Revista Multidisciplinar do Nordeste Mineiro, v1, 2022/01
ISSN 2178-6925

CRIMES CIBERNÉTICOS E O GOLPE DO "BENEFÍCIO DO GOVERNO"

CYBER CRIMES AND THE "BENEFIT OF THE GOVERNMENT" SCAM

Douglas Mota Pereira

Acadêmico de Direito pela faculdade Alfa Unipac, Brasil.E:mail: dricamci@hotmail.com

Victor Pereira dos Santos Guerra

Acadêmico de Direito pela faculdade Alfa Unipac, Brasil.E:mail: ehopereira449@gmail.com

Emerson Barrack Cavalcanti

Bacharel em Direito. Pós-Graduado em Direito Público e Privado. Bacharel Licenciatura Plena em Matemática. Pós Graduando – MBA em Coaching com ênfaseem Mentoring para Gestão de Pessoas. Professor no Curso de Direito para as disciplinas: Direito do Consumidor. Introdução à Ciência Política e Teoria do Estado. Direito Civil I. História e Introdução ao Estudo do Direito. Formas Consensuais de Resolução de Conflitos. Direito Constitucional.

ALFA UNIPAC - Teófilo Otoni, Brasil

E-mail: cavalcanti.ebc@gmail.comProfessor

Recebido 10/12/2021 - Aceito 01/02/2022

Resumo

Este artigo científico abordará a área de direito que rege relacionamentos de domínio virtual. E tem como objetivo discutir o posicionamento da legislação digital no Brasil acerca dos crimes cibernéticos acontecidos durante a pandemia pelo Covid 19, em especial ao golpe do “Benefício do Governo”. Como o uso da Internet aumentando naturalmente, crimes são cometidos todos os dias e essa tendência está aumentando, já que a maioria das pessoas ficam quase 24 horas conectadas por dia. Todavia, diante da atual crise pandêmica que a população mundial está vivendo, e dos medos que a atormentam, muitos criminosos estão usufruindo do campo da tecnologia da informação para cometer cibercrimes, como o escolhido para ser tratado neste estudo o “Golpe do Governo”. Com mensagens maliciosas mandadas para os celulares da população, hackers levam o usuário a fornecer dados pessoais que poderão ser roubados por eles. A metodologia aplicada fora a bibliográfica, sendo assim diversas obras doutrinarias foram consultadas para a elaboração desde, também fora consultado sites do governo como o “planalto” para fundamentação legal do mesmo. Por fim pretende-se concluir com medidas assecuratórias no intuído de proteger do mundo dos cibercrimes.

Palavras-chave: Cibercrimes; Golpe do Governo; Legislação;

Digitalização;Pandemia.

Abstract

This scientific article will address the area of law that governs virtual domain relationships. And it aims to discuss the positioning of digital legislation in Brazil regarding cybercrimes that occurred during the Covid 19 pandemic, in particular the "Government Benefit" coup. As Internet usage naturally increases, crimes are committed every day and this trend is increasing as most people are connected almost 24 hours a day. However, given the current pandemic crisis that the world population is experiencing, and the fears that plague it, many criminals are enjoying the field of information technology to commit cybercrimes, such as the one chosen to be treated in this study as the "Government Coup". With malicious messages sent to the population's cell phones, hackers lead the user to provide personal data that could be stolen by them. The methodology applied was the bibliographical one, so several doctrinal works were consulted for the elaboration since, government websites such as the "plateau" were also consulted for its legal basis. Finally, the intention is to conclude with assurance measures in order to protect the world from cybercrime.

Keywords: Cybercrimes; Government coup; Legislation; Digitization; Pandemic.

1 Introdução

A tecnologia trouxe vida a um nível sem precedentes na imaginação humana nos últimos anos. Atualmente as pessoas já nascem em um ambiente cercado pela tecnologia que por sua vez está em constante evolução. Diante disso pode-se dizer que os nascituros são nativos digitais. Não há dúvidas alguma que a invenção da internet é um dos avanços mais significativos da humanidade durante todo o século. São inúmeras as atividades que podem ser realizadas totalmente pela Web, quebrando barreiras impeditivas de décadas anteriores como as barreiras de tempo e espaço.

Todavia, infelizmente, todos os benefícios que a tecnologia da informação traz para o ser humano, também trazem sérios riscos para o mesmo. A capacidade de ocultar IDs na Internet atrai uma nova geração de criminosos que são difíceis de detectar. Deve-se notar que as pessoas são capazes de desenvolver personalidades virtuais que muitas vezes se diferem de suas personalidades no mundo real.

Como o já ocorrido anteriormente grandes descobertas que deveriam facilitar e melhor a condição humana, são usadas para destrui-los, foi assim com a invenção dos aviões, cujo seu uso foi distorcido para algo tão ruim quanto a guerra, e está sendo assim com a internet, onde pessoas maliciosas á utilizam para ameaçar os direitos humanos, cometendo atos ilícitos denominados cibercrimes.

Atualmente a população nacional e mundial vêm se recuperando de uma fase nunca vivida por nossa geração, a recuperação pandêmica causada pelo Sars- Cov- 2 que dizimou milhares de vidas e afetou a vida econômica de todas as nações. Não havendo possibilidade de trabalho, devido ao isolamento social obrigatório, o Governo

Federal disponibilizou para a população uma quantia de variou entre R$150,00 a

R$1.200,00, enchendo os olhos de golpistas digitais espalhados em todos os cantos do mundo. Uma investigação da empresa internacional de segurança cibernética Kaspersky identificou pelo menos 18 aplicativos falsos com benefícios nomeados na Play Store, que tinham apenas uma finalidade, roubar dados das pessoas que continham menos informação e buscavam desesperadamente por um meio de sustento.

Na mesma premissa, salienta-se que tem sido árdua a tarefa dos legisladores em tratarem de crimes cometidos nesta nova na esfera social, que violam os princípios da liberdade, o princípio da segurança, e prejudicam os direitos públicos das pessoas. Portanto, a questão norteadora desse artigo pretende responder de forma satisfatória. Como a legislação vigente poderá ser aplicado e executada no intuito de assegurar os direitos das pessoas e punir os criminosos que optam por tal conduta?

Para o embasamento teórico desde trabalho buscou-se realizar pesquisas bibliográficas e em webiográficas para encontrar subsídios para fundamentação dos pontos-chave de combate ao crime cibernético. Encontra-se aqui um método de revisão de literatura com abordagem qualitativa. Os dados do foram organizados por busca bibliográfica e organizados de acordo com a temática exigida. Para elaboração desde artigo utilizou-se de escritos em língua portuguesa publicadas entre 2015-2021 como Google Scholar e Scielo.

No capítulo 1, será abordado a evolução do Direito Virtual, uma das áreas mais crescentes no ramo jurídico, e o nascimento de todos os princípios básicos e instituições que foram cumpridos e aplicados, bem como novas instituições e elementos de pensamento jurídico em todas as áreas.

Compreender os desenvolvimentos tecnológicos e as ameaças cibernéticas ajuda a compreender as necessidades de conhecimento do crime cibernético em relação aos níveis conceituais e de classificação. Portanto no capitulo 2 fornecerá informações sobre o cibercrime, sua definição e como ocorre no Brasil.

O Capítulo 3, abordará o tema central de nosso estudo, que é o crime digital conhecido como “Golpe do Governo”, nele trataremos de assuntos deverasmente importantes para a população como por exemplo: Como os mecanismos utilizados pelos criminosos para aplicação do os desafios da luta pela justiça contra o crime cibernético.

Por fim, concluir-se-á com uma breve explanação dos autores acerca do estudado e as medidas assecuratórias encontradas pelos mesmos a fim de encontrar uma medida legal para proteção dos direitos humanos frente aos crimes cibernéticos

2 Objetivos

O seguinte estudo tem por objetivo discutir o posicionamento da legislação digital no Brasil acerca dos crimes cibernéticos acontecidos durante a pandemia pelo Covid 19, em especial ao golpe do “Benefício do Governo”.

3 Revisão da Literatura

3.1 DIREITO DIGITAL

A partir da criação da tecnologia, muitos novos modelos de negócios surgiram em todo o mundo, e em quase todos os setores. O resultado gerado foram interesses legítimos em torno de prestadores de serviços, produtores de tecnologia, usuários e consumidores, que refletiram diretamente nos princípios constitucionais da livre iniciativa e a livre concorrência no mercado (LIMA, 2016)

> Diante da transição para pontos de venda e relacionamento com o cliente e-commerce e plataformas online, tornou-se necessária a análise do contexto histórico, técnico e jurídico, permitindo assim a verificação das ações e indícios empreendidos nos demais países no tocante a tecnologias, produtos, serviços e seu impacto na sociedade (LIMA, 2016).

O Direito Digital é um desses desdobramentos recentes impulsionado pelo desenvolvimento do direito como ciência e que inclui um novo campo social com base nas propriedades tecnológicas.

Consoante, leciona o Doutor em Direito Mario Antônio Lobato de Paiva (2002): Direito Informático "*o ramo autônomo atípico da ciência jurídica que congrega as mais variadas normas e instituições jurídicas que almejam regulamentar as relações jurídicas estabelecidas no ambiente virtual".*

Sendo assim, pode-se conceituar o Direito Digital como sendo um conjunto de normas e conceitos doutrinários que estudam e padronizam as relações nas quais a tecnologia da informação é o fator primordial e cria direitos e obrigações secundários. Trata-se de um estudo aprofundado que utiliza todos os princípios codificados do Estado de Direito que regulam as relações dos mais diversos meios de comunicação, inclusive o de TI (ALMEIDA FILHO, 2005).

3.2 Evolução do Direito Digital no Brasil

O surgimento do Direito Digital resultou de um grande número de mudanças muito rápidas no curto prazo que forçam as relações sociais, seu alcance dentro e fora de seu ambiente operacional e a construção de suas funções.

Inicialmente, a lei era comum, mas não atendia às situações de origem técnica,

principalmente aquelas vinculadas à internet, aos poucos algumas decisões que tem sido tomada veem fornecendo para o problema da insegurança comercial e jurídica.

Uma dessas soluções é a implementação do Marco Civil da Internet, instituído pela lei nº. 12.965/201 de idealização peculiar, pela sua criação e discussão com um amplo leque de cidadãos participantes do fórum de discussão promovidas pelo Parlamento brasileiro em audiências online.

Haikal (2016) enfatiza que "um dos temas abordados pela Lei, gerador de debates, é a responsabilidade civil, por divulgar conteúdos em rede." A Lei fornece um conjunto de obrigações para os proprietários de sites. Os proprietários do site devem remover o conteúdo quando for devida a reclamação, além de manter um registro de suas atividades, caso sejam obrigados a indenizar aqueles que sofreram os danos publicados em suas postagens.

Outra solução plausível a ser destacada é dissolução do Direito Digital como ramo do Direito, assim como o Direito Tributário, Direito do Trabalho, Direito Cível e Direito Penal.

Salienta-se que além se ser considerado autônoma aos outros ramos do direito, o Direito Digital tornou-se essencial para o bom funcionamento das demais áreas da ciência que ele pertence. Portanto, o direito digital é interdisciplinar porque atua em um ambiente onde as relações jurídicas ocorrem nas mais diversas situações. Resumindo, seu impacto é reconhecido por quase todos os departamentos regulatórios em um ambiente virtual. Paiva (2003, p.02), aponta algumas formas quando a interdisciplinaridade do direito eletronico da seguinte forma:

> Direito Constitucional– O direito informático tem uma estreita relação com o Direito Constitucional porquanto a forma e panejamento da estrutura e órgãos fundamentais do Estado, é matéria constitucional. Deve ser ressaltado que dito manejamento e forma de controlar a estrutura e organização dos órgãos do Estado, se leva cabo por meio da informática, colocando o Direito Informático na berlinda, já que com o devido uso que é dado a estes instrumentos informáticos, se levará a uma idônea, eficaz e eficiente organização e controle destes entes.
> Propriedade Intelectual - a interrelação entre o Direito Digital e a propriedade intelectual é primordial e enseja uma série de preocupações por parte dos estudiosos, advindas de implicações jurídicas provenientes da facilidade de reprodução e utilização da propriedade intelectual, que pode ser violada com um simples toque de comando por intermédio de um computador; a tecnologia digital permite cópias perfeitas, enquanto que a *Internet* sem fronteiras propicia rápida disseminação das cópias, sem custo de distribuição;
> Direito Penal– O vínculo estabelecido entre essas duas matérias é evidente. Várias condutas criminosas tem sido perpetradas com o auxílio das

novas tecnologias que necessitam de específicas regulamentações com o objetivo de coibir ilícitos penais. [PAIVA, Mário Antônio Lobato de. P.02. 2003]

Portanto, verifica-se que o Direito Digital é um avanço da própria ciência do direito, como um novo campo que ainda não foi discutido, e ainda como todos os campos do direito existentes conhecidos. Todavia, não se deve esquecer que mesmo com sua necessidade para os outros ramos, a autonomia do direito digital é legítima em face da sua possibilidade inovações relacionais.

3.3 Crimes Cibernéticos

Notoriamente, a pandemia trouxe uma série de problemas a diversos países, que afetaram a vários setores importantes para o bom funcionamento do Estado, como a econômica, a política, a cultural e é claro a saúde. No entanto, os brasileiros, a partir de março de 2020, precisaram se preocupar com um outro setor, o digital.

Com as recomendações sobre distância social e parte da população em casa, as pessoas passam muito tempo em conexão, para trabalho, estudo ou lazer. Assim, com esse aumento no uso da Internet, os cibercriminosos começaram a ver brechas na adoção de novos golpes, principalmente usando como vítimas pessoas com pouca experiência online.

Fraude bancária, malware, roubo de dados, disseminação de vírus e muitos outros crimes são cometidos por meio de aplicativos de mensagens, mídia social, e-mail e sites. Tudo é feito por quem quer usar pessoas físicas ou jurídicas para ganhar dinheiro. Os golpes mais comuns que ocorrem durante a quarentena são golpes, cartões de crédito, WhatsApp duplicado, golpes de motoboy e falsos helpdesks (CRYPTO ID, 2021).

De acordo com a Fortinet Threat Intelligence Insider América Latina, empresa especializada em análise de incidentes de segurança cibernética, o Brasil realizou mais de 3 bilhões de ataques pela Internet entre desde o início da pandeia até o momento. A empresa preocupada com a crescente ciber-ataques, alerta seus usuários sobre as diversas campanhas de phishing criadas a fim de procurar vulnerabilidades no dispositivo usada e assim baixar malwares como o “Cavalo de Troia”.

> Durante este trimestre, foram detectadas na América Latina várias tentativas de execução de código remoto a dispositivos GPON e D-Link, que são usados principalmente para oferecer serviços de conectividade residencial. Isso nos mostra como os criminosos estão tentando comprometer os trabalhadores remotos, interceptando suas comunicações e redirecionando-os para sites maliciosos. Por outro lado, foi detectado novamente um aumento na distribuição de malware baseado na web na região. Para isso, diferentes campanhas de phishing têm sido utilizadas, nas quais usuários

comprometidos veem suas redes sociais compartilhando anúncios e sites falsos sem o seu consentimento. Se os usuários clicam em um desses

> anúncios, eles serão redirecionados sorrateiramente para a página de destino do kit de exploração. Esses kits de exploração podem procurar vulnerabilidades para baixar algum tipo de malware, por exemplo, cavalos de Tróia que, além de gerar persistência, procuram criar "pop-ups de cavalos de Tróia" ou anúncios que contêm código malicioso oculto para espalhar e infiltrar informações [FORTINET; 2021; On-line]

Esse aumento significativo deve-se principalmente a home offices e o tempo extra que todos gastam em informática e telefones celulares. Especialistas do setor afirmam que o aumento do uso da Internet aumentou o interesse dos cibercriminosos por esse tipo de ataque. Portanto, é preciso ficar atendo, pois os cibercriminosos estão espalhados em todo o mundo, prontos para aproveitar crise do coronavírus para explorar pessoas em casa que dependem de soluções digitais para suas atividades diárias.

3.3.1 Conceito de Crime Cibernético

O crime cibernético é apenas o ato de usar um computador ou tecnologia de computador para cometer um crime, ou o ato de que um computador ou veículo de computador é objeto de um crime. O crime cibernético é uma pratica ilícita que viola direitos fundamentais de outra pessoa, pelo uso de crimes relacionados à informática. Em termos gerais, o crime cibernético inclui todas as atividades criminosas cometidas com o uso de computadores ou tecnologia da informação (ALEXANDRE JUNIOR, 2019).

Simas (2014, p. 12) em sentido *stricto* afirma, “quem que o meio informático surge como parte integradora do tipo legal, ainda que o bem jurídico protegido não seja digital”. Rocha (2017, p. 03) simplifica, conceituando cibercrimes apenas como “práticas ilícitas na internet”.

Consoante, Jesus e Milagre (2016, p. 9), assegura que tais crimes trata-se de “fatos típicos e antijurídicos cometidos por meio dá, ou contra a tecnologia da informação, ou seja, um ato típico e antijurídico, cometido através da informática em geral”.

Nesta perspectiva, Rossini (2004) leciona:

> O conceito de ‘delito informático’ poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou

fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.

Adiante, a legislação brasileira, por intermédio da Lei n. 12.737, de 30 de novembro de 2012, dispõe sobre a tipificação criminal de delitos informáticos; alterando o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – Código Penal; e dando providências, especifica, em seu Art. 154-A, os crimes cometidos por meios informacionais:

> Art. 154-A. Invadir disposto informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismos de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita" (BRASIL, 2012, s.p.).

O crime na Internet também é conhecido como crime digital, crime cibernético, crime cibernético digital, crime de alta tecnologia, crime cibernético e outros. No entanto, este estudo considera o valor de usar o termo cibercrime.

A relação entre crime e internet pode parecer difícil, mas, como mencionado antes, são crimes mais graves, como roubo de informações pessoais, fotos íntimas, cópia de cartões e informações comerciais confidenciais e muito mais. Portanto, conhecer os principais conceitos de cibercrimes cometidos no Brasil e no mundo é essencial para resguardar a segurança do cidadão de bem.

3.4 Principais Condutas Criminosas Cibernéticas

O surto de crimes cibernéticos afeta não apenas o ambiente digital, mas também ofende moralmente e materialmente suas vítimas. Em seguida, explica-se- a os 3 principais tipos de crimes cibernéticos utilizados na atualidade.

3.4.1 Crimes contra a honra

Uma análise da honra do ponto de vista objetivo é caracterizada por uma imagem usufruída aos olhos da sociedade. Por outro lado, do ponto de vista objetivo, é definido como os sentimentos do indivíduo pela sua própria dignidade. Existem três tipos de crimes que são frequentemente cometidos em ambientes virtuais: **calúnia, difamação e injúria**.

Calúnia é definida como o ato de ser acusado sem realmente ter cometido um crime. Um exemplo de calúnia virtual ocorreu na rede social "Facebook". No caso, uma mulher foi falsamente informada pela polícia, acusada de ter sequestrado uma criança

para praticar magia negra. O rápido compartilhamento de imagens espalhou informações falsas, resultando no assassinato de um civil considerado criminoso.

A difamação ocorre quando uma pessoa é acusada de prejudicar publicamente a sua reputação. Neste caso não é necessário envolver um crime como a calúnia, basta uma simples acusação. Um exemplo, João Soares (nome fictício) postou uma foto de outra pessoa do grupo de vendas, expondo que este não o entregou o produto pedido, criando uma mancha no perfil do vendedor. Ressalta-se que o “art. 138 dispõe a calúnia como a imputação falsa de fato definido como crime. Portanto, a calúnia ofende a honra objetiva de quem a sofre” (MEDEIROS; UGLALDE, 2020)

E a injuria acontece quando, o dano ocorre quando o comportamento humilhante de uma pessoa afeta sua honra subjetiva, independentemente de sua visão da comunidade. Os exemplos incluem comentar na foto de alguém "ladrão" e outras formas de crime que tocam o coração da vítima.

Mesmo os crimes contra honra estando previstos no Código Penal, nos artigos 138, 139 e 140, as sanções são brandas e, quando ocorrem em ambiente virtual, o reparo é complicado porque beira a impossibilidade. Portanto, é necessário fortalecer as sanções de uma série de leis e implementar medidas para enfrentar as violações de dignidade cometidas na web.

3.4.2 Pornografia infantil e pedofilia.

A pedofilia é caracterizada como um desvio sexual em que o objeto sente atração sexual pela criança. De acordo com a psicologia e a psiquiatria, é uma ação, não um ato e, portanto, uma atração desviante. A pedofilia na Internet pode ocorrer de várias maneiras (SANCHES; ANGELO, 2018).

Martinelli (2000) define as formas do delito de duas maneiras:

> Pelas “home pages” e por correio eletrônico. Na primeira opção, os gerenciadores das páginas recebem uma quantia dos usuários (através de depósito ou catão de crédito) que dispõe de um acervo de fotos e vídeos. Na segunda opção o material é distribuído de um usuário a outro, diretamente

A partir do elencando artigos 240 e 241 do Estatuto da Criança e do Adolescente alterados em 2008 pela Lei 11.829, são expostos comportamentos característicos dos pedófilos. Esses crimes são rejeitados pela sociedade e, muitas vezes, resultam em penalidades para os responsáveis pelas alterações do ECA. A maior barreira para esse comportamento é identificar quem está por trás da pornografia e das conversas abusivas com crianças. As penas não são tão leves como no caso de crimes invasivos,

mas a pornografia e a pedofilia continuam sendo os crimes mais comuns cometidos no ambiente virtual.

3.4.3 Estelionato e fraudes virtuais

Estudo realizado pela Federação do Banco do Brasil (Febraban) mostra que o número de tentativas de fraudes financeiras contra brasileiros aumentou durante a covid19. Nesse período, a agência registrou um aumento de 80% no crime cibernético (fraude na Internet). As principais infrações incluem roubo de identidade, roubo e venda de dados comerciais, fraude por terceiros em sites de varejo online, fraude em seguros, caridade e arrecadação de fundos. Existem créditos fraudulentos e roubos de cartão que vêm com ele (TIBURSKI, 2020).

De acordo com a interpretação da Suprema Corte, transações fraudulentas no ciberespaço são características de peculato. No entanto, não é fácil definir padrões precisos para atividades cibercriminosos, especialmente para comércio.

O Direito Penal no artigo 171 define peculato como “obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.

Ao inserir a cláusula acima no contexto de peculato, o estelionato é definido como forma de crime que ilude a vítima visando a sua situação de vulnerabilidade e a leva ao erro, normalmente, o criminoso envia um e-mail falso para a vítima, que contém um link que redireciona a vítima para a página de compra. Este é o mecanismo usado para obter os dados bancários.

Um golpe de fraude e estelionato que ficou bem conhecido e encheu os bolsos dos cibercriminosos durante a pandemia, foi o “Golpe do Governo”, crime este que abordaremos detalhamento nos próximos capítulos.

3.5 Golpe do Governo

É de conhecimento geral a crise e histeria vivenciada pela população mundial, ocasionada pela epidemia de Covid19, que gerou além de medo, o desemprego em massa. Por isso, o governo disponibilizou uma ajuda de custo para a população que se encontrava em vulnerabilidade devido a propagação da doença. Diante destes fatos, muitos criminosos viram ali uma oportunidade excepcional para aplicar golpes para obter indevidamente os dados das pessoas, para que com isso pudessem sacar o auxílio dos cidadãos.

Em geral, o crime cibernético é um crime cometido pela Internet ou com o auxílio da Internet para consumo. Os cibercriminosos - como são chamados os

perpetradores desses crimes - usam a tecnologia e a Internet para aplicar vários golpes e persegui-los em todo o país. E essa prática tem evoluído diariamente durante

a disseminação do novo coronavírus, principalmente devido à carência da população e à falta de informação.

De acordo que o benefício emergencial foi desembolsado pelo governo, o número de fraudes na concessão desse benefício, fora crescendo gradualmente, tanto que o crime ficou nacionalmente conhecido como “golpe do governo”, como veremos a seguir na explanação do tema.

3.5.1 Como se Aplica

A aplicabilidade desse crime se dá por diversos meios eletrônicos (ligações, WhatsApp, faceboock, página na internet, sites, aplicativos), que encaminham os usuários a links onde pede-se informais que dariam acesso ao benefício emergencial emitida pelo governo federal.

Em ambos os casos, a partir do momento em que a vítima acessa um endereço de Internet ou baixa um aplicativo, seu dispositivo / computador é infectado por malware. Como resultado, os criminosos cibernéticos têm acesso a todas as informações, dados e conteúdo deste dispositivo / computador, deixando a vítima em um estado constante de vulnerabilidade grave.

Os criminosos persuadem as vítimas a clicar nas mensagens enviadas para leis sob o pretexto de se aproveitarem delas. Quando a vítima clica, ela é redirecionada para uma página falsa, geralmente idêntica à que ela normalmente visita. Ao inserir o nome de usuário e senha para acessar a página, os dados são encaminhados para os criminosos. Em seguida, uma mensagem de erro é exibida e o usuário é redirecionado para a página real da rede social. Desta forma, o criminoso tem acesso aos dados da vítima, que não percebe que foi enganada (RIO DE JANEIRO. ON-LINE).

Este comportamento é definido pelo direito digital como fraude(phishing) e é considerado crime na acepção do artigo 154-A do Código Penal, como já analisado anteriormente neste artigo (DOMINGUES, 2020).

De acordo com Gil (2000. p. 114)

> Ação intencional e prejudicial a um ativo intangível causada por procedimentos e informações (software e bancos de dados), de propriedade de pessoa física, ou jurídica, com o objetivo de alcançar benefício, ou satisfação psicológica, financeira e material.

Preocupados com o aumento do phishing, durante o período pandêmico, e com

o número significativo de pessoas que se queixavam de ter seus benefícios “roubados”, o governo do Rio de Janeiro, montou uma cartilha que ensina a população

há como não se tornar mais uma vítima dos criminosos, no texto os elaboradores mencionam em quadro quatro dicas simples, mais bem usuais, são elas:

> 1 - Nunca abra anexos ou links de mensagens não solicitadas.
> 2 - Nunca forneça suas informações pessoais.
> 3 - Mantenha o seu navegador, antivírus e sistema operacional sempre atualizados.
> 4 - Sempre confira se o endereço acessado é realmente o endereço correto. [Rio de Janeiro. Cartilha contra crimes virtuais. On-line]

O Supremo Tribunal de Justiça, configura esse tipo de ato ilícito como fraude, bem como estelionato. Não é fácil conceituar as características exatas desta conduta criminal, principalmente por elas acontecerem virtualmente. Todavia, essa modalidade de fraude vem tomando notoriedade de acordo que mais pessoas se formam vítimas destes criminosos.

Atualmente o Facebook, WhatsApp e Instagram, aparecem como os aplicativos de rede social mais comumente usados e mais conhecidos, mundialmente. Existem outros aplicativos, todavia, eles não se destacam, sendo assim não estão sendo considerados prioritários para a justiça, porém não se deve desconsiderá-los. Em uma sucinta pesquisa na internet é possível encontrar diversos destes aplicativos, como por exemplo; GoSMS Pro, Im+, WeChat, BBM, Viber, Ebuddy, ooVoo, Clipchat, ChatOn e ChompSMS. Então, deve-se ficar atento pois, pode-se deduzir que cibercriminosos também podem utilizar esses outros aplicativos em um momento conveniente.

3.6 Medidas Legais

Quanto as medidas legais o doutrinador Ramos (2017, p. 38), leciona que “a Convenção sobre o Cibercrime uma vez que não dita às regras, mas sim orienta sobre o tema, deixando a critério de cada País, criar sua própria legislação específica”.

Portanto, entende-se pelo exposto que cabe ao governo estabelecer as normas, bem como as peculiaridades que atendam os crimes cibernéticos, na finalidade de sancionar os cibercrimes.

Entretanto, com os avanços tecnológicos atuais, tornou-se visível o quão despreparado estava o código penal, frente aos momentos históricos ao qual o país se encontra, restando ao direito a missão de conciliar as difíceis tarefas das instituições penais com a constante mudança tecnologia (PACHECO, 2011, p. 06). Embora houve modificações na legislação, ainda há conjunto simplificado de regras que tipificam as

condutas ilícitas virtuais.

Salienta-se que “existe uma ineficácia na normatização dos crimes virtuais em frente aos desafios que a sociedade informatizada apresenta” (MAIA, 2017). Como por exemplo as Leis 12.735/2012 (BRASIL, 2002), 12.737/2012 (BRASIL, 2012), e 12.965/2014 (BRASIL, 2014), que embora estejam vigorando por muitos anos, ainda não são suficientes ao combate efetivo dessas atividades criminosas. Causando dificuldades aos aplicadores do Direito, pois não se encontra analogias aos crimes devido a sua natureza taxativa no Código Penal Brasileiro.

Porém, no final de maio, o Governo Federal aprovou a Lei nº 14.155 de 2021 e a publicou no Diário Oficial da União. Com as novas regras, as vítimas de intrusão de equipamentos de informática, furto fraudulento e apropriação indébita de recursos públicos passaram a ter mais proteção nesse ambiente.

A lei é derivada do projeto de lei 4.554 / 2020 do senador Izalci Lucas (PSDB-DF), aprovado pelo Senado no início deste mês. O texto altera a Lei Penal (Decreto nº 2.848, de 1940) para aumentar as penas, como intrusão de dispositivo, furto legal e corrupção que ocorrem em meio digital, independentemente de estar conectado à Internet.

De acordo com a nova redação do código, o crime de invasão de equipamentos de informática será punido com pena de prisão e multa de um a quatro anos e, se a intrusão causar prejuízos econômicos, aumentará de um terço para dois terços. Anteriormente, as penas aplicáveis eram reclusão e multas de três meses a um ano.

Por outro lado, se a intrusão resultar na obtenção de conteúdos de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações confidenciais ou dispositivos de intrusão controlados remotamente não autorizados, será punida com pena de prisão de dois a cinco anos e multa. Antes da aprovação da nova lei, essas penas iam de seis meses a dois anos, mais multas.

No caso de penas de reclusão, o sistema de cumprimento de sentença pode ser fechado. Por outro lado, a detenção aplica-se a condenações mais leves e não permite o cumprimento do sistema fechado.

3.7 Quanto aos meios de prova

Para os crimes virtuais, existem obstáculos na coleta e coleta de evidências, pois a maior dificuldade nas investigações criminais relacionadas a esses crimes é a falta de evidências que comprovem o comportamento criminoso.

O argumento do STJ é que as provas obtidas diretamente dos dados armazenados no celular do réu são ilegais. O precedente do tribunal entende que, sem

autorização judicial prévia, mensagens de texto, mensagens de texto e conversas por

meio do WhatsApp e outros aplicativos obtidos diretamente pela polícia durante uma prisão in loco são inválidos.

Com intuito de exemplificar o tema, analisa-se o caso da AgRg no RHC 92.801, onde os policiais civis tiveram acesso às mensagens que apareciam no celular WhatsApp do réu no momento da prisão pelo delito, sem ordem judicial. De acordo com o quinto grupo, as provas obtidas tornaram-se ilegais e devem ser retiradas dos autos, juntamente com outras provas obtidas diretamente deles.

> AGRAVO REGIMENTAL NO RECURSO ORDINÁRIO EM HABEAS CORPUS. NOVOS ARGUMENTOS HÁBEIS A DESCONSTITUIR A DECISÃO IMPUGNADA. INEXISTÊNCIA. TRÁFICO DE DROGAS. NULIDADE. ACESSO AOS DADOS ARMAZENADOS EM TELEFONE CELULAR (MENSAGENS DE "WHATSAPP") DURANTE A PRISÃO EM FLAGRANTE. AUSÊNCIA DE AUTORIZAÇÃO JUDICIAL. NULIDADE DAS PROVAS. RECONHECIMENTO. AGRAVO INTERPOSTO PELO MINISTÉRIO PÚBLICO DESPROVIDO. I - É assente nesta Corte Superior de Justiça que o agravo regimental deve trazer novos argumentos capazes de alterar o entendimento anteriormente firmado, sob pena de ser mantida a r. decisão vergastada pelos próprios fundamentos. II - A jurisprudência das duas Turmas da Terceira Seção deste Tribunal Superior firmou-se no sentido de ser ilícita a prova obtida diretamente dos dados armazenados no aparelho celular, relativos a mensagens de texto, SMS, conversas por meio de aplicativos (WhatsApp), obtidos diretamente pela polícia no momento da prisão em flagrante, sem prévia autorização judicial. III - In casu, os policiais civis obtiveram acesso aos dados do aplicativo WhatsApp armazenados no aparelho celular do agravado no momento da prisão em flagrante, sem autorização judicial, o que torna a prova obtida ilícita, e impõe o seu desentranhamento dos autos, bem como dos demais elementos probatórios dela diretamente derivados. Agravo regimental desprovido.

Segundo o ministro que denunciou o caso, Felix Fischer, os dados são armazenados no celular por meio do envio ou recebimento de dados por meio de mensagens SMS, programas ou aplicativos de mensagens ou mesmo e-mail, relativos à privacidade e aos direitos de privacidade dos separado, portanto, é inviolável, nos termos do art. 5º, X, da Constituição Federal.

Mougenot, acredita que a prova é um instrumento utilizado pelo sujeito do litígio para comprovar os fatos da causa, ou seja, as acusações presumidas pelas partes como base para o exercício da tutela jurisdicional. (MOUGENOT, 2019, p. 467)

Eugênio Pacelli apud Medeiros e Ugleno:

> “A prova judiciária tem o objetivo claramente definido: a reconstrução dos fatos investigados no processo, buscando a maior coincidência possível com a realidade histórica, isto é, com a verdade dos fatos,

> tal como efetivamente ocorrido no espaço e no tempo. A tarefa, portanto, é das mais difíceis, quando não impossível: a reconstrução da verdade". (PACELLI, 2017, p. 174)

Observa-se, que nem todas as evidências podem ser utilizadas, pois algumas evidências só podem ser coletadas por meio de autorização judicial, se você não fizer isso, elas serão inválidas ou até mesmo inutilizáveis.

4 Considerações Finais

O objetivo principal deste artigo fora destacar o aumento dos crimes cibernéticos, nesta nova era digital em que vivemos. A comodidade da Internet e os preços acessíveis dos computadores e dispositivos móveis têm levado a um rápido aumento do número de usuários no ambiente de rede, portanto, a mesma proporção de crimes cibernéticos também tem aparecido.

A condicionalidade do tempo e do espaço torna o mundo virtual, uma área diversificada para todos os tipos de transações, ou mesmo como mecanismo de grande utilidade acadêmica e científica. No entanto, a internet e seus recursos criaram a ideia de liberdade irrestrita faz com que as pessoas sintam a possibilidade de serem protegidas do anonimato proporcionado pela tecnologia. Por outro lado, todas essas facilidades estão chegando acompanhado por uma nova forma de crime chamada cibercrime, uma vez que tais atos criminosos envolvem uma nova forma espacial, o ciberespaço.

O Código Penal Brasileiro representa diversas ações adequadas ao ambiente de rede, mas suas penalidades são relativamente leves e não são suficientes para coibir a implementação dessas ações. Como por exemplo o como "golpe do governo que pode ser tipificado no Código Penal como fraude(phishing) e é considerado crime na acepção do artigo 154-A, pois não há uma previsão legal que defina a ação em si como um crime.

Dessa forma, a falta de legislação específica contra o crime cibernético exacerbou a ideia de que a Internet é uma terra sem lei. No entanto, é necessário promulgar legislação para tratar de crimes cometidos em ambientes virtuais porque são comuns e podem causar danos reais às vítimas. A punição proporcional é uma forma de controlar esses comportamentos criminosos, pois sabendo que eles podem reagir de forma dolorosa, bandidos ou mesmo pessoas comuns irão supervisionar seu comportamento.

Referências

ALEXANDRE JÚNIOR, J. C. **Cibercrime: um estudo acerca do conceito de crimes informáticos.** Revista Eletrônica da Faculdade de Direito de Franca, v. 14, n. 1, jun. 2019.

ALMEIDA FILHO, José Carlos de Araújo. **Direito Eletrônico ou Direito da Informática**? Informática Pública vol. 7 (2): 11-18, 2005. Disponível em: https://docero.com.br/doc/xn1v0n5 Acesso em 10 de jun. 2021.

ALVES, Marcelo de Camilo Tavares. **Direito Digital.** Goiânia, 2009. 9-10 Pdf. Disponivel em https://docero.com.br/doc/xc0vec Acesso em 10 de jun. 2021.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos**; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial [da] União, Brasília, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso em: 26 de agos.2021.

_____. Decreto de Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Brasília, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm . Acesso em: 17 abr. 2021.

_____. Lei n° 8.069 de 13 de julho de 1990. **Estatuto da Criança e do Adolescente.** Diponivel em http://www.planalto.gov.br/ccivil_03/leis/l8069.htm Acesso dia 16 de agos. De 2021

_____. Lei nº 12.965, de 23 de abril de 2014 **(Marco Civil da Internet**). Disponível em: Acesso em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm 17 abr. 2021.

_____. Lei nº 14.155, de 27 de Maio de 2021 (Alterição do Código Penal) Disponivel me: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm Acessado em 22 de set. De 2021

COLARES, Rodrigo Guimarães. **Cyber crimes: os crimes na era da** https://jus.com.br/artigos/3271/cybercrimes-os-crimes-na-era-da-informatica Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 7. 10 de jun. 2021.

CRYDPTO ID; site. **Crescimento de crimes cibernéticos na pandemia: como não ser uma vítima. 28** de abril de 2021 Disponível em: https://cryptoid.com.br/identidade-digital-destaques/crescimento-de-crimes-ciberneticos-na-pandemia-como-nao-ser-uma-vitima/ Acesso em 24 de agos. 2021.

FORTINET; site. **Thret Intelligence Insider. Q1/2021** Disponível em: https://www.fortiguardthreatinsider.com/pt/bulletin/Q1-2021 Acesso em 24 de agos. 2021.

GIL, Antônio de Loureiro. **Fraudes Informatizadas**. 2ª edição, 1ª tiragem, 2000

HAIKAL, Victor Auilio. Enfim, o marco civil da internet. In: PINHEIRO, Patrícia Peck (coord.). Direito digital aplicado 2.0. 2.ed. São Paulo: Thomson Reuters, 2016.

JESUS, D. de; MILAGRE, J. Antonio. Manual de Crimes Informáticos. São Paulo: Saraiva, 2016.

LIMA, Glaydson de Farias. **Manual de direito digital: fundamentos, legislação e jurisprudência**. Curitiba, Appris, 2016.

MACEDO, Luiz Fernando Belizário. **CIBERCRIMES: A INTERNET COMO FERRAMENTA NA EXECUÇÃO DE CRIMES VIRTUAIS E O COMBATE REALIZADO PELO DIREITO PENAL BRASILEIRO.** Faculdade evangélica de Rubiataba. Disponível em: http://45.4.96.19/bitstream/aee/17848/1/2020%20-TCC%20-LUIZ%20FERNANDO%20BELIZ%c3%81RIO%20MAC%c3%8aDO.pdf Acesso em 10 de jun. 2021.

MAIA, T. S. F. **Análise dos mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro.** Universidade Federal do Ceará. Faculdade de Direito, Curso de Direito, Fortaleza, 2017. Disponível em: http://www.repositorio.ufc.br/bitstream/riufc/31996/1/2017_tcc_tsfmaia.pdf Acesso em 07 de jun. 2021.

MARTINELLI. J.P. O. Aspectos relevantes da criminalidade. Disponivel em: https://jus.com.br/artigos/1829/aspectos-relevantes-da-criminalidade-na-internet. Acesso em 26 de agos. 2021

MEDEIROS, G.S; UGLENO J.C.R. **Crimes Cibernéticos: Considerações Sobre a Criminalidade na Internet.** https://ambitojuridico.com.br/cadernos/direito-penal/crimes-ciberneticos-consideracoes-sobre-a-criminalidade-na-internet/ Acesso em 26 de agos. 2021.

RAMOS, E. D. Crimes cibernéticos: análise evolutiva e Legislação penal brasileira. Curso de Direito da Universidade Federal do Rio de Janeiro. 2017. Disponível em: https://pantheon.ufrj.br/bitstream/11422/6911/1/EDRamos.pdf Acesso 07 de jun. 2021.

PACHECO, Wilfredo Enrique Pires . **Manual de Responsabilização Penal dos Hackers, Crackers, e Engenheiros Sociais.** Disponivel em: https://www.conjur.com.br/dl/guia-crimes-digitais.pdf Accesso em: 07 de jun. 2021.

PAIVA, Mário Antônio Lobato de. **Ciência do Direito Informático** maio, 2002. Disponível em: https://egov.ufsc.br/portal/sites/default/files/anexos/30390-31543-1-PB.pdf Acesso em 04 de ago. 2021

_____, Mário Antônio Lobato de. **Primeiras linhas em Direito Eletrônico**. Novembro, 2002. Disponível em: Primeiras linhas em Direito Eletrônico - Página 2/4 - Jus.com.br | Jus Navigandi. Acesso em 25 de jun. de 2021**.**

REVISTA, Âmbito Jurídico. Os institutos do Direito Informático. Disponível em: Os institutos do Direito Informático - Âmbito Jurídico - Educação jurídica gratuita e de qualidade (ambitojuridico.com.br). Acesso dia 22 de jun. de 2021

ROCHA, A. A. **Cibercriminalidade: os crimes cibernéticos e os limites da liberdade de expressão na internet.** Faculdade de Ensino Superior e Formação Integral. Curso de Direito. São Paulo, 2017. Disponível em: https://www.faef.br/userfiles/files/23%20-%20CIBERCRIMINALIDADE%20E%20OS%20LIMITES%20DA%20LIBERDADE%20DE%20EXPRESSAO%20NA%20INTERNET.pdf 24 de agos. 2021

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal.** São Paulo: Memória Jurídica, 2004.

SANCHES. A.G; ANGELO. A.E. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em: https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil Acesso em 24 de agos.

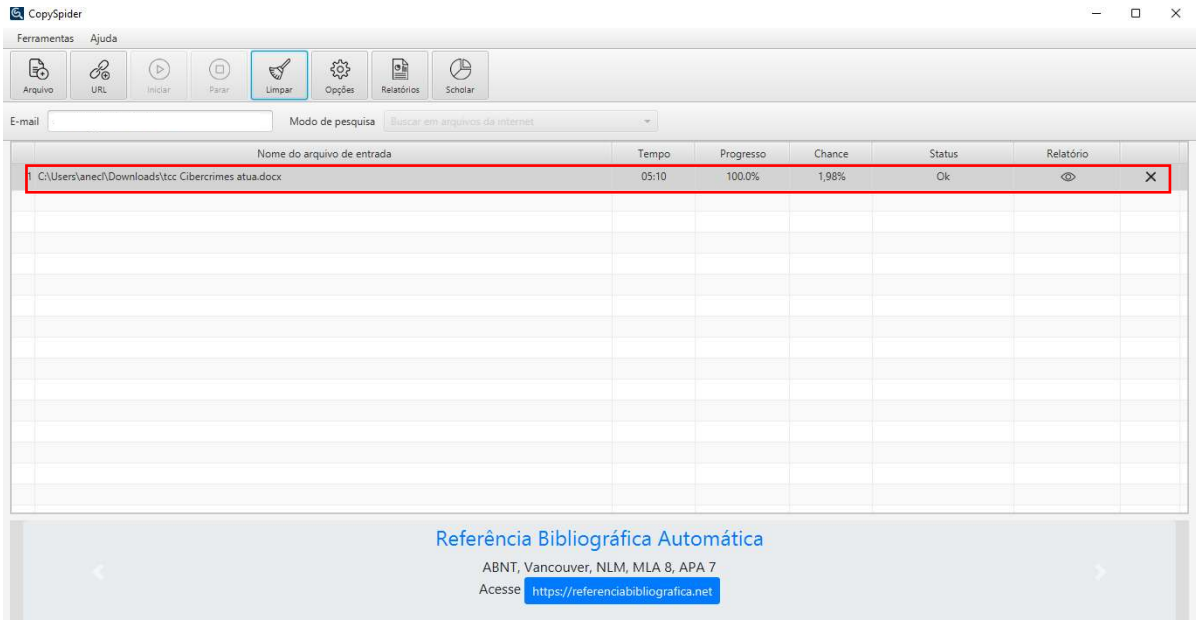
SANTOS, Coriolano Aurélio Almeida Camargo. **ATUAL CENÁRIO DOS CRIMES CIBERNÉTICOS NO BRASIL.** Diponivel em: http://p-web01.mp.rj.gov.br/Informativos/2_cao/2010/marco_abril/ATUAL_CENARIO.pdf Acesso em 10 de jun. 2021.

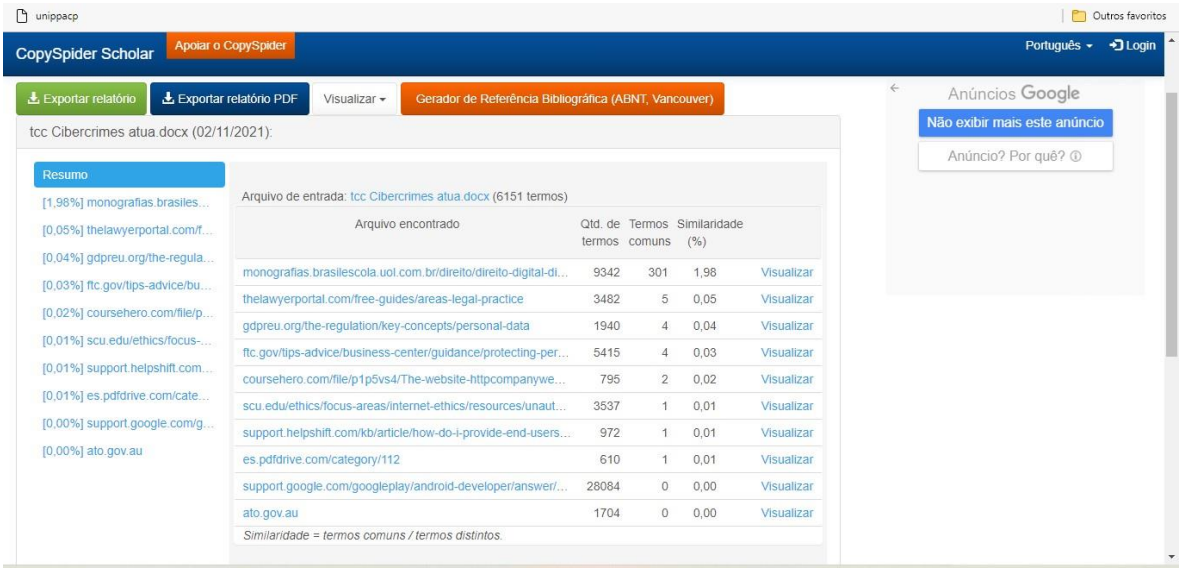
SIMAS, Diana Viveiros de. **O cibercrime**. 2014. 168f. Dissertação (Mestrado em Ciências Jurídico Forenses). Universidade Lusófona de Humanidades e Tecnologias. Lisboa. 2014

STF. **AgRg no RECURSO EM HABEAS CORPUS Nº 92.801 - SC (2017/0322640-7).** Diponivel em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1689703&num_registro=201703226407&data=20180326&formato=PDF Accesso em 20 de set. 2021.

TIBURSKI. Pricilla. Crescimento sobre golpes em operações online atinge cada vez mais vítimas na internet. UMSP. Diponivel em: http://www.metodista.br/rronline/fraudes-digitais-aumentam-80-durante-a-pandemia Acesso 26 de agos de 2021

Relatório de Plágio





Ficha de Acompanhamento

Faculdade Presidente Antônio Carlos de Teófilo Otoni

FICHA DE ACOMPANHAMENTO INDIVIDUAL DE ORIENTAÇÃO DE TCC

Atividade: Trabalho de Conclusão de Curso – Artigo/Monografia.
Curso: Direito **Período:** 9º **Semestre:** 2º **Ano:** 2021

Professor (a): Emerson Barrack Cavalcanti

Acadêmico: Douglas Mota Pereira

Tema: CRIMES CIBERNÉTICOS E O GOLPE DO "BENEFÍCIO DO GOVERNO"	**Assinatura do aluno** Douglas M. Pereira
Data(s) do(s) atendimento(s)	Horário(s)
Agosto	Horários diversos
Setembro	Horários diversos
Outubro	Horários diversos

Descrição das orientações:

Orientações bibliográficas, desenvolvimento estrutural e normativo, revisão e correção.

Considerando a concordância com o trabalho realizado sob minha orientação, **AUTORIZO O DEPÓSITO** do Trabalho de Conclusão de Curso do (a) Acadêmico (a) **Douglas Mota Pereira.**

Emerson Barrack Cavalcanti
Professor - Mat.: 2601419

Faculdade Presidente Antônio Carlos de Teófilo Otoni

FICHA DE ACOMPANHAMENTO INDIVIDUAL DE ORIENTAÇÃO DE TCC

Atividade: Trabalho de Conclusão de Curso – Artigo/Monografia.
Curso: Direito **Período:** 9º **Semestre:** 2º **Ano:** 2021

Professor (a): Emerson Barrack Cavalcanti

Acadêmico: Victor Pereira dos Santos Guerra

Tema: CRIMES CIBERNÉTICOS E O Ggolpe do "BENEFÍCIO DO GOVERNO"		**Assinatura do aluno** Victor Pereira dos Santos Guerra
Data(s) do(s) atendimento(s)	Horário(s)	
Agosto	Horários diversos	Victor Pereira dos Santos Guerra
Setembro	Horários diversos	Victor Pereira dos Santos Guerra
Outubro	Horários diversos	Victor Pereira dos Santos Guerra

Descrição das orientações:

Orientações bibliográficas, desenvolvimento estrutural e normativo, revisão e correção.

Considerando a concordância com o trabalho realizado sob minha orientação, **AUTORIZO O DEPÓSITO** do Trabalho de Conclusão de Curso do (a) Acadêmico (a) **Victor Pereira dos Santos Guerra.**

Emerson Barrack Cavalcanti
Professor - Mat.: 2601419

Digitalizado com CamScanner