PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

ARTIGO CIENTÍFICO

CRIMES CIBERNÉTICOS NO BRASIL

INVASÃO DE DISPOSITIVO INFORMÁTICO E ESTELIONATO VIRTUAL

ORIENTANDA: BIANCA STEFANY RIBEIRO DOS SANTOS

ORIENTADOR: PROF. GIL CESAR COSTA DE PAULA

GOIÂNIA
2023

BIANCA STEFANY RIBEIRO DOS SANTOS

CRIMES CIBERNÉTICOS NO BRASIL

INVASÃO DE DISPOSITIVO INFORMÁTICO E ESTELIONATO VIRTUAL

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Prof. Orientador: Mestre Gil Cesar Costa de Paula

GOIÂNIA
2023

BIANCA STEFANY RIBEIRO DOS SANTOS

CRIMES CIBERNÉTICOS NO BRASIL

INVASÃO DE DISPOSITIVO INFORMÁTICO E ESTELIONATO VIRTUAL

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientador: Prof. Gil Cesar Costa de Paula Nota

_____

Examinador Convidado: Prof. Titulação e Nome Completo Nota

SUMÁRIO

CRIMES CIBERNÉTICOS NO BRASIL

INVASÃO DE DISPOSITIVO INFORMÁTICO E ESTELIONATO VIRTUAL

Bianca Stefany Ribeiro dos Santos[1]

RESUMO

Em face do cenário atual, na qual os avanços tecnológicos evoluem dia após dia, trazendo consigo o real significado de globalização, oferecendo oportunidades de comunicação e exploração no âmbito virtual; nessa oportunidade indivíduos se aproveitam para explorar e lesar os usuários da rede. O presente estudo tem como objetivo conceituam-se crimes cibernético, bem como invasão de dispositivo informático no Brasil seu impacto social e examinar o papel da legislação brasileira na luta contra crimes cibernético.

Palavras-Chave: Crime Cibernético**.** Legislação brasileira. Internet

ABSTRACT

In view of the current scenario, in which technological advances evolve day after day, offering opportunities for communication and exploration in the virtual environment; in this opportunity, individuals take advantage to exploit and harm network users. The present study aims to conceptualize cybercrimes, as well as hacking of computer devices in Brasil and examine the role of Brazilian legislation in the fight against cybercrimes.

Keywords: Cybercrime. Brazilian legislation. Internet

[1] Acadêmico (a) do Curso de Direito da Pontifícia Universidade Católica de Goiás, bianca_stefany15@hormail.com

INTRODUÇÃO

No presente artigo tem como intuito explora e contextualizar crimes cibernético e explanar sobre invasão de dispositivo e crimes no ambiente virtual, o estudo será executado por meio de pesquisas bibliográficas, jurisprudências e normas do sistema jurídico brasileiro e com o apoio de artigos da Internet.

A sociedade tem sofrido grandes mudanças atualmente, nota-se que com os grandes avanços tecnológicos tem aberto espaços para os crimes virtuais que caracterizado por todo e qualquer crime realizado no âmbito virtual, estes crimes podem gerar danos às pessoas ou seu patrimônio. Inúmeros relatos de pessoas que são lesadas ou ofendia no meio virtual; conhecido, parente, amigo ou um familiar próximo, passou por alguma situação de golpe invasão de dispositivo, extorsão, estresse emocional, danos à reputação das vítimas e fraude na internet., esse indivíduo perdeu seu dinheiro ou teve suas redes sociais invadida por criminosos, como ocorreu com a triz Carolina Dieckmann que teve seu e-mail hackeado e fotos intimas vazadas, na época o caso repercutiu tanto que foi sancionada a Lei Brasileira 12.737/2012.

Com a tentativa de proteger os bens e integridade do indivíduo a legislação brasileira sancionou leis com tipificação criminais para delitos informático, Lei nº 12.965 de 23 de abril de 2014, Marco Civil da Internet, Lei nº 13.709, de 14 de agosto de 2018 proteção de dados, mas com toda essa tentativa não foi capaz de suprir as necessidades jurídicas.

Nessa narrativa a dificuldade de tratar esses crimes é pela agilidade com que eles acontecem, e podendo na maioria das vezes, os crimes não deixa rastro ou quem realizou.

1 ASPECTOS HISTÓRICOS E CONCEITUAIS DOS CRIMES CIBERNÉTICOS

1.1 BREVE CONTEXTO HISTÓRICO E EVOLUÇÃO DA INTERNET

Na medida em que a sociedade se desenvolvia ia trazendo com ela transformações e evoluções, exemplo disso foi a revolução Francesa e a revolução industrial que trouxe consigo direito fundamentais, no entanto os desenvolvimentos trazidos pela revolução sempre acompanham problemas, com a internet não foi diferente.

A internet surgiu em meio a guerra fria, no Estados Unidos em 1969, Inicialmente chamada de *Arpanet*, a princípio sua função era interligar laboratórios de pesquisa naquele mesmo ano foi enviado o primeiro e-mail, da universidade da California para universidade de Stanford, a partir disso passou a ser usado entre os militares e a defesa norte-americana. Em 1982 a Arpanet passou a ser chamada de internet e se expandiu para outros países como Suécia, Dinamarca e Holanda (JORGE, 2013), já no Brasil, a conexão à internet chegou em meados dos anos de 1988, por intermédio de instituições acadêmicas de São Paulo e Rio de Janeiro. Contudo em 1995 a internet começou a ser comercializada no país; o ministério da comunicação decide torna definitivo e expandir a comercialização, (BRASIL ESCOLA, 2008).

Nesse sentido a evolução da internet foi sendo perceptiva ao passar dos anos.

> Como tudo que evolui tem seus benefícios e prejuízos a tecnologia digital não seria diferente e como consequência desses avanços surge os crimes cibernéticos, porque em vez dos internautas usarem como instrumento de bom uso, fizeram ao contrário, usando para cometer delitos virtuais. COLARES 2002.

A modernização da internet não parou de crescer desde então, e muitos acreditam que foi a maior criação tecnológica já inventada, nesse sentido foi levando um crescimento digital e com ela possibilidades virtuais para a prática de violências.

1.2 CRIMES CIBERNÉTICOS

Os crimes cibernéticos ou crimes virtuais, consistem na ausência física do autor e na prática de conduta criminosa realizada por qualquer pessoa, de forma anônima ou não, por meio do uso de aparelho de dispositivo informático conectado à rede de internet. conforme (Colares, 2022) “Dessa forma, são crimes que podem admitir sua consecução no meio cibernético: calúnia, ameaça, divulgação de segredo, dano, apropriação indébita, estelionato (...)”

Nessa perspectiva, o site Brasil escola explica o conceito de crimes virtuais:

> Crime virtual ou crime digital pode ser definido como sendo termos utilizados para se referir a toda a atividade em que um computador ou uma rede de computadores são utilizados como uma ferramenta, uma base de ataque ou como meio de crime. Infelizmente, esta prática tem crescido muito já que esses criminosos virtuais têm a errada impressão que o anonimato é possível na Web e que a Internet é um mundo sem lei (BRASIL ESCOLA, 2008).

Contudo essa prática não é realizada apenas pelo individuo com conhecimento avançado em tecnologia, esse delito vem se tornando cada vez mais comum entre a sociedade.

1.3 DO CONCEITO CRIME CIBERNÉTICO

O termo cibercrimes surgiu na França no fim da década de 90, após uma reunião do grupo G8, composto pelos países mais ricos do mundo na qual originou-se que crimes cometidos por dispositivos eletrônicos utilizando a internet seria denominado cibercrimes, o delito começou com uso de aparelho para espionagem pois ela seria uma das estratégias das forças armadas norte-americanas, e intensificou para outros delitos.

Conforme Damásio (2016) sobre o conceito jurídico de crimes cibernético: “Crime informático é um fenômeno inerente às transformações tecnológicas que a sociedade experimenta e que influenciam diretamente no Direito Penal”, e para Gimenes (2013, p.01) “o crime virtual é qualquer ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão em que um computador conectado à rede mundial”.

Os crimes cibernéticos causam impactos sociais, econômicos e jurídicos, nos últimos anos foram marcados pelos avanços tecnológicos e marcado pela modernidade, mas também responsável pelos diversos crimes que se espalham cada vez mais.

De acordo com Joslaine Redivo (2022):

> Os crimes cibernéticos crescem de modo avassalador, por isso os avanços tecnológicos se inovam cada dia mais rápido, infelizmente esses crimes se espalham na web de forma que se torna difícil a identificação dos usuários que praticam delitos virtuais, devido seu anonimato. As consequências dos crimes cibernéticos são gravíssimas, gerando prejuízos imensuráveis, não somente para a vítima, mas também para a segurança dos sistemas de informações e banco de dados como um todo.

Assim os crimes cibernéticos estão ligados a qualquer prática ilícita, na qual internet se torna uma pioneira para cometer o crime, podendo atingir tanto pessoas ficar ou jurídica gerando prejuízos aos usuários.

2 O DIREITO PENAL BRASILEIRO E OS CRIMES CIBERNÉTICOS

2.1 CONCEITO LEGAL DE CRIME CIBERNÉTICO

Com o crescimento dos crimes virtuais no Brasil, o ordenamento jurídico teve que estabelecer Leis com tipificações penais, para delitos informáticos e enquadrar a essa nova realidade, Sydow explica sobre a conduta delituosa:

> O criminoso informático pode cometer mais de uma conduta lesiva ao mesmo tempo, podendo estar em diversos lugares simultaneamente, contando ainda com o fato de ser, muitas vezes, discreto e silencioso. Além disso, culturalmente, a sociedade ainda conta com uma postura omissiva e, nem sempre, denuncia as condutas ofensivas (SYDOW, 2009).

Essas condutas, segundo a doutrina, são classificadas em duas, crimes próprios e impróprios, os crimes próprios são aqueles que o computador é o objeto para pratica o delito tendo a prática e a consumação no âmbito virtual como invasão, modificação ou ataques de hackers já os impróprios são os que

utilizam o computador e internet para intermédio de delitos que reproduzem efeitos na “vida real” como por exemplo a falsificação de documento.

Com o avanço da legislação brasileira, entrou em vigor em 2012 Leis de crimes informático, conhecida como Lei Carolina Dieckman nº 12.737, posteriormente em 2014, sanciona-se a Lei nº 12.965 Marco Civil da Internet. Em seguida no ano de 2016 foi apresentado o relatório final da Comissão Parlamentar de Inquérito (CPI) que teve como presidente a Deputada Maria do Carvalho (PSDB) e relator deputado Esperidião Amim (PP), o relatório designado para investigar crimes cibernético.

2.2 A LEGISLAÇÃO PENAL BRASILEIRA

Já pautada ao longo desse projeto, os artigos 154-A e 154-B, que fora acrescido no Código Penal brasileiro, foi tipificado como crime de invasão de dispositivo informático, e em 2014 regula os direitos e deveres dos usuários Lei 12.965/2014 Marco Civil.

Em 2018 foi aprovada pelo presidente Michel Temer, a Lei Geral de Proteção de Dados (LGPD). Lei Nº 13.709, de 14 de agosto de 2018 que dispõe:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A lei sancionada para a proteção de dados pessoais, bem como proteger os direitos fundamentais das pessoas. Posteriormente, em 28 de maio de 2021, publicado do diário oficial da união a Lei 14.155, de 2021 sancionada pelo Presidente Jair Bolsonaro, prever penas mais dura contra crimes virtuais a lei altera o Código Penal Decreto-Lei 2.848, de 1940, dispõe:

> 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:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

O interesse ou até mesmo esforço para mudanças e cumprimentos da legislação contra crimes cibernéticos é ineficaz, pois deixa de atender diversas necessidades.

Sobre a ineficácia Ferreira discorre:

> A ineficácia na normatização nos crimes virtuais, ainda não foi suprida para um combate efetivo contra estes delitos, por isso diante dessa dificuldade encontrada, ou até mesmo pela natureza taxativa do Código Penal, á uma grande impossibilidade da aplicação da analogia nos crimes virtuais. (FERREIRA, 2015, p.44).

A fragilidade das aplicações corresponde a uma serie de crimes ao longo do tempo.

2.3 TIPOS DE CRIME CIBERNÉTICO

Os crimes cibernéticos não têm apenas efeito no ambiente virtual, também produz efeito no elemento moral e material, aqui destaco alguns cibercrimes mais comuns:

2.3.1 Cyberbullying: é a conduta de bullying no ambiente virtual como redes sociais, Email e entre outros é caracterizado pela perseguição, humilhação e constrangimento, o condutor da prática utiliza de criação de apelidos, confecção de montagens ou divulgação de imagens constrangedoras da vítima. Dados de um estudo, realizado pelo Instituto de Pesquisa Ipsos, indicaram que um em cada cinco pais em todo o mundo tem um filho que já foi vítima de cyberbullying. No Brasil, mais de 25% dos pais sabem que o filho foi vítima de cyberbullying pelo menos uma vez. Para aparar as vítimas de Cyberbullying entrou em vigor em 2015 a Lei 13.185 “Art. 1º Fica instituído o Programa de Combate à Intimidação Sistemática (Bullying) em todo o território nacional.” que prevê medidas de conscientização e apoio a vítima.

2.3.2 Crimes contra honra: os crimes classificados contra honra são injúria calúnia e difamação, tipificados no código penal nos artigos 138, 139 e 140. O autor expõe na internet de modo indevida fotos e opiniões próprias de outrem, que se faz espalha-se nos aplicativos de mensagens de forma mentirosa.

2.3.3 Pornografia infantil: A pornografia infantil na internet, compreende como: produzir, vender, adquirir e publicar vídeos envolvendo crianças e adolescentes ou aliciá-los para realizarem atividades sexuais ou para se exporem de forma pornográfica.

Os “pedófilos” utilizam do ambiente virtual para praticarem o delito, se aproveitando da fragilidade e inocência da criança. A prática de pornografia infantil já existe a décadas, mas intensificou com o avanço da internet como destaca GOMES:

> A pornografia infantil virtual é responsável por problemas de dimensões múltiplas, justamente por ser a internet um veículo rápido, cômodo, barato e seguro para transportar e comercializar filmagens e fotos degradantes e sádicas envolvendo crianças em cenas de sexo, circulando 24 horas por dia na rede” (GOMES, 2008, p. 16-17).

Por isso entrou em vigor em novembro de 2005 a Lei 11.892 que tipificou o crime de pornografia infantil pela internet, “Finalmente, a lei ampliou a criminalização dos agentes que buscam jovens em programas de comunicação, com o fim de praticar ato libidinoso” (NUCCI, 2018, p. 24). Dessa forma o condigo penal institui punição para o indivíduo que promove pornografia infantil.

3 ESTELIONATO VIRTUAL

Com a chegada da covid-19 as pessoas se virem isoladas e o meio de se comunicar ou se conectar de certa forma com outras pessoas, era a internet através de seus smartfones ou computadores, manter-se conectado se tornou essencial para estudar, trabalhar ou se divertir, mas tudo conectado as redes, sem poder sair de casa para ir ao supermercado, ir em lojas ou ir ao trabalho por conta da quarentena. Os lojistas como meio de “salva” seus negócios acharam um meio de empreender seus negócios através das redes sociais, e com apenas um click as pessoas tinha sua compra em casa e com a modificação e facilidade que tudo isso trouxe na internet abriu brecha para o aumento dos crimes digitais.

O estelionato virtual acontece quando o criminoso engana outrem no ambiente virtual, com avanço da tecnologia e os desenvolvimentos dos “smartphones” os estelionatos evoluíram na mesma proporção, é comum que as vítimas sejam enganadas através de e-mails, sites falsos ou redes sociais.

Os hackers como são chamados o indivíduo que pratica essa conduta ilícita, surgiu na década de 60, nos Estados Unidos e geralmente tendem a ter um alto conhecimento tecnológico, induzindo a vítima ao erro. A internet evolui, os fraudadores também se renovam com novas modalidades de golpes, alguns tão específicos que são até difíceis de definir qual a punição correta a ser aplicada (Texeira 2019), os hackers se aproveitam das brechas do mudo virtual para adquirir vantagem patrimonial por meio de falsidade sendo o sujeito ativo dessa modalidade. A legislação brasileira tentou moldar a conduta nos artigos:

> Art. 171 - 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 um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis. (Vide Lei nº 7.209, de 1984)

O crime de estelionato, previsto no artigo 171 do Código Penal, teve alteração. A lei 14.155, de 27 de maio de 2021, acrescentou e alterou alguns parágrafos no supramencionado dispositivo legal. Dentre as mudanças, foram incluídos os §2°-A e B, que tratam da fraude eletrônica:

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
>
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

Na teoria a legislação amparou a tipificação da conduta, tentando no máximo proteger as vítimas, mas na prática a quantidade de crimes virtuais aumentaram, sendo o Brasil uns dos países com mais ataques de crimes virtuais, isso se dá, pois, a dificuldade de identificar os criminosos fica cada vez mais

difícil, conforme dados divulgados pela Fortinet “O Brasil sofreu mais de 3,2 bilhões de tentativas de ataques cibernéticos em 2021. O país lidera o ranking da América Latina, que contabilizou um total de 7 bilhões de tentativas durante o período”.

3.1 PROBLEMÁTICA DA INVESTIGAÇÃO NOS CRIMES CIBERNÉTICOS

Uma das principais dificuldades para a aplicação da legislação no país e a falta de provas, o lapso temporal e profissionais capacitados para combater crime virtuais, pois os criminosos se escondem atras de máquinas e acham forma de burlar os sistemas operacionais para não ser encontrado, como explica SOARES:

> A tecnologia da informática é detentora de grande complexidade e dinamismo sem igual, o que faz com que os órgãos investigativos e judiciários não estejam adequadamente preparados para lidar com esta nova criminalidade e a cada uma de suas repentinas mudanças. Não muito dificilmente serão encontrados agentes públicos sem qualquer conhecimento sobre as tecnologias e das informações necessárias para uma melhor prestação da proteção estatal aos cidadãos nos órgãos responsáveis pela persecução penal. (SOARES 2018)

Em razão disso é necessário que esses profissionais, bem como os órgãos destinados a esse combate, se atualizem, pois, utilizam de ferramentas “vulnerável” para investigação dos crimes, tendo em vista que as principais finalidades no processo de investigação é encontrar o sujeito que raramente é localizado ou descoberto o que muitas das vezes gera impunidade para os infratores como explica Cavalcante.

> Isso porque no caso de crimes de menor potencial ofensivo, como é o exemplo dos crimes contra a honra e crime de invasão de dispositivo informático, existe grande chance de o crime prescrever antes mesmo de entrar em um efetivo processo contra o praticante do crime. Isso ocorre porque as penas previstas para esses crimes são baixas (até dois anos), o que significa que é muito fácil ocorrer prescrição retroativa pela pena aplicada em concreto (CAVALCANTE, 2012).

Os meios de obtenção de provas respaldados pela legislação brasileira são: a análise de Logs e servidores, interceptação de correspondência eletrônica, análise de pacotes de dados, Identificação de sites, reconhecimento facial, captação ambiental, entre outros. A problemática desse cenário é que ao realizar as investigações criminais, é a dificuldade no primeiro momento, de identifica a forma que o crime aconteceu, o local que ocorreu, em segundo momento busca localizar o endereço de IP (número que identifica o dispositivo na rede), após a identificação do IP do infrator, o setor de investigação da polícia entra em contato com a empresa que disponibiliza o número na rede, e só assim identifica o criminoso mas em sua maioria as empresas se negam a fornecer dados e somente com autorização do judicial fornecem o necessário, são dificuldades como essas que possibilitam o aumento significativo desses crimes.

Reforça-se que para combater crimes cibernético a legislação bem como o governo precisa de estratégia para prevenir os delitos, em primeiro lugar a campanhas de conscientização aos internautas, principalmente para crianças e adolescentes, da mesma maneira que a legislação brasileira precisa de atualização para as novas ondas de crimes cibernéticos, criação de delegacias especializadas com mais recurso e estruturas, canais de denúncia e a especialização de profissionais capacitados.

CONCLUSÃO

O artigo apresentado é uma análise dos crimes cibernéticos no Brasil explicando várias espécies, é evidente que os crimes virtuais têm ganhado uma grande proporção atualmente junto a evolução eletrônica e a globalização sendo um fenômeno indispensável atualmente, por sua vez, a internet, é o ícone da globalização e com o tempo se expandiu em todas as partes do mundo, verificamos que todos com acesso à Internet estão expostos e provavelmente poderão se tornar vítima algum dia.

Por todo percurso do artigo foi exposto espécies de crimes virtuais e a maneira em que ocorre, considerável, deve-se destacar que as lacunas deixadas dentro das leis brasileiras contra crimes virtuais dão-se na abertura para que mais crimes dentro dessa área sejam simplesmente cometidos, bem como, a problemática da falta de leis especificas pois os crimes cibernéticos têm ações que não estão tipificados em lei, mas que sabemos que precisa de uma atualização, entretanto, uma legislação adequada não é o suficiente o bastante. Assim como a dificuldade que o judiciário tem para encontrar e localizar os criminosos que se escondem através do anonimato das telas, na qual dificulta aplicar a devida sanção.

Entende-se que de forma positiva, o Código Penal tem sido como base para punir partes dos crimes virtuais ocorridos no Brasil. Porém, apesar deste otimismo a legislação brasileira ainda carece de legislações

Conclui-se que Cibercrimes estão presente no dia a dia das pessoas, de maneira que a sociedade deve se atentar aos cuidados ao acessar site e redes sociais para que tenha suas privacidades e seus bens preservadas,

REFERENCIAL

ABRANET. **Brasil sofreu metade dos ataques hackers direcionados para a América Latina**. Abranet, 2021. Disponível em: https://www.abranet.org.br/Noticias/Brasil-sofreu-metade-dos-ataques-hackers-direcionados-para-a-AmericaLatina3431.html?UserActiveTemplate=site%2Cmobile%252Csite#.YoLUkejMLIU. Acesso em: 09 setem. 2023

CAVALCANTE, Márcio André Lopes. **Primeiros comentários à Lei n.° 12.737/2012, que tipifica a invasão de dispositivo informático**. 2012. Disponível em: http://www.dizerodireito.com.br. Acesso em: 22 setembro 2023

CHAVES, Fábio Barbosa; TEIXEIRA, Filipe Silva. **Os crimes de fraude e estelionato cibernético e a proteção do consumidor no e-commerce**. 2020. Disponível em: <https://conteudojuridico.com.br>. Acesso em: 07 setem. 2023

COLARES, Rodrigo Guimarães. Cybercrimes: **os crimes na era da informática**. 2002. Jus.com.br. Disponível em: https://jus.com.br/artigos/3271/cybercrimes-os-crimes-na-era-da-informatica. Acesso em: 25 maio 2023.

ESCOLA, Equipe Brasil. **"Internet no Brasil**"; Brasil Escola.Disponívelem:https://brasilescola.uol.com.br/informatica/internet-no-brasil.htm. Acesso em 31 de maio de 2023

GIMENES, Emanuel Alberto Sperandio Garcia. **Crimes virtuais. Revista de Doutrina da 4ª Região**, Porto Alegre, n. 55, ago. 2013. Disponível em: <https://revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html> Acesso em: 17 jun 2023

GOMES, Luiz Flavio. **Divulgação de cenas de sexo na internet, envolvendo crianças e adolescentes, é crime?** Revista IOB de Direito Penal e Processo Penal. Porto Alegre, 2008, p. 16 – 17.

JESUS, Damásio de MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016

NUCCI, Guilherme de Souza. **Estatuto de Criança e do Adolescente Comentado**. 4. ed. rev. amp e atual. Rio de Janeiro: Editora Forense, 2018.

DORIGON, Alessandro; SOARES, Renan Vinicius Oliveira**. Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 23, n. 5342, 15 fev. 2018. Disponível em: https://jus.com.br/artigos/63549. Acesso em: 10 set. 2023.

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática**. 2009. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009. Disponível em: Acesso em: 20 jul 2023

REDIVO, Joslaine. **Crimes cibernéticos: no mundo durante a pandemia covid-19 e seus impactos Conteúdo Jurídico**. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/58541/crimes-cibernticos-no-mundo-durante-a-pandemia-covid-19-e-seus-impactos. Acesso em: 22 maio 2023.

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

WENDT, Emerson; JORGE, Higor Vinicius Nogueria. **Crimes Cibernéticos: Ameaças e Procedimentos de Investigação**. 2. ed. Rio de Janeiro: Brasport, 2013. Disponível em: Acesso em: 17 jun 2023.

PUC GOIÁS | Núcleo de **Prática Jurídica**

PONTIFICIA UNIVERSIDADE CATÓLICA DE GOIAS
Pró-Reitoria de Graduação
Escola de Direito, Negócios e Comunicação
Curso de Direito
Núcleo de Prática Jurídica
Coordenação Adjunta de Trabalho de Curso

2

TERMO DE AUTORIZAÇÃO DE PUBLICAÇÃO DE PRODUÇÃO ACADÊMICA

O(A) estudante Bianca Stefany Ribeiro dos Santos
do Curso de Direito, matrícula _____,
telefone: 99320156 4, e-mail bistefany68@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado Crimes cibernéticos no Brasil e estelionato virtual, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JEPG): Som (WAVE, MPEG, AIFF, SNS); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 30 de Agosto de 2023.

Assinatura do(s): autor(es): Bianca Stefany

Nome completo do autor: Bianca Stefany Ribeiro dos Santos

Assinatura do professor- orientador: _____

Nome completo do professor-orientador: _____

PUC GOIÁS | Núcleo de **Prática Jurídica**

PONTIFICIA UNIVERSIDADE CATÓLICA DE GOIAS
Pró-Reitoria de Graduação
Escola de Direito, Negócios e Comunicação
Curso de Direito
Núcleo de Prática Jurídica
Coordenação Adjunta de Trabalho de Curso

2

TERMO DE AUTORIZAÇÃO DE PUBLICAÇÃO DE PRODUÇÃO ACADÊMICA

O(A) estudante Bianca Stefany Ribeiro dos Santos
do Curso de Direito, matrícula _____,
telefone: 99320154, e-mail bistefany68@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado Crimes cibernéticos no Brasil e estelionato virtual, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JEPG): Som (WAVE, MPEG, AIFF, SNS); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 30 de Agosto de 2023.

Assinatura do(s): autor(es): Bianca Stefany
Nome completo do autor: Bianca Stefany Ribeiro dos Santos
Assinatura do professor- orientador: _____
Nome completo do professor-orientador: _____

gov.br Documento assinado digitalmente
GIL CESAR COSTA DE PAULA
Data: 20/09/2023 19:53:33-0300
Verifique em https://validar.iti.gov.br