# CYBER CRIMES IN BRAZIL

**RAFAELA DE ARAÚJO PATRÍCIO**: Graduanda em Direito, Centro Universitário de Santa Fé do Sul – SP, UNIFUNEC

LETICIA LOURENÇO SANGALETO TERRON[1]

(orientadora)

**RESUMO**: Atualmente a internet propicia facilidades no dia a dia do cidadão, a um clique disponibilizando notíciais em tempo real, bem como a possibilidade de resolução de temáticas diárias, ao mesmo tempo em que a inernet proporciona tantos pontos positivos com ela está ligado também os crimes cibernéticos. O objetivo deste artigo é apontar as formas de crimes cibernéticos no Brasil, bem com suas penalidades no judiciário brasileiro, analisando sua eficácia, bem como seus reflexos na sociedade brasileira. A presente pesquisa fundamentou-se na coleta de dados de artigos, periódicos bem como a legislação brasileira aplicável, doutrinas e jurisprudências, afim de embasar a pesquisa.

Palavras-chave: Crimes Cibernéticos. Crimes cibernéticos no Brasil. Lei Carolina Dieckman.

**ABSTRACT:** Currently, the internet provides facilities in the daily life of the citizen, at one click, providing news in real time, as well as the possibility of solving daily issues, at the same time that the internet provides so many positive points with it, it is also linked to cybers crimes . The purpose of this article is to point out the forms of cybers crimes in Brazil, as well as their penalties in the Brazilian judiciary, analyzing their effectiveness, as well as their reflexes in Brazilian society. The present research was based on the collection of data from articles, periodicals as well as the applicable Brazilian legislation, doctrines and jurisprudence, in order to support the research.

Keywords: Cybers Crimes. Cybers crimes in Brazil. Carolina Dieckman Law.

## INTRODUÇÃO

Atualmente o mercado encontra-se globalizado, no qual gera oportunidades de empreendimendos e consumo, porém é necessário cuidados por parte do consumidor, no que diz respeito a transações comerciais.

A tecnologia da informação por meio da internet, smartphones, tablets e

[1] Docente do Centro Universitário de Santa Fé do Sul – SP, UNIFUNEC

notbooks possibilita a realização de transações comerciais, acompanhamento de notícias em tempo real.

O mundo globalizado têm proporcionado cada vez mais comodidade, ao mesmo tempo que deixando sucestível a ações criminosas por meio deste canal, possibilitando aos criminosos cometer delitos variados.

O cibercrime é um conjunto de delitos perpretados utilizando-se de redes informáticas, utlizando-se de computadores, facilitando atividades ilícitas.

A criminologia " é a ciência que estuda os crimes e os criminosos, e, portanto, a criminalidade". Dentro desse contextto, a doutrina condiz que a criminologia refere-se aos atos infracionais cibernéticos perpretados atualmente.

É possível, em delitos cometidos via internet, por meio de identificação do IP da máquina na qual foi utilizado identificar o responsável seja proprietário ou usuário do equipamento.

Por volta dos anor 80, houve um aumento no índice de crimes, tais como manipulações de caixas bancários, pirataria de programas e também pornografia infantil.

Atualmente, o grande desafio do Direito é conceder ao usuário a devida segurança e proteção no que diz respeito as atividades desenvolvidas por meio da internet, possibilitando a redução dos prejuízos material e pisicológicos proporcionados pelos crimes cibernéticos a suas vitímas.

Dentro deste contexto, o objetivo é apontar a utilização do Direito Penal Brasileiro, relacionando as legislações bem como suas atualizações referentes aos crimes cobernéticos como também as políticas para seu combate. Para tanto, é necessário compreender quanto aos objetivos específicos: caracterizar e conceituar o cibercrime; os principais crimes cibernéticos cometidos no Brasil; constatar as leis atuais que amparam a proteção e o tratamento de dados dos usuários; analisar os desafios no combate aos crimes cibernéticos.

Nesta pesquisa será utilizado o método de revisão de literatura com análise qualitativa. Os dados serão colhidos pelo método de levantamento bibliográfico, organizando-os conforme o método dedutivo.

Utilizadas como base de dados foram o Google Scholar, Scielo, artigos, livros e doutrinas com lígua portuguesa.

A Revisão de Literatura consiste em elaborar uma pesquisa obedecendo as normas de formatação exigidadas.

Para Cardoso et al (2010, p. 7) " cada investigador analisa minuciosamente os trabalhos dos investigadores que o precederam e, só então, compreendido o testemunho que lhe foi confiado, parte para a sua própria aventura"

É necessário que o pesquisador possua prazer no tema escolhido, facilitando a pesquisa, sem que cause sofrimento, considerando suas limitações de conhecimento, atentando-se ao tema dentro de sua área de conhecimento.

O levantamento de dados com revisão bibliográfica é a localização e obtenção de documentos afim de analisar a disponibilidade do material que será fundamentado a pesquisa, realizado por meios dos canais supracitados.

A pesquisa destina-se ao emprego da internet para fins de crimes cibernéticos no Brasil entre os anos de 2020 a 2022, bem como o efetivo papel do Direito Penal brasileiro afim de combater tais delitos.

No Capítulo 3.1 será abordado o conceito de crimes virtuais, Já no Capítulo 3.2 será apontado a tipificação dos crimes cibernéticos, bem como são perpretados no Brasil. No Capítulo 3.3 será apontado o índice de crimes cibernéticos no país, no período de 2019 a 2022.

O Capítulo 3.4 destaca a aplicação do Direito PenaL Brasileiro, sua leguislação atual, apontando a necessidade uma melhor efeitividade legislativa afim de sanar as ações criminosas, fundamentando nas doutrinas e legisladores.

## 2 Conceito de Crimes Cibernéticos

Criada em 1969, nos Estados Unidos, chamada de Arpanet, a internet, visando tinha associar laboratórios de pesquisa.

A rede era parte integrante do Departamento de Defesa norte-americano, o mundo passa pelo auge da Guerra Fria. (SILVA, 2001)

A Arpanet era uma comprovação de que permaneceria a comunicação entre militares e cientistas independente de caso de bombardeio. Elementos que funcionavam de maneira independente dos eventuais problemas.

Em meados do ano de 1982, a utilização do Arpatnet tornou-se expressivo no meio acadêmico. (SILVA, 2001)

De ínicio, a utilização era restrita aos EUA, porém expandiu-se para diversos países, tais como: Holanda, Dinamarca e Suécia, sendo então utilizado com o nome de internet. (SILVA, 2001)

Os meios acadêmicos e científicos só possuiram acesso á rede durante quase

duas décadas, sendo liberado somente em 1987 seu uso comercial nos EUA.

Em meados de 1992, surgiram várias empresas que proveram o acesso à rede de internet no país. No mesmo período, criado pelo Laboratório Europeis de Fpisica de Partículas (Cern) a World Wide Web, mais conhecida como "w.w.w", passando a ser utilizada afim de possibilitar acesso a informações a qualquer usuário da internet. Partindo daí, entao, sua difusão da rede de forma global. (SILVA, 2001)

Atualmente, o indice de usuários de internet chegam a 250 milhoes em todo o mundo. Constando que até o fim do ano de 2004, a criclação de e-mails em âmbito mundial chegou em torno de 35 bilhões de mensagens diárias, sendo quase 90% de seus usuários localizam-se me países industrializados. (SILVA, 2001)

Estados Unidos e Canadá representam 57% do total, conforme relatório da Organização Internacional do Trabalho. Sendo liberado no Brasil a exploração para fins comerciários liberadas no ano de 1995. (SILVA, 2001)

Universidades como as federais do Rio Grande do Sul e do Rio de Janeiro estavam conectadas à rede desde 1989.

A Fundação de Amparo à Pesquisa de São Paulo (Fapesp) conectou-se um ano depois. (SILVA, 2001)

Os crimes ciberneticos ou cibercrimes são definidos como todo ato ílicito utilizado por meio de computador ou tecnologia de informação afim de atingir o ato criminoso, sendo estes meios objeto de um crime.

Os cibercrimes assosciam-se ao fenônemo da criminalidade de informações, violando os direitos e garantias fundamentais. (JÚNIOR, 2019)

De forma ampla, a criminilidade cibernética inclui toda e qualquer atividade ilícita perpretada por meio de meios de tecnologia da informação ou computadores.

Para Simas (2014, p.12) "quem que o meio in formático surge como parte integradora do tipo legal, ainda que o bem jurídico protegido não seja digital".

Os delitos realizados via internet recebem diversas denominações tais como: crime digital, crime cibernético, cibercimes, crimes informáticos dentre outros. (JÚNIOR, 2019)

## 3 CASO CAROLA DIECKMAN

No ano de 2012 a atriz Carolina Dieckmann foi vítima de ataque de hackers, no qual teve fotos íntimas vasadas, trinta e seis fotos pessoais da atriz foram publicadas na internet, redes sociais e compartilhadas via Wathsap.

A atriz recebeu ameaças de extorsão, no qual o hacker enviou ao seu empresário duas imagens via e-mail, pedindo a quantia de 10 mil reais para que não fossem divulgadas. (G1, 2012)

De início suspeitaram-se de que as fotos pudessem ter sido copiadas quando o computador da atriz foi levado para conserto.

Logo a polícia localizou e identificou os hackers no interior de Minas Gerais e São Paulo, descartando a suspeita de que os funcionários do estabelecimento que havia sido consertado o computador da atriz pudessem ter copiado as imagens. (G1, 2012)

Em uma entrevista realizada pelo G1 a atriz relata que sua maior preocupação era de que o filho com até então 13 anos, possuisse acesso as fotos na sua ausência, para que pudesse explicar os fatos ao filho. Relatou ainda que estava em São Paulo quando recebeu a notícia por meio de seu empresário acerca do vazamento das fotos. Ao saber, a atriz ligou para su residência pedindo que a internet fosse desconectada até que ela pudesse conversar com seu filho mais velho. "Minha preocupação era só falar para desligar a internet, porque não queria que ele tivesse acesso áquilo" realtou a atriz. (G1, 2012)

Em 13 de maio de 2012, exibido em uma reportagem pelo programa Fantástico, dois dos criminosos foram pegos pela polícia. (SOUZA, 2019)

Conforme a matéria exibida:

> "Carolina Dieckmann procurou a polícia no último dia 7, uma segunda-feira: 36 fotos pessoais da atriz tinham sido publicadas na internet na sexta anterior. Carolina vinha recebendo ameaças de extorsão desde o fim de março, mas disse que não tinha registrado queixa até então para evitar ainda mais exposição. Na delegacia, ela contou que estava tendo problemas nas suas contas em sites de relacionamentos desde o ano passado. Disse que foi a empregada que atendeu o telefonema de um homem que dizia ter fotos dela. Em seguida, o homem mandou duas imagens para o empresário de Carolina e pediu R$ 10 mil para não divulgar. A primeira suspeita da atriz foi de que as fotos pudessem ter sido copiadas – há dois meses - quando o equipamento foi levado para conserto. Técnicos e responsáveis pela loja chegaram a ser ouvidos. Os advogados dela tentaram impedir na Justiça que sites continuassem divulgando as fotos" (G1, 2012d, [s/p]).

Após a repercussão do caso, em 30 de novembro de 2012, foi homolagada a Lei

12.737/2012, no qual dispõe acerca da tipificação criminal de crimes cibernéticos, altera o Decreto-Lei nº 2.848, de 07 de dezembro de 1940-Código Penal; e dá outras providências. (BRASIL, 2012)

O caso da atriz foi apenas mais um de muitos casos ocorridos, porém com grande repercussão dentro da sociedade. A atriz não foi a única mulher a sofrer com a exposição na mídia. Existem muitos casos em que mulheres sofreram o mesmo constrangimento.

### 3.2 Walter Delgatti Netto, o "Vermelho"

Walter Delgati Neto, morador da cidade de Araraquara, conhecido como "Vermelho", ficou conhecido após invadir aplicativos de mensagens de figuras públicas entre elas o até então Ministro da Justiça Sérgio Moro, Detan Dellagnol, de jornalistas e do presidente Jair Bolsonaro.

Quatro pessoas entre eles Walter Delgati Neto foram acusadas de fazer parte de uma quadrilha que realizavam crimes cibernéticos, sendo hackeados em torno de 1.000 autoridades, sendo magistrados das cortes superiores até Rodrigo Maia, presidente da Câmara.

Baseado na Operação Spoofing, o jiz Federal de Brasília Vallisney de Oliveira decretou as prisões executadas pela polícia federal. (OLIVEIRA, 2019)

Na ocasião Walter Delgatti Neto, confessou à polícia federal que repassou o material ao site The Intercept. (OLIVEIRA, 2019)

O conteúdo repercutiu em vários meios de comunicação, revelando diálogos realizados no auge da Operação Lava-Jato, Delgatti afirmou que repassou todo o conteúdo ao referido site de forma anônima, diretamente ao fundador do site, Glenn Grenwald.

Foram rastreados por meio de endereços de IP (número de identificador de computador na Internet) utilizados para invadir o aplicativo de mensagens Telegram, na ocasião os agentes conseguiram identificar os suspeitos. (OLIVEIRA, 2019)

Walter Delgati Neto concedeu uma entrevista à Revista Veja em 12 de Fevereiro de 2021, no qual relata que já foi admirador da investigação, a Operação Lava Jato, e contou que invadiu o Telgram ( aplicativo de mensagens) de Deltan Dallagnol por ter se identificado com o procurador após acompanhar uma palestra em uma universidade na cidade de Ribeirão Prwto, que até então "o Vermelho" era estudante do curso de Direito, o objetivo era se informar acerca das investigações já mencionadas, porém ao acessar a conta Walter constatou que o referido procurador não deletava nenhum de seus arquivos.(FARAH, 2021)

O hacker afirma ainda: *" Eu era um fã. Mas, assim que entendi a manipulação deles, eu me senti enganado. Vi que a Lava-Jato era mais política do que jurídica."* (FARAH, 2021)

## 4. CRIMES CONTRA MOEDAS VIRTUAIS

As criptomoedas são moedas digitais, que pode circular sem a necessidade de uma autoridade monetária central, é uma espécie de dinheiro, criadas por técnicas de criptografias que possibilitam as transações comerciais atualmente, por meio digital.

Diante desse conceito, as principais criptomoedas são a Bitcoin, Ethereum e o Litecoin, nas quais utilizam-se da tecnologia Blockhain, na qual mantém registro inviolável de suas transações. (EXAME, 2022)

O Bitcoin, é uma das criptomoedas mais utilizadas em transações, este tipo de moeda digital é criada por meio de códigos de computador, garantidas com criptografia avançada, mantida por uma rede globalizada, no qual qualquer um pode ser integrante deste banco. (EGEWARTH, 2020)

Essas moedas digitais podem ser utilizadas como meios de segurança e privacidade ao realizar transações. Porém, torna-se um atrativo aos cibercriminosos, visto que os hackers invadem os computadores, exigindo pagamentos em troca de informações adquiridas ilegalmente dos computadores das vítmas, sendo o meio de pagamento por meio da moeda virtual "Bitcoin". (EGEWARTH, 2020)

Em 12 de maio de 2017, ocorreu grande ataque de hackers, que invadiram computadores de mais de cem países, acarretando prejuízos bilionários aos atingidos pelo ataque.

No Brasil foram quatorze estados incluindo o Distrito Federal que registraram ataques cibernéticos a empresas e órgãos públicos.(PRESSE, 2017)

Após a invasão os hackers solicitaram o pgamento de uma quantia de 300 e 600 milhões de dólares em Bitcoins por meio de um computador infectado.

Conforma o BitcoindBrasul (2017) entende-se por bitcoins:

> "uma tecnologia digital que permite reproduzir em pagamentos eletrônicos a eficiência dos pagamentos com cédulas. Pagamentos com bitcoins são rápidos, baratos e sem intermediários. Além disso, eles podem ser feitos qualquer pessoa, que esteja em qualquer lugar do planeta, sem limite mínimo ou máximo de valor" (BITCOINDBRASIL, 2017, p. 1).

Virus de resgate são utilizados para embralhar arquivos existentes no computador alvo utilizando de uma chave criptografada, no qual os criminosos exigem pagamentos de suas vítimas afim de receber essa chave retomando os arquivos originais. (PRESSE, 2017)

Assim os hackers, utilizando-se desta tecnologia, encontraram maneiras de receber valores em forma de moeda virtual de vítimas que tiveram seus computadores infectados, não sendo possível rastrear contas bancárias.(BERTOLUCCI, 2022)

Outro golpe envolvendo a mineração Bitcoin, é utilizado por PIX, no qual promete lucros elevados, sendo divulgado até por via Instagran, o que chama atenção é que os perfis divulgadores são perfis que já foram alvos de hackers em rede social.

O golpe é utilizado os perfis do Instagram publicando nos stories destes perfis, prometendo dobrar o dinheiro das vítimas, sendo como meio de interção contas hackeadas afim de mostrar o sucesso de tal operação que gera altos rendimentos. (BERTOLUCCI, 2022) Em uma matéria realizada peo site Yahoo!esportes expôs por meio de prints como acontece este tipo de golpe, conforme as imagens a seguir.

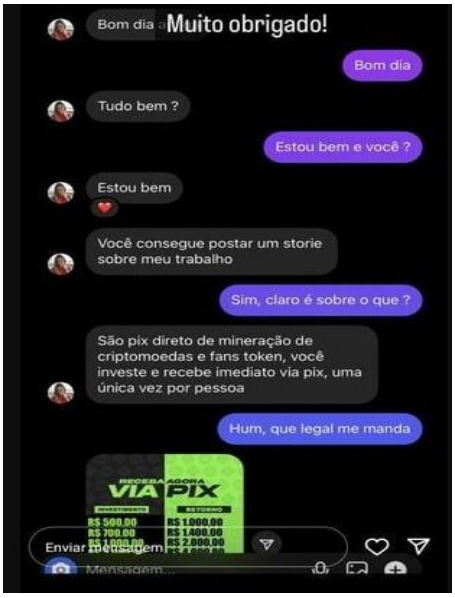


Figura 1 Golpista conversa com conta hackeada

Fonte: Yahoo!esportes

## 4.1 Aplicação Penal Quanto aos Crimes Cibernéticos

É sabido que toda e qualquer sociedade necessita de normas e legislações afim de manter a ordem social, devendo haver para cada tipo de delito uma legislação afim de impor as sanções penais. Dessa forma, os cibercrimes são divididos em crimes virtuais mistos, puros e comuns. (AURÉLIO, 1995)

Para Aurélio (1995) os crimes cibernéticos puros são: *"Toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas"*

Nesse sentido, os crimes puros observa-se ações dos criminosos na internet, utilizando-se de conhecimento sobre a informática para cometer crimes contra os usuários comuns.

Já os crimes virtuais mistos são delitos coemtidos por meio de ações perpretadas por um indivíduo que possui acesso a informações do meio jurídico, protegidas pela internet, porém este tipo de delito é utilizado o computador afim de obter vantagem para a efetivação do crime.

Aurélio (1995) explica acerta da denominação de misto:

> "Incidiram normas da lei penal comum e normas da lei penal de informática. Da lei comum, por exemplo, pode-se aplicar o artigo 171 do Código Penal combinado com norma de mau uso de equipamento e meio de informática. Por isso não seria um delito comum apenas, incidiria a norma penal de informática, teríamos claramente o concurso de normas (AURÉLIO, 1995)."

Assim, os crimes virtuais mistos estão previstos no ordenamento jurídico brasileiro, possibilitando a punição na legislação penal comum como também na legislação especial.

A doutrina penal brasileira prevê pena de detenção de 3 (três) meses a 1 (um) ano e multa. Ainda, a Lei supracitada expressa que a pena perpreta ao agente que produz, oeferta, distribui, comercializa ou divulga conteúdo, dispositivos ou programas de computadores visando a prática delituosa; caso resulte em prejuízo econômico; ou resulte na invasão a obtenção de conteúdo, sendo a pena de reclusão de 6 (seis) meses a 2 (dois) anos e multa. Em casos de delitos criminosos graves, a pena pode ser aumentada em casos contra a Administração Pública Minicipal, Estadua ou Federal. (JÚNIOR, 2019)

A Lei nº 12.737/12, mais conhecida como "Lei Carolina Dieckmann", visto que a atriz brasileira foi vítima de crime cibernético ao ter seu computador invadido, sendo divulgado imagens e utlizando-se como forma de extorsão, tal dispositivo legal prevê:

> "Art. 154-A Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou

> tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
>
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4º Na hipótese do § 3ºaumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos;
>
> II - Presidente do Supremo Tribunal Federal;
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal". (BRASIL, LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.)

Porém a Lei supracitada ainda é alvo de discussão no meio jurídico, visto que embora tipifique os crimes cibernéticos, Nascimento (2019, p.16) afimar que: "não tenha conseguido prever todos os possíveis delitos e também ser tecnicamente frágil".

A lacuna da referida legislação está especificação do tipo penal acrescido no Código Penal em seu artigo 154-A supracitado.

Diante de tal contexto, os demais crimes cibernéticos são julgados fundamentados nos efeitos dos danos causados.

## 5 DISCUSSÕES

No Brasil, houve um aumento dos crimes cibernéticos durante a pandemia, no ano de 2020, foram regsitrados 156.692 casos regisrados por meio de denúncias anônimas, conforme dados apontados pela Central Nacionals de Denúncias de Crimes Cibernéticos. (GARRETT, 2021)

Em maio de 2022 um levantamento realizado pela CNESG (Confederação Nacional das Seguradoras) apontou um aumento pela procura por seguros cibernéticos de 41,5%, nos três primeiros meses do ano de 2022, comparando-se ao mesmo período de 2021.

Ainda o referido estudo, demonstram os gastos que as empresas brasileiras obtiveram apromadamente a R$ 34,5 milhões de reais em seguros contra ataques cibernéticos, em março as seguradoras chegaram a arrecadar R$ 13 milhões.

O presidente da CNSEG Dyogo Oliveira afirma que: "Ainda teremos um crescimento grande do setor. Os ataques cibernéticos têm sido cada vez mais frequentes e a proteção oferecida pelo seguro é uma tranquilidade a mais para as empresas evitarem maiores prejuízos."

A Lei nº 12.737, de 30 de novembro de 2012, dispõe acerca da tipificação criminal dos crimes cibrnéticos, altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, do CP (Código Penal):

> " 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 vunerabilidades para obter vantagem "ilícita". (BRASIL, 2012, s.p.)"

Atualmente a internet é um dos meios mais utilizados por criminosos, afim de violar dados pessoais, utilizndo-se de diversos meios para usurpar os direitos e garantias fundamentais de suas vitimas.

Para Lima Xavier (2015) é um dos fatores que dificulta o Estado em aplicar a sanção adequada.

Brookshear (2013) afirma que:

> " Com o avanço da tecnologia, conectar-se à rede mundial de

> computadores ficou cada vez mais acessível, ainda mais com a popularização dos smatphones, aparelhos celulares, que possuem recursos que possibilitam tal acesso, ou seja, "o que há pouco era meramente um telefone evoluiu para um pequeno computador de propósito geral que acabe na palma da mão" Os celulares evoluíra a tal ponto que além de sereme utilizados com a finalidade de possibilitarem a comunicação via telefone móvel, eles equiparam-se a pequenos computadores, repletos de aplicativos que possuem uma diversidade de funções." (BROOKSHEAR, 2013, p.10)

A supracitada, ficou conhecida com o nome da referida atriz em razão de grande repercussão social, dentro do dispositivo legal abordaram-se elementos que visam elucidar as principais dúvidas.

Atualmente os principais crimes cibernéticos perpretados estão relacionados á transações comerciais, crimes contra a pessoa tais como: difamação, calúnia, divulgação de dados pessoais e imagens íntimas, violações de informações, crimes contra o patrimônio, pedofilia dentre outros.

## 6 CONCLUSÃO

A evolução da internet e da utilização das mídias sociais foi um dos maiores avanços tecnológicos nas últimas décadas, proporcionando facildades a um clique.

Porém, com tantos avanços tecnológicos, trouxe consigo a evolução de delitos por meio da internet e mídias sociais, gerando vários tipos de crimes perpretados por estes meios.

Diante de tal exposto, tornou-se primordial a elaboração de lei  a respeito da tipificação criminal de crimes cibernéticos, afim de conter e prevenir tais delitos.

De tal forma, a Lei nº 12.737/12, apontada e analisada dentro desta pesquisa, trouxe a tipificação do crime de invasão de dispositivos informáticos.

A legislação brasilira atual ainda é suficiente quanto sua punição e combate aos crimes cibernéticos. Todavia, é necessário um apoio melhor policial quanto políticas públicas que incentivem a proteção do Estado, o que ainda deixa muito a desejar neste quesito, fator que dificulta o combate a estes tipos de crimes.

Diante de tal pesquisa conclui-se que a  Lei "Carolina Dieckmann" é um grande início para combater os crimes cibernéticos, porém ainda há muito a que se melhorar no que diz respeito a estruturação dos órgãos competentes, para que possam realizar de forma eficaz as investigações e as punições cabíveis.

## REFERÊNCIAS


BERTOLUCCI, Gustavo. Golpe da mineração de Bitcoin com PIX no Instagram é nova moda dehackers. Publicado em 24 de junho de 2022. Disponível em: https://esportes.yahoo.com/golpe-da-minera%C3%A7%C3%A3o-bitcoin-com-120619454.html. Acesso em 13 de setmbro de 2022.

BITCOINDBRASIL. O que é Bitcoind? 2017. Disponível em: <https://www.bitcoinbrasil.com.br/o-que-e-bitcoin/>. Acesso em 13 de setmbro de 2022.

BRASIL. **Lei n. 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 – Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 – Código Penal Militar, e a Lei n. 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistemas eletrônicos, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outas providências**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em 19 ago. 2022.

BRASIL. **Lei n. 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 19 ago. 2022.

BRASIL. Lei n. 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. Brasília, DF, [2012]. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato20112014/2012/Lei/L1273.htm. Acesso em 05 de setembro de 2022.

BROOKSHEAR, J. Glenn. **Ciência da Computação: Uma visão abrangente**. Porto Alegre:
Bookman, 2013 http://www.revistajrg.com/index.php/jrg/article/view/122/201

CARDOSO, T., Alarcão, I. & Celorico, J. (2010). **Revisão da literatura e sistematização do conhecimento**. Porto: Porto Editora.

EGEWARTH, Arthur Bernardo. **Os crimes cibernéticos e a ineficácia da lei "Carolina Dieckmann"**. Publicado em 06 fev. 2020. Disponível em: http://bibliodigital.unijui.edu.br:8080/xmlui/handle/123456789/6497. Acesso em 15 de agosto de 2022.

EXAME, Solutions. Criptomoedas: o que são e como começar a investir?. Publicado em 06 de junho de 2022. Disponível em: https://exame.com/conta-em-dia/planejar/criptomoedas-comecar-investir/. Acesso em 12 setem. 2022

FARAH, Tatiana.**Eu era fã da Lava-Jato", diz hacker que vazou mensagens de Moro. Publicado em 12 fev. 2021. Disponível em: https://veja.abril.com.br/politica/eu-era-fa-da-lava-jato-diz-hacker-que-vazou-mensagens-de-moro/. Acesso em 11 de set. 2022.**

G1. Polícia encontra hackers que roubaram fotos de Carolina Dieckmann. Disponível em: http://g1.globo.com/fantastico/noticia/2012/05/policia-encontra-hackers-que-roubaram-
fotos-de-carolina-dieckmann.html. 2012d. Acesso em 02 setembro de 2022.

G1.**Carolina Dieckmann fala pela 1ª vez sobre fotos e diz que espera 'justiça'**. Publicado em 14 de maio de 2012. São Paulo. Disponível em: https://g1.globo.com/pop-arte/noticia/2012/05/carolina-dieckmann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html. Acesso em 01 de setembro de 2022.

GARRETT, Filipe. **Crimes Cibernéticos: entenda o que são e como denunciar**. Disponível em: https://www.techtudo.com.br/noticias/2021/08/crimes-ciberneticos-entenda-o-que-sao-e-como-denunciar.ghtml. Publicado em 9 ago. 2021. Acesso em 20 ago. 2022.

GONÇALVES, Jonas Rodrigoi. **COMO FAZER UM PROJETO DE PESQUISADE UM ARTIGO DE REVISÃO DE LITERATURA**. Revista JRG de Estudos Acadêmicos -Ano II (2019), volume II, n.5(ago./dez.) -, ISSN: 2595-1661. Disponível em: http://revistajrg.com/index.php/jrg/article/view/121/199. Acesso em 18 ago. 2022.

JANONE, Lucas. **Procura por seguros cibernéticos cresce mais de 40% no 1º trimestre, diz pesquisa.** Publicado em 26 maio de 2022. Disponível em: https://www.cnnbrasil.com.br/business/procura-por-seguros-ciberneticos-cresce-mais-de-40-no-1o-trimestre-diz-pesquisa/. Acesso em 20 ago. 2022.

JÚNIOR, Júlio César Alexandre. **CIBERCRIME: UM ESTUDO ACERCA DO CONCEITO DE CRIMES INFORMÁTICOS**. Revista Eletrônica da Faculdade de Direito de Franca. ISSN 1983-4225 – v.14, n.1, jun. 2019. Disponível em: http://revista.direitofranca.br/index.php/refdf/article/view/602. Acesso em 19 ago. 2022.

OLIVEIRA, Joana. **Prisão dos "hackers", o que se sabe até agora e as perguntas sem resposta. São Paulo. Publicado em 25 julh. 2019. Disponível em: https://brasil.elpais.com/brasil/2019/07/25/politica/1564057812_794353.html. Acesso em 11 setem.2022**

PASINATO, D. C. de A. **A tecnologia da informação na investigação policial**. 2017. Disponível em: <http://www.arcos.org.br/artigos/a-tecnologia-da-informacao-na-investigacao-policial/>. Acesso em: 16 ago. de 2022.

PEIXOTO, A. **Criminologia**. 4ª ed. – São Paulo: Saraiva, 1953.

PRESSE, F. Ataque de hackers 'sem precedentes' provoca alerta no mundo. 2017. In: G1.
Portal de Notícias. Disponível em: http://g1.globo.com/tecnologia/noticia/ataque-de-hackers-sem-precedentes-provoca-alerta-no-mundo.ghtml. Acesso em 13 de setmbro 2022.

SILVA, J. L; MASCARENHAS, S. A. N. Gestão de bullying e cyberbullying na universidade – Desafio para a orientação educativa e convivência social e ética no ensino superior – Estudo com estudantes da UFAM (Brasil. Revista Amazônica). 2010. Disponível em: < http://encurtador.com.br/sCMQ3>. Acesso em: 16 ago. 2022.

SILVA, Leonardo Werner. **Rede foi criada em 1969, nos EUA. Folha de SãoPaulo Cotidiano. S**ão Paulo, domingo, 12 de agosto de 2001. Disponível em: https://www1.folha.uol.com.br/fsp/cotidian/ff1208200103.htm. Acesso em 31 de ago. 2022

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

SOUZA. Adílio Junior.A Lei Carolina Dieckmann analisada sob o prisma da Análise do Discurso. d on Line Rev. Mult. Psic. V.13, N. 45. p. 204-226, 2019 - ISSN 1981-1179. Disponível em: https://idonline.emnuvens.com.br/id/article/view/1700/2499. Acesso em 10 de stemb. 2022.