FACULDADE DE ILHÉUS CESUPI

COLEGIADO DO CURSO DE DIREITO
COORDENAÇÃO DE TCC
ARTIGO CIENTÍFICO

A FRAGILIDADE DO ORDENAMENTO JURÍDICO QUANTO AO CIBERCRIME: CRIMINOSOS POR TRÁS DE UMA TELA, VITIMAS EXPOSTAS EM SUAS VIDAS REAIS

Ilhéus, Bahia
2022

FACULDADE DE ILHÉUS CESUPI

COLEGIADO DO CURSO DE DIREITO
COORDENAÇÃO DE TCC
PROJETO DE PESQUISA

ALÍCIA CASTRO RAMOS

A FRAGILIDADE DO ORDENAMENTO JURÍDICO QUANTO AO CIBERCRIME: CRIMINOSOS POR TRÁS DE UMA TELA, VITIMAS EXPOSTAS EM SUAS VIDAS REAIS

Projeto de pesquisa entregue para acompanhamento como parte integrante das atividades de TCC I do Curso de Direito da Faculdade de Ilhéus.

Área de concentração: Direito Penal
Orientador. Prof. Jackson Novaes

Ilhéus, Bahia
2022

A FRAGILIDADE DO ORDENAMENTO JURÍDICO QUANTO AO CIBERCRIME: CRIMINOSOS POR TRÁS DE UMA TELA, VITIMAS EXPOSTAS EM SUAS VIDAS REAIS

RESUMO: O presente projeto tem por objetivo identificar e contextualizar o fenômeno dos cibercrimes, apresentando os conceitos pertinentes. A era tecnológica chegou, e com ela a insegurança dos usuários com os crimes digitais. Para tanto busca-se explanar as vulnerabilidades e as lacunas que o ordenamento jurídico vigente possui enquanto tal tema. No Brasil, o conceito de cibercrime é mais amplo, pois pode ou não estar conectado à internet. É inegável que a internet tornou-se parte de nossas vidas, mas, como se tem notado, essa segurança não é infalível e o conceito do cibercrime está fortemente em debate. A evolução dos meios digitais gerou oportunidades para novos tipos de condutas criminosas e a jurisprudência ainda não consegue acompanhar os mesmos, deixando assim grande fragilidade para a resolução da pratica de tais delitos. A resolutividade para a problemática tem sido o uso das leis já existentes, e abordagem os direitos fundamentais reconhecidos pela Constituição Federal de 1988. Mas é evidente que apenas essas soluções não são inteiramente eficazes, sendo assim, havendo a necessidade da criação de novas leis protetoras e mais rigor nas fiscalizações das leis já existentes contra a fragilidade do usuário, que por ventura poderá transfigura-se no futuro em uma vítima.

Palavras-chave: Cibercrimes.Tecnologia. Vulnerabilidade. Crime digital

SUMÁRIO

+

1. INTRODUÇÃO

A integração e à amplificação da internet otimizou a troca de informações, o alcance do espaço virtual tem tomado proporções imensas, conjuntamente ao aumento da quantidade de usuários. A presente pesquisa possui como objetivo examinar a ocorrência dos crimes cibernéticos, exaltando os perigos causados por um regramento insuficiente sobre tal temática.

Um grande problema ainda reside no rastreamento dos infratores, tendo em vista que a busca pelos indivíduos infratores se torna extremamente difícil, pois por vezes o autor do crime reside em outro país ou mascara seu endereço do Protocolo de Internet para diversos servidores tornando difícil ter conhecimento da sua localização. Sendo que as dificuldades não param por aí.

São muito comuns os crimes cometidos na internet relacionados tanto à pessoa, como injúria, calúnia, difamação, ameaça, crime de falsa identidade, divulgação de material confidencial, ato obsceno, apologia ao crime e estupro virtual, quanto à ataques cibernéticos, como aqueles promovidos por hackers que ao se utilizarem de vírus, infectam computadores de usuários e empresas e logo em seguida solicitam dinheiro em troca dos dados sequestrados, tal qual violação de sistemas de segurança.

Atualmente um dos grandes combates do Direito é garantir aos usuários a proteção no ambiente virtual. Por isso é importante a prevenção e cuidado sobre como é divulgado e exposto informações pessoais, pois, por mais simples e inocente pareça ser, a mesma pode usada de diferentes formas para obter dados que possibilitam os crimes cibernéticos.

É fundamental obtermos conhecimento sobre quais os crimes mais comuns cometidos por esses infratores e as leis que buscam conferir proteção jurídica às pessoas expostas a esses delitos, tais como a Lei de crimes cibernéticos (12.737/12), a Lei do Marco Civil da internet (12.965/14), a Lei Geral de Proteção de Dados (13.709/18), os direitos fundamentais reconhecidos pela Constituição Federal de 1988 e a Emenda Constitucional (EC 115), que inclui a proteção de dados pessoais entre os direitos e garantias fundamentais.

2. PROBLEMA

O aumento do alcance da rede mundial de computadores trouxe inúmeros benefícios, como também, vulnerabilidades para seus usuários. O nosso meio de vida foi modificado e

antes os crimes que eram cometidos de forma física agora são praticados no meio virtual, prejudicando tanto quanto antes. Devido a sua constante evolução, os cibercrimes estão sempre acompanhando o seu ritmo e inovando, porém, a legislação tem dificuldades para acompanhar o mesmo. Com isso surge a problemática na proteção dos dados da comunidade. Segundo Cassanti (2014, p.03) é definido Cibercrime:

> Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cibercrime. Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital.

Cibercrimes são os delitos penais cometidos por meio digital ou que estejam envolvidos com a informação digital. Foi tipificado na lei 12.737/2012, que o conceitua, no art. 154-A como:

> 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.

Os recentes ataques de hackers e vazamentos de dados pessoais de milhões de brasileiros chamaram a atenção para a urgência do combate aos cibercrimes. O número de crimes virtuais cometidos pela internet vem aumentado de modo alarmante, segundo especialistas reunidos em audiência pública interativa na Comissão de Ciência e Tecnologia.

3. HIPÓTESES

O ordenamento jurídico brasileiro contemporâneo não está preparado para assegurar a segurança jurídica necessária para a sociedade mediante os crimes no âmbito virtual. A conjectura de estudar e analisar sobre cibercrimes, sua evolução e a conjuntura jurídica, diante desses estudos, capaz de transpor de forma célere os desafios que hoje o ordenamento jurídico brasileiro enfrenta ao reprimir os delitos virtuais. A Lei 12.737/12, conhecida como Lei Carolina Dieckmann, uma forma de tentativa do Estado de reprimir essas novas condutas praticadas no âmbito virtual, fez-se necessário à criação de tipos penais que ainda não eram previstos na legislação. Apesar dos referidos direitos estarem garantidos pela legislação vigente,

ainda existe lacunas legislativas que podem dificultar e até mesmo impossibilitar a aplicabilidade para o fim almejado, vindo a criar uma insegurança jurídica.

4. OBJETIVOS

4.1. Objetivo Geral

Identificar as principais causas que colaboram para o crescimento demasiado dos crimes digitas, procurando percebe-se e assim, identificar a origem do problema. Para que sejam reduzidos e extinguidos, determinando assim o controle dentro do espaço virtual.

4.2. Objetivos Específicos

Criar de leis que protejam as vítimas que foram expostas e tiveram seus dados roubados, fornecendo as mesmas um auxilio jurisdicional. Assegurar os usuários que forem prejudicados, tenham seu devido apoio para resolução e transtornos causados pelos crimes digitais. Projetos para educar a comunidade, para que não divulguem suas informações de forma ingênua, assim tornando mais difícil o acontecimento dos delitos.

5. JUSTIFICATIVA

Consegue-se constatar e perceber que existe uma ausência de reconhecimento sobre os cibercrimes, são poucos os autores que abordam especificamente sobre esse tema. Visto que há muito a ser explorado, mostra-se necessário conhecer aspectos jurídicos que envolvem e configuram o tema, visando assim, compreender a legislação existente e formular novas normas constitucionais que tratem especificamente sobre esse tema.

Atualmente, o crime digital não tem ganho a devida atenção, sendo tipificado por apenas algumas leis, sendo que, algumas não são nem especifica para o devido tema. Por essa razão, é necessário chamar a atenção para este ambiente, expondo uma serie de meios que permitam enxergar novas percepções sobre este problema que vem cada vez mais assombrando os usuários da rede.

O presente projeto, busca como foco contribuir no desenvolvimento de métodos jurídicos e institucionais de resolução ao cibercrime. Uma vez que, com a adaptação da legislação e fiscalização será possível combater esses delitos.

6. REFERENCIAL TEÓRICO

Explanado o problema deste estudo, este capítulo consiste em uma base teórica acerca dos assuntos que envolvem o déficit e os projetos já existentes no ordenamento jurídico em relação a proteção dos usuários do espaço virtual.

6.1. CIBERCRIME X A LEGISLAÇÃO BRASILEIRA

Com o fim da Segunda Guerra Mundial, diversas tecnologias foram criadas, desenvolvidas e aprimoradas, porém, por muito tempo, a acessibilidade a tais instrumentos era restrita ao uso militar.

A Internet que conhecemos como um meio acessível à população surgiu na década de 90, vindo a se massificar a partir de então. Há mais ou menos quinze anos que a Internet conquista rapidamente espaços cada vez maiores na sociedade. Em um momento inicial, chegou-se a acreditar que esse espaço fosse “terra de ninguém”.

Isso facilitou o cometimento de crimes online e o aparecimento de novos delitos, fazendo surgir o termo cibercrime. O direito, visando acompanhar as demandas que surgem na sociedade, busca regular esse ciberespaço que parecia tão abstrato e distante de nossa realidade. Lévy define o ciberespaço como "o espaço de comunicação aberto pela interconexão mundial de computadores e das memórias dos computadores’’.

> O ciberespaço (que também chamarei de rede) é o mais novo meio de comunicação que surge da interconexão mundial de computadores. O termo especifica não apenas a infra estrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo.

O princípio da legalidade e o princípio anterioridade da lei penal, com previsão legal no artigo 1º do Código Penal e na Constituição Federal de 1988 no artigo 5º, inciso XXXIX, segundo o qual “não há crime sem lei anterior que o defina, nem há pena sem prévia cominação legal”.

De acordo com Kunrath (2017, p.57) alega que:

> Em decorrência do princípio da legalidade ou da anterioridade da lei penal, a insuficiência ou a ausência de norma penal tipificando os crimes digitais limita a função punitiva estatal, uma vez que influencia na sensação de insegurança e impunidade, com repercussão negativa para a sociedade brasileira e, em especial, para a comunidade internacional, que há mais de uma década vem chamando a atenção para a necessidade e urgência de controle e prevenção de condutas delituosas no ciberespaço. (KUNRATH, 2017, p.57).

Desse modo, a legislação brasileira tem dificuldade em acompanhar a evolução tecnológica, pois a cada dia surge um novo delito nesse ambiente, do qual o legislador não é capaz de caminhar em paralelo com essas evoluções, e consequentemente os crimes virtuais não recebem as devidas punições, deixando a sensação de impunidade.

A Lei Carolina Dieckmann é a Lei Nº 12.737/2012 e é uma alteração no Código Penal Brasileiro voltada para crimes virtuais e delitos informáticos. Com o avanço da tecnologia e a democratização e o acesso facilitado às redes sociais, o sistema judiciário brasileiro viu a necessidade de tipificar crimes cometidos no ambiente virtual.

Seu projeto foi apresentado no dia 29 de novembro de 2011 e sua sanção se deu em 2 de dezembro de 2012 pela presidente Dilma Rousseff. Esse foi o primeiro texto que tipificou os crimes cibernéticos, tendo foco nas invasões a dispositivos que acontecem sem a permissão do proprietário.

Vale destacar que, em nosso país, é comum as leis levarem anos para serem aprovadas, mas, nesse episódio, ela foi sancionada por conta da pressão midiática após uma ocorrência com a personalidade famosa — o que fez com que seu processo de aprovação demorasse o período recorde de apenas um ano.

A Lei Nº 12.737/12 impacta o Direito Penal, pois acrescenta os artigos 154-A e 154-B ao Código Penal Brasileiro. Além disso, altera a redação dos artigos 266 e 298. A norma trata de uma tendência do Direito: segurança no ambiente virtual.

Sua redação prevê os crimes que decorrerem do uso indevido de informações e materiais pessoais que dizem respeito à privacidade de uma pessoa na internet, como fotos e vídeos.

O primeiro artigo, 154-A, trouxe o crime chamado “Invasão de dispositivo informático”, que consiste na invasão de qualquer dispositivo informático alheio, como computadores, smartphones, tablets etc., independentemente se estiver conectado à internet ou não.

O ato deve ser praticado mediante violação de mecanismo de segurança e ter o objetivo de adulterar, obter ou destruir dados sem autorização do proprietário do dispositivo. A norma

também se aplica a quem instalar vulnerabilidades (como vírus) nos dispositivos para obter vantagens ilícitas.

Aquele que produzir, oferecer, distribuir, vender ou difundir um programa de computador ou dispositivo que permite a prática também sofrerá as consequências do crime.

A ação desse crime procederá mediante representação, ou seja, o Ministério Público (MP) somente oferece a denúncia se o ofendido solicitar, exceto nos casos em que o crime é cometido contra a administração pública (direta ou indireta) — ou seja, qualquer poder do governo municipal, estadual ou da União, como também empresas concessionárias de serviços públicos. O texto ainda acrescenta os parágrafos 1º e 2º no artigo 266, fazendo com que incorra com as mesmas consequências do artigo quem interrompe, impede ou dificulta serviços de informação que sejam públicos. Ademais, a pena é dobrada quando o ato é cometido em calamidades públicas (situação anormal como desastres naturais).

A pena do crime de invasão de dispositivos é a de detenção entre 3 meses e 1 ano mais multa, mas há um aumento de 1/6 da pena caso resulte em prejuízos econômicos à vítima.

Quando o crime resulta na obtenção de conteúdo de comunicações privadas, segredos comerciais ou industriais, controle remoto de dispositivos ou dados sigilosos, a pena será de reclusão de 6 meses a 2 anos mais multa — isso se o ato não constituir crime mais grave.

Nesse último caso, a pena ainda aumenta em 2/3 se houver transmissão, divulgação ou comercialização dos dados obtidos. Por fim, a pena pode aumentar de 1/3 até metade se o crime for praticado contra as seguintes autoridades:

- prefeito, governador ou presidente da república;
- presidente do Supremo Tribunal Federal (STF);
- presidentes dos órgãos legislativos municipais, estaduais ou da União, como Senado Federal, Câmara Municipal, Câmara Legislativa etc.;
- dirigentes máximos da administração municipal, estadual ou federal.

6.2. COOPERAÇÃO JURIDICA INTERNACIONAL E O BRASIL

Em 23 de novembro de 2001, ocorreu a Convenção sobre Cibercrimes na cidade de Budapeste, que entrou em vigor em 1º de julho de 2004. (WENDT, 2019, p.20). A Convenção trata-se de tipificar os crimes virtuais como infrações de sistemas; as infrações relacionadas aos

crimes com computadores; os crimes que envolvem pedofilia; e as violações de direitos autorais. Ainda, trata da competência e cooperação internacional, deixando a critério das partes decidirem quem será a jurisdição mais apropriada para o procedimento legal. (SILVA; BARRETO; KUFA, 2020, p.103).

Pode-se afirmar que a Convenção trata basicamente de harmonizar os crimes praticados no âmbito virtual e as formas de persecução. O Brasil adotou à Convenção no ano de 2021. A Convenção de Budapeste tem como objetivo facilitar a cooperação internacional para combater o cibercrime. Elaborado pelo Comitê Europeu para os Problemas Criminais, com o apoio de uma comissão de especialistas, o documento lista os principais crimes cometidos por meio da rede mundial de computadores e foi o primeiro tratado internacional sobre crimes cibernéticos. A Convenção já foi assinada por mais de 60 países e é utilizada por outros cerca de 160 como orientação para as legislações locais.

Entre as questões tratadas na Convenção de Budapeste estão a criminalização de condutas, normas para investigação e produção de provas eletrônicas e meios de cooperação internacional. Em seminário realizado pela Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados, o Ministério Público Federal (MPF) defendeu a urgência na aprovação do PDL para oficializar a adesão do Brasil ao tratado. O pedido foi feito pelo procurador da República George Lodder, que integra o Grupo de Apoio sobre Criminalidade Cibernética da Câmara Criminal do MPF (2CCR/MPF). Na ocasião, ele ainda defendeu a inclusão, na legislação brasileira, da obrigação de sites e plataformas comunicarem os órgãos de persecução penal sobre caso de crimes praticados por seus usuários.

7. METODOLOGIA

O tipo de pesquisa a ser utilizada no presente projeto será descritiva, tendo como base um levantamento de dados através das fontes: legislação brasileira e internacionais, artigos e notícias relacionadas ao Crime Digital; e fontes secundárias: serão feitas análises dos trabalhos de especialistas (artigos). Logo em seguida, será realizada a construção das ideias e dos textos, para que fosse possível uma análise do material coletado, e detectar as possíveis falhas e lacunas.

Mediante a análise e metodológica utilizada, será capaz de se chegar a sugestões preventivas e coercitivas mais elaboradas, para que os possíveis delitos na área digital sejam dificultados, como também, a proteção e segurança dos usuários que sofreram a tentativa dos cibercrimes. É visto que o ordenamento jurídico, apesar de existir leis, ainda assim, necessita do aumento de medidas protetivas e fiscalizações, sobre tal tema.

8. CRONOGRAMA

ANO: 2022

ETAPAS	FEV	MAR	ABR	MAIO	JUN	JUL	AGO	SET	OUT	NOV	DEZ
PROJETO DE PESQUISA		X	X	X	X						
Escolha do tema		X									
Definição do professor-orientador			X								
Relatórios de orientação			X	X	X						
Definição do problema de pesquisa		X	X								
Objetivos e Justificativa			X	X							
Referencial teórico			X	X	X						
Aspectos metodológicos				X	X						
Redação final do Projeto de Pesquisa					X						
Banca de Arguição											
ARTIGO											
Relatórios de orientação											
Atualização da Introdução											
Atualização do referencial teórico											
Instrumento de pesquisa											
Coleta e Análise dos dados											
Resultados e Discussão											
Considerações finais											
Redação final da Monografia											
Defesa Pública											

9. ORÇAMENTO

Material de Consumo	**Quantidade**	**Preço Unitário**	**TOTAL**
Papel A4 (resma)			
Cartucho de Impressora – Preto			
Cartucho de Impressora – Color			
Tonner			
Subtotal			
Material Permanente	**Quantidade**	**Preço Unitário**	**TOTAL**
Livros			
Impressora			
Pen drive			
Notebook			
Subtotal			
Outros serviços e encargos	**Quantidade**	**Preço Unitário**	**TOTAL**
Transporte (litros/combustível)			
Fotocópia Monocromática			
Fotocópia Colorida			
Encadernação			
Subtotal			
SUBTOTAIS			
Material de Consumo			
Material Permanente			
Outros serviços e encargos			
TOTAL GERAL			**0,00**

10. REFERÊNCIAS

Lei Carolina Dieckmann: você sabe o que essa lei representa? - FMP - Fundação Escola Superior do Ministério Público. FMP - Fundação Escola Superior do Ministério Público. Disponível em: <https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/>. Acesso em: 25 jun. 2022.

NATHANA ALVES RODRIGUES. **CIBERCRIMES: OS DESAFIOS NA ATUAL LEGISLAÇÃO BRASILEIRA**. Jus.com.br. Disponível em: <https://jus.com.br/artigos/93970/cibercrimes-os-desafios-na-atual-legislacao-brasileira>. Acesso em: 25 jun. 2022.

FOGLIATTO, Juliana. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos**. Jus.com.br. Disponível em: <https://jus.com.br/artigos/77225/os-crimes-ciberneticos-e-os-meios-que-a-policia-utiliza-para-a-identificacao-dos-criminosos>. Acesso em: 25 jun. 2022.

INSTITUTO BRASILIENSE DE DIREITO PÚBLICO -IDP ESCOLA DE DIREITO DE BRASÍLIA -EDB CURSO DE GRADUAÇÃO EM DIREITO PATRÍCIA BERTO BUANI A COMPATIBILIDADE ENTRE O ORDENAMENTO JURÍDICO BRASILEIRO E A CONVENÇÃO SOBRE CIBERCRIMES. BRASÍLIA JULHO/2020. [s.l.: s.n., s.d.]. Disponível em: <http://191.232.186.80/bitstream/123456789/2808/1/TCC%20_PATR%c3%8dCIA%20BERTO%20BUANI%20_DIREITO_2020.pdf>. Acesso em: 25 jun. 2022.

DE, Jefferson ; GOMES, Queiroz. **UNIVERSIDADE FEDERAL DO CEARÁ FACULDADE DE DIREITO DEPARTAMENTO DE DIREITO PÚBLICO SOCIEDADE DA INFORMAÇÃO E A CRIMINALIDADE INFORMÁTICA: AS CORRELAÇÕES ENTRE A LEGISLAÇÃO BRASILEIRA E A CONVENÇÃO DE BUDAPESTE SOBRE CIBERCRIMES FORTALEZA**. [s.l.: s.n.], 2017. Disponível em: <https://repositorio.ufc.br/bitstream/riufc/26379/1/2017_tcc_jqgomes.pdf>.