PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
PROJETO DE TRABALHO DE CURSO I

CRIMES VIRTUAIS NO BRASIL: ELEMENTOS CONFIGURADORES

ORIENTANDO – DANIEL FREDERICK E SILVA SALUSTIANO
ORIENTADOR – PROF. GOIACY CAMPOS DOS SANTOS DUNCK

GOIÂNIA
2021

DANIEL FREDERICK E SILVA SALUSTIANO

CRIMES VIRTUAIS NO BRASIL: ELEMENTOS CONFIGURADORES

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).

Prof. Orientadora – Goiacy Campos dos Santos Dunck

Prof. Convidado – Luiz Carlos de Pádua Bailão

GOIÂNIA

2021

DANIEL FREDERICK E SILVA SALUSTIANO

CRIMES VIRTUAIS NO BRASIL: ELEMENTOS CONFIGURADORES

Data da Defesa: 09 de junho de 2021.

BANCA EXAMINADORA

_____

Orientador: Prof. Goiacy Campos dos Santos Dunck

Nota

_____

Examinador Convidado: Prof. Luiz Carlos de Pádua Bailão

Nota

SUMÁRIO

CRIMES VIRTUAIS NO BRASIL: ELEMENTOS CONFIGURADORES

Daniel Frederick e Silva Salustiano

Resumo

O Direito está diretamente ligado a sociedade e a evolução da mesma, conforme a sociedade se desenvolve o direito tem por objetivo de acompanhá-la. Assim, com o avanço tecnológico, fez-se necessário que o Direito tutele aqueles que são vítimas dos crimes que passaram a ser perpetuados em ambiente virtual. O presente artigo buscará verificar as formas de se analisar um crime virtual, pontuar os crimes que são praticados via computador e internet, a busca de sua autoria, suas peculiaridades e sua evolução histórica, e expor a legislação em relação a crimes virtuais, analisar os novos institutos do Direito digital e como a mesma age em cada crime e qual codificação é usada.

Palavras-chave: ambiente virtual**;** cibercrime; direito.

INTRODUÇÃO

A informática oferece ambiente fértil e ilimitado para práticas ilícitas contra os direitos alheios, tipificados como crimes virtuais. A legislação brasileira, apesar de ser grande e complexa, carece de normas jurídicas que reprimam os diversos aspectos do crime virtual, disseminados em cibe terrorismo, fraudes online, invasão de sistemas, pornografia eletrônica, pirataria, etc., por este e outros motivos se faz necessária a discussão acerca dos crimes virtuais, como será feito neste artigo através da apresentação dos objetivos seguidos dos problemas e das hipóteses. Se baseia em pesquisas bibliográficas, artigos, documentos e pesquisas, objetivando conhecer os pensamentos disponíveis sobre o tema.

O direito tem uma relação direta com a sociedade e com o seu desenvolvimento, o direito visa acompanhá-lo. Portanto, com o avanço da tecnologia, essas leis são necessárias para a proteção das vítimas de crimes que existem há muito tempo em ambientes virtuais. Este artigo tem como objetivos a verificação e análise do crime virtual, encontrar seu autor, sua particularidade e sua evolução histórica, e revelar a legislação relacionada ao

crime virtual, seu comportamento em cada tipo de crime e a tipificação utilizada, pois a falta do mesmo que é encontrado hodiernamente no ordenamento jurídico brasileiro faz-se gerar uma lacuna legislativa que encoraja a continuidade da prática delitiva, tornando assim difícil a punição daqueles que se aproveitam dessa falta de previsão legal.

Com o avanço tecnológico e a evolução do mundo globalizado a distância de troca de informações foi encurtada se tornando bem mais rápido e fácil. A relação entre essas pessoas é estabelecida principalmente por meio de dispositivos eletrônicos conectados à Internet. Diferentes culturas, diferentes raças e pessoas completamente diferentes. E novas relações começaram a aparecer e se formar novos relacionamentos. Com o desenvolvimento tecnológico, o relacionamento se estreitou. É por isso que a lei deve se adaptar a esta nova realidade e acompanhar a segurança da informação para que esta nova sociedade digital não se transforme num pesadelo para quem a utiliza e, em última análise, prejudique as suas imagens e / ou património. Desde a sua criação, o direito tem procurado acompanhar o desenvolvimento da sociedade, portanto, com o desenvolvimento da sociedade, o direito deve encontrar um mecanismo que atenda às suas necessidades emergentes ao longo do tempo, e ajustá-lo quando necessário. Assim, com o avanço da tecnologia e sua inserção no cotidiano das pessoas, fez-se imperioso o Direito tutelar as relações que passaram a ser desenvolvidas em ambiente virtual.

Diante do rápido crescimento tecnológico vivenciado pela coletividade, hodiernamente, bem como a crescente onda de descobertas neste campo, dentre elas, a internet como uma das principais inovações dos últimos séculos, o Direito acaba por não ser tão efetivo a ponto de evoluir no mesmo ritmo que a sociedade, em razão do Processo Legislativo brasileiro ser demasiadamente moroso. Fato este que explica o problema da falta de tipificação legal dos crimes virtuais.

Agora que mais e mais pessoas estão conectadas à Internet por meio de laptops, smartphones e tablets, o cibercrime é uma ameaça maior e é um dos programas mais lucrativos do mundo do crime. Existem muitos tipos de crimes cibernéticos, por exemplo os crimes isolados, como a instalação de um vírus que pode roubar seus dados pessoais e crimes persistentes, como bullying virtual,

extorsão, distribuição de pornografia infantil e organização de ataques terroristas.

O interesse por esse assunto surgiu por se tratar de um tema atual e cada vez mais presente no cotidiano das pessoas. Ademais, esta questão ainda gera muitas dúvidas no tocante às formas de resguardar os direitos daqueles que são lesados através de qualquer meio virtual, bem como quem teria competência para processar e julgar os crimes realizados por esse meio.

O método de pesquisa a ser empregado no desenvolvimento do presente estudo será o dedutivo, iniciando-se pela análise histórica do surgimento dos crimes virtuais, bem como seus conceitos e os crimes que ocorrem no meio cibernético. Ressalta-se que o método dedutivo tem como objetivo de explicar o conteúdo das premissas, através de uma cadeia de estudo em ordem descendente, partindo-se dos conceitos gerais aos particulares, no intuito de alcançar uma conclusão final.

Este estudo se desenvolverá a partir de uma pesquisa teórica acerca do assunto, levantamentos bibliográficos, revistas, revistas eletrônicas, artigos, entre outros recursos que serão amplamente explorados.

Outrossim, será também aplicado o método comparativo, visto que será analisado as diferenças entre a legislação nacional e internacional, comparando-se, assim, as linhas de raciocínios existentes nas referidas, levando o leitor técnico ou leigo a melhor se situar do assusto em que pretendemos nos aprofundar.

O presente artigo foi objeto de uma pesquisa frente aos principais autores que discorrem sobre a relação do Direito Penal com os crimes que ocorrem em ambientes virtuais, utilizando para tanto o método dedutivo, sendo que foi feita uma pesquisa bibliográfica a partir de um material que já versava sobre o assunto, constituído de livros e artigos disponíveis em sítios na internet.

O artigo também versará sobre questões como a evolução histórica e os conceitos dos crimes virtuais, além de analisar a classificação de referidos crimes, sua autoria e o que a legislação nacional e internacional versam sobre o assunto.

SEÇÃO I- Evolução histórica dos crimes virtuais.

Na década dos anos 70 nos Estados Unidos foi desenvolvido um sistema para o puro e único uso militar, ele se baseava em comunicação, transmissão e armazenamento de dados, só que mais tarde veio a se tornar o que hoje conhecemos como internet, podendo até se dizer que ele se tornou uma das mais magnificas inovações desses dois últimos séculos.

Alguns anos depois os crimes virtuais já eram conhecidos, tendo a eclosão de várias modalidades de crimes e até o surgimento do termo Hacker para aqueles que invadiam e furtavam sistemas e softwares, mas só na década dos anos 80 que eles consolidaram com a criação dos famosos “vírus” que eram ferramentas ou arquivos que disseminavam anarquia e confusões nos computadores, podendo até ser possível controlar e roubar dados.

A pirataria veio forte também, se tratando do uso, fabricação e o compartilhamento ilegítimo de bens, ou seja, de softwares, cópia de vídeos, filmes e até mesmo músicas, tal serviu como a porta para o crime de pedofilia e abusos sexuais na internet que vem atualmente ainda se demonstrando uma ameaça muito constante no meio virtual, sobre esse assunto temos as palavras de Kalb,

> Alguns dos motivos para que o abuso sexual e a publicação de fotos e vídeos pornográficos aumentasse significativamente foram a “confidencialidade de usuários de salas de bate-papo; hospedagem de *sites* nos mais variados países, dificultando a identificação e a prisão dos responsáveis; pouca legislação específica para crimes de informática etc. […]. (EUA, KALB, 2008).

Com o aumento dos crimes virtuais a preocupação em localizar, identificar os culpados para poder levá-los a justiça se tornou prioridade juntamente com a preocupação em relação a proteção dos usuários da internet. A procura pelos criminosos possuem muitas variáveis por se tratar de um ambiente globalizado, onde os acessos e os crimes poderiam vir de qualquer parte do mundo, se tornando quase impossível capturar e julgar todos os infratores, por isso a atenção em fortificar a proteção de dados se tornou prioridade também. Kevin Mitnick(citação) foi um dos mais famosos Hackers do mundo, ele atualmente vem treinando e conscientizando com seu livro “A Arte de Enganar”, que traz sobre a facilidade que se tem para roubar dados de usuários na internet e da fragilidade dos usuários por não terem conhecimento e educação na área virtual e informática os tornando negligentes com suas informações pessoais.

> A história ensina que o progresso é inerente ao homem, e que fomos feitos para evoluir e inovar e incondicionalmente buscar o avanço, contudo com muitos avanços pode-se ter também o retrocesso, em que no meio de tantos benefícios, indivíduos procuram oportunidades para se beneficiar com a falta de conhecimento do que é novo. Desta forma nos deparamos com a internet, e com os crimes que a envolvem. (Brasil, CRUZ, 2018)

O objetivo inicial da Internet era o armazenamento e o transporte de dados sigilosos entre os governos, tendo sua importante e notável participação naquela época delicada, mas, com o término da Guerra Fria, veio a ser utilizada na área da educação em universidades, onde deu se a popularização desse instrumento revolucionário.

Apenas em 1995 que a internet começou a ser usada no Brasil, por intermédio da Agência Nacional de Telecomunicações (Anatel), os serviços de internet eram regulados pela **Norma 004/95**, qual seja a norma de **Uso de Meios da Rede Pública de Telecomunicações e os Serviços de Conexão à Internet**, que dispõe da definição de Internet como:

> Nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores, bem como o "software" e os dados contidos nestes computadores. (BRASIL, 1995)

Por se tratar de um ambiente muito amplo e versátil a internet constantemente teve seus problemas com relação a segurança de seus sistemas, e sempre houve aqueles que exploraram essa fragilidade, Fabrizio Rosa (2002, p. 53-54) dá o conceito desses crimes como sendo:

> A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. o „Crime de Informática" é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. assim, o „Crime de Informática "pressupõe does elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. a expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à

> honra, ao patrimônio público ou privado, à Administração Pública etc. (Brasil, ROSA, 2002)

Com a velocidade que essa tecnologia veio evoluindo paralelamente os cibercrimes também, a legislação por um tempo se manteve inerte, se fazendo necessário a criação da mesma para a resolução de impunidade dos crimes, criando assim a **Convenção sobre Criminalidade do Conselho Europa** com o objetivo para a ampliação das leis que previnem tal delito.

No Brasil, os crimes virtuais só ficaram em evidências quando ocorreram várias invasões em sites governamentais. Dando assim o reconhecimento popular e a necessidade de soluções legislativas para tal insegurança, decretando, na Constituição Federal de 1988, normas relacionadas à incumbência do Governo em questões de cibercrimes.

No momento atual existem basicamente duas leis que discorrem e legislam sobre cibercrimes. A **Lei 12.735/2012 e a 12.737/2012**, popularmente renomada como a Lei Carolina Dieckman, por ter sido implementada após ter sido expostas fotos intimas roubadas do próprio computador da atriz. Este ocorrido novamente mostrou-se a necessidade de nova regulamentação sobre esses crimes, tipificando muitas condutas ilícitas que ocorriam no mundo virtual e prevendo penas para as mesmas.

Seção II- Configuração jurídica e *modus operandi.*

Os crimes virtuais são atitudes ilícitas cometidas por indivíduos que se aproveitam das brechas dos sistemas digitais, e da fragilidade dos usuários leigos, para praticarem suas fraudes, podendo ser feitas através de dispositivos como o celular, tablet, notebook ou computador. O conceito de crimes virtuais diverge conforme cada autor, porém o fundamento resume-se ao meio empregue para o delito ser a internet e o dispositivos que fazem uso da mesma.

O delinquente pode atingir a vítima com crimes contra a pessoa, sendo eles calúnia, injúria, difamação, discriminação ou preconceito. Ou ainda crimes contra o patrimônio pessoal ou público, estelionato, furto etc.

Podendo ser classificados de duas maneiras crimes puros e crimes próprios. A primeira divisão tem o objetivo de atingir o sistema de um

computador, seja a parte física ou de dados, geralmente praticado por hackers podendo se dividir em crimes mistos em que o alvo não é o computador, mas os bens da vítima, ou seja, a internet é utilizada como meio para realizar o crime, como, por exemplo, transferências ilícitas de bens e/ou valores, crimes comuns são aqueles que utilizam a internet para realizar o crime, sendo assim reconhecidos pela lei, como o caso da pornografia infantil que já é abordado no Estatuto da Criança e do Adolescente. A segunda divisão compreende a seguinte classificação: crimes próprios aqueles praticados exclusivamente por meio de computadores e crimes impróprios aqueles que atingem o bem comum sendo o meio virtual apenas uma das formas de execução do crime, podendo ser praticado por outros meios.

Há ainda quem ousa em aplicar golpes em departamentos públicos ou grandes empresas, nas palavras de Frederico Cattani, advogado criminalista, professor e especializado em crimes econômicos, temos que: “Ter um plano para casos de ataque cibernético é igual a manter treinamentos para caso de incêndio”, e expõe ainda que:

> Os agentes e firmas que lidam com matérias sensíveis ao empresariado e com impacto no mercado econômico são alvos recorrentes desses crimes e, por isso, estão investindo cada vez mais em profissionais e sistemas para manter suas bases de dados seguras. Trata-se de uma política interna de planejamento contra os crimes virtuais. Deve-se ter em mente que essa criminalidade está muito à frente das regras penais atuais, e a velocidade de uma investigação policial não acompanha a contenção de prejuízos em um cenário de perda ou sequestro de informações. (Brasil, CATTANI, 2018)

Diferente dos outros crimes, os crimes virtuais são executados por alguém que contém habilidades e experiência tecnológica em aparelhos eletrônicos que conectam à internet, se proteger destes crimes não é fácil, porém há algumas ações de segurança que podem ajudar, como evitar fazer downloads de sites suspeitos ou desconhecidos, verificar com cautela a genuinidade de e-mails, principalmente de remetentes desconhecidos, jamais fornecer dados, logins e senhas.

De acordo com a Revista Exame, o Brasil é o 4º país com mais usuários conectados à internet no mundo, o que nos remete ao problema da impunidade e o anonimato em que os hackers se encontram. Um relatório do Norton Cyber Security começou no início de 2018 e listou o Brasil como o país com o segundo maior número de casos de crimes cibernéticos, perdendo apenas para a China.

Em 2017, aproximadamente 62 milhões de brasileiros foram afetados por alguns crimes cibernéticos. Os usuários de smartphones e aplicativos WhatsApp são os maiores alvos dos cibe criminosos. Phishing é a prática mais comum usada por golpistas e inclui o envio de conversas ou mensagens falsas com links fraudulentos. Por exemplo, quando esse link é aberto, os dados do usuário podem ser roubados ou apontar para uma loja online falsa.

Sergio Marcos Roque (2007, p. 25), dá o conceito de crimes virtuais da seguinte forma “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material”.

II.II- Modalidades

Existem diversas possibilidades de se cometer um crime virtual, por a internet estar em constante evolução, inova também a todo momento novas modalidades de crimes virtuais, dentre estes os principais são:

Furto

O crime de furto, tipificado no artigo 155 do Código Penal “Subtrair, para si ou para outrem, coisa alheia móvel”, se inicia através do um furto de informações e dados, geralmente logins e senhas, que futuramente serão utilizados para subtrair valores, geralmente através de banklines que são sites ou aplicativos de bancos, fazendo transferências, pagamentos, etc.

O furto não deve ser confundido com o estelionato que está descrito no artigo 171 também do Código Penal, “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”, pois no estelionato, a vítima sabe que está transferindo a posse de seu bem para outro, porém, no furto, ela não tem a consciência de que a posse de seu bem está passando para outro. Nas palavras do Doutrinador Damásio E. De Jesus:

> No furto, a fraude ilude a vigilância do ofendido, que, por isso, não tem conhecimento de que o objeto material está saindo da esfera de seu patrimônio e ingressando na disponibilidade do sujeito ativo. No estelionato, ao contrário, a fraude visa a permitir que a vítima incida em erro. Por isso, voluntariamente se despoja de seus bens, tendo consciência de que eles estão saindo de

> seu patrimônio e ingressando na esfera de disponibilidade do autor. (BRASIL, DAMÁSIO)

O crime de estelionato pode também ocorrer virtualmente também, quando a vítima é enganada através de *e-mails* enviados pelos criminosos que se passam por sites de lojas, bancos entre outros, solicitando dados como informações de cartões de crédito, dados de conta bancária, logins e senhas etc.

Difamação e injúria

Estas modalidades estão descritas, respectivamente, nos artigos 139 e 140 do Código Penal, sendo a difamação “Difamar alguém, imputando-lhe fato ofensivo à sua reputação” e a injúria “Injuriar alguém, ofendendo-lhe a dignidade ou o decoro”. Aqui entramos no campo das fake news, onde o criminoso busca ofender a vítima através da internet, seja publicando algo em redes sociais, compartilhando imagens editadas etc.

Invasão

Descrita no artigo 154 do Código Penal:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Ocorre geralmente através de “*malware*” que é a abreviação de *malicious software*, que viabiliza o acesso do criminoso ao seu dispositivo informático, o “*malware*” se instala através de *downloads* de fontes não confiáveis, assim, todos os dados que a vítima possui em seu dispositivo passa a ser também de conhecimento do delinquente, permitindo assim que ele obtenha vantagens ilícitas sob a vítima.

Compartilhamento de imagem íntima

Responde também por difamação ou injúria quem compartilha imagem íntima de alguém, e ainda por danos morais baseado no artigo 5**º,** inciso V da Constituição Federal, este crime causa prejuízos imensuráveis que perduram por toda a vida da vítima. Se a imagem compartilhada for de uma pessoa menor de 18 anos de idade, o crime se enquadra no artigo 241º A do Estatuto da Criança e do Adolescente, que diz:

> Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

O compartilhamento de imagem íntima vulgarmente conhecido como *nudes,* é uma prática comum pelos brasileiros, o que torna esse crime frequente. Os crimes virtuais são tão frequentes que existem delegacias especializadas para tais práticas.

Por mais que não pareça, os crimes cibernéticos, que são crimes cometidos pela internet, são tão comuns que já existem até delegacias próprias para a realização de denúncias.

Seção III- Legislações brasileiras acerca de crimes virtuais.

A informática oferece ambiente fértil e ilimitado para práticas ilícitas contra os direitos alheios, tipificados como crimes virtuais. A legislação brasileira, apesar de ser grande e complexa, carece de normas jurídicas que reprimam os diversos aspectos do crime virtual, disseminados em cibe terrorismo, fraudes online, invasão de sistemas, pornografia eletrônica, pirataria etc. Assim, se percebe que cada vez mais os crimes digitais vêm ocorrendo e assustando a população brasileira e mundial, esse projeto de pesquisa tem como fundamento alertar a população sobre uma realidade crescente e que precisa ser discutida e combatida o quanto antes, pois com leis antigas e pouco voltadas para a área tecnológica, as brechas são imensas, fazendo com que muitas das vezes, esses hackers passem impunes.

Segundo pesquisa da empresa Symantec, 80% dos brasileiros acreditam que não haverá punição para um crime cometido pela internet, nem que sua autoria será identificada. O estudo é indicativo de que o brasileiro não confia nos meios de repressão ao crime digital e que potenciais criminosos se sentem confortáveis para praticar seus delitos, sob o véu do anonimato e a certeza da impunidade. O Direito está diretamente ligado a sociedade e a evolução da mesma, conforme a sociedade se desenvolve o direito tem por objetivo de acompanhá-la. Segundo pesquisa TIC Domicílios, 126,9 milhões de pessoas usaram a rede regularmente em 2018, o equivalente a 70% da população brasileira. Assim, com o avanço tecnológico, fez-se necessário que o Direito

tutele aqueles que são vítimas dos crimes que passaram a ser perpetuados em ambiente virtual.

A Lei nº 12.735, de 2012, estabeleceu a estrutura e profissionalização da Polícia Judiciária para o combate ao crime cibernético, e por meio do inciso II do § 3º de seu artigo 20, objetivando a cessação de transmissões radiofônicas, televisivas, eletrônicas ou publicações por qualquer meio da prática, indução ou incitação de discriminação de raça, cor, etnia, religião ou procedência nacional.

O Decreto nº 7.962 de 2013 regulamenta a Lei de Defesa do Consumidor relacionada ao comércio eletrônico e as chamadas vendas online, e tem como objetivo proteger o consumidor da insatisfação com os produtos adquiridos e possíveis fraudes.

Os fornecedores são obrigados, por exemplo, a fornecer nomes de vendas e números de CNPJ em locais facilmente visíveis nos sites de vendas e a fornecer aos consumidores endereços físicos e eletrônicos. O Decreto também criou regras específicas para ofertas nos sites de compra coletiva e obrigou a apresentação de sumário do contrato ao consumidor antes da celebração do mesmo, ficando também o fornecedor responsável por informar os meios para o direito de arrependimento da compra pelo consumidor.

De grande relevância, o Marco Civil da Internet, Lei 12.965/2014, trouxe diversas inovações, dentre elas estão:

Garantia da liberdade de expressão, comunicação e manifestação de pensamento, na Internet, nos termos da Constituição Federal;

Proteção da privacidade e proteção dos dados pessoais, sendo vedada a utilização comercial de dados pessoais dos internautas, sem consentimento expresso do usuário; Neutralidade da rede, não podendo os provedores de acesso discriminar ou privilegiar determinados tipos de conteúdo, tratando de forma isonômica quaisquer pacotes de dados;

Aplicação da Lei brasileira para provedores sediados no exterior; Quebra de dados ou informações particulares dos usuários, assim como a retirada de conteúdos de sites ou redes sociais só ocorrerão mediante determinação judicial. Exceção feita aos casos de “pornografia de vingança”, quando fotos ou conteúdos íntimos de uma pessoa são vazados para a rede. Nesse caso, a própria vítima da violação da intimidade poderá solicitar a retirada diretamente a quem estiver hospedando tal conteúdo;

Partes interessadas poderão requerer ao juiz, com o propósito de formar prova em processo judicial cível ou penal, que ordene ao responsável pela guarda, o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

A legislação brasileira carece de leis específicas para tipificar os crimes virtuais, e não podemos usar analogia para prejudicar o réu, só para beneficiar. Atualmente contamos apenas com duas leis para crimes virtuais, uma delas é a lei 12.737, de 30 de novembro de 2012, popularmente conhecida como Lei Carolina Dieckmann, criada após o computador de Carolina sofrer uma invasão, e ter sido copiado dele fotos e conversas íntimas que foram divulgados na internet.

O artigo 154-A estabelece a celebridade de incriminar o agente que possa burlar os mecanismos de segurança, adulterando, invadindo ou ate mesmo destruindo a privacidade de terceiros, bem como a operação de vulnerabilidade com a finalidade de adquirir vantagem ilegais. Contudo, este dispositivo exige a necessidade de que o mecanismo de segurança desse aparelho seja violado indevidademente, definindo, portanto, como fato atípico se inexistente tal mecanismo de segurança. Os artigos 154-A e 154-B, dizem o seguinte:

> Invasão de dispositivo informático
> **Art. 154-A**. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.
> 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I – Presidente da República, governadores e prefeitos;
> II –Presidente do Supremo Tribunal Federal;

> III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal;
> IV – Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
> Ação penal
> **Art. 154-B**. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime for cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.
> Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.

Crimes considerados menos graves, como os da seção 154-A "Invasão de dispositivo informático" terá a pena de três meses a um ano de detenção e multa de trânsito. Por outro lado, as condutas mais danosas, como a obtenção por invasão de conteúdo "Comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas" também pode ser condenado a seis meses a dois anos de prisão, além de multa.

Já os artigos 266 e 298 trazem que:

> **Art. 266** – Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento.
> Pena – detenção, de um a três anos, e multa.
> 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> 2º Aplicam-se as penas em dobro se o crime for cometido por ocasião de calamidade pública.
> Falsificação de documento particular
> **Art. 298** – Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
> Pena – reclusão, de um a cinco anos, e multa.
> Falsificação de cartão
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

Com relação ao crime cibernético de pornografia infantil, o Estatuto da Criança e do Adolescente conta com o artigo 241 para tratar com rigor os crimes nesse âmbito. Em relação ao bullying na internet, a Lei Nº 13.185 de 2015 aborda perfeitamente essa questão. No que diz respeito a preconceito de raça ou cor, temos o artigo 20 da Lei Nº 7.716 de 1989.

Falsificação de documentos nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime for cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

A outra lei também sancionada em 30 de novembro de 2012 é a Lei 12.735, que trata sobre a necessidade as delegacias especializadas em crimes virtuais, e traz em seu artigo 4º: “Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

CONCLUSÃO

A uma, extrai deste artigo científico que a prática de crimes virtuais é muito comum no Brasil, que esse tipo de crime é uma modalidade que evolui em paralelo à tecnologia, e estamos vivendo na época da mesma, ou seja, os crimes virtuais sofrem uma evolução exacerbada pois surgem novas modalidades e são atualizadas as existentes à medida em quem a tecnologia evolui, e como a tecnologia evolui muito rápido, a legislação carece de celeridade para acompanhar os delitos.

Ainda, no mundo virtual há uma sensação muito grande de anonimato, fazendo com que o criminoso se sinta escondido da justiça, o que faz do crime virtual ser uma prática fácil a qualquer tipo de pessoa, pois não há a violência que existe no crime de roubo, por exemplo, geralmente é um crime praticado de dentro de casa, sentado em um computador.

Finalmente, em se tratando do nosso país, não possuímos um amparo legislativo muito amplo, contamos apenas com duas leis específicas para tratarmos dos crimes virtuais, fazendo com que os responsáveis pela aplicação da lei tenham que se empenhar e esquadrinhar as outras legislações existentes para dar o devido cumprimento legal da justiça.

Os avanços conseguidos pelas leis aqui elencadas, dividem especialistas da área jurídica. Uns enfatizam a necessidade de uma lei específica de combate aos crimes cibernéticos mais abrangente e detalhada. Citam como exemplo crimes como ameaça, calúnia, injúria e difamação. A repercussão de tais crimes é muito maior quando praticados por meio virtual, e as penas brandas em relação aos prejuízos e transtornos ocasionados às vítimas, uma vez que as sentenças estão previstas por artigos do Código Penal, que é de 1940, retratando uma realidade de um mundo completamente diferente.

Para outros especialistas, entretanto, as leis criadas são suficientes quando aliadas a legislação já existente, faltando desenvolvimento tecnológico para as nossas polícias e órgãos públicos responsáveis pela fiscalização e controle do mundo virtual no país, poderem identificar e punir os criminosos cibernéticos com maior precisão, facilidade e rapidez.

REFERÊNCIAS

AMARGO Aranha Filho, Adalberto José Queiroz Telles de; “Crimes na Internet e a legislação vigente”; artigo publicado na Revista Literária de Direito, no 44, p. 23, outubro-dezembro/2002.

ABRUSIO, Juliana Canha; BLUM, Renato Ópice. Crimes eletrônicos.

BOITEUX, Luciana. Crimes informáticos: Reflexões sobre política criminal inseridas no contexto internacional atual. Revista Brasileira de Ciências Criminais – Instituto Brasileiro de Ciências Criminais – número 47 – Editora Revista dos Tribunais de 2004.

CASTRO, Carla Rodrigues Araújo de; “Crimes de Informática e seus Aspectos Processuais”.

CASSANTI, Moisés de Oliveira. Crimes virtuais, vítimas reais. São Paulo: Brasport, 2014.

CATTTANI - http://www.fredericocattani.com.br/blog/categoria/frederico-cattani-9, 01 de março de 2021.

CORRÊA, Gustavo Testa, “Aspectos Jurídicos da Internet”.

COSTA, Ana Maria Nicolaci da; “Na malha da Rede”. Os impactos íntimos da Internet.

CRUZ - http://www.fredericocattani.com.br/blog/categoria/frederico-cattani-9. 01 de março de 2021.

DELMANTO, Celso; Código Penal Comentado.

FILHO, José Carlos de Araújo Almeida. “Processo Eletrônico e Teoria Geral do Processo Eletrônico.”

GOUVÊA, Sandra; “O Direito na Era Digital”. Crimes praticados por meio da Informática.

KRUEL, Eduardo. “Processo Judicial Eletrônico e Certificação Digital na Advocacia”.

LEGISLAÇÃO SOBRE INTERNET NO BRASIL, material elaborado pela Consultoria Legislativa da Câmara dos Deputados: http://www.truzzi.com.br/blog/2010/07/13/legislacao-sobre-internet-no-brasil-material-para-download/

ROSA, Fabrízio; “Crimes de Informática”.

SANTOS, Coriolano Aurélio de Almeida Camargo. Comissão dos Crimes de Alta Tecnologia da OAB/SP. “As múltiplas faces dos crimes eletrônicos e dos fenômenos tecnológicos e seus reflexos no mundo jurídico”: http://www.oabsp.org.br/comissoes2010/crimes-alta-tecnologia/livro-sobre-crimes-eletronicos

VIANNA, Túlio Lima; “Fundamentos de Direito Penal Informático”. Do acesso não autorizado a sistemas computacionais.

RESOLUÇÃO n˚038/2020 – CEPE

ANEXO I

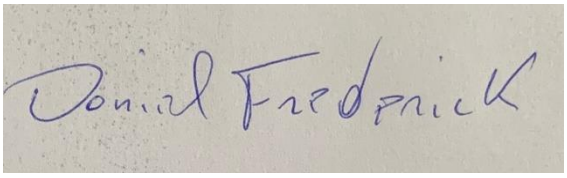
APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O estudante **Daniel Frederick e Silva Salustiano**, do Curso de **DIREITO,** matrícula 2016.1.0001.30955, telefone: 62 985113140, e-mail: daniel_frederick@hotmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado "**CRIMES VIRTUAIS NO BRASIL: ELEMENTOS CONFIGURADORES"** gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 01 de junho de 2021.

Assinatura do autor:



Nome completo do autor: Daniel Frederick e Silva Salustiano

Assinatura do professor-orientador:

Nome completo do professor-orientador: Goiacy Campos dos Santos Dunck