FACULDADES INTEGRADAS RUI BARBOSA-FIRB

LEONARDO BORELLI LEANDRO

CRIMES DIGITAIS

ANDRADINA – SP

JUNHO/2023

LEONARDO BORELLI LEANDRO

CRIMES DIGITAIS

Trabalho de Conclusão de Curso apresentado nas Faculdades Integradas Rui Barbosa – FIRB, sob orientação da Professora Esp. Ana Paula Biagi Terra, como requisito parcial para obtenção do título de bacharel em Direito.

ANDRADINA – SP
JUNHO/2023

LEONARDO BORELLI LEANDRO

CRIMES DIGITAIS

Trabalho de Conclusão de Curso apresentado à banca examinadora como requisito parcial para obtenção do Bacharelado em Direito nas Faculdades Integradas Rui Barbosa – FIRB. Defendido e aprovado em ___ de _____ de 2023 pela banca examinadora constituída por:

Prof(a). Esp. Ana Paula Biagi Terra (orientadora)
Instituição: Faculdades Integradas Rui Barbosa - FIRB

Prof(a). MSc. _____
Instituição: Faculdades Integradas Rui Barbosa - FIRB

Prof(a). MSc. _____
Instituição: Faculdades Integradas Rui Barbosa – FIRB

NOTA: ( ) Aprovado ( ) Reprovado

Andradina, ___ de _____

Dedicatória

Aos meus familiares, com gratidão.

AGRADECIMENTOS

Agradeço primeiramente a Jesus Cristo, pois sem ele nada conseguiria.

Agradeço também a minha família, meu pai, minha mãe e meus irmãos que foi minha base e meu pilar fundamental sempre incentivando e apoiando para todos os meus objetivos.

Agradeço aos meus colegas por todas amizades desenvolvidas, lições, ensinamentos e apoio, que levarão comigo até o fim.

Agradeço aos meus professores e mestres no decorrer deste tempo, pela oportunidade de aprender sobre o direito.

Agradeço a minha Orientadora professora Ana Paula Biagi por toda compreensão e ensinamento que teve comigo, sem dúvidas foi muito fundamental para esse encerramento.

É com muito prazer e gratificante ter conseguindo encerrar mais uma etapa da minha vida, o qual foram cincos anos de muito estudo, investimento, dificuldades, porém graças a Deus com o apoio de todos os mencionados foi concluído.

Essas são minhas palavras apenas gratidão, gratidão por tudo e todos.

RESUMO

BORELLI LEANDRO, L. **Crimes Digitais.** Trabalho de Conclusão de Curso (Graduação em Direito). Faculdades Integradas Rui Barbosa – FIRB, 2023.

O presente trabalho propõe um esclarecimento entre os crimes virtuais e a legislação atual vigente. O trabalho tem por objetivo demonstrar com o avanço dos crimes cibernéticos houve um acompanhamento correto da lei brasileira, bem como os reflexos na sociedade desse delito. Logo depois de uma análise da evolução histórica penal, do conceito dos crimes digitais, das espécies de crimes e suas legislações vigentes foi evidenciado que a legislação brasileira conseguiu acompanhar até certo ponto, tendo carências que precisam de melhorias. Ainda sim explanou os diversos reflexos dos crimes digitais causados a sociedade e suas normatizações. O presente estudo foi formulado metodologicamente por meio da pesquisa bibliográfica com abordagem dedutivo-qualitativa, sendo debatido e analisado por meio de leis, doutrinas, jurisprudências, como também notícias de jornais on-line e dados estatísticos. Após a criação de todos os quatros capítulos deste trabalho é concluído a potencialidade que um delito digital pode causar na vida de pessoas, bem como as leis brasileiras conseguiram andarem similarmente com o avanço ciber criminal até um ponto, precisando de aperfeiçoamento e pessoas capazes de executá-las. Assim a contribuição desse estudo não é só para quem tem o interesse em entender o mundo criminal virtual jurídico, acadêmicos, mas bem como todas as pessoas que estão de alguma forma conectada e utilizam da internet.

Palavras-chave: Crimes. Digitais. Leis. Reflexos

ABSTRACT

BORELLI LEANDRO, L. **Crimes Digitais.** Trabalho de Conclusão de Curso (Graduação em Direito). Faculdades Integradas Rui Barbosa – FIRB, 2023.

This paper proposes a clarification between cybercrimes and the current legislation in force. The work aims to demonstrate that with the advance of cybercrime there was a correct monitoring of the Brazilian law, as well as the consequences of this crime on society. Soon after an analysis of the penal historical evolution, the concept of digital crimes, the species of crimes and their current legislation, it was evidenced that the Brazilian legislation has been able to follow up to a certain point, having deficiencies that need improvement. Still, it explained the several consequences of digital crimes caused to society and their regulations. The present study was methodologically formulated by means of bibliographic research with a deductive-qualitative approach, being debated and analyzed by means of laws, doctrines, jurisprudence, as well as online newspaper news and statistical data. After the creation of all four chapters of this work, the potentiality that a digital crime can cause in people's lives is concluded, as well as the fact that Brazilian laws have managed to walk similarly with the cyber criminal advance to a point, needing improvement and people capable of executing them. Thus, the contribution of this study is not only for those who are interested in understanding the virtual criminal legal world, academics, but also for all people who are somehow connected to and use the internet.

Keyword: Crimes. Digital. Laws. Reflexes

SUMÁRIO

1 INTRODUÇÃO

Crimes Digitais podem ser considerados toda atividade lesiva cometidos no espaço cibernético, mas propriamente dito como delitos na internet, em que visa à danificação de um computador em si ou utiliza como instrumento para a ação criminosa já configurada na norma penal.

As formas mais conhecidas popularmente para esse tipo penal consistem na prática, clonagens de cartões de créditos, links falsos para fraudar dados e dinheiro, fake News e até a invasão de sistemas operacionais para danificações.

Em paralelo a isso no Brasil têm-se normas penais que surgiram com o decorrer da evolução da sociedade, tecnologia e do avanço dos crimes virtuais, como a lei da Carolina Dieckmann, n° 12.737/2012, Marco Civil da Internet, LGPD (Lei Geral de Proteção de Dados Pessoais) e Lei n °14.155 de 2021. Embora a criação dessas normas, ainda sim continua aumentando-se os crimes digitais, mostrando uma lacuna quanto a esse crime.

Dessa forma este estudo propõe a responder, com o avanço dos crimes cibernéticos houve um acompanhamento correto da lei? E quais os reflexos na sociedade desse delito?

O objetivo geral do presente estudo é analisar se com o avanço dos crimes cibernéticos houve um acompanhamento correto da lei brasileira, bem como os reflexos na sociedade desse delito.

Especificamente, os objetivos serão: Conceituar os crimes Digitais, desde a evolução histórica penal até a reflexão desse crime no cenário brasileiro.

Verificar quais tipos de crimes digitais.

Examinar não só as legislações vigentes, como também o avanço das infrações cibernéticas, identificando autores e sua punição.

É de grande valia os esclarecimentos a respeito da criminalidade virtual para a sociedade, tendo em vista que atualmente a internet é “terra sem lei", pois pessoas se escondem através dela para pensamentos e xingamentos ofensivos, causando injúrias e difamação, atentando contra a dignidade humana, honra privacidade e muitas vezes sem nenhuma punição. Igualmente, é correto afirmar a velocidade com que se propaga uma foto, um arquivo, dados pessoais, uma notícia, que quando é de caráter privado, pode trazer danos irreparáveis à vítima, não só financeiro, mas

como, emocional físico e moral. Por isso é de interesse social, em virtude que hoje o meio virtual rege a vida das pessoas e é como no mundo físico, ninguém está totalmente seguro,

Cientificamente, a pesquisa é de suma importância na medida em que será analisada a criminalidade cibernética sob as normas legais vigentes, bem como os impactos da atual legislação para aqueles que venham a querer, futuramente estudar os crimes digitais, podendo ser utilizado os resultados para estudos futuros.

Assim, o aspecto jurídico é o fator mais contundente deste estudo, visto que a abordagem do assunto permitirá aos profissionais do direito realizarem uma análise acerca do tema envolvendo os meios eletrônicos, sua utilização, crimes, cuidados neste ambiente, a honra, privacidade e a dignidade da pessoa humana, pois hoje todo mundo é dependente desse meio virtual, ainda mais na área jurídica.

Para alcançar os resultados pretendidos, o estudo será perseguido por meio da pesquisa bibliográfica com abordagem dedutivo-qualitativa, de modo que será debatida através do texto penal e da análise doutrinária, bem como notícias de jornais on-line e dados estatísticos.

2 EVOLUÇÃO DA HISTÓRIA PENAL

Desde os primórdios, as regras de convivência já eram violadas, tendo em vista que a natureza do homem sempre foi má, embora o propósito de Deus não fosse esse, como na criação do mundo no livro de Gênesis encontrado na Bíblia Sagrada, em que o homem violou uma ordem de Deus, no qual era proibido comer do fruto da árvore do conhecimento do bem e do mal.

Logo então, iniciou a primeira perspectiva do direito penal, sendo a punição de expulsão do casal do jardim do Éden. Após isso o homem não parou mais de cometer crimes contra seu próximo até nos dias de hoje. (GRECO, 2023).

O significado de pena deriva tanto do latim quanto do grego, sendo *“poena”* de castigo e punição e *“poine”* de um significado de pureza, de limpar uma transgressão ou crime pela pena. Já para o doutrinador Fernando Capez (2022, p. 191) entende-se pena com uma “Sanção penal de caráter aflitivo...”.

Assim o Direito penal desde o início tem-se por objetivo de controlar a sociedade para que viva em harmonia, punindo determinados infratores pela prática delituosa, mesmo que no início de tudo isso não era transcrito, não tinha um código definido. Nesse sentido podemos afirmar que se tem a primeira fase de um direito penal, que é o Direito penal primitivo, que continha um emocionalismo e misticismo das pessoas, acreditando em Deuses, ou seja, todos os eventos naturalísticos prejudiciais que aconteciam, entendia que era uma forma de uma comunicação divina com eles, corrigindo pelos seus atos, mais propriamente pecado.

Conforme a evolução da sociedade o direito penal não ficou para trás, chegando à fase das Vinganças. A primeira fase da vingança é conhecida como Vingança Privada, embora tenha uma corrente minoritária que classifica como segunda fase.

Na Vingança privada caso alguém cometesse algum mal ou prejuízo ao seu próximo o mesmo tinha o direito de devolver este mal, sendo que poderia ser qualquer tipo de ação, causando então uma disparidade, assim sendo uma forma punição (retribuição) pelo cometimento do delito, como por exemplo, a pessoa quebra a casa do vizinho, o vizinho poderia retribuir este mal da forma que ele bem entendesse. É de boa valia ressaltar que a vingança poderia ser praticada pela

pessoa ofendida (vítima), família e também pelo grupo em que ela se encaixava e tinha convívio.

Desse modo a Vingança privada teve um caráter fundamental, pois a partir dessa desproporção, surgiu uma necessidade de proporcionalidade, visto que a pessoa tinha que devolver na mesma medida e não conforme sua concepção, nascendo então os primeiros traços do princípio da proporcionalidade, em que na época era a Lei de Talião – “olho por olho, dente por dente”. Esse entendimento pode ser confirmado pelo professor Greco (2023, p. 16) que diz:

> A Lei de Talião pode ser considerada um avanço em virtude do momento em que foi editada. Isso porque, mesmo que de forma incipiente, já trazia em si uma noção, ainda que superficial, do conceito de proporcionalidade. O “olho por olho” e o “dente por dente” traduziam um conceito de Justiça, embora ainda atrelada à vingança privada.

Após isso, entra-se na segunda fase da vingança, a Vingança Divina, no qual foi uma das épocas que mais cometeram crimes bárbaros, tendo em vista que acreditavam que a prática de um crime era uma ofensa aos seus deuses, podendo gerar ira deles e por isso mereciam o castigo, como forma de limpá-los pela transgressão cometida.

Outro ponto importante é que a pena era aplicada pelos sacerdotes, pois tinha o contato direto com os divinos.

Essa época ficou marcada pelo misticismo, como no caso dos fenômenos naturais que acontecia, a população da época entendia que tempestades, surgimento de pragas e entre outros era pela falta omissão da punição a alguém que trouxe este mal e assim o castigo era aplicado a todo mundo grupo (GONÇALVES, 2022).

Nessa linha, a segunda vingança é considerada um direito religioso, marcado pelo código de Manu, conforme o ensinamento de Noronha, que diz :

> É o direito penal religioso, teocrático e sacerdotal. Um dos principais Códigos é o da Índia, de Manu (Mânava, Dharma, Sastra). Tinha por escopo a purificação da alma do criminoso, através do castigo, para que pudesse alcançar a bem-aventurança. Dividia a sociedade em castas: brâmanes, guerreiros, comerciantes e lavradores. Era a dos brâmanes a mais elevada; a última, a dos sudras, que nada valiam.”
>
> Revestido de caráter religioso era também o de Hamurabi. Aliás, podemos dizer que esse era o espírito dominante nas leis dos povos do Oriente antigo. Além da Babilônia, Índia e Israel, o Egito, a Pérsia, a China etc”. (NORONHA, 2004, apud GRECO, 2023, p.17)

A última fase das vinganças é classificada como vingança pública, no qual o poder de punir sai das mãos da igreja e vai para o Estado sendo o detentor do *jus puniendi (direito* do estado de punir).

O Estado como detentor do direito de punir, utiliza a pena como meio de proteção a ele, haja vista que o mesmo era soberano. Assim embora no primeiro momento passe a ter uma ideia de que teria uma redução de punições, castigos severos e que seriam de forma justas em virtude que o Estado assumiu para si a responsabilidade de punição, é totalmente equivocada, visto que o poder está nas mãos do Estado soberano que era governado pelo o rei, o qual utiliza da maneira que bem entendesse, punindo de formas desumanas, como pena de morte, mutilação e entre outras.

A terceira vingança ainda sofre resquícios da vingança divina, visto que as leis severas começam a prevalecer para que tenha controle da sociedade, fazendo com que a sociedade sofra mortes desumanas, por mutilações e outros tipos. (MESTIERE, 1999, p.26, apud GRECO, 2023, p.18).

No decorrer da evolução do direito penal temos o Direito Penal de Roma e da Grécia antiga como importante processo na evolução, tendo em vista que o Romano trouxe consigo o primeiro código romano escrito, que no caso era a Lei das doze Tábuas, tendo sido criado por Gaius Terentillius, que continha sobre propriedade, poder pátrio, sucessão e tutela, delitos, organização e procedimento judicial e entre outros. Em relação ao Direito da Grécia Antiga sua evolução na norma penal versa sobre a pena sair de caráter religioso e começar a ter uma base moral e civil, como diz Rogério Greco (2023, p.18) “Após passar pelos períodos da vingança privada e da vingança divina, numa terceira época, denominada “histórica”, a pena deixou de se assentar sobre fundamento religioso, passando a ter uma base moral e civil,...”

Assim o Direito Penal foi evoluindo pouco a pouco, em que chega numa fase no qual o povo já estava exausto de sofrer pelo poder absolutista, em que aplicavam penas meramente de interesse próprio, cruéis e desumanas, desse modo começando as reivindicações e exigências de seus direitos, marcando então, com a época que mudou o direito penal, sendo o período Humanista.

Nesse período tem-se três grandes marcos, sendo o Iluminismo, Cesare Bonesana (Marquês de Beccaria) e a Revolução Francesa.

O Iluminismo foi um importante movimento europeu entre meados do século XVII e XVIII, o qual pensadores iluministas contribuíram de forma significativa no que concerne nas punições dessumas aplicadas pelo o Estado, visto que a pena se baseava em um aspecto de aflição, no corpo do homem, ou seja, toda prática do homem que não fosse de acordo com o Estado pensava, era morte, tortura e outros meios de sofrimento físico e psicológico, sem necessidade de provas. Assim o Iluminismo traz consigo uma mudança, baseado na razão, uma mudança de pensamento, em que necessariamente precisava de provas para condenação do indivíduo e não mais somente no descontento do Estado, fazendo o homem sair de uma esfera como imprestável, conforme explica doutrinador Greco (2023, p.22):

> O período iluminista teve importância fundamental no pensamento punitivo, uma vez que, com o apoio na “razão”, o que outrora era praticado despoticamente, agora, necessitava de provas para ser realizado. Não somente o processo penal foi modificado, com a exigência de provas que pudessem conduzir à condenação do acusado, mas, e sobretudo, as penas que poderiam ser impostas. O ser humano passou a ser encarado como tal, e não mais como mero objeto, sobre o qual recaía a fúria do Estado, muitas vezes sem razão ou fundamento suficiente para a punição.

Nesse sentido em 1764 baseando nas ideias iluministas foi publicada a obra que mudou a história do Direito Penal, que foi a obra de Cesare Bonesana, Mârques de Beccaria que nasceu em Milão na Itália, conhecida como dos delitos e das penas.

Essa obra trazia a finalidade do direito penal, para que necessariamente servia, por que aplicar uma pena, qual objetivo de uma pena. Ainda sim também mostrou as injustiças do sistema, que trazia consigo métodos bárbaros, os abusos praticados pelos que detinha o poder, a desigualdade com aqueles que tinham menos recursos, diferente daqueles que tinha poder, revelando em sua obra o sentimento do povo, parecendo com os dias atuais.

Dessa forma sua obra teve grande sucesso, sendo um impacto contra o sistema que era instituído na época, consagrando se assim princípios de suma relevância que até hoje são utilizados, como princípio da legalidade (ninguém pode ser preso se não tiver lei) presunção de inocência (enquanto não for comprovada sua culpa, é inocente, ninguém pode ser condenado sem uma sentença, tem que ter provas), dignidade da pessoa humana e também a teoria do pacto social, também relata sobe a obscuridade da lei, pena de morte, o qual era visto de maneira repulsiva, pois se nem as pessoas podem tirar sua vida, por que o estado poderia

tirar assim as penas teriam que ser preventivas e não aflitivas, evitando novo cometimento de delitos. Por causa disso sua obra mudou a forma como era vista o ser humano, pois agora ele tinha que ser tratado com dignidade e seus direitos, sem desproporcionalidade e desigualdade das penas, trazendo então o pacto social, um pacto que diz que por sermos integrantes de uma sociedade já estávamos de acordo com esse pacto, de maneira tácita, o qual assim abriríamos mãos do nosso direito de liberdade, para que prevalece o direito de todos, caso descumprisse alguma norma desse pacto, entretanto esse pacto teria que observar os direitos do cidadão de forma correta, baseando na dignidade do ser humano e não tirando a vida do mesmo.(GRECO, 2023).

Essa obra é tão e tão atual, que parece que estamos no mesmo sistema, visto que nosso governo age como se não conhecesse a realidade de nossa sociedade, tomando decisões totalmente equivocadas, criando leis que só beneficiam a classe mais rica e oprime a mais inferior, por mais grave que seja o crime; sua obra ainda explica os dias atuais, os ricos fazem o que querem, enquanto os pobres são presos por delitos simples (GRECO, 2023).

Vale ressaltar sua atualidade e importância para evolução do Direito Penal, que temos decisões utilizando os conceitos de Beccaria, visto que queriam uma condenação exacerbada, conforme decisão do tribunal de justiça do Distrito Federal que diz:

> Tribunal de Justiça do Distrito Federal e Territórios TJ-DF- Recurso de Agravo: RAG 20130020161064 DF 0016973 10.2013.8.07.0000 (TJ-DF)
> (...) PARA PROPORCIONAR ESSAS CONDIÇÕES DE PLENA REINTEGRAÇÃO SOCIAL , PARA MUITOS UTÓPICA, E CONCRETIZAR O SONHO DE CESARE BECCARIA, SONHADO HÁ MAIS DE DUZENTOS ANOS, É IMPRESCINDÍVEL APARTICIPAÇÃO DA FAMÍLIA. CABE,EVIDENTEMENTE EM CASOS COMO ESTE. (...)” (BRASIL,2013).

Assim o direito penal começa a crescer, chegando à fase da Revolução Francesa em 1789, o qual trouxe consigo a mudança de pena, sendo agora a privação da liberdade e não aflição do corpo, visto que antigamente já tinha institutos para privar o preso, porém era somente para aguardar seu julgamento, que logo após julgamento era provavelmente morto.

Em seguida têm-se as escolas penais, tendo sua relevância nesse cenário de evolução do direito penal, em que a escola clássica mostra ideia de que as sanções

era uma forma de retribuição pelo ato delituoso cometido e não de vingança, perfazendo a justiça. Já a positiva estuda a “cabeça” do indivíduo para verificar se realmente ele é criminoso ou não, o que faz ele torna-se um criminoso e quais fatores, embora hoje seja considerada ultrapassada, mas teve grande relevância para criação de outras ciências que se utilizam até os dias atuais. Contudo, os pontos negativos dessas escolas é que a clássica tinha uma falha na reeducação do delinquente e a positiva na omissão de sanções que deveriam ser impostas a ele.

Por fim tem a Escola da Nova defesa Social, após o final da segunda guerra mundial, nesse período criminalista preocupa-se com a prevenção do crime, com uma reforma prisional, no qual o objetivo não está somente na privação da liberdade, que é importante, porém o ponto central é a ressocialização do indivíduo, aplicando então medidas educativas, para que o mesmo possa aprender com os seus atos e não cometer mais.

Desse modo podemos analisar como o direito penal foi evoluindo historicamente, socialmente, culturalmente com cada período da história, em que hoje se chegou à fase tecnológica em que também precisa de novas atualizações, embora se tenha conceitos atualizado, precisa de novos conceitos, uma vez que hoje a sociedade é totalmente dependente do sistema digital e tecnológico, necessitando de meios, formas, leis que asseguram a proteção e tranquilidade de utilizar desses meios, sem fugir na essência do Direito Penal.

3 DENIFIÇÃO DE CRIMES DIGITAIS

Com o avanço da globalização foi possibilitado com que as pessoas tivessem acesso a diversos produtos, tecnologias, ferramentas, culturas e entre outros. Dentre esses está a internet, que facilitou a comunicação com qualquer pessoa de qualquer lugar do mundo, viabilidade de compras on-line, trabalhos remotos, acesso às informações, lazer, educação, pagamentos a distância e mais. Entretanto com a expansão da tecnologia e da internet que trouxe diversos benefícios já mencionados, também proporcionou a realização de crimes, transformando o ambiente virtual no meio perigoso e inseguro.

Quando se fala de Crimes virtuais, antes é necessário que entenda o conceito básico de crime trazido pela doutrina. No Brasil não há um conceito definido pelos legisladores, assim tendo que se basear nos conceitos doutrinários. (GRECO, 2023).

Dessa maneira, segundo a doutrina crime é separado sobre três conceitos: conceito formal, material e analítico. Em que pese este trabalho não pretende aprofundar na teoria geral do crime, mas apresentar as concepções utilizadas atualmente, em virtude do grande dissenso.

Crime formal é considerado toda conduta tipificada na lei, conforme o princípio da legalidade, artigo 5, inciso II da Constituição Federal de 1988 (BRASIL,1988), que diz: “II - ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei”.

Já crime material é toda conduta que viole o bem jurídico que é protegido, de forma relevante, o qual é importante para o convívio em sociedade (GRECO, 2023). Por fim crime analítico é mais complexo, sendo toda conduta que traz consigo fato típico, ilícito e culpável, que conforme a doutrina majoritária adota a Teoria Tripartida do crime.

Segundo ensina Sánchez Herrera (1905 p. 79):

> Hoje, a maioria dos códigos penais do mundo moderno reproduzem na definição de delito a grande conquista dogmática: o delito é um comportamento típico, antijurídico e culpável. Sem embargo, isso nem sempre foi assim; foi necessário um longo processo de desenvolvimento dogmático que concretizou somente em 1906 esse conceito tripartido de delito. Desde esse momento dito progresso é irreversível 24. (apud GRECO, 2023, p. 183).

Neste contexto, sobre crimes virtuais não existe uma nomenclatura correta determinada pelos doutrinadores, assim quando se fala de crimes virtuais pode ser chamada de crimes cibernéticos, crimes digitais, cibercrime, crime informático, crimes eletrônicos e entre outros. Neste trabalho será usada diversas nomenclaturas para evitar a repetição.

Crimes cibernéticos é toda prática ilícita realizada por um dispositivo eletrônico, sendo computadores, celulares, ainda mais na internet. A execução desse delito pode ocorrer de várias maneiras, desde o roubo de informações pessoais, bem como a danificação de sistemas operacionais.

Ratifica nesse sentido o professor Tarcísio Texeira (2022) ao dizer que crimes digitais são considerados aqueles realizados através de meios informáticos, no qual o são computadores, celulares, tabletes e outras aparelhos informáticos e são

somente instrumentos para alcançar a prática delituosa. Além disso, também deve ser compreender como crime quando o objetivo é danificação os sistemas e meios informáticos, como no caso os computadores, celulares e entre outros.

Para Damásio e Milagre (2016, p. 20):

> Conceituamos crime informático como o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do Direito Informático, que é o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Em verdade, pode-se afirmar que, no crime informático, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal.

No mesmo raciocínio delito informático é dado como toda ação típica, antijurídica, culpável pela utilização de processamento automático ou eletrônico de dados ou sua transmissão, ou contra. (FERREIRA, 1992 p.141 e 142, apud TEXEIRA, 2022, p. 223).

3.1 Crimes próprios ou puros

Assim como no direito penal brasileiro que classifica os crimes em próprios e impróprios, nos crimes cibernéticos não é diferente, seguindo a mesma regra. A doutrina classifica crimes próprios ou puros (são a mesma coisa) como atos criminosos contra o sistema computacional e contra os dados e programas contidos nele ali, sendo como exemplo: invasão de dispositivos conectados na rede ataque de negação de serviço, alteração e destruição de dados e entre outros; é de suma importância ressaltar que os bens jurídicos violados são necessariamente os sistemas de dados, eletrônicos e de telecomunicações. (CRESPO, 2011).

Os delitos informáticos são divididos em duas classificações, que pode ser entendido crime próprio pela conceituação de Texeira (2022, p. 224):

> A classificação utilizada por muitos, sendo a propósito a que será adotada neste texto, é a que fazem Hervé Croze e Yves Bismuth,271 dividindo os cri-mes de informática em duas modalidades.
>
> Quanto à primeira modalidade, diz respeito aos atos dirigidos contra o sistema de informática, subdivididos em: atos contra o computador (ou seja, contra o próprio material informático, o computador propriamente dito e seus

> componentes e suportes como os disquetes e fitas magnéticas); e atos contra os dados ou programas de computador (contra as informações do computador, pela cópia não autorizada das informações, alteração ou destruição de dados dos suportes).
> Esta modalidade que é a pura criminalidade informática. São também conhecidos como crimes de informática próprios, praticados por meio da infor-mática; sem ela são impossíveis a execução e a consumação do delito. São tipos penais relativamente novos, pois surgiram a partir do desenvolvimento e expansão da informática, sendo a informática o bem penalmente tutelado.

3.2 Crimes impróprios ou impuros

Referente aos crimes digitais impróprios ou impuros são aqueles em que já existe previsão legal na norma penal. Desse jeito é considerado todo ato delituoso cometido por intermédio da informática e seus sistemas, tornando meramente como instrumento, um meio para a execução prática ilícita. São considerados exemplos: falsificação de documentos, crimes contra honra, estelionato, furtos virtuais, ameaças, contra a liberdade individual e entre outros.

Neste tipo de classificação o bem jurídico violado não é o sistema computacional, tendo em vista que ele é somente utilizado como ferramenta para o alcance principal do crime. (JULIANA BERTHOLDI, 2020). Os bens jurídicos dos impróprios já são tutelados na legislação penal.

Crimes impuros podem ser definidos:

> b) crimes informáticos impróprios: em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Para estes delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais;" (DAMÁSIO; MILAGRE, 2016, p.20).

Com isso fica mais visível e fácil a identificação da classificação dos crimes e a diferenciação de próprio e impróprio, ajudando a detectar qual tipo delituoso se encaixa, sempre lembrando que ambos utilizam os computadores e meios tecnológicos para execução, toda via a diferença está no objetivo da ação, sendo puro nos computadores, dados e tudo que envolve isso, enquanto o impuro um ato ilícito já descrito na norma penal, sendo só um meio para tal conduta, o meio virtual.

3.3 O reflexo dos crimes virtuais no Brasil e sua normatização

O mundo cada vez mais tem avançado quanto a tecnologia, de tal forma que sua principal utilização tem sido por meio da internet. Nos dias atuais existe uma crescente dependência da sociedade quanto à internet, de modo que no Brasil esses dados tem crescido em grande escala nos últimos anos, que segundo dados extraídos do IBGE (Instituto Brasileiro de Geografia e Estatística) apontam que no ano de 2021 a internet chega a 90% dos domicílios dos pais, sendo 6 pontos a mais que em 2019 o qual foi de 84 %. (NERY; BRITTO, 2022).

Assim com essa dependência dos meios virtuais da sociedade, é indispensável que se tenha controles de segurança, normas eficientes punitivas para criminosos, para que as pessoas, empresas e órgãos públicos possam usufruir das melhores maneiras possíveis, sem que sejam prejudicados por algum ataque, visto que hoje maioria dos serviços, comunicações, lazeres são realizados por meio dessa conexão.

Entretanto não é o que ocorre no cenário mundial e nacional, como no Brasil, é o quinto país no mundo mais afetado por crimes cibernéticos, segundo a divisão de investigação sobre suspeita de atividade criminosa virtual que é a Crime Complaint Center (Centro de reclamações sobre crimes na Internet). (IG TECONOLOGIA, 2023).

Os crimes virtuais quando cometidos na sociedade podem e trazem impactos negativos, danos irreversíveis e prejuízos econômicos, ratificado segundo Bertholdi (2020, p. 9):

> É neste cenário que muitas pessoas físicas, empresas e organizações acabam com dados comprometidos, roubo de informações estratégicas, além de prejuízos financeiros e à imagem. Ante a ofensa a esses bens jurídicos, o Direito Penal passa a ser chamado à ação.

No mundo corporativo quando se tem o cometimento de um delito cibernético, tal reflexo pode ser sentido como prejuízos financeiros, desempregos, fechamentos de empresa, malefício ao consumidor, prejuízo na economia nacional e entre outros. Dentro dessa área, os crimes mais sofridos são de ataques ransomware, que compõe uma prática de sequestro de dados, sendo um software utilizado por hackers que impede o acesso ao sistema da empresa ou criptografa os dados e para o desbloqueio e o resgate dos dados, pedem um resgate de dinheiro. No Brasil tem algumas empresas recentes que sofreram tais ataques, como a empresa de

alimentos JBS que segundo dados da vinculados nos jornais G1 (G1, 2021), no ano de 2021 a empresa pagou US$ 11.000.000,000 milhões de dólares em Biticoin aos autores do ataque para restabelecimento dos seus dados na Austrália e nos Estados Unidos. A loja Renner também foi outra empresa que vivenciou o ataque rasomware, toda via conseguiu o resgate sem grandes prejuízos segundo o site Tecmundo. (PAYÃO, 2021).

Assim esses prejuízos podem ir além dos financeiros, visto que quando acontece tal delito isso pode afetar a fama da empresa, afastando os consumidores, o qual segundo Soares De Mattos (2020, p.24) diz:

> Com a análise desse dados, é possível afirmar que os prejuízos financeiros dos cibercrimes para as empresas são realmente altos, e diversas vezes vão além do dano imediato. Mas é importante lembrar que os danos ultrapassam a esfera financeira, isso porque, a depender do tipo de negócio exercido pela empresa há em consequência do crime uma quebra de sigilo e de confiança entre os clientes e a empresa- o que certamente gera boicote por parte dos clientes.

As agências e entidades governamentais, bem como também hospitais e energia tem sido alvos preferenciais dos hackers, tendo em vista a vulnerabilidade e fragilidade de seus sistemas de proteção contra esses crimes virtuais, o lucro fácil e rápido, em que no Brasil como de costume tem-se uma morosidade normativa quanto a esse tipo, proporcionando o estimulo cada vez mais desse delito (ANDRADE, 2015).

O sistema legislativo brasileiro possibilitou o avanço dos delitos informáticos, tendo se novas formas, modelos e práticas de crimes, enquanto o as leis continuam num processo de aprimoramento e estudo, mostrando então ineficiência do seu ordenamento.

No caso das agências e entidades governamentais os reflexos podem ser enormes para sociedade, visto que podem viabilizar novas guerras, ataques, mortes. Desta maneira é necessário que se tenha um cuidado maior e uma celeridade quanto a este tipo normativo, pois hoje praticamente o mundo é digital, de tal maneira que em alguns estados do Brasil, como no estado de São Paulo há o programa São Paulo Sem Papel que visa à redução e eliminar o trâmite de papel na administração pública.

Neste contexto qualquer descuido e despreparo dos órgãos nacionais, pode ser fatal, levando até a morte, com exemplo um caso na Alemanha no dia 10 de setembro de 2020 que segundo a matéria do G1 a mulher faleceu por não conseguir ser atendida emergencialmente no hospital em Duesseldorf, pois o hospital havia sido vítima de um ataque de ransomware o que ocasionou a interrupção de suas operações, fazendo a mesma ter que se transferir para o local mais próximo a 32 quilômetros de distância, morrendo então pela espera da transferência. (ROHR, 2020).

Isso fica claro os danos que esse ataque pode proporcionar a sociedade brasileira e mundial, sendo explicado conforme material publicado na Privacy Tools (Privacy Tools, 2020):

> Conforme Bruno Porto, sócio e líder de Saúde da PwC Brasil, os dados das organizações de saúde são mais visados pois “São dados completos e mais ricos que os dados financeiros”.
> Eduardo Batista, também sócio e líder de Cibersegurança da PwC Brasil, reforça: “O cartão de crédito eu posso bloquear. Mas um prontuário eletrônico é o seu passado e ele é imutável. Isso tem muito mais valor”, afirma.

O usuário final, que são todas as pessoas que acessam a internet para várias atividades também são visados pelos ciber criminosos, sendo o dia inteiro, visto que os mesmos conseguem até burlar máquinas que são exatas, quanto mais os homens que são imperfeitos. Assim tem-se como as principais práticas aos usuários finais como crimes de extorsão sexual, golpes financeiros e entre outros.

Os danos desses crimes podem ser irreversíveis, como numa divulgação de fotos privadas, como no caso de uma adolescente de 16 anos de Veranópolis-RS que tirou sua própria após ter fotos vazadas pelo seu ex-namorado, segundo a notícia da Terra (TERRA, 2023). Outro fator na questão de divulgação de fotos íntimas, além do suicídio são os transtornos mentais que são causados as vítimas que tem sua imagem comprometida aliada com a violação de sua honra e a imagem, carregando um sentimento de culpa, que conforme um estudo feito por Laís Barbosa Patrocínio numa tese de doutorado, sob a orientação da pesquisadora Paula Bevilacqua que foi publicado no site de jornal da CNN BRAISL, que relata Laís:

> É o caso de distúrbios alimentares e estados depressivos; quem já tinha predisposições desenvolveu. Outra consequência importante é o sentimento de culpa, relatado tanto pelas vítimas como pelos

> profissionais. É uma culpabilização externa que acaba virando interna e vai minando a autoestima.
> Além disso, o dano se dá sobretudo nas relações. Muitas das entrevistadas relataram que o que mais machuca não é a vergonha da exposição, mas o fato de não serem apoiadas por familiares e amigos (LAÍS, apud ROCHA, 2022).

Deste modo é correto afirmar o perigo da internet e o cuidado que se deve ter neste mundo tecnológico, uma vez que um descuido pode ser fatal, podendo afetar toda sociedade e a vida privada e social.

O mundo hoje está cada vez mais conectado e globalizado, surgindo à necessidade de identificar e punir o indivíduo não se limitando só no mundo físico, bem como no mundo virtual (BERNARDES, 2016).

A legislação brasileira demorou muito para ter a primeira norma quanto aos crimes digitais, visto que a internet chegou ao Brasil em 1988. Como de costume a lei do Brasil é repressiva e não preventiva, isto é, espera acontecer o delito primeiro para depois analisar qual lei utilizar, como punir, qual tipificação e etc.

Devido a isso, a primeira lei a surgir quanto à tipificação dos crimes virtuais foi em 2012, conhecida como a lei Carolina Dieckmann (12.737/2012). Essa lei surgiu após o caso de 2011 da invasão e compartilhamento de dados e fotos da atriz Carolina Dieckmann, evidenciando o despreparo do direito brasileiro, que é repressivo, esperando acontecer primeiro para depois punir, porém já havia uma grande necessidade da tipificação penal, que foi explícito e evidenciado por esse caso de uma atriz famosa tomar conta da sociedade e da mídia.

Nesse cenário era visível que não se tinha uma lei para se abarcar quanto a tipificação do crime virtual, todavia algumas práticas que são cometidas na internet já estão previstas na lei penal.

A lei n 12.737/2012 embora tenha várias críticas, seu maior destaque foi por ter trazido o risco sobre os crimes virtuais e a internet, contribuindo para o chamado de controle de criminalidade, alterando alguns artigos do código penal. (DAMÁSIO e MILAGRE, 2016).

Logo após as começar vigorar as leis 12.735/2012 e 12.737/2012, tivemos outras leis relacionadas ao cenário informático.

4 ESPÉCIES DE CRIMES VIRTUAIS

Progressivamente tem sido aumentado as condutas criminosas por meios virtuais, isso se dá pelo o avanço tecnológico e morosidade da legislação vigente, que demora em acompanhar com as novas modalidades delituosas neste cenário, podendo ser entendido conforme Pannain e Pezzella (2015, p.4):

> A Internet possibilita, assim, a vivência da utopia de um mundo que reduziu o seu tamanho, pois nunca os seres humanos dos mais diversos locais estiveram tão próximos. Esse espaço de comunicação cuja inserção é viabilizada pela rede mundial de computadores, onde a informação é o fator-chave, tem papel relevante na divulgação quase que imediata de manifestações por parte dos indivíduos.
> Noutro viés, pressuposto para a inserção e participação da pessoa na sociedade da informação é a proteção de seus direitos fundamentais pelo Estado.

Dentre os vários crimes que são cometidos na atualidade, será abrangido os mais recorrentes que são os de: Crimes de Invasão de dispositivo informático, contra a honra, estelionato, sextorsão, ransomware e entre outros.

4.1 Invasão de dispositivo informático

Esse crime está previsto no artigo 154-A do código Penal, o qual foi inserido pela a lei de n° 12.737 de 2012, mais popularmente conhecida como a Lei da Carolina Dieckmann, que relata:

> 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.(BRASIL,1940).

Para ser considerada a conduta criminosa basta apenas a invasão no dispositivo informático, sendo um computador, tablet, celular e entre outros, independente se irá conseguir ou não objetivo final, que no caso a consiste em Obter, Adulterar ou Destruir os dados ou informações daquela invasão.

Ainda sim é importante mencionar que o meio informático pode estar ou não estar conectado a uma rede e sua invasão decorre de uma violação indevida dos mecanismos de segurança, ou seja, violar os mecanismos de segurança do usuário, como: antivírus, antimalware, antispyware, senhas e entre outros. Logo, o Brasil

pune com o art.154-A do Código penal apenas a invasão de acesso ilegítimo forçado, que rompe, que quebra, como no caso os mecanismos de segurança (DAMÁSIO e MILAGRE, 2016).

Nesse mesmo artigo ainda integra outro tipo de conduta delituosa, que é a instalação de vulnerabilidades, caracterizada como Cavalos de Troias, que oculta um malware em um arquivo ou pasta, tendo diversos vírus, com o objetivo de controlar o computador, roubar dados e informações. A finalidade de essa ação obter vantagens ilícitas, mas não precisa alcançar tal finalidade, basta apenas a instalação para a configuração do tipo penal.

Tal entendido de duas condutas fica aperfeiçoado, segundo o Doutrinador Capez (2023, p. 188):

> Nosso entendimento: há dois crimes. O tipo se compõe de duas partes distintas e identificáveis.
>
> Na primeira, o agente invade dispositivo alheio com o fim especial de obter, adulterar ou destruir dados. Na segunda, ele instala vulnerabilidades com o fim especial de obter vantagem ilícita. Duas finalidades diversas: invadir visando à obtenção, adulteração ou destruição de dados ou informações; instalar para obter vantagem ilícita. O crime de invasão possui uma qualificadora prevista no § 3º, não incidente sobre o delito de instalação constante da parte final do caput.
>
> A exigência da finalidade especial de obter vantagem ilícita, restrita à segunda figura típica (instalar vulnerabilidades), é equivocada e desvirtua o crime, cujo objeto jurídico é a tutela da intimidade e não do patrimônio, tanto que se encontra fora do título relativo aos crimes contra o patrimônio.

Um exemplo de um crime realizado e podendo ser punido por esta lei, é o caso da atriz Carolina Dieckmann em 2011 que teve seu computador invadido e sendo expostos seus arquivos pessoais e fotos íntimas na internet.

Aqui neste artigo o objeto jurídico é a intimidade, vida pessoal, a segurança da informação e também os arquivos e dados no dispositivo (CAPEZ, 2023).

O sujeito ativo pode ser qualquer pessoa e o passivo é o responsável que tem esses dados, informações do dispositivo informático.

O elemento subjetivo é o dolo e pode também ser considera a tentativa, desde momento que se inicia e não consegue a obtenção por circunstâncias alheias a sua vontade.

A forma equiparada desse crime é previsto no parágrafo § 1º, que incorrerá na mesma pena de detenção, de 3 (três) meses a 1(um) ano, e multa , quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador

com o intuito de permitir a prática da conduta definida no caput (BRASIL, 1940), isto é a pessoa utiliza um programa como o cavalo de troia para passar as outras pessoas, sendo vendendo, oferecendo e outras ações , com o intuito de permitir que aconteça o crime.

As majorantes desse crime dá-se de acordo com o § 2 º que se refere aumento da pena de um sexto a um terço se da invasão resultar em prejuízo econômico, porém esse aumento refere-se ao art.154-A, parágrafo §1° somente, ou seja se daquela venda de um cavalo de troia resultar em prejuízo econômico aumenta a pena (CAPEZ,2023).

Outra majorante segue prevista no § 5 º, que traz consigo o aumento de pena de um terço à metade se o crime é for praticado contra Presidente da República, governadores, prefeitos, presidente do STF (Supremo Tribunal Federal) e outras autoridades.

O parágrafo § 3 º no texto da lei traz a conduta típica qualificada que se diz:

> § 3 º 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.

Nessa qualificadora pode ser entendido não só como a obtenção de e-mails, segredos de empresa, mensagens e entre outros, mas também o controle remoto não autorizado, que é uma manipulação de dados dos sistemas informáticos tudo a distância, não sendo o controle remoto de uma televisão como conhecemos (CAPEZ, 2023).

Por fim tem-se a majorante do parágrafo § 3 º encontrada o § 4 º que relata um aumento da pena de um a dois terços se houver a divulgação, comercialização ou transmissão a terceiro daqueles e-mails, mensagens, segredos e entre outros.

4.2 Estelionatos Digitais

O Estelionato Digital é uma conduta criminosa que vem tendo aumento de incidências mais e mais, em vista da expansão tecnológica e o fácil acesso aos meios de comunicações ligadas a internet.

Tal prática de Estelionato já está configurada há muito tempo no código penal em seu artigo 171, que consiste na realização de golpes, em que os delinquentes enganam as vítimas para obter algum tipo de vantagem ilícita, sendo dinheiro, acesso a informações e etc.

No mesmo passo em que surgiram novas tecnologias, também evoluiu as novas de modalidades de Estelionato, sendo no caso o Estelionato Digital, que consiste na mesma prática que é de enganar as pessoas para obter vantagem ilícita, todavia por meios digitais, principalmente por meio dos celulares.

Visando coibir este tipo penal que só aumentou ainda com o advento da pandemia do Covid-19, foi criada uma nova qualificação, no caso a Fraude eletrônica, pela Lei n° 14.155, de 2021 alterando o Código Penal, mais popularmente como Estelionato Digital.

A redação da lei desse tipo penal diz:

> 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. (Incluído pela Lei nº 14.155, de 2021) (BRASIL, 1940).

De acordo como prevê a norma acima, a pena no tipo penal digital aumentou-se, visto que o estelionato comum é de reclusão de um a cinco anos, e multa e o digital é reclusão, de quatro a oito anos e multa. Continuando, o texto penal traz que tanto a vítima e o terceiro são induzidos ao erro e o criminoso se utiliza das informações fornecidas por eles, pelo meio das redes sociais, contatos telefônicos, envio de correio eletrônico fraudulento ou qualquer outro meio fraudulento análogo (GRECO, 2023).

Nesse sentido tem-se a primeira situação que é a por meio das redes socias, que segundo ensina Rogério Sanches Cunha:

> a) por meio de redes sociais: atualmente são muito comuns os anúncios promovidos em redes sociais como Facebook e Instagram. Não raro, são anúncios fraudulentos, manobras ardilosas para atrair pessoas que forneçam seus dados;(CUNHA, 2013, apud GRECO, 2023, p. 710).

Assim, conforme ilustração do Doutrinador Sanches Cunha, os crimes cometidos por redes sociais têm-se alguns tipos mais cometidos segundo a reportagem do canal Record, em que um levantamento feito pelas as delegacias de

Estelionatos e Crimes Cibernéticos do Brasil no ano de 2022, em que diversos registros foram feitos, sendo: Crime da Tabela do Pix e Falsos anúncios. (RICTV, 2023).

A Tabela do Pix é um crime que faz o anúncio por meio das redes sociais, como Facebook e Instagram, em que se o criminoso publica geralmente por um perfil falso, que traz a mensagem na publicação “multiplica-se pix de R$ 50,00 (cinquenta reais) para R$ 250,00 (duzentos e cinquenta reais), ou seja, a pessoa faz um pix a uma determinada conta de R$ 50,00 (cinquenta reais) esperando ter o retorno fácil de R$ 250,00 (duzentos e cinquenta reais), porém isso não ocorre, a vítima perde seu dinheiro e nunca mais o vê.

Ainda nesse cenário tem a segunda situação de acordo com o código penal, que é o crime por contatos telefônicos, sendo um exemplo recorrente envolvendo cartões de crédito, assim o criminoso telefona a alguém se passando pela instituição financeira bancária da vítima, alegando indícios de fraude do cartão, requerendo informações sigilosas, como senha do cartão, CPF para que assim o fraudador possa fazer saques, compras e empréstimos e entre outras práticas (CUNHA, 2013, apud GRECO, 2023, p.710). Esse golpe também é conhecido como Golpe do WhatsApp falso, um dos crimes mais cometidos atualmente, o fraudador finge ser conhecido da vítima ou alguma instituição, induzindo a passar uma quantia a uma determinada conta, em que a vítima acreditando na história meticulosa do mesmo, acabe efetuando tendo prejuízo financeiro.

A terceira situação consiste no envio de correio eletrônico fraudulento. O agente envia um e-mail, imitando caracteres de empresas ou órgãos públicos, que por meio de um link disponibilizado acessado pela vítima, o estelionatário pode obter dados pessoais, dados bancários e outras informações CUNHA, 2013, apud GRECO, 2023, p.710).

Por fim tem-se o último tipo elencado considerado “por qualquer outro meio fraudulento análogo”, sendo um exemplo sites falsos, em que são feitos por estelionatários, parecidos com sites verdadeiros, no qual ali se vende carro em leilão e também cópias de outros sites de grandes lojas nacionais conhecidas. Assim o comprador acreditando por estar com um preço bem abaixo efetua compra, porém nunca recebe o bem, caindo em mais um golpe por meio da internet.

As majorantes dos Estelionatos Digitais são encontradas nos § 2º-B e § 3º, o qual o segundo retrata um aumento um terço a dois terços, se o crime é praticado

mediante a utilização de servidor mantido fora do território nacional. A relevância do resultado gravoso faz com que o juiz aplique essa majorante, pois tal a utilização de um servidor mantido fora do território nacional dificulta a investigação (GRECO, p.710, 2023).

Já o § 3º menciona aumentará a pena se o crime for realizado contra entidade de direito público, no caso a União, Estado, Distrito Federal, municípios, autarquias e outras entidades de direito público. Também se enquadra os institutos de economia popular, assistência social ou benéfica, que segundo Greco (2023, p.711) são:

> Entidades de direito público interno são a União, os Estados, os Municípios, o Distrito Federal, suas autarquias e entidades paraestatais. Instituto de economia popular, conforme esclarece Hungria, "é todo aquele que serve a direto interesse econômico do povo ou indeterminado número de pessoas (bancos populares, cooperativas, caixas Raiffeisen, sociedades de mutualismo etc.). Instituto de assistência social ou de beneficência é o que atende a fins de filantropia, de solidariedade humana, de caridade, de altruístico socorro aos necessitados em geral, de desinteressado melhoramento moral ou educacional."20

4.3 Crimes Contra a Honra

Outro tipo de crime que tem grande proporção na sociedade brasileira, com a expansão da internet e das redes sociais são os crimes contra a honra, já previsto legalmente na norma Penal brasileira.

A Honra é um direito fundamental garantido pela Constituição Federal, em sua redação no art. 5, inciso X, não podendo ser violada. Desse modo ela merece a devida proteção, visto que o homem que tem a sua imagem, figura respeitada e reconhecida por seus atos, tende a serem mais felizes, encontrando a paz interior, o que proporciona uma respeitabilidade e um comportamento adequado as normas jurídicas instituídas e devido a isso que o direito tem o interesse em protegê-la, uma vez que sem ela, os homens estariam desguarnecidos de amor-próprio, tornando pessoas mais frágeis e suscetíveis aos cometimentos desonestos e ilícitos (NUCCI, 2023).

Segundo a classificação da doutrina majoritária a honra é divida em dois tipos, sendo a subjetiva e a objetiva. A honra objetiva consiste na reputação da pessoa, o que as pessoas pensam daquela pessoa, o que a sociedade pensa

daqueles cidadãos de seus atos, sua imagem, o qual pode ser evidenciado segundo o entendimento do doutrinador Jesus (2020, p.223) “Honra objetiva é a reputação, aquilo que os outros pensam a respeito do cidadão no tocante a seus atributos físicos, intelectuais, morais etc.”.

Referente à honra subjetiva é correto afirmar que é considera como uma análise que cada pessoa tem de si mesma, isto é o que cada um pensa sobre si, que conforme Rogério Greco (2023, p. 268) “...honra subjetiva cuida do conceito que a pessoa tem de si mesma, dos valores que ela se auto atribui e que são maculados com o comportamento levado a efeito pelo agente.”

No Código Penal encontram-se os três tipos de crimes contra honra, sendo: Calúnia, Difamação e Injúria, mais precisamente, conforme redação abaixo:

> Calúnia
> Art. 138. Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena – detenção, de seis meses a dois anos, e multa.
> Difamação
> Art. 139. Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena – detenção, de três meses a um ano, e multa.
> Injúria
> Art. 140. Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena – detenção, de um a seis meses, ou multa. (BRASIL, 1940).

Na internet as pessoas parecem que criam coragem para falar coisas que pessoalmente não teriam coragem, assim atuam crendo que são invisíveis e que a internet é uma terra sem lei, podendo imputar xingamentos, fatos e opiniões ofensivas a qualquer pessoa, sem se preocupar com a veracidade das informações e da reputação, dignidade e o decoro do ofendido, pois uma foto, um vídeo, uma mensagem e qualquer publicação tem a capacidade de ser visualizada por milhares de pessoas, logo não podendo fazer o que bem acha.

A Calúnia é um delito em que ocorre a imputação de fato definida como crime a outra pessoa, porém essa imputação é falsa, isto é a pessoa diz que “fulano” cometeu certo crime, porém não se confirma, o fato é falso. Assim nesse crime exige o elemento normativo “Falsamente”, necessitando a imputação realizada pelo agente seja falsa, entretanto se o crime realmente ocorreu então a atribuição ao terceiro não pode ser considerado calúnia. (JESUS, 2020).

Diferente do que ocorre na calúnia, na difamação também se imputa fato, todavia, esse fato não é constituído como um delito, mas sim uma ofensa a honra

objetiva do terceiro, qualificando como uma conduta ofensiva, maculando a reputação de pessoa. Como por exemplo: “fulano” diz a terceiros que tal pessoa está traindo a outra pessoa. Embora mesmo que seja verdade, tal comentário não é correto, em virtude que isso ofende a honra objetiva da pessoa.

Esse conceito pode ser ratificado de acordo com Nucci (2023, p.238):

> Com isso, excluiu os fatos definidos como crime – que ficaram para o tipo penal da calúnia –, bem como afastou qualquer vinculação à falsidade ou veracidade destes. Assim, difamar uma pessoa implica divulgar fatos infamantes à sua honra objetiva, sejam eles verdadeiros ou falsos.
> Reitere-se: o agente deve fazer referência a um acontecimento, que possua dados descritivos como ocasião, pessoas envolvidas, lugar, horário, entre outros, mas não um simples insulto. Dizer que uma pessoa é caloteira configura uma injúria, ao passo que espalhar o fato de que ela não pagou aos credores “A”, “B” e “C”, quando as dívidas X, Y e Z venceram no dia tal, do mês tal, configura difamação.

Conforme artigo 140 do Código Penal o delito de Injúria configura na prática de alguém ofender a dignidade ou o decoro de outrem, ou seja, são basicamente os xingamentos, em que visa atribuir a outro, uma qualidade negativa, seja física, intelectual ou psicológica. Aqui não existem fatos, mas sim ofensas isoladas, no qual no meio virtual é visto com frequência. A injúria se constitui pela atribuição ofensiva as pessoas, alcançando a dignidade ou decoro da mesma, em que a dignidade se refere ao sentimento de honra e valor moral, como exemplo: “pilantra, “safado”; já o decoro a nossa consciência sobre si mesmo, o respeito por si, como exemplo: “lesado mental”, “jumento” (HUNGRIA, apud ESTEFAM, 2022).

Assim diferente da difamação e da calúnia, na injúria não existe a imputação de fatos, mas atribuição de qualidade e conceito negativos, o que recai sobre atributos físicos, morais ou intelectuais da vítima (ESTEFAM, 2022).

Como visto nos crimes contra honra, busca-se a proteção da honra, logo é correto afirmar que a objetividade jurídica é a honra, merecendo a tutela. Conseguinte na calúnia e na difamação segundo conceito majoritário doutrinário a objetividade jurídica é a honra objetiva, a reputação da vítima; enquanto na injúria visa-se a proteção da honra subjetiva, tutelando a dignidade ou decoro da mesma.

Outrossim, encontra-se no código penal a chamada Exceção da Verdade no crime de Calúnia, conforme artigo 138, § 3°, (BRASIL, 1940) que diz:

> § 3o Admite-se a prova da verdade, salvo:
> I – se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;
> II – se o fato é imputado a qualquer das pessoas indicadas no I do art. 141;
> III – se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível

A Exceção da verdade é um dispositivo de defesa para um sujeito que imputou um fato descrito como crime e caso prove que aquele fato é verdadeiro, o mesmo não responderá por tal delito, contudo conforme incisos I, II, III, trazem as hipóteses que mesmo que prove a verdade, ainda continuará respondendo pelo crime de calúnia.

Para Nucci entende:

> Trata-se de um incidente processual, que é uma questão secundária refletida sobre o processo principal, merecendo solução antes da decisão da causa ser proferida, previsto no § 3.º do art. 138. É uma forma de defesa indireta, por meio da qual o acusado de ter praticado calúnia pretende provar a veracidade do que alegou, demonstrando ser realmente autor de fato definido como crime o pretenso ofendido.
>
> Como regra, pode o réu ou querelado assim agir porque se trata de interesse público apurar quem é o verdadeiro autor do crime. Imagine-se que Fulano diga ter Beltrano matado alguém em determinada ocasião, mas que o fato não foi devidamente apurado pela polícia. Caso Beltrano o processe, alegando ter sido vítima de calúnia, pode Fulano ingressar com a "exceção da verdade", dizendo que pretende demonstrar a veracidade do alegado, pois o Estado tem interesse em conhecer a autoria do homicídio, crime de ação pública incondicionada. Além disso, se falou a verdade, não está preenchido o tipo penal ("imputar falsamente fato definido como crime"). (2023, p.235).

Eles continuam a responder por que pretendem a proteção objetiva da honra dele. Os sujeitos ativos na calúnia não são somente que imputa um fato falso definido como crime, mas também quem espalha, propaga e divulga, com fulcro no artigo 138, parágrafo 1°, recebendo a mesma pena de quem faz a calúnia, pois conforme já dito está atingindo a reputação do indivíduo.

Assim trata-se de um crime formal, pois não é necessário o alcance ao resultado de causar dano a honra, correspondendo em crime instantâneo, consumando-se no exato momento em acontece, não sendo permanente, afetando somente um objeto jurídico: a honra objetiva (JESUS, 2020).

A exemplo da calúnia na difamação também se encontra exceção da verdade, todavia, só é validada se a ofensa é para um funcionário público e se ela

corresponde aos exercícios de suas funções, conforme artigo 139, Parágrafo único. Então compreende um mecanismo de defesa aos funcionários públicos.

Diferente na injúria não existe a exceção da verdade, visto que não contém uma atribuição de fato, mas somente de uma qualidade negativa a pessoa, assim sendo um xingamento isolado e sendo incorreta a produção de verdade (JESUS, 2020).

Desta maneira, esses crimes contra honra são tão corriqueiros no ambiente virtual, que existem inúmeros casos nas mídias, jornais, redes socias e registrados nas delegacias de polícias, sem contar os que não são registrados. Como no caso de acontecimento de calúnia recentemente em 2023 no Brasil a um jogador de futebol da Sociedade Esportiva Palmeiras, em que um influenciador teria postado um vídeo nas redes sociais, insinuando que o jogador estaria envolvido em esquemas de aposta esportiva, por causa de um passe errada numa saída de jogo do meio de campo, em que o mesmo chutou a bola para lateral, durante uma partida contra o Vasco da Gama no dia 23 de abril de 2023. (FERRI, 2023).

Assim como visto tal imputação falsa ao jogador fere sua dignidade e sua honra, podendo assim trazer prejuízos a sua imagem, visto que todos agora passam a assistir sob outra análise, duvidando de seu profissionalismo e até mesmo podendo prejudicar em futuras negociações com outros clubes.

Por isso é importante destacar que a internet embora tenham um grande espaço para expor a liberdade de pensamento e expressão, que também são direitos constitucionais garantidos no artigo 5 da Constituição Federal, esse direito não pode ser absoluto, visto no momento que atinge, fere a honra, reputação e a imagem da pessoa, tal direito deve ser impedido.

Esse conflito entre a liberdade de expressão e a honra, são esclarecidas por análise de Coelho e Branco:

> O conflito que ocorre entre a liberdade de expressão do indivíduo, protegido constitucionalmente e as condutas que atingem a honra (objetiva ou subjetiva) das vítimas é latente. Sabe-se que a liberdade de expressão não pode ser exercida livremente e que é necessário ponderar o direito de se expressar com o direito de outros, devendo os agressores responder por seus excessos. Entretanto, nem sempre as condutas realizadas pela internet são punidas penalmente, quer seja por conta da dificuldade de se comprovar o real infrator (anonimato) quer seja pela falta de preparo do Estado para lidar com tal situação (COELHO; BRANCO, 2016 apud ASSUNÇÃO, p.15, 2018).

Desta maneira é certo afirmar que o direito a liberdade de se posicionar nunca deve ser limitado, somente quando atingir e afetar a honra de alguém, visto que segundo a doutrina entende que não é crime o animus criticandi (criticar alguém), ainda mais no ambiente virtual que qualquer pessoa do mundo de qualquer lugar consegue ter acesso a esses atos libidinosos. Logo, baseando-se no famoso ditado do filósofo inglês Herbert Spencer "A liberdade de cada um termina onde começa a liberdade do outro", assim deve caminhar a liberdade de expressão, pensamento juntos com a possibilidade de denegrir a honra de outrem.

4.4 Ataques de Ransomware

O ataque de Ransomware é um tipo de ataque conhecido como sequestro de dados e informações sigilosas, tendo maiores incidências como vítimas no mundo corporativo, sendo empresas de médio e grande porte e órgãos públicos.

Ransom em inglês significa resgate, assim esse tipo de ataque é realizado por hackers que através de malware (software malicioso) impede o acesso aos dados ou criptografam os dados armazenados em um servidor, exigindo um resgate em dinheiro geralmente por criptomoedas para reestabelecimento desses dados e informações (BOMFATI; KOLBE JUNIOR, 2020).

Os prejuízos causados por um ataque de Ransoware podem ser enormes e variáreis, visto que, depende de cada caso concreto, contudo esses danos geralmente tendem a ser financeiros. Outro dano causado que implica sobre este crime é o atraso e a demora de dias, semanas e meses para o reestabelecimento de determinada empresa, instituição ou órgão, o que além de causar danos patrimoniais, podem afetar a vida de outras pessoas que dependem de um determinado serviço ou produto desses órgãos e empresas.

Os danos causados por ataque desse tipo são péssimos e tendem a cada vez mais piorar, podem ser de muitos milhões para empresas e organizações multimilionárias e para multibilionárias. Além disso, os resgates também podem ser destruidores a empresas e organizações de pequeno porte (GRIMES, 2022).

Alguns exemplos podem evidenciar esses danos, de diferentes modos, como no caso mais conhecido, justamente por ter sido o maior ataque de ransomware em

valor de resgate até o momento do mundo, totalizando um valor de 70 (setenta) milhões de dólares a empresa Kaseya, uma empresa norte americana de T.I (tecnologia da informação), uma provedora de soluções de T.I para empresas. A empresa sofreu um ataque, sendo explorado por uma falha em seu software, prejudicando não somente a si mesma, como também seus mais de 40 mil clientes no mundo todo. (TILTUOL, 2021).

Outro caso de dano cometido por esse software foi na Irlanda, em que o sistema de saúde de Dublin ficou sob o poder dos sequestradores digitais, sendo obrigado a paralisar seus sistemas, em que um programa malicioso bloqueou os dados, liberando só após o pagamento 20 milhões de dólares, para que assim não divulgassem informações dos pacientes, entretanto o governo Irlandês não efetuou o pagamento, que devida pressão, os hackers acabaram liberando uma chave de acesso, voltando o sistema, porém o sistema demorou mais de meses para voltar ao seu funcionamento normal, o que trouxe danos aos pacientes, tendo filas de espera, consultas e vacinação, sem contar dano que poderia ser causado por não ter o histórico da pessoa (GLOBOPLAY, 2021).

Conforme visto o ataque de Ransomware tem cada vez mais se espalhado pelo mundo inteiro e aumentando cada vez mais os números de caso segundo uma matéria publicada no site techtudo.com (HUAWEI, 2023) houve “um aumento de 51% no volume de ataques quando comparado ao ano anterior”. Essa comparação é de 2021 como 2020.

Logo, devido a esse crescimento o governo brasileiro tem tido preocupação quanto a esses crimes, pois várias empresas como: Embraer, JBS e também os órgãos públicos como: o STJ, o Ministério de Saúde e entre outros sofreram esses incidentes.

Nessa circunstância no atual cenário brasileiro tem um projeto de lei n° 879 de 2022 que está em tramitação neste momento que este trabalho é regido. Essa PL 879/22 objetiva a criminalização do golpe de ransomware, pois não contém instituto legal para esse ataque no Brasil, que seria alterado o decreto lei de n° 2.848, de 7 de dezembro de 1940, Código Penal, para assim qualificar o crime de invasão de dispositivo informático quanto houver a obtenção de dados pessoas (§ 3º do art.154-A) e criação do crime de sequestro de dados informáticos, conhecido por ataque de ransomware (art.154-C).

Entretanto existe alguns estudiosos, juristas, doutrinadores, que entendem que a criação desse tipo penal seria desnecessária, conforme Emanuela de Araújo Pereira advogada criminalista e mestre em Direito Penal e Ciências Criminais pela Universidade Sevilha (Espanha) que publicou no site do Conjur (PEREIRA,2023):

> Portanto, a perspectiva apresentada em síntese neste artigo, indica a desnecessidade do Projeto de Lei nº 879/2022 que busca a criação do tipo penal "sequestro de dados informáticos". Vimos que, se inserido o art. 154-C ao Código Penal, será uma prolixidade normativa do legislador, uma vez que já existe previsão legal para a tutela dos bens jurídicos individuais propostas no referido delito.

Sob este aspecto fica evidenciado o despreparo normativo brasileiro, que embora exista no artigo 154-A o crime de invasão, o novo conceito de um tipo criminal além de atualizar e evoluir de acordo com as mudanças sociais e tecnológicas, garantirá segurança jurídica, combatendo o crime organizado digital e desestimulando este tipo penal, que no Brasil tem fácil acesso, devido o despreparo quanto a este tema, que tem só crescido no Brasil, sob o aspecto da justificativa da PL. n° 879, de 2022.

Além do mais, outro aspecto que a norma brasileira deverá avançar é com relação a dificuldade de encontrar os criminosos virtuais, embora hoje no Brasil possui algumas delegacias especializadas, visto que nada adiantará avançar com as leis cibernéticas e não ter técnicos e pessoas preparadas para executá-las, o que estaria por igual o nosso atual cenário jurídico, legislativo e executivo, sendo um dado que pode ser comprovado a pouca quantidade de delegacias que existem no Brasil de crimes cibernéticos, sendo apenas 18 segundo dados da Safernet (SAFERNET, 2023).

5 LEGISLAÇÕES

Assim como na maioria dos temas tem suas leis, nos crimes digitais não é diferente, em que pese neste capítulo será analisado as legislações vigentes a respeito dos crimes virtuais no Brasil.

Os doutrinadores e legisladores tiveram um choque de realidade, com o avanço da tecnologia e da internet, tendo que elaborar institutos e normas capazes de coibir a progressão dos delitos cibernéticos e trazer segurança aos navegantes.

Uma tarefa muito árdua, tendo que atualizar a cada instante, aperfeiçoando a temática desse conceito virtual, pois se trata um assunto novo para sociedade, tendo em vista que no Brasil os delitos avançam muito mais rápidos dos que as normas, em que cada dia que passa os criminosos estão se aperfeiçoando com técnicas inovadoras, o que infelizmente não ocorre nas normas, podendo ser confirmada pela a criação da primeira lei quanto a esse assunto em 2012.

Portanto, o ambiente virtual e sua grande mutação, gera um desafio aos legisladores e juristas para que sempre tenha institutos capazes de impedir a expansão ciber criminosa e transformar o ambiente virtual o mais seguro possível.

5.1 Lei de Azeredo n° 12.735 de 2012

Esta lei ficou marcada como a lei de Azeredo, devido o Eduardo Azeredo ex Senador criador desse projeto n lei - PL-84/99 (OLIVEIRA, 2013).

O intuito dessa lei foi impedir a práticas de crimes nas redes, alterando assim o Código Penal (decreto Lei n. 2.848/1940) e o Código Penal Militar (lei n°7.716/1989), que em art. 1 tipifica condutas realizadas mediante uso de sistema eletrônico, digitais ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.

Já no seu artigo 4° relata a possibilidade que a polícia judiciária na estruturação de órgãos especializados para o combate aos cometimentos criminosos nas redes de computadores, sistemas informatizados ou dispositivos de comunicações (JESUS, 2016).

Desse modo a lei de Azeredo foi de suma importância, pois foi o primeiro passo no direito criminal virtual.

5.2 Lei Carolina Dieckmann – n° 12.737/2012

A lei da Carolina Dieckmann foi sancionada em 2012, em virtude que a atriz Carolina Dieckmann teve seu computador invadido, o qual foi exposto fotos íntimas da atriz, além de sofrer tentativa de extorsão.

Desse modo essa lei trouxe novos tipos penais alterando o Código Penal, com intuito de atender a demanda afetada do setor financeiro antiga, no que se refere aos golpes e fraudes financeiros, pois existia uma grande carência e ânsia para tal norma, mesmo considerada uma lei bem restrita, em comparação aos projetos que percorriam sobre o Congresso Nacional. Portanto foi aprovada, uma lei básica, sem polêmica, não regulamentou os crimes cibernéticos, valendo-se do famoso ditado, que a lei é como um remédio, deve ser inserido em poucas doses para não prejudicar os pacientes (JESUS, 2016).

Nela contém três tipos de crimes, sendo previsto nos artigos 154-A, art.266 e 298. No artigo 154-A, conforme já mencionado em outros tópicos trouxe o principal tipo criminal, sendo a Invasão de dispositivo informático, com pena de reclusão, de 1 (um) a 4 (quatro) anos, e multa.

No art.154-A prevê o crime de Invasão de dispositivo informático, o qual contém dois verbos principais sendo invadir (transgredir, violar com força) e instalar. Referente a invasão a mesma tem que ser violação, uma quebra com força do dispositivo informático e não por acidente, em que objeto material do crime é o dispositivo informático que pode ser entendido como um computador, tablet, smartphones e outros com a mesma finalidade. Ainda sobre a invasão, deve ser rompido o dispositivo informático de uso alheio, assim sendo de uma terceira pessoa e não seu, com o objetivo de obter, destruir ou adulterar os dados contidos naquele dispositivo, sem autorização expressa ou tácita, pois se tiver autorização não corresponde em crime, mas um fato atípico. Já em relação a instalação de vulnerabilidades (mecanismos maliciosos a gerar abertura no sistema) é nada mais e nada menos do que um meio de preparação para a violação do computador, com a finalidade de obter vantagem ilícita. Desse modo o doutrinador equiparou a instalação com a invasão para fins de criminalização, o qual se um agente comete os dois tipos penais, somente responderá por um crime, diferente se for dois agentes e cada comete um tipo, que cada um responderá por ser crime. Vale ressaltar que esse crime é um crime formal (não precisa produzir resultado naturalístico, mas a lesão do bem jurídico), instantâneo, já se consuma no momento da realização e aceita tentativa, sendo seu elemento subjetivo o dolo e por fim objeto

jurídico a ser protegido são vários como: a vida privada, à honra, a intimidade, à inviolabilidade de comunicação e correspondência e à livre manifestação do pensamento. (NUCCI, 2023).

O § 1º, do artigo 154-A, traz em sua redação a forma equiparada do crime, em que incorrerá na mesma pena do caput desse artigo, quem produzir (criar), oferecer (apresentar algo a alguém), distribuir (entregar as pessoas), vender (colar a venda mediante o dinheiro) e difundir (propagar) dispositivo ou programa de computador, com o intuito de permitir prática da conduta de invasão (elemento subjetivo), sendo considerada também uma forma de preparação para a realização da invasão, tendo como sujeito ativo e passivo qualquer pessoa, não se admitindo tentativa, visto como um crime formal, com seu objeto jurídico os mesmos do caput e o elemento subjetivo o dolo e o elemento subjetivo específico já citado. (NUCCI,2023).

Por sua vez, o § 2º, do artigo 154-A, descreve causa de aumento de pena, em que se da invasão resultar em prejuízo econômico. Deste modo observa-se que além da invasão a privacidade, ocorre também o prejuízo econômico, exaurindo o crime. Portanto haverá um aumento de 1/3 (um terço) a 2/3 (dois terços) desse prejuízo, em que sempre valerá do prejuízo econômico, isto é, quando maior prejuízo, maior elevação de pena.

Em relação § 3º, do artigo 154-A, expõe a forma qualificada do crime de invasão, tendo em vista que se da invasão resultar em outro resultado, que é a obtenção conteúdo de comunicações eletrônicas privadas, segredos comercias, industriais e informações sigilosas terá um regime de pena diferenciado, sendo de reclusão, de 2 (dois) a 5 (cinco) anos, e multa. Ainda nesse parágrafo também contém outro resultado do crime de invasão, que no caso é o controle remoto não autorizado do dispositivo que foi invadido, que significa ter o controle sobre o dispositivo da vítima mesmo a distância. (NUCCI,2023).

O § 4º e § 5º, do artigo 154-A descreve os aumentos de pena devido a forma qualificada contida no parágrafo § 3º, em que o § 5º refere-se o aumento em virtude da vítima, como exemplo autoridades públicas: Presidente, Governador, Ministros e outros.

Outrossim, essa lei alterou também o artigo 266 sobre o crime de Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, por meio do parágrafo 1° que incorrerá na mesma

pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento, no qual conforme o § 2º aplicará o dobro da pena se o crime for cometido em calamidade pública.

Concluído, o último delito trazido por essa lei é uns dos crimes que são mais cometidos no Brasil no mundo cibernético, que é Falsificação de Cartão equiparando-se ao crime contido no art.298 de falsificação de documento particular, conforme redação abaixo:

> Falsificação de cartão
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.(BRASIL, 1940).

Assim é importante destacar a relevância que esta lei trouxe, embora trouxe poucos conceitos, mas foram conceitos essenciais para o primeiro passo quanto a criminalização cibernética.

5.3 Lei do Marco Civil da Internet – n°12.965/2014

A lei de n° 12.965 de 2014 é conhecida pela lei do Marco Civil na internet, recebeu este nome de civil, justamente para marcar a uma oposição de um projeto de lei penal na época que buscava a criminalização algumas práticas realizadas na internet que os usuários faziam (ANDRADE, 2022).

Antes de 2014 não tinha uma lei específica na internet que conferia os direitos e deveres dos usuários, assim com a promulgação dessa norma, o intuito foi regular os direitos e deveres dos usuários na internet, bem como auferindo princípios fundamentos.

O Marco foi elaborado sobre três principais princípios sendo: Liberdade, Privacidade e Neutralidade.

A liberdade permite que os usuários possam ter o livre acesso, produção e compartilhamento de qualquer tipo de conteúdo, não podendo o banimento por qualquer pessoa, somente por autoridade pública, conforme artigo 3 desta lei que aduz sobre o direito a liberdade na internet:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I – garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; (BRASIL, 2014)

Com relação a neutralidade segundo o entendimento de Besbesco (BABESCO, 2018) “Neutralidade: proíbe que os provedores de conexão façam qualquer distinção de velocidade entre as páginas da internet”. Destarte tal princípio foi de suma importância para o consumidor, visto que as empresas agora não podem cobrar valores, mensalidades diferentes por cliente, como no caso um aplicativo de streaming da Netflix e outros, sendo apenas permitida a cobrança por pacotes diferentes devido às atribuições a mais ou a menos naquele pacote, como no caso da Netflix existem quatros tipos de planos diferentes, pelas condições de resoluções e telas simultâneas.

O artigo 9 dessa lei versa sobre essa neutralidade que deve ser ter:

> Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação (BRASIL, 2014).

Por fim a privacidade que vem para garantir a inviolabilidade sobre os dados e comunicações dos usuários, conforme disposto no § 3º do artigo 11 dessa lei , que diz:

> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação,
> informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à
> coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações. (BRASIL, 2014).

Diante desse contexto levantado nota-se o grande avanço quanto a uma norma eficiente garantindo aos usuários a liberdade de expressão, sem censura, a privacidade de seus dados para que possam utilizá-la da melhor maneira possível.

5.4 Lei Geral de Proteção de Dados Pessoais – n° 13.709/2018

A Lei Geral de Proteção de Dados Pessoais conforme o próprio nome já menciona, é a lei criada para proteção dos dados pessoais das pessoas, regulando as coletas e o tratamento desses dados, não podendo ser espalhados.

A LGPD modifica a atuação das empresas nas coletas dos dados pessoais, sendo obrigado a protegê-los, assim tendo um olhar mais crítico no tratamento dos dados (FERNANDES, 2021).

Esses dados são nomeados como dois tipos, sendo os identificáveis e os sensíveis. Os dados identificáveis são aqueles que servem para saber quem é essa pessoa, a identificação da mesma, como RG, CPF e entre outros.

Já os sensíveis são atribuídos as características peculiares do indivíduo como raça, religião, gostos e entre outros. (FERNANDES, 2021).

Assim caso as empresas não se enquadrem no tratamento e coleta desses dados e sejam vazados, mesmo que sejam por ataque como no ransomware, serão multadas em até 2 % (dois por cento) do faturamento bruto ou até R$ 50.000.000,00 (cinquenta milhões de reais), com fulcro no artigo 52, inciso II abaixo:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; (BRASIL, 2018).

Como visto sua criação e elaboração foi de grande relevância, pois ela garante a liberdade, privacidade de seus dados podendo saber quem está coletando e para que fim, possibilitando ainda a escolha de aceitação ou não, trazendo uma segurança virtual.

5.5 Lei 14.155 de 2021

Esta lei foi aprovada sobre o projeto de lei 4.554/2020, alterando assim o Código Penal para agravar os crimes de invasão de dispositivo, furto e estelionato cometidos de forma eletrônica ou pela internet.

Trazendo para o aspecto digital, a lei tem consideráveis avanços, em virtude expansão ciber criminosa, sendo útil e necessário o agravo das penas para tentar frear esse avanço criminal.

Em virtude disso endureceu a crime de invasão de dispositivo informático, art.154-A do Código penal alterando a pena de detenção, de 3 (três) meses a 1 (um) ano, e multa para reclusão, de 1 (um) a 4 (quatro) anos, e multa. Além do mais também modificou o texto do artigo 154-A retirando a necessidade de invadir o dispositivo mediante violação indevida de mecanismo de segurança, pois era um empecilho penal desnecessário, visto que barra para a consideração de crime o dispositivo que tivesse um mecanismo de segurança instalado (NUCCI, 2023).

A lei também enrijeceu § 2º e § 3º do artigo 154-A, modificando respectivamente a pena da majorante da forma qualificada da invasão. A alteração do § 2º foi de um sexto a um terço se resultar em prejuízo econômico da invasão para um terço a dois terços; já no § 3º foi pena de reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, caso a conduta não constituir crime mais grave, para reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

Finalmente no cenário virtual, também inseriu uma nova modalidade penal, conforme já dito em outro tópico o chamado Fraude Eletrônico, mais popularmente conhecido com Estelionato Digital, no artigo 171, § 2º-A e § 2º-B do Código Penal, conforme redação abaixo:

> Estelionato
> 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
> 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. (BRASIL, 1940).

Sob essa perspectiva é importante ressaltar a relevância de criação dessa lei, pois sem dúvida terá um impacto nos criminosos virtuais, aderindo penas mais

severas aos criminosos para coibir esse avanço criminal. Em que a legislação brasileira conseguiu de certo modo ter um acompanhamento, porém esse acompanhamento ainda precisa de muitas melhorias.

6 CONCLUSÃO

No decorrer deste estudo observou-se que houve uma crescente cada vez mais em novas modalidades criminosas no ambiente virtual, tendo a legislação brasileira conseguindo acompanhar até certo ponto, com morosidade, entretanto há muito que progredir em normas e profissionais capacitados para elaborá-las e executá-las. Ainda assim, demonstrou os reflexos que os crimes cibernéticos trazem na sociedade, afetando os órgãos públicos, empresas e a vida privada pessoal, tendo capacidade de parar uma cidade e um país a depender do crime.

Dessa maneira, o presente estudo demonstrou os objetivos alcançados, tendo evidenciado a conceituação dos crimes digitais e suas espécies, bem com a evolução histórica penal e as normas atuais vigentes no sistema brasileiro, trazendo os impactos causados que um crime virtual pode ocasionar a uma nação.

A metodologia apresentada foi suficiente para embasar todo conteúdo delituoso cibernético atual presente no brasil.

Este trabalho procurou fazer uma discussão entre os crimes virtuais atualmente, os novos tipos, leis e o perigo quanto a este delito podem ocasionar, trazendo assim uma contribuição para o meio acadêmico, virtual e também de quem acessa a internet.

Sugere-se que estudos posteriores possam se validar deste trabalho, visto que demonstra, após muitas pesquisas e estudo, o embasamento de conceitos doutrinários, juristas, leis e dados. Desse modo pode-se compreender o funcionamento do crime virtual no meio jurídico, a potencialidade que um crime virtual é capaz de alcançar e o acompanhamento das leis com novas práticas criminais, para que cada vez mais o crime digital vem ser combatido por todos.

Em síntese, é de suma importância tratar esse assunto (crimes digitais) gradativamente mais, tendo em vista que hoje o mundo é dependente do espaço virtual, haja vista que qualquer atividade que se faça, utiliza-se se desse meio, como numa simples compra de produtos na loja física ou virtual (feita pelo celular),

pagamentos, transferências, prestações de serviços, lazer, educação e entre outras atividades. Assim, o avanço tecnológico cresceu tanto a modo de atingir a todos, trazendo agilidade, comodidade, economicidade, praticidade, com esse mundo cada vez mais acelerado, precisando das informações e serviços para ontem, sendo exemplo: o pagamento de boletos, que antigamente o sujeito tinha que se deslocar até a lotérica para fazer o pagamento em dinheiro, mudando-se radicalmente hoje, no qual a pessoa faz o pagamento pelo celular do aplicativo de seu banco, em qualquer lugar que esteja conectado a rede de internet, sendo basicamente o celular um computado, podendo fazer tudo por ele. Então embora trouxesse todos esses confortos e praticidades, trouxe também a insegurança, tornando o ambiente virtual inseguro e perigoso, atrativo para os criminosos, devido a vulnerabilidade dos sistemas brasileiros e falta de conhecimento da população sobre esse tema, necessitando assim proteção e segurança, como mundo físico em que se tem policiamentos e seguranças.

Diante de tudo isso que foi dito, os crimes digitais devem ser vistos sob uma perspectiva, não podendo ser visto como um tipo qualquer, pois seus perigos e danos têm a potencialidade de serem catastróficos e irreversíveis, possibilitando não só prejuízos financeiros e econômicos, mas também danos psicológicos, físicos, a honra da pessoa; fechamentos de empresas, paralisação de hospitais, postos e até controle de uma nação.

Por isso é vital tratar sobre esse tema, uma vez que afeta a todos, precisando assim de aperfeiçoamento das leis, novos estudos, profissionais capacitados e adequados, para a segurança mínima de todos, já que, infelizmente o cidadão brasileiro e nosso sistema judiciário, legislativo e executivo, só acreditam e se importa quando é atingido, porém chegará um dia que não terá outra chance, assim é necessário de ação e impacto o quanto antes, para que todos possam usufruir das maravilhas benéficas que o mundo digital pode proporcionar.

REFERÊNCIAS

ANDRADE, Leonardo. **Cybercrimes na deep web: as dificuldades jurídicas de determinação de autoria nos crimes virtuais**: A internet cresce de forma ubíqua e decentralizada, diversos segmentos do conhecimento humanos foram tocados pelo tecido cibernético. Dessa forma, bens jurídicos tutelados estão dispostos nesse ambiente virtual, atraindo cada vez mais cybercriminosos.. [*S. l.*], 3 jun. 2015. Disponível em: https://jus.com.br/artigos/39754/cybercrimes-na-deep-web-as-dificuldades-juridicas-de-determinacao-de-autoria-nos-crimes-virtuais. Acesso em: 14 maio 2023.

ANDRADE, Walmar. **Marco Civil da Internet ? tudo o que você precisa saber sobre a lei fundamental da Internet**: O que é o Marco Civil da Internet e como advogados e empresas podem se adaptar para cumprir as disposições da Lei 12.965/2014. Confira o guia completo.. [*S. l.*], 2022. Disponível em: https://walmarandrade.com.br/marco-civil-da-internet/. Acesso em: 15 maio 2023.

ATAQUE hacker colossal atingiu 1milhão de PCs em 17 países, FBI investiga. São Paulo-SP, 5 jul. 2021. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/07/05/ataque-hacker-colossal-atingiu-1-milhao-de-pcs-em-17-paises-fbi-investiga.htm. Acesso em: 15 maio 2023.

ATAQUES de ransomware crescem e estimulam busca por segurança para armazenamento de dados: Solução desenvolvida pela Huawei é a primeira certificada com o mais alto nível do NIST Cybersecurity Framework na China. [*S. l.*], 3 jan. 2023. Disponível em: https://www.techtudo.com.br/noticias/2023/01/ataques-de-ransomware-crescem-e-estimulam-busca-por-seguranca-para-armazenamento-de-dados.ghtml. Acesso em: 15 maio 2023.

BABESCO, Lucas. **Marco Civil da Internet: entenda como ele afeta sua empresa**. [*S. l.*], 2018. Disponível em: https://blog.starti.com.br/marco-civil-da-internet/. Acesso em: 15 maio 2023.

BERTHOLDI, Juliana. **Crimes Cibernéticos**. Curitiba: Contentus, 2020. Disponível em: https://plataforma.bvirtual.com.br/Leitor/Publicacao/184412/pdf/0?code=niFPKovd5/qoq+9Cx6WParW9y6cX/6GoM1TEcHIvR/z/GO+ebqt/zokMGoQY7DcklCZqIN8v7eevmEZu3sRjyQ==. Acesso em: 14 maio 2023.

BOMFATI, Cláudio Adriano; KOLBE JUNIOR, Armando. **Crimes cibernéticos**. Curitiba-PR: Intersaberes, 2020. Disponível em: https://plataforma.bvirtual.com.br/Leitor/Publicacao/179734/pdf/1?code=9PCZuooFDs7v0Le6iQXwsNP5hMpAuU4bSDP13IyXecLsnJ1doN0mZWtvIZWE8E0mjo8M9AvnwcAjWSGLSZKGEw==. Acesso em: 15 maio 2023.

BRASIL é o 5º país do mundo mais afetado por crimes cibernéticos: País também está entre os 10 que mais sofrem ataques por ransomware, sistema malicioso que sequestra dados. [*S. l.*], 15 abr. 2023. Disponível em: https://tecnologia.ig.com.br/2023-04-15/brasil-quinto-pais-mais-afetado-crimes-ciberneticos.html. Acesso em: 14 maio 2023.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios TJ-DF. - **Recurso de Agravo: RAG 20130020161064 DF 0016973 10.2013.8.07.0000.** Tribunal de Justiça-DF. Rel.Gilberto Pereira de Oliveira. Brasília, DF, 2013. Disponível em : <https://www.jusbrasil.com.br/jurisprudencia/tj-df/116084135>. Acesso em 14 de maio de 2023.

BRASIL. **Constituição Da República Federativa Do Brasil De 1988.** Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 14 de maio de 2023.

BRASIL. **DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940 – CÓDIGO PENAL**. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em 15 de maio de 2023.

BRASIL. **LEI Nº 12.965, DE 23 DE ABRIL DE 2014.** Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 15 de maio de 2023.

BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018- Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 15 de maio de 2023

BRASIL. **LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em 15 de maio de 2023,

BRASIL. **LEI Nº 14.155, DE 27 DE MAIO DE 2021.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm>

CAPEZ, Fernando. **Curso de direito penal, v. 1:**: parte geral: arts. 1º a 120. 27. 27. ed. São Paulo: Saraiva Jur, 2023. v. 1. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786553626096/epubcfi/6/2[%3Bvnd.vst.idref%3Dbody001]!/4/2[cover-image]/2%4041:92. Acesso em: 14 maio 2023.

CAPEZ, Fernando. **Curso de direito penal, v. 2**: parte especial: arts. 121 a 212. 23. ed. São Paulo-SP: Saraiva Jur, 2023. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786553626126/epubcfi/6/2[%3Bvnd.vst.idref%3Dbody001]!/4/2[cover-image]/2%4050:77. Acesso em: 15 maio 2023.

CRESPO, Marcelo Xavier de Freitas. **Marcelo Xavier de Freitas**. [*S. l.*]: Saraiva Jur, 2011. Disponível em:

https://app.minhabiblioteca.com.br/reader/books/9788502136663/epubcfi/6/2[%3Bvnd.vst.idref%3Dcover]!/4/2/2%4051:41. Acesso em: 15 maio 2023.

DE FREITAS BERNARDES, Victor. DOS CRIMES VIRTUAIS COMETIDOS SE UTILIZANDO DO ANONIMATO DA DEEP WEB. *In*: DE FREITAS BERNARDES, Victor. **DOS CRIMES VIRTUAIS COMETIDOS SE UTILIZANDO DO ANONIMATO DA DEEP WEB**. Orientador: Prof. Me. André Luis de Paula Borges. 2016. Trabalho de Conclusão de Curso (Direito) - Universidade Católica de Brasília, São Paulo-SP, 2016. Disponível em: https://repositorio.ucb.br:9443/jspui/bitstream/123456789/9433/1/VictordeFreitasBernardesTCCGraduacao2016.pdf.pdf. Acesso em: 14 maio 2023.

DELEGACIAS Cibercrimes. [*S. l.*], 2023. Disponível em: https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em: 15 maio 2023.

ESTEFAM, André. **Direito penal, v. 2: parte especial**: arts. 121 a 234-C. 9. 9. ed. São Paulo-SP: Saraiva Jur, 2022. v. 2. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786555596564/epubcfi/6/2[%3Bvnd.vst.idref%3Dcover.xhtml]!/4/2[cover]/2%4050:77. Acesso em: 15 maio 2023.

FERNANDES, Mirian. **Leis de Privacidade online: uma viagem pelo tempo!**. [*S. l.*], 2021. Disponível em: https://blog.starti.com.br/leis-de-privacidade-na-internet/. Acesso em: 15 maio 2023.

FERRI, Thiago. **Gabriel Menino, do Palmeiras, vai à Justiça após insinuação de que está envolvido em esquema de apostas**: Um influenciador é um dos que estão na mira da equipe jurídica do meio-campista. Lance em questão é a saída de bola no segundo tempo do empate com o Vasco, em jogo do Brasileirão. São Paulo-SP, 9 maio 2023. Disponível em: https://ge.globo.com/futebol/times/palmeiras/noticia/2023/05/09/gabriel-menino-do-palmeiras-vai-a-justica-apos-insinuacao-de-que-esta-envolvido-em-esquema-de-apostas.ghtml. Acesso em: 15 maio 2023.

GONÇALVES, Victor Eduardo Rios. **Curso de direito penal, v. 1:**: parte geral (Arts. 1º a 120). 6. ed. São Paulo: Saraiva Jur, 2022. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786553623118/epubcfi/6/2[%3Bvnd.vst.idref%3Dcover.xhtml]!/4/2[cover]/2%4050:77. Acesso em: 14 maio 2023.

GRECO, Rogerio. **Curso de direito penal, v. 1:**: artigos 1º a 120 do Código penal. 25. ed. Rio de Janeiro: Atlas, 2023. v. 1. Disponível em: https://pergamum.ufms.br/pergamum/biblioteca_s/minhabiblioteca.php?arquivo=aHR0cHM6Ly9pbnRlZ3JhZGEubWluaGFiaWJsaW90ZWNhLmNvbS5ici9ib29rcy85Nzg2NTU5Nzc0NTkz. Acesso em: 14 maio 2023.

GRECO, Rogerio. **Curso de direito penal, v. 1**: artigos 1º a 120 do Código penal. [*S. l.*]: Atlas, 2023. v. 1.

GRECO, Rogerio. **Curso de direito penal, v. 2**: artigos 121 a 212 do Código Penal. 20. ed. [*S. l.*: *s. n.*], 2023. v. 2. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786559774579/epubcfi/6/2[%3Bvnd.vst.idref%3Dcover]!/4/2/2%4051:53. Acesso em: 15 maio 2023.

GRIMES, Roger. **Manual de proteção contra ransomware**: como criar um plano de segurança cibernética. Porto Alegre-RS: Bookman, 2022. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9788582605851/epubcfi/6/6[%3Bvnd.vst.idref%3Dfr.xhtml]!/4[ross]/2/4/2%4051:58. Acesso em: 15 maio 2023.

INTERNET já é acessível em 90,0% dos domicílios do país em 2021. [*S. l.*]: Estatísticas Sociais, 16 set. 2022. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021. Acesso em: 14 maio 2023.

JBS diz que pagou US$ 11 milhões em resgate a ataque hacker em operações nos EUA: Empresa afirmou que pagamento foi feito para reduzir problemas relacionados à invasão e evitar vazamento de dados.. [*S. l.*], 9 jun. 2021. Disponível em: https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-pagou-11-milhoes-em-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghtml. Acesso em: 14 maio 2023.

JESUS, Damásio de. **Direito penal 2**: parte especial: crimes contra a pessoa a crimes contra o patrimônio (arts. 121 a 183). 36. ed. São Paulo-SP: Saraiva, 2020. v. 2. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9788553619863/pageid/0. Acesso em: 15 maio 2023.

JESUS, Damásio de. **Manual de crimes informáticos**. São Paulo: Saraiva Jur, 2016. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9788502627246/epubcfi/6/4[%3Bvnd.vst.idref%3Dcatalografica.html]!/4[abertura]/2/10/1:58[004%2C.3]. Acesso em: 14 maio 2023.

NERY , Carmen; BRITTO , Vinícius. **Internet já é acessível em 90,0% dos domicílios do país em 2021**. [*S. l.*]: Estatísticas Sociais, 16 set. 2022. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021. Acesso em: 14 maio 2023.

NUCCI, Guilherme de Souza. **Curso de direito penal, v. 2**: parte especial: arts. 121 a 212 do Código Penal. 7. ed. Rio de Janeiro-RJ: Forense, 2023. v. 2. Disponível em:

https://app.minhabiblioteca.com.br/reader/books/9786559647217/epubcfi/6/2[%3Bvnd.vst.idref%3Dhtml1]!/4/2/2%4048:79. Acesso em: 15 maio 2023.

OLIVEIRA, Jôline Cristina. **O CIBERCRIME E AS LEIS 12.735 E 12.737/2012**. 2013. Trabalho de Conclusão de Curso (Direito) - UNIVERSIDADE FEDERAL DE SERGIPE CENTRO DE CIÊNCIAS SOCIAIS APLICADAS, São Cristóvão ? SE, 2013. Disponível em: https://www.conteudojuridico.com.br/open-pdf/cj045489.pdf/consult/cj045489.pdf. Acesso em: 15 maio 2023.

ORGANIZAÇÕES diferentes pedem estratégias para proteção de dados diferentes: A criptografia tem se mostrado uma necessidade para todo um mercado que busca mais segurança sobre os seus dados. Conforme as habilidades dos hackers vão se tornando mais sofisticadas, as soluções tradicionais vão se tornando também mais defasadas, gerando uma demanda gigantesca e diária de bons recursos de criptografia, de modo que essas empresas possam reduzir os riscos para seus sistemas.. [*S. l.*], 2020. Disponível em: https://www.privacytools.com.br/organizacoes-diferentes-pedem-estrategias-para-protecao-de-dados-diferentes/. Acesso em: 14 maio 2023.

PANNAIN, Camila Nunes; PEZZELLA, Maria Cristina Cereser. LIBERDADE DE EXPRESSÃO E HATE SPEECH NA SOCIEDADE DA INFORMAÇÃO. *In*: PANNAIN, Camila Nunes; PEZZELLA, Maria Cristina Cereser. **LIBERDADE DE EXPRESSÃO E HATE SPEECH NA SOCIEDADE DA INFORMAÇÃO**. 2015. Tese (Direito) - Universidade Federal de Santa Maria, [*S. l.*], 2015. Disponível em: https://periodicos.ufsm.br/REDESG/article/view/19432/pdf. Acesso em: 15 maio 2023.

PAYÃO, Felipe. **Lojas Renner sai do ar após infecção com ransomware**. [*S. l.*], 19 ago. 2021. Disponível em: https://www.tecmundo.com.br/seguranca/223412-lojas-renner-sai-ar-infeccao-ransomware.htm. Acesso em: 14 maio 2023.

PEREIRA, Emanuela de Araújo. **Reflexões sobre o crime de invasão de dispositivo informático e o PL 879/22**. [*S. l.*], 5 maio 2023. Disponível em: https://www.conjur.com.br/2023-mai-05/emanuela-pereira-invasao-dispositivo-informatico-pl-879#author. Acesso em: 15 maio 2023.

POLÍCIA faz lista de golpes mais aplicados pelos estelionatários em 2022. Curitiba-PR: RICtv, 2023. Disponível em: https://www.youtube.com/watch?v=GL6nXVFxD2Y&t=610s. Acesso em: 15 maio 2023.

ROCHA, Lucas. **Estudo: divulgação não autorizada de imagens íntimas impacta saúde mental de mulheres**: Pesquisa conduzida por especialistas da Fiocruz Minas aponta que mulheres sofrem danos como depressão, fobias, transtorno alimentar e dificuldades de se relacionar socialmente. São Paulo-SP, 29 mar. 2022. Disponível em: https://www.cnnbrasil.com.br/saude/estudo-divulgacao-nao-autorizada-de-imagens-intimas-impacta-saude-mental-de-mulheres/. Acesso em: 14 maio 2023.

ROHR, Altieres. **Paciente morre após hospital que sofria ataque cibernético suspender atendimento na Alemanha**: Autoridades que investigam o caso avaliam possibilidade de denunciar invasores por homicídio.. [*S. l.*], 21 set. 2020. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2020/09/21/paciente-morre-apos-hospital-que-sofria-ataque-cibernetico-suspender-atendimento-na-alemanha.ghtml. Acesso em: 14 maio 2023.

RS: adolescente comete suicídio após ter fotos íntimas divulgadas na web. [*S. l.*], 20 nov. 2013. Disponível em: https://www.terra.com.br/noticias/brasil/policia/rs-adolescente-comete-suicidio-apos-ter-fotos-intimas-divulgadas-na-web,1b975df8bd472410VgnVCM5000009ccceb0aRCRD.html. Acesso em: 14 maio 2023.

SEQUESTRO digital: veja como agem as quadrilhas de ?ransomware?. [*S. l.*]: Fantástico, 2021. Disponível em: https://globoplay.globo.com/v/9716455/. Acesso em: 15 maio 2023.

SOARES DE MATTOS, Marília. **Núcleo de combate aos cibercrimes**. Curitiba-Pr: Contentus, 2020. Disponível em: https://plataforma.bvirtual.com.br/Leitor/Publicacao/186529/pdf/0?code=hJhPzCHmE7R9Cn9hiOxp76VvrMMLcwUi/8aLI5H70zGuaxb3zRbGZ6ppTCo9yK6gSuujkR0++ogvI/XdmGHY1A==. Acesso em: 14 maio 2023.

TEIXEIRA, Tarcísio. **Direito digital e processo eletrônico**. 6. ed. rev. São Paulo: Saraiva Jur, 2022. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786555596946/epubcfi/6/2[%3Bvnd.vst.idref%3Dcover.xhtml]!/4/2[cover]/2%4050:77. Acesso em: 14 maio 2023.