados com o auxílio do aplicativo *DataMelt* (versão 7, 2020).

3. Resultados e Discussão

3.1. Procedimentos da perícia forense computacional

De acordo com Pereira e Oliveira (2019), essa categoria de perito forense segue algumas etapas específicas de investigação. A começar pela Etapa 1. Coleta – trata-se da fase que o perito realizado busca, coleta e catalogação de dados que podem ser considerados ativos e inativos, isto é, explícitos e ocultos, devendo eles serem preservados. O perito forense deve coletar conforme a ordem de volatilidade, a considerar os dados mais inconstantes e em seguida os equipamentos quede devem ser embalados, etiquetados e suas identificações registradas para a condução da investigação. Nessa primeira etapa qualquer erro prejudicaria todo o processo investigativo, porque falha nesse momento de coleta de informações poderia comprometer a decisão da justiça (SOUZA, 2017).

A Etapa 2 – trata-se da fase para procurar os dados fotos, vídeos e informações escondidas nas evidências coletadas, selecionando e utilizando ferramentas e também técnicas para extração de informações importantes para o caso sempre mantendo a integridade das Informações obtidas (SOUZA, 2017). Em seguida, a Etapa 3 – que por meio da análise realiza-se exames sobre evidências importantes e relevantes para a investigação. E assim, por meio da Etapa 4 – o relatório que é a faze final para condução da escrita dos procedimentos usados na investigação, quais os dados que foram recuperados durante a mesma contendo relevância para o caso. O relatório deve ser produzido com escrita adequada que garanta a compreensão e o entendimento por parte de todos.

Uma perícia forense em uma máquina suspeita envolve vários conhecimentos técnicos e o emprego de ferramentas adequadas para análise, utilização a qual é justificada pela necessidade de não alterar o sistema analisado (PEREIRA; OLIVEIRA, 2019). As técnicas de investigação estabelecida, durante uma investigação, dependem do tipo de crime que foi cometido. Por exemplo, se o crime for de acesso não autorizado o perito buscará evidências de conexão, de arquivos confidenciais que foram alterados ou roubados, de logs. Se o crime for de pornografia o perito deve identificar, vídeos, fotos, mensagens e muitas dessas analisem são conduzidas na hora, conhecida como análise online, que consiste na investigação do equipamento ainda em funcionamento que permite a identificação do flagrante dos processos em execução, portas abertas no sistema e pela rede. Na análise online a preservação da evidência é o principal foco para não alterar logicamente os dados coletados e garantir que não sejam perdidos. Para que isso não aconteça utiliza-se a cadeia de custódia.

Conforme comentado acima, a cadeia de custódia é um registro detalhado das evidências que foram coletadas. Este processo de registro deve conter: a identificação de todas as evidências coletadas; as informações de quais pessoas tiveram acesso às elas (no momento do flagrante); onde elas estavam (fisicamente) no momento da coleta; registro de trânsito das evidências entre os peritos e mídias. Estes cuidados preservam as responsabilidades conhecidas institucionalmente e garantem a qualidade nas fases dos processos de investigação. Assim, poderão ser evitados questionamentos no tribunal sobre a legitimidade das informações coletadas na investigação (PEREIRA; OLIVEIRA, 2019).

Tal procedimento preponderante é muito importante para a garantia e transparência na apuração criminal quanto à prova material, sendo relato fiel de todas as ocorrências da evidência, vinculando os fatos e criando um lastro de autenticidade jurídica entre o tipo criminal, autor e vítima (EDINGER, 2016). Propõe que se entenda por cadeia de custódia "o conjunto de

procedimentos que visa garantir a autenticidade dos materiais que serão submetidos a exames, desde a coleta até o final da perícia realizada" (BONACCORSO, 2005). De acordo com o mesmo autor, a cadeia de custódia é uma lista de todas as pessoas que estiverem de posse de um item de evidência. Porque será ferramenta para documentação que contêm toda identificação de evidência e de indivíduos que custodiaram o item. No campo da investigação, o perito forense coletará evidências embaladas e levadas ao laboratório, comumente, o profissional coleta evidência não necessárias para a condução do caso em processo, no entanto não se deve deixar de lado qualquer evidência significativa, a seguir abordará o que é uma evidência digital e seus tipos para obter informações.

3.2. Evidências digitais e *cybercrimes*

Existem diversas evidências para se comprovar um determinado delito, e que podem ser qualquer tipo de dados armazenados em diferentes dispositivos com a finalidade de coletar e devidamente preservado para depois serem analisados pela perícia. A evidência é um resquício, mediante a oportunidade esmiuçar exames, análises e interpretações de dados pertinentes, os quais se enquadram inequívoca e objetivamente na circunscrição do delito (CHAQUIAN FILHO *et al*., 2018). Conforme esses autores os *cybercrimes* podem ser categorizados como: documentais, ameaças através de endereços eletrônicos (*e-mails*), *softwares* maliciosos, vídeos e fotos de pornografia infantil, evidências de conexões de redes estabelecidas entre computadores, mensagens de *Short Message Service* (SMS) e qualquer dado que possa armazenar em dispositivos móveis. Portanto, as evidências são provenientes de *cybercrimes* cometidos por criminosos digitais, com a finalidade de ser utilizada para a solução de um caso, no mundo virtual há uma variedade de crimes que são cometidos diariamente sem o conhecimento dos usuários.

Os *cybercrimes* acontecem porque as tecnologias por mais avançadas que sejam elas possuem falhas de segurança, permitindo que os criminosos digitais explorem suas vulnerabilidades. Portanto, qualquer descuido do usuário será uma porta de entrada (COSTA *et al*., 2021). Contudo, com o decorrer das décadas dos anos 2000, as práticas dos crimes vêm se inovando, os alvos também têm variado, mas isso não significa que os crimes tradicionais são esquecidos. Portanto, os usuários ainda não têm tomado os cuidados necessários. Os *cybercrimes* envolvendo um computador, sistema, rede de computadores ou qualquer outro meio eletrônico com acesso não autorizado provocando danos a pessoas físicas e jurídicas (CHAQUIAN FILHO *et al*., 2018).

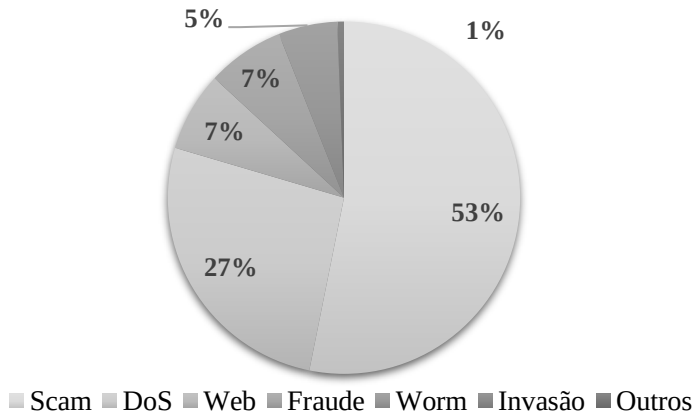
De acordo com Almeida *et al.* (2015, p.215), os *cybercrimes* podem ser classificados como: (i) *cybercrime* puro: qualquer conduta envolvendo a parte de *hardware* ou *software* de um computador, sendo assim toda conduta pratica contra os componentes do computador e seus dados; (ii) *cybercrime* misto: conduta que emprega a internet para realizar o crime, o foco não é o computador da vítima, as todo bem jurídico; (iii) *cybercrime* comum: é a conduta que emprega a internet como ferramenta para cometer delitos, sendo o principal a pornografia infantil onde se utiliza plataformas desde as salas de bate-papo aos *e-mails*; (iv) *cybercrime* próprio: conduta onde ocorre a violação do sistema, no entanto, trata-se do crime onde ocorre roubo de dados, alteração ou exclusão de dados; e por fim (v) *cybercrime* impróprio: conduta que emprega o computador para cometer o delito ao bem jurídico como forma de injúria, difamação ou fraude.

Com altíssimo crescimento do número de usuário no mercado da tecnologia no Brasil, por consequência também cresceu o número de registro de *cybercrimes*, que por sua vez não é

diferente de um crime tradicional perante a justiça. Um estudo desenvolvido pela empresa de segurança *Cybersegurança Symanter* (2018), por meio de um formulário *online*, incluindo a previsão e coleta de informações em outras fontes de dados, resultou em que mais de 62 milhões de usuários sofreram *cybercrimes* no Brasil apenas no ano de 2017 (Figura 1).

Apesar do número de vítimas estar crescendo todos os anos, os usuários ainda comentem algumas falhas em relação ao emprego de tecnologias digitais. Paralelamente a esse contexto, dos mais de 62 milhões de registros de *cybercrimes* no Brasil, é importante destacar que os *cybercrimes* ganharam destacaram foram o *Scan* (53,16%) que tem como finalidade coletar informações dos usuários para realizar um ataque *cybernético* e *Dos* (26,41%) cuja finalidade é tirar um computador de serviço (Figura 1).

Figura 1- Percentuais de incidentes reportados ao CERT.br.



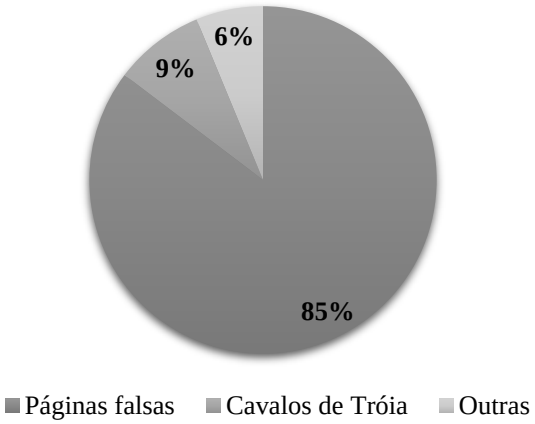
Conforme Amorim (2021, p.23), atualmente é possível delinear um mapeamento dos tipos de ataques *cybernéticos*, (i) *Scan*: técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo principal de identificar computadores ativos e coletar informações sobre eles como. Por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas é possível associar possíveis vulnerabilidade aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados; (ii) *Denial of Sevice* (DoS): técnica pela qual um atacante emprega um computador para tirar de operação um serviço, um computador ou uma rede conectada à internet. Quando empregada de modo coordenada e distribuída, isto é, quando um conjunto de computadores é utilizado no ataque *cybernético*, recebe o nome de navegação de serviço distribuído, ou *Distribuited Denial of Service* (DDoS); (iii) *Web*: um exemplo singular de ataque *cybernético* objetivando o comprometimento de servidores *Web* ou desfigurações de páginas na internet; (iv) Fraude: técnica a qual um golpista busca induzir um usuário a fornecer informações confidenciais ou conduzir um pagamento adiantado mal-intencionado, com a promessa de futuramente receber algum tipo de benefício; (v) *Worm*: são notificações de atividades maliciosas em relação ao processo automatizado de propagação de códigos maliciosos na rede; (vi) Invasão: trata-se de ataque praticado por um golpista, o que resultado no acesso não autorizado a um computador ou rede de computadores.

Conforme um levantamento de dados desenvolvido pela Associação Brasileira de Comércio Eletrônico (2017), o crime de fraude

vem aumentando ano a ano, e segundo o mesmo estudo, há uma onda criminosa ocorrendo no Brasil. Essa onda de crimes tem se propaga sem muita resistência dos comerciantes do país a fora. Um dos crimes mais frequentes são páginas falsas, em que os golpistas criam armadilhas para induzir os usuários a entrarem em sites maliciosos, e expondo a compartilhar conteúdos ilícitos, dessa maneira obtendo dados confidenciais dos usuários. As principais páginas falsas são sites de recrutamento de empregos, em que os interessados perante a necessidade acabam sendo enganados e tornando-se mais uma vítima. Os *cybercriminosos* usam *sites* de empresas famosas para enganar facilmente os usuários vulneráveis. Os sites falsos podem até organizar processos seletivos enganosos, e bancos e redes sociais falsas. Conforme mostra a Figura 2, o percentual de notificações de tentativas de fraudes no ano de 2017 foi muito alto. E o pior, a situação piorou com o aumento do crime de páginas falsas correspondendo a 85,32%.

Segundo Reis (2018, p.32), estudo o qual discutiu sobre um mapeamento geral das categorias de tentativas de fraudes mais comuns em sites falsos na internet. A começar por (i) páginas falsas: são tentativas de fraude com objetivos financeiros envolvendo o uso de sites falsos; (ii) Cavalos de Troia: trata-se de um programa desenvolvido para executar funções para as quais foi aparentemente projetado, também executa funções maliciosas e sem os usuários perceberem.

Figura 2- Percentuais de tentativas de fraudes reportadas ao CERT.br.



3.3. Legislação brasileira e atuação de polícia técnica forense

Com o aumento dos *cybercrimes* durante a pandemia do Covid-19 e a proteção jurídica as vítimas, em relação aos golpes, violação de dados, desrespeito a dignidade humana e aos danos causados pelos criminosos. Além disso, outro aspecto a considerar é a irresponsabilidade do Estado perante as vítimas, onde deveria ser assegurado os direitos e garantias pela Constituição Federal, CPP, CP e pelas Leis de n° 12.737/2012, 12.695/2014, 13.709/2018, 14.155/2021, 14.132/2021. Isso porque, segundo o modelo de provisão de operação de serviços de investigação e equipamentos tecnológicos, assim como seus limites na construção de políticas administrativas, como delegacias de crimes de informática são pouco disponíveis, decorrente desses fatores houve um aumento significante nos números de crimes *cybernéticos*, por falta de investimento para ampliar e desenvolver técnicas e procedimentos informáticos apropriados. Enquanto isso, o Estado pouco injeta recursos que priorizem políticas públicas que possam inibir a atuação dos golpistas ou informar a população de como proteger seus dados pessoais e até mesmo

de evitar extorsões. A solução mais justa seria identificar o criminoso ou o local que está sendo realizado o ato ilícito, no qual seria uma forma para proporcionar condições melhores a população e as vítimas que sofreram algum tipo de dano ao indivíduo e seu patrimônio. De acordo com Lima e Soares (2022, p.9), as leis tiveram que se modernizar com o avanço tecnológico. Com surgimento da informática e sua ampla e rápida disposição à sociedade e passou a exigir também com rapidez, soluções que o Direito não estava preparado para resolver. Diante desse contexto, a necessidade social aparenta estar desprovida da tutela do Direito e a busca ansiosa por regular a matéria pode provocar a criação de leis excessivas e desnecessárias.

Diante disso, com a utilização inapropriada das técnicas e procedimentos informáticos, é preciso um relevante impacto da tecnologia nas relações jurídicas, especificamente no âmbito do Direito Penal (GOMIDES, 2020). Contudo, é perceptível mudanças provocadas pela informatização amplamente disponível. Por consequência, a atualização da legislação não acompanhou a velocidade dessas mudanças, por isso de certa forma a aplicação da lei não foi totalmente adequada, e sim na medida do possível para se enquadrar ao caso concreto e aos novos tipos de condutas lesivas nos tipos penais já existentes. Isto posto, está cada vez mais dificil e custoso garantir a eficiência das leis e proporcionar a paz aos indivíduos, por causa do aumento significante dos *cybercrimes*, como evidenciado através dos dados no ano de 2020 levantados por Gomides (2020, p.34). A pesquisa disponibilizou para empresas e sociedade em geral, uma plataforma de denúncia anônima, através Central Nacional de Denúncias de Crimes Cybernéticos, foram contabilizados 156.692 registros de denúncias anônimas apenas no ano de 2020.

Contudo, segundo Aguiar (2015, p.202), os *cybercrimes* são difíceis de ser identificado, por isso é crucial que o legislador penal elabore normas próprias para coibir a atuação dos criminosos digitais. Para identificá-los e puni-los, primeiramente deve-se diferenciá-los e conceituá-los, propiciando assim leis mais claras e específicas, de forma a alcançarem seu objetivo primordial, que é o de regulamentar o comportamento do ser humano em sua vida cotidiana.

3.3.1. Lei Carolina Dieckmann

A Lei 12.737 de 30 de novembro de 2012, também conhecida como Lei Carolina Dieckmann, representa avanços, aplicando penas para pessoas que cometem *cybercrimes*. No entanto, ainda é ineficaz em muitos aspectos. Um dos pontos negativos desta Lei é a punição estabelecida para ressocialização do criminoso. A maior pena que foi estabelecida referente ao *cybercrime* é de dois anos com a possibilidade de auferir aumento de um sexto a dois terços apenas. Portanto, é uma pena muito abaixo do esperado para quem pratica um crime dessa gravidade. Porque, os danos causados lesados são irrecuperáveis, por isso as penas deveriam ser mais rígidas e efetivas conforme o grau de violação dos direitos da vítima. Outra considerada brecha observada nessa Lei é que a qualificação do crime está relacionada com a violação dos mecanismos de segurança, mediante a isso, se o ambiente virtual não possui mecanismos de proteção deixaria uma brecha para não ser considerado como crime (LEITE, 2022).

Com o passar do tempo, é possível perceber que a Lei Carolina Dieckmann se faz necessário uma atualização, porque deixou de atender diversas necessidades da sociedade, é possível constatar diversa lacunas existentes nesta lei. Então, apesar dos aspectos negativos expostos, porque é um avanço significativo para que haja maiores reflexões e evolução dessa Lei. Portanto, a Lei Carolina Dieckmann precisa de algumas adaptações a realidade atual, porque o ambiente

virtual está em constante evolução e sendo assim os hackers também estão encontrando novas maneiras de prejudicar possíveis vítimas. Pompeu (2022, p.28) discute em seu trabalho sobre a ineficácia na normatização nos crimes virtuais, ainda não foi suprida para um combate efetivo contra estes delitos. E muito por isso, mediante a essa dificuldade, ou ainda pela natureza taxativa do Código Penal, á uma grande impossibilidade da aplicação da analogia nos crimes virtuais.

Diante do cenário histórico e jurídico acima, a Lei 14.155/2021, de 27 de maio de 2021, atualiza a lei Carolina Dieckmann. Modificando o tipo penal do delito e incluiu formas qualificada e majorada ao furto mediante fraude e ao estelionato. Sobre a atualização da lei: segue um dos pontos alterados Código Penal, Art. 154-A – Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita. Alterou a redação criada pela Lei Carolina Dieckmann Retirou o requisito anterior de ser "mediante violação indevida de dispositivo de segurança" Aumento a pena estabelecida pela Lei Carolina Dieckmann, que era de "de detecção, de 3 meses a 1 ano" para "reclusão, de 1 (um) a 4 (quatro) anos." No § 3º, aumentou a pena para "reclusão, de 2 (um) a 5 (quatro) anos" – se houver acesso a comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas ou o controle remoto do dispositivo invadido.

Essa adaptação a nova realidade, tomou as punições mais rígidas, porque a lei anterior apresentava várias lacunas que provocam indecisões e injustiças devido a desqualificações e não enquadramentos de *cybercrimes*. Mas com a sua atualização, alterou-se as penas que antes eram somente detenção e passou a ser reclusão (GUMIERO, 2022). Então, o regime inicial de pena pode ser fechado e antes podia ser semiaberto ou aberto. Anteriormente, qualquer falta de controle podia ser usada para tentar desqualificar o crime, como por exemplo a simples falta de senha no celular da vítima. Com a modificação desta lei, as penas podem chegar até 8 anos de prisão e multas, podendo ser agravadas em casos em que os crimes forem praticados com o uso de servidor fora do Brasil ou se a vítima for idosa ou vulnerável.

3.3.2. Lei Lucas Santos

Com a instauração da internet em todos os segmentos comerciais, é notório que as novas tecnologias de informação e comunicação (TICs) vêm ganhando bastante espaço no cotidiano da sociedade em geral. Diante de tantas inovações em TICs, não vieram só benefícios da agilidade das oportunidades, mas também vieram alguns transtornos indesejáveis que podem provocar afetar a honra das pessoas que utilizam a internet. Alguns problemas sociais como o *bullying* praticado com crueldade contra pessoas que são consideradas mais "frágeis" em relação a outras. Esta prática consiste em menosprezar o indivíduo, além de buscar meios para rebaixar a qualidade de seus pares. Esta prática é comum em muitos ambientes, seja na escola, trabalho, associações. Ocasionando momentos de perturbação física e psicológica deixando a vítima em situação constrangedora (OLIVEIRA, 2019).

Na contemporaneidade, o *bullying* ganhou um espaço mais abrangente, a internet tornou essa prática ainda mais devastadora, porque o *bullying* que era praticado apenas em pequenos ambientes, passou a ser praticado nas redes sociais, aplicativos de bate-papo e outras plataformas que viralizam informações confidenciais, as quais podem tomar proporções negativas irreparáveis para integridade pessoal e profissional. Passando a ser conhecido como *cyberbullying*, com tudo isso, aumentou significativamente não só o nível de alcance de

visualizações, como também as consequências causadas pelo *cyberbullying* (REIS, 2021).

Atualmente, as consequências são tão drásticas que algumas pessoas chegam a cometer suicídio. Temos como exemplo de grande repercussão, o caso de Lucas Santos. Lucas postou um vídeo em uma rede social com seu amigo e recebeu várias mensagens preconceituosas, ele cometeu suicídio logo em seguida por não ter aceitado os comentários maldosos (SOARES, 2022). Diante da triste situação, a Câmara de Vereadores de Natal, no estado do Rio Grande do Norte, a Assembleia Legislativa do Rio Grande do Norte/RN e a Câmara dos Deputados Federais criaram o Projeto de Lei Lucas Santos. Os objetivos dessas leis foram incluir medidas de conscientização, prevenção e combate à depressão, automutilação e ao suicídio, nos projetos pedagógicos elaborados pelas escolas públicas e provadas.

Na esfera Federal, foi sancionada a "Lei Lucas Santos" de combate ao *cyberbullying*, com nº 7.193. A lei foi sancionada dia 15 de setembro de 2021. Em relação ao sancionamento da lei na Prefeitura de Natal/RN, determina que as escolas da rede municipal pública e privada de Natal realizem projetos com palestras, seminários e/ou outros meios de exposição e ensino com objetivo da conscientização dos alunos. Os alunos com faixa etária entre 12 (doze) e 14 (catorze) anos serão orientados na produção de apresentações próprias, após estudo, de temas relacionados à conscientização do uso saudável das redes sociais e combate ao *cyberbullying*. As emissoras de rádio e televisão, que gozarem de isenções, patrocínios ou benefícios, também farão parte do processo de educação (MACHADO, 2022).

É possível compreender que esses projetos de lei quando aprovados e efetivados visam a conscientização e o uso saudável das redes sociais e a inibição das ações maldosas do *cyberbullying*. Essas medidas podem ser capazes de evitar suicídios de jovens em virtude de agressões virtuais. O bullying é um conceito específico e muito bem definido, uma vez que se não se deixa confundir com outras formas de violência. Isso se justifica pelo fato de apresentar características próprias, dentro elas, talvez a mais grave seja a propriedade de causar traumas ao psiquismo de suas vítimas e envolvidos (MACHADO, 2022).

A evolução da tecnologia influenciou significativamente nas interações humanas, por isso novas categorias de *bullying* surgiram através da utilização de aparelhos e equipamentos de comunicação (celular e internet), que são capazes viralizar informações nem sempre autênticas, como calunias e maledicências. Essa forma de *bullying* é conhecida como *cyberbullying* (MACHADO, 2022). Nos últimos anos, em consequência da prática do *cyberbullying*, alguns adolescentes que sofreram com esse tipo de comportamento acabaram cometendo o suicídio. O caso de maior repercussão nacional foi o de Lucas Santos, onde ele se tornou referência para a criação de um projeto de lei de esferas da municipal a federal, com o intuito de punir e evitar o surgimento de novos casos.

Certamente, é crucial para o bem-estar dos usuários das redes sociais, evitar compartilhar conteúdos que depreciem, menosprezem, diminuam qualquer pessoa. Cabe ressaltar, que o compartilhamento deste conteúdo pode ser considerado crime: calúnia, difamação ou injúria, dependendo de onde se enquadrar o conteúdo compartilhado. Porque não sabemos como está o psicológico da vítima.

3.4. Desenvolvimento de uma solução

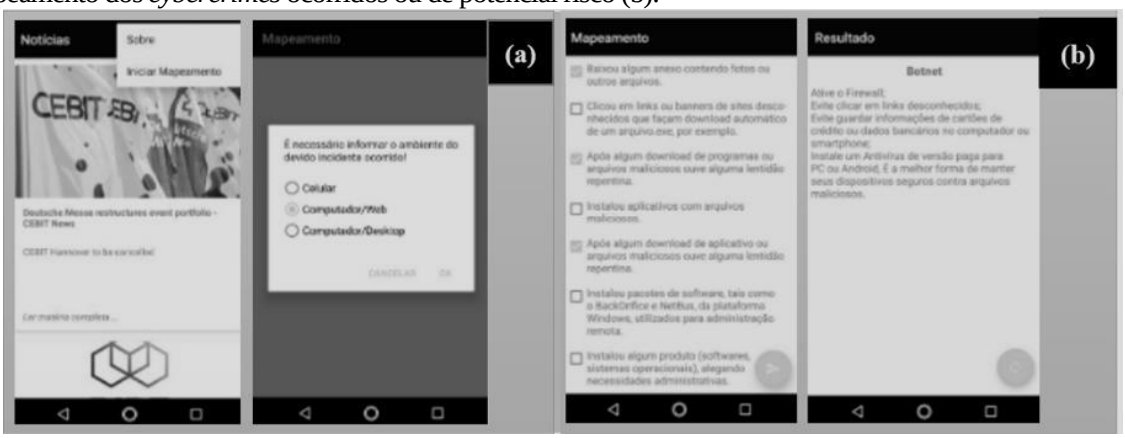
Diante do aumento da utilização das tecnologias e o descuido das pessoas física e jurídicas em relação aos riscos frequentes de crimes cibernéticos. É necessária ampla divulgação do bom uso das tecnologias e facilitar o acesso a instruções que possam contribuir com a proteção de dados confidenciais. Desse modo, é

preciso entender o papel da Perícia Forense Computacional e Crimes *Cybernéticos*, com a finalidade de criar uma aplicação para que os usuários tenham acesso a informação sobre crimes digitais e sobre a atuação dos peritos forenses computacionais.

Pereira e Oliveira (2019, p.10) propuseram uma solução aos *cybercrimes*, os autores criaram um aplicativo Android e uma aplicação *Web*, no qual irá divulgar informações sobre os *cybercrimes* e atuação dos peritos forenses computacional sobre eles, para que os usuários sejam notificados sobre essas informações. No entanto, o usuário também terá acesso a um mapeamento das notificações para que possam visualizar potenciais riscos de sofrer com algum tipo de *cybercrime*.

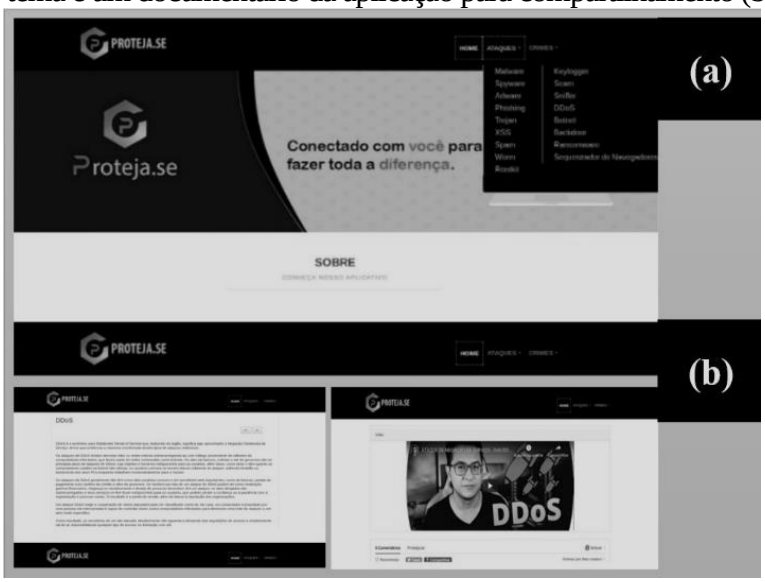
Na Figura 3 (a) ilustra a *homepage* do aplicativo do usuário terá acesso ao *News* de notícias, na segunda tela, os usuários poderão marcar a opção do tipo de plataforma de sua escolha, do tipo de crime que poderá sofrer. Na Figura 3 (b) ilustra a terceira tela poderão ser habilitadas opções de identificação dos eventos ocorridos em sua plataforma, então, ao finalizar o processo a aplicação realizará um mapeamento para disponibilizar aos usuários o resultado de qual tipo de crime ele sofreu ou que corre risco de sofrer, além de ser informado a qual departamento deverá recorrer para resolver seu problema.

Figura 3- *Homepage* e segunda página do aplicativo (a) e opções de identificação dos eventos ocorridos e mapeamento dos *cybercrimes* ocorridos ou de potencial risco (b).



A tela principal do usuário que terá acesso a informações sobre estudos de crimes digitais para despertar um interesse no assunto, para que os usuários continuem navegando pela aplicação, e também apresentação informações sobre o aplicativo *proteja.se* a fim de fazer um *marketing* e convencer os usuários a fazer *download* do aplicativo e visualizar com frequência o *News* (Figura 4 (a). Em relação ao mapeamento, os usuários terão acesso no menu 26 opções de busca, tanto de *cyberataques* quanto de crimes digitais do momento como um *Feed* de noticiais. Nessa página poderão obter informações de prevenção, remoção de vírus ou denunciar um crime. Para os usuários desinteressados em muita leitura, na página estão disponíveis vídeos explicando sobre o tema e um documentário da aplicação para compartilhamento (Figura 4 (b).

Figura 4- Apresentação informações sobre o aplicativo *proteja.se* a fim de fazer um *marketing* e convencer os usuários a fazer o *download* do aplicativo e visualizar com frequência o *News* (a) e vídeos explicando sobre o tema e um documentário da aplicação para compartilhamento (b).



Pereira e Oliveira (2019, p.11) empregaram algumas ferramentas para criarem essas aplicações, como linguagem *Java*, linguagem essa criada por *Sun Microsystems* que permite comunicar com o computador com a finalidade de manipular os dados. Ou seja, é uma linguagem orientada a objeto e isso permite que o desenvolvedor *realize* a modelagem dos objetos no projeto definindo estruturas e operações que dão fundamentação ao conceito de herança e polimorfismo que permite o programador selecionar as funcionalidades do sistema para seu efetivo funcionamento.

No entanto, também se trata de uma linguagem estaticamente aplicada, a vantagem dela é uma linguagem simples por ser multiplataforma. Ou seja, o programador consegue ser mais eficiente e produtivo por não precisar se preocupar com a infraestrutura, mas também poderá compilar o projeto em diferentes plataformas, proporcionando maior desempenho no desenvolvimento da aplicação (TEIXEIRA, 2014).

Outra linguagem utilizada foi *Ruby*, que é nova em comparação às outras, uma linguagem limpa e direta, toda orientada a objetos, mais simples de se aprender e trabalhar, mesmo sendo multiplataforma. Sendo assim, suportada por diversos tipos de sistemas operacionais como *Linux, Windows, Solares* e outros. Essa linguagem possui muitas *features* como o *Ruby Gems*, (uma biblioteca gratuita disponível na internet), *Code Blocks, Maxins* (resposta à herança múltipla), tipagem dinâmica e outras características (REIS, 2014).

Outra ferramenta empregada foi *Framework Rails*, essa ferramenta proporcionou praticidade para escrever a aplicação para *Web*. Comparada a outros, este permite que as funcionalidades de um certo sistema possam ser implementadas de forma incremental graças aos padrões e conceitos adotados. Essa ferramenta permite adotar metodologias ágeis de desenvolvimento e gerenciamento de projetos (CARVALHO NETO, 2017).

API de Notícias foi outra ferramenta empregada por Pereira e Oliveira (2019) para desenvolver uma solução aos *cybercrimes*. Trata-se de uma API de código aberto e de fácil implementação, em que se pode visualizar notícias de qualquer manchete do mundo todo e em tempo real. Além disso, os usuários podem optar por uma ou mais fontes confiáveis de

notícias e ainda definir uma temática de novidades diárias (BOTTON, 2022).

Os autores também empregaram *database Firebase*, trata-se de um banco de dados fornecido pela *Google*. Essa ferramenta é utilizada para armazenar dados de aplicações mobile em tempo real sincronizando os dados. Além disso, é uma árvore em formato de JSON, em que os dados são armazenados em forma de nodos, deixando uma infraestrutura de forma prática, com uma modelagem ágil e simples. O *Firebase* é uma solução simples e completa de *back – end* para desenvolvimento tanto *mobile* quanto *Web*. E, é oferecido como serviço pela *Google*, sendo hospedado e mantido em seus *datacenters* (LUPCHINSKI, 2015).

Pereira e Oliveira (2019, p.12) utilizaram a Plaforma *Android*, originalmente foi construída com base no sistema operacional *Linux*, contendo diversas ferramental podendo criar aplicações para diferentes dispositivos móveis. As funcionalidades e recursos da plataforma mudaram ao decorrer das necessidades dos desenvolvedores e usuários. O *Android* é uma plataforma para tecnologia móvel completa, envolvendo um pacote com programas para *smartphones*, porque é um sistema operacional *middleware*, aplicativos e interface do usuário (ROSA; FAVARO, 2018).

4. Conclusões

Esse estudo disponibiliza informações na forma de instruções preventivas contra crimes *cybernéticos*. Isso através da conscientização dos procedimentos orientados pela Perícia Forense Computacional. Foram explicitadas as evidências e as categorizações dos crimes digitais, assim como as principais instruções de como evitá-las e inibi-las.

Foi possível compreender as atualizações da legislação brasileira e da atuação dos peritos forenses computacionais por meio da polícia técnica. E por fim, foi apresentada uma solução digital para combater os crimes *cybernéticos* principalmente nas redes sociais e foi apresentado também o acolhimento de ideias para manter o bem-estar dos usuários, seja pessoa física ou jurídica. Foram descritos os processos de desenvolvimento da solução digital supracitada como aplicação para dispositivos móveis ou plataforma *Web*.

5. Referências

AGUIAR, P. P. M. **Gestão jurídico-estratégica do cybercrime no contexto da cyberdemocracia.** 2015. 262 p. Dissertação (Mestrado Profissional em Gestão nas Organizações Aprendentes) – Universidade Federal da Paraíba, João Pessoa, 2015. Disponível em:< https://repositorio.ufpb.br/jspui/handle/123456789/14244?locale=pt_BR>. Acesso em: 15 jan. 2023.

ALMEIDA, J. J.; MENDONÇA, A. B.; CARMO, G. P.; SANTOS, K. S.; SILVA, L. M. M.; AZEVEDO, R. R. D. Crimes cybernéticos. **Cadernos de Graduação – Ciências Humanas e Sociais Unit**, v.2, n.3, p.215-236, 2015. Disponível em:< https://periodicos.set.edu.br/cadernohumanas/article/view/2013>. Acesso em: 29 dez. 2022.

AMORIM, R. X. **Estudo sobre ferramentas de instrução em ambientes computacionais: um mapeamento sistemático**. 2021. 36 f. Monografia (Bacharelado em Sistemas de Informação) – Universidade Federal do Amazonas, Itacoatiara, AM, 2021. Disponível em:< https://riu.ufam.edu.br/handle/prefix/5877>. Acesso em: 17 jan. 2023.

BONACCORSO, N. S. **Aplicação do exame de DNA na elucidação de crimes**. 2005. 156 p. Dissertação (Mestrado em Direito Penal) – Universidade de São Paulo, São Paulo, 2005. Disponível em:< https://www.teses.usp.br/teses/disponiveis/2/2136/t

de-15092010-145947/publico/DISSERTACAO_MESTRADO_NORMA_BONACCORSO.pdf>. Acesso em: 07 jan. 2023.

BOTTON, F. F. "**Roubamos sem dar tiro**": uma etnografia de grupos de fraudadores no espaço virtual. 2022. 113 p. Dissertação (Mestrado em Antropologia) – Universidade de São Paulo, São Paulo, 2022. Disponível em:< https://www.teses.usp.br/teses/disponiveis/8/8134/tde-10062022-105118/pt-br.php>. Acesso em: 11 jan. 2023.

CARVALHO NETO, L. R. **Escalabilidade em aplicações Web**: estudo de caso em um sistema Ruby on Rails. 2017. 34 f. Monografia (Bacharelado em Engenharia de Software) – Universidade Federal do Rio Grande do Norte, Natal, 2017. Disponível em:< https://repositorio.ufrn.br/handle/123456789/34240 >. Acesso em: 22 jan. 2023.

CHAQUIAN FILHO, E.; DUARTE, S. L. O.; LACERDA, L. C. A importância da preservação da evidência digital nos crimes cybernéticos. **Diálogos – Economia e Sociedade**, v.2, n.2, p.89-109, 2018. Disponível em:< http://periodicos.saolucas.edu.br/index.php/dialogos/article/view/50>. Acesso em: 23 jan. 2023.

CHEN, L. M.; CHEN, M. C.; LIAO, W.; SUN, Y. S. A scalable network forensics mechanism for stealthy self-propagating attacks. **Computer Communications**, v.36, n.13, p.1471-1484, 2013. https://doi.org/10.1016/j.comcom.2013.05.005

COSTA, A. B.; SILVA, F. B.; MATOS, H. G.; FREIRE, I. L. C. A importância da computação forense no combate a crimes cybernéticos. **Revista Ibero-Americana de Humanidade, Ciências e Educação**, v.7, n.12, p.801-814, 2021. https://doi.org/10.51891/rease.v7i12.3503

EDINGER, C. Cadeia de custódia, rastreabilidade probatória. **Revista Brasileira de Ciências Criminais**, v.120, p.8-10, 2016. Disponível em:< https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:artigo.revista:2016;1001128397>. Acesso em: 02 fev. 2023.

DINH, H. T.; LEE, C.; NIYATO, D.; WANG, P. A survey of mobile cloud computing: architecture, applications, and approaches. **Wireless Communications and Mobile Computing**, v.13, n.18, p.1587–1611, 2011. https://doi.org/10.1002/wcm.1203

GOMIDES, L. A. S. **A tecnologia e o direito penal: os novos paradigmas da investigação criminal.** 2020. 42 f. Monografia (Bacharelado em Direito) – Universidade Evangélica de Goiás, Anápolis, GO, 2020. Disponível em:< http://repositorio.aee.edu.br/bitstream/aee/16881/1/Monografia%20-%20LEONARDO%20GOMIDES.pdf>. Acesso em: 05 fev. 2023.

GUMIERO, B. B. **Futuro da ciência criminal: abordagem jurídica e prática acerca da utilização do cyberespaço por cybercriminosos e cyberterroristas.** 2022. 72 f. Monografia (Bacharelado em Direito) – Centro Universitária Antônio Eufrásio de Toledo, Presidente Prudente, SP, 2022. Disponível em:< http://www.ct.ufpb.br/pos/contents/pdf/bibliovirtual/dissertacoes-2009/arnaldo-sobrinho-cibercrime-e-cooperacao-penal-internacional.pdf>. Acesso em: 04 jan. 2023.

GUPTA, S.; KUMAR, P.; ABRAHAM, A. A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment. **International Journal of Distributed Sensor Networks**, v.9, n.3, e364575, 2013. https://doi.org/110.1155/2013/364575

HANSMAN, S.; HUNT, R. A taxonomy of network and computer attacks. **Computers & Security**, v.24, n.1, p.31-43, 2005. https://doi.org/110.1016/j.cose.2004.06.011

JEONG, E.; LEE, B. An IP Traceback Protocol using a Compressed Hash Table, a Sinkhole Router and Data Mining based on Network Forensics against Network Attacks. **Future Generation Computer Systems**, v.33, p.42–52, 2013. https://doi.org/110.1016/j.future.2013.10.023

KHAN, S.; SHIRAZ, M.; WAHAB, A. W. A.; GANI, A.; HAN, Q.; RAHMAN, Z. B. A. A Comprehensive Review on Adaptability of Network Forensics Frameworks for Mobile Cloud Computing. **The Scientific World Journal**, 2014. https://doi.org/110.1155/2014/547062

KIM, A. C.; PARK, W. H.; LEE, D. H. A study on the live forensic techniques for anomaly detection in user terminals. **International Journal of Security and its Applications**, v.7, n.1, p.181-188, 2013. Disponível em:< http://article.nadiapub.com/IJSIA/vol7_no1/17.pdf >. Acesso em: 21 dez. 2022.

LEITE, S. C. **Crimes digitais contra a honra e o cerceamento da liberdade de expressão**. 2022. 43 f. Monografia (Bacharelado em Direito) – Pontifícia Universidade Católica de Goiás, Goiânia, 2022. Disponível em:< https://repositorio.pucgoias.edu.br/jspui/handle/123456789/3978>. Acesso em: 16 dez. 2022.

LIMA, P. V. S.; SOARES, M. L. P. **Crimes cybernéticos**: a deficiência da legislação penal brasileira e os projetos de leis governamentais. 2022. 24 f. Monografia (Bacharelado em Direito) – Universidade Potiguar, Natal, 2022. Disponível em:< https://repositorio.animaeducacao.com.br/bitstream/ANIMA/25256/1/TCC%20FINAL%20MATHEUS%20E%20PEDRO%20ATUALIZADO.pdf>. Acesso em: 11 dez. 2022.

LUPCHINSKI, R. L. P. **Desenvolvimento de uma Aplicação de Página-Única e Banco de Dados Não-Relacional para Organização e Controle de Eventos Esportivos**. 2015. 70 f. Monografia (Bacharelado em Ciência da Computação) - Universidade Federal do Rio Grande do Sul, Porto Alegre, 2015. Disponível em:< https://lume.ufrgs.br/handle/10183/138226>. Acesso em: 15 jan. 2023.

MACHADO, J. S. **Cyberbullying**: direcionamentos para uma discussão em sala de aula. 2022, 115 p. Dissertação (Mestrado em Educação) – Universidade Estadual Paulista "Julio de Mesquita Filho", Araraquara, SP, 2022. Disponível em:< https://repositorio.unesp.br/handle/11449/217983>. Acesso em: 21 dez. 2022.

OLIVEIRA, M. A. N. **Bullying em uma escola pública no município de Piraquê – TO, autopercepção e sofrimento**. 2019. 70 f. Monografia (Licenciatura em Letras) - Universidade Federal do Tocantins, Araguaína, TO, 2019. Disponível em:< https://repositorio.uft.edu.br/handle/11612/4283>. Acesso em: 10 jan. 2023.

PEIXOTO, S. C. **A eficiência da descentralização na computação forense do Departamento de Polícia Técnica do estado da Bahia**. 2012. 124 p. Dissertação (Mestrado em Administração Pública e de Empresas) – Escola Brasileira de Administração Pública e de Empresas, Fundação Getúlio Vargas, 2012. Disponível em:< https://bibliotecadigital.fgv.br/dspace;handl/handle/10438/9805>. Acesso em: 12 jan. 2023.

PEREIRA, K. da S.; OLIVEIRA, F. M. de. Perícia forense computacional e crimes cibernéticos. **Revista Interdisciplinar do Pensamento**

Científico, v.5, n.15, p.210-2028, 2019. http://dx.doi.org/10.20951/2446-6778/v5n2a15

POMPEU, A. L. B. C. **Crimes cybernéticos**: a ineficiência da Lei Carolina Dieckmann. 2022. 41 f. Monografia (Bacharelado em Direito) – Faculdade de Inhumas, Inhumas, GO, 2022. Disponível em:< http://65.108.49.104/bitstream/123456789/509/2/Template%20de%20TCC%20Direito%202021%20%281%29.docx.pdf>. Acesso em: 20 dez. 2022.

REIS, A. P. **Análise de vulnerabilidades de segurança em sistemas de Internet Banking utilizando ferramentas de código aberto.** 2018. 46 f. Monografia (Bacharelado em Sistemas de Informação) – Universidade Federal de Uberlândia, Uberlândia, MG, 2018. Disponível em:< https://repositorio.ufu.br/handle/123456789/24152 >. Acesso em: 11 dez. 2022.

REIS, E. L. S. (Eds.). **Crimes digitais impróprios: uma abordagem constitucional e crítica diante da violação de direitos alheios**: insegurança na legislação vigente e a (falta de) intepretação de texto no âmbito digital. 1. ed. Curitiba: Appris, 2021. 169p. Disponível em:< https://books.google.com.br/books/about/Crimes_Digitais_Impr%C3%B3prios_Uma_Abordage.html?id=GjVPEAAAQBAJ&redir_esc=y>. Acesso em: 21 dez. 2022.

REIS, P. M. P. **Identificação, Análise e Avaliação de Linguagens de Programação Adequadas ao Desenvolvimento de Agentes Móveis Multi-Plataforma**. 2014. 141 p. Dissertação (Mestrado em Engenharia Informática – Computação Móvel) – Escola Superior de Tecnologia e Gestão, Instituto Politécnico de Leiria, Portugal, 2014. Disponível em:< https://iconline.ipleiria.pt/handle/10400.8/1357>. Acesso em: 15 nov. 2022.

ROSA, D. J.; FAVARO, E. N. **Desenvolvimento de um aplicativo móvel para Food Service utilizando a Plataforma Android**. 2018. 102 f. Monografia (Tecnologias da Informação e Comunicação) – Universidade Federal de Santa Catarina, Araranguá, SC, 2018. Disponível em:< https://repositorio.ufsc.br/handle/123456789/192039>. Acesso em: 24 nov. 2022.

RUSSO, R. A. **A tutela da privacidade de dados na era do Big Data**. 2019. 136 p. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica de São Paulo, São Paulo, 2019. Disponível em:< https://tede2.pucsp.br/handle/handle/23113>. Acesso em: 14 nov. 2022.

SHIRAZ, M.; GANI, A. A lightweight active service migration framework for computational offloading in mobile cloud computing. **The Journal of Supercomputing**, v.68, n.2, p.978–995. https://doi.org/110.1007/s11227-013-1076-7

SHIRAZ, M.; GANI, A.; KHOKHAR, R. H.; BUYYA, R. A Review on Distributed Application Processing Frameworks in Smart Mobile Devices for Mobile Cloud Computing. **IEEE Communications Surveys & Tutorials**, v.15, n.3, p.1294-1313, 2013,. https://doi.org/110.1109/SURV.2012.111412.00045

SOUZA, A. Z. Etapas no processo de computação forense: uma revisão. **Acta de Ciências e Saúde**, v.5, n.3, p.99-111, 2017. Disponível em:< https://www2.ls.edu.br/actacs/index.php/ACTA/article/view/138/128>. Acesso em: 02 nov. 2022.

TEIXEIRA, C. P. **Um modelo de processos de gestão de federações de provedores e serviços de software**. 2014. 164 p. Dissertação (Mestrado em Engenharia de Automação e Sistemas), Universidade Federal de Santa Catarina, Florianópolis, 2014. Disponível em:< https://repositorio.ufsc.br/bitstream/handle/123456789/132440/332923.pdf?sequence=1&isAllowed=y >. Acesso em: 30 out. 2022.

TZANAKAKI, A.; ANASTASOPOULOS, M. P.; ZERVAS, G. S.; ROFOEE, B. R.; NEJABATI, R.; SIMEONIDOU, D. Virtualization of heterogeneous wireless-optical network and IT infrastructures in support of cloud and mobile cloud services. **IEEE Communications Magazine**, v.51, n.8, p.155–161, 2013. https://doi.org/110.1109/mcom.2013.6576354

WANG, S., ZHANG, Z.; KADOBAYASHI, Y. Exploring attack graph for cost-benefit security hardening: A probabilistic approach. **Computers & Security**, v.32, p.158-169, 2013. https://doi.org/110.1016/j.cose.2012.09.013

ZAWOAD, S.; HASAN, R. Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. **Computer Science**, 2013. https://doi.org/110.48550/arXiv.1302.6312