Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

THYAGO HENRIQUE SILVA BATISTA

CIBERCRIMES:

UMA ANÁLISE SOB A PERSCEPTIVA DA LEGISLAÇÃO BRASILEIRA

ASSIS - SP

2021

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

THYAGO HENRIQUE SILVA BATISTA

CIBERCRIMES:

UMA ANÁLISE SOB A PERSCEPTIVA DA LEGISLAÇÃO BRASILEIRA

Projeto de pesquisa apresentado ao curso de Direito do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando: Thyago Henrique Silva Batista
Orientador: Eduardo Augusto Vella Gonçalves

ASSIS – SP

2021

FICHA CATALOGRÁFICA

B333c BATISTA, Thyago Henrique Silva
Cibercriminalidade: crimes virtuais e a livre manifestação do pensamento / Thyago Henrique Silva Batista. – Assis, 2021.

25p.

Trabalho de conclusão do curso (Direito). – Fundação Educacional do Município de Assis-FEMA

Orientador: Ms. Eduardo Augusto Vella Gonçalves

1.Cibercrimes 2.Crimes virtuais

CDD 342.1152

CIBERCRIMINALIDADE

CRIMES VIRTUAIS E A LIVRE MANIFESTAÇÃO DO PENSAMENTO

THYAGO HENRIQUE SILVA BATISTA

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis como requisito parcial para obtenção do grau de Bacharel em Direito, avaliado pela seguinte comissão examinadora:

Orientador: _____
Eduardo Augusto Vella Gonçalves

Examinador: _____
Edson Fernando Pícolo de Oliveira

Assis/SP
2021

AGRADECIMENTOS

Agradeço aos meus pais Nilson e Luciana por terem me apoiado até aqui, e a Deus por ter amparado meus estudos com sabedoria. Ao professor Eduardo Augusto Vella Gonçalves por seus ensinamentos, pela paciência e incentivo, sem eles não seria possível a conclusão deste trabalho. Enfim, a todos que colaboraram de alguma forma para que eu chegasse até aqui. Obrigado.

RESUMO

O presente trabalho busca apresentar a cibercriminalidade com base em revisão de literatura científica. Em primeiro momento, o texto traz uma breve definição de crimes virtuais. Nesse sentido, são analisados seus conceitos, suas especificidades e o modo de atuação característico de cibercriminosos. Também são realizados comentários sobre a engenharia social necessária para a consolidação do delito. A partir de tal entendimento, realiza-se uma análise na legislação brasileira referente ao assunto, em especial a Lei 12.737/2012 e o Artigo 154-A do Código Penal desenvolvido em conjunto com a mesma, bem como impactos de sua aplicação na resolução de crimes virtuais. As referências base para a fundamentação teórica do trabalho referente à definição de cibercrimes foram artigos provenientes de diversos países, além da própria legislação brasileira, utilizada para realizar análise acerca de sua aplicação em diversas possibilidades de crimes virtuais. O que se concluiu com base na pesquisa foi a necessidade de implantar leis mais específicas para evitar lacunas legislativas na punição para cibercrimes.

Palavras-chave: Cibercrimes; Cibercriminalidade; Legislação brasileira; Direito eletrônico.

ABSTRACT

This paper seeks to present cybercrime based on a review of scientific literature. First, the text provides a brief definition of cybercrimes. In this sense, its concepts, its specificities and the characteristic mode of action of cybercriminals are analyzed. Comments are also made about social engineering to consolidate the crime. Based on this understanding, an analysis of the Brazilian legislation on the matter is carried out, in particular Law 12,737/2012 and Article 154-A of the Penal Code developed in conjunction with it, as well as the impacts of its application in the resolution of cyber crimes. The base references for the theoretical foundation of the work regarding the definition of cybercrimes were articles from different countries, in addition to the Brazilian legislation itself, used to analyze its application in various possibilities of cybercrime. What was concluded based on the research was the need to implement more specific laws to avoid legislative loopholes in the punishment for cybercrime.

Keywords: Cybercrime; Cyber criminality; Brazilian legislation.

LISTA DE TABELAS

LISTA DE QUADROS

SUMÁRIO

1. INTRODUÇÃO

Os crimes de informação passaram a ocorrer muito antes do advento da internet. Apesar de melhorias em comunicações serem de grande benefício para a humanidade no geral, foram responsáveis por proporcionar ambiente para uma nova modalidade de crimes. Os crimes virtuais se modificaram em conjunto com a evolução presenciada pelos meios de comunicação, por vezes com desenvolvimento maior em comparação com a quantidade de leis existentes para combater tais delitos.

Atualmente os crimes cometidos na internet são classificados como cibercrimes. O aprimoramento rápido e contínuo das tecnologias presente desde o início da globalização faz a prática de tal conduta criminosa se tornar cada vez mais comum, uma vez que existem inúmeras possibilidades de utilizar o ambiente online como ferramenta para cometer delitos.

Em contrapartida com o crescimento dos crimes virtuais, a legislação brasileira apresenta grande necessidade de modernizar as sanções legislativas para tais criminosos. A criação de determinadas leis com punições específicas se deu recentemente, mas a cibercriminalidade está distante de ser combatida de modo satisfatório no país.

Com tais problemáticas em mente, o trabalho se propõe a analisar os cibercrimes e sua aparição nos dispositivos legais brasileiros. Para contextualizar a análise de legislação e apresentar definições iniciais, em primeiro momento, são realizados breves comentários acerca do conceito de cibercrimes, suas categorias e formas de atuação de cibercriminosos.

Em seguida, o texto traz considerações a respeito da abordagem legal brasileira para com a cibercriminalidade e possíveis aspectos de melhoria. Nesse sentido, são trazidos dispositivos legais como a Lei 12.737/2012, conhecida como Lei Carolina Dieckman, responsável por tipificar cibercrimes e o artigo 154-A do Código Penal, no qual se prevê detenção e multa para crimes virtuais. Outros projetos de lei são também analisados como possibilidades de correção nas deficiências presentes na legislação.

Por fim, os resultados obtidos por meio da pesquisa são analisados e debatidos. Espera-se que o trabalho possa auxiliar na criação de novas pesquisas científicas relacionadas ao tema, contribuindo para melhorar os dispositivos legais referentes à cibercriminalidade.

2. CIBERCRIMES

2.1 Breve definição de cibercrimes

De acordo com a definição de Alexandre Júnior (2019, p. 343), um cibercrime pode ser definido como “todo ato em que o computador ou meios de tecnologia da informação serve para atingir um ato criminoso ou em que um computador ou meios de tecnologia da informação é objeto de um crime”. Tal modalidade de crime possui diversas nomenclaturas “dentre elas pode-se citar: crimes virtuais, digitais, informáticos, fraude informática, delitos cibernéticos, cibercrimes, entre outras” (ANTONELLI; ALMEIDA, 2016 p. 3).

Em outras palavras, os crimes virtuais compreendem qualquer atividade criminosa realizada por meio de computadores ou qualquer outro meio da tecnologia da informação. O aumento da cibercriminalidade brasileira se justifica pelo crescimento exponencial do número de usuários da internet, como evidencia a tabela abaixo:

Tabela 1: Estimativa de usuários da internet no Brasil

Ano	Número de Usuários
2005	21% da população
2010	35% da população
2015	57,5% da população
2019	74% da população

Fonte: Elaborado pelo autor com base nos dados do TIC – IBGE.

O número de usuários da internet no país aumentou consideravelmente em curto período de tempo. Não obstante, a perspectiva mundial em relação à internet se alterou com a passar dos anos, como aponta Lins (2013, p. 42):

> Essa contínua interação por meio da rede criou novos hábitos, novos modos de viver. As pessoas permanecem conectadas, a todo momento, pelas redes sociais. Informam-se, trocam ideias, marcam compromissos, negociam empregos, aderem a movimentos políticos pelas redes sociais.

O desenvolvimento notável da internet como ferramenta para inúmeros propósitos trouxe consigo um novo ambiente, com novos crimes característicos e a necessidade de criar mecanismos legislativos para combatê-los. Ainda que determinados cibercrimes sejam consolidações de crimes já previstos no Código Penal[1], o *modus operandi* dos criminosos se torna diferente em ambiente virtual.

A seguir, será realizada classificação dos tipos de cibercrimes.

2.2 Tipos de cibercrimes

Ao noticiar o número crescente de usuários da internet, a Comissão da Europa realizou em 2001, por meio da Convenção Sobre a Cibercriminalidade[2], um tratado internacional de direito penal e processual que prevê as modalidades de crimes virtuais e suas respectivas punições. Em resumo, a Convenção firmou as seguintes infrações:

Quadro 1: Infrações previstas na Convenção Sobre a Cibercriminalidade

Infrações relativas à confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informatizados.

- Acesso ilícito de informações
- Intercepção ilícita
- Interferência nos dados
- Interferência no sistema de dados
- Utilização indevida de equipamentos

Infrações relacionadas com computadores.

- Falsificação relacionada com computadores
- Fraude relacionada com computadores

Infrações relacionadas com o conteúdo.

- Infrações relacionadas com pornografia infantil

Infrações relacionadas com a violação dos direitos do autor e dos direitos conexos.

- Violações dos direitos de propriedade intelectual

Fonte: CONSELHO DA EUROPA, 2001

[1] Tratam-se de cibercrimes impróprios, a serem explicados na seção seguinte.
[2] Também conhecida como Convenção de Budapeste.

Outra classificação adotada por teóricos do direito divide os cibercrimes em próprios e impróprios (ANTONELLI; ALMEIDA, 2016, p. 3). Os cibercrimes próprios são aqueles em que o tanto o meio como o objeto do crime são sistemas tecnológicos. Um bom exemplo de cibercrime próprio é o acesso não autorizado a informações, popularmente conhecido como *hacking*.

Já os cibercrimes impróprios ocorrem quando os sistemas tecnológicos servem de ferramenta para a realização de um crime já previsto na legislação. Tal modalidade busca atingir um bem jurídico por meio de facilidades proporcionadas pela tecnologia.

2.3 Formas de atuação de cibercriminosos

A atuação de cibercriminosos se torna cada vez mais sofisticada, em conjunto com o desenvolvimento das práticas tecnológicas envolvidas na consolidação de tais infrações. Alguns dos meios utilizados para consolidar crimes como roubo de informações pessoais, falsidade ideológica, disseminação de vírus e acesso a dados pessoais são (HELP NET SECURITY, 2019):

- Tailored Ransomware[3] (ou “ransomware sob medida”): consiste em programas desenvolvidos especialmente para conseguir informações de um grupo específico de indivíduos. Pesquisas demonstram que essa modalidade de ataque ganhou mais força com a pandemia (STANKARD, 2021), já que grande parte dos comércios e serviços passou a realizar atividades em meio virtual.
- Living Off the Land (popularmente conhecido como LoTL): São ataques realizados via malware[4], mas possuem o diferencial de não depender de nenhuma instalação para funcionarem.
- Phishing: Trata-se de um ataque no qual “o atacante cria, por exemplo, uma réplica de uma página da web existente para enganar os usuários, para que eles enviem dados ou senhas” (SILVEIRA; REALAN; AMARAL, 2017). A réplica costuma ser de grande semelhança ou até mesmo igual ao site original, motivo pelo qual o phishing é um dos cibercrimes mais comuns. Apesar de sua existência não ser recente, a especialização dos cibercriminosos praticantes de tal delito é contínua.

[3] Software utilizado para bloquear o computador, que se utiliza de extorsão para desbloqueá-lo.

[4] Termo utilizado para caracterizar softwares maliciosos, cujos impactos podem ser inúmeros no computador do usuário.

Além dos crimes citados, existem inúmeros outros. Mas é importante destacar a base dos cibercrimes: a engenharia social (ES). Nesse sentido, é importante compreender o conceito de engenharia social e sua aplicação por cibercriminosos, como bem explicam Coelho, Rasma e Morales (2013, p. 40):

> Existem várias formas de ataques, sempre explorando a fragilidade e a ingenuidade das pessoas. Estes ataques podem ter dois enfoques diferentes: o físico, como local de trabalho, lixo, telefones; e o psicológico, como persuasão, criando confiança, ou simplesmente, sendo gentil.

Ou seja, a engenharia social está relacionada à capacidade do criminoso de convencer suas vítimas a fornecer dados por livre e espontânea vontade, ao se aproveitar da confiança das mesmas em determinada organização, corporação ou indivíduo. Um exemplo claro da aplicação da ES são os sites manipulados via phishing, nos quais o criminoso se aproveita da confiança da vítima em determinado endereço eletrônico para obter seus dados.

Com isso, fica claro que a atuação de cibercriminosos está longe de ser simplória. Muito pelo contrário, os cibercrimes são constituídos de diversos mecanismos para consolidar condutas criminosas, além de possuírem grande potencial de dano em virtude da quantidade de informações comprometedoras, confidenciais e pessoais na internet.

2.4 Fake news e liberdade de expressão

Um dos crimes que se expandiu por meio da tecnologia é a propagação de notícias falsas, conhecidas como *fake news*. Essas notícias são criadas com o intuito de prejudicar ou legitimar determinado ponto de vista, em detrimento dos fatos. Por esse motivo, podem causar grande impacto na sociedade, especialmente no processo democrático. Informações falsas interferem até mesmo na campanha eleitoral, o que impede a democracia de ser exercida plenamente pelos cidadãos.

Outro fator preocupante é a velocidade com que notícias falsas se espalham. Na rede social *Twitter*, por exemplo, a velocidade de compartilhamento pode ser até seis vezes maior em relação às notícias verdadeiras (VOSOUGHI, ROY, ARAL, 2018).

Isso acontece, pois, a natureza das informações manipuladas é apelativa. Os textos que compõem as notícias falsas apelam para o emocional do leitor/espectador.

De acordo com Farias, Azevedo, Monteiro (2018, p. 3):

> Não há segredos de que a internet trouxe facilidade e rapidez aos usuários do mundo inteiro em fazer compartilhamento de vídeos, imagens, áudios, documentos, notícias, enfim, trouxe efetiva proximidade de interação social entre as pessoas no mundo virtual. No entanto, da mesma forma que há infinidade de benefícios, também há dentro deste cenário uma grande preocupação que vem sendo diariamente discutida, é a chamada Fake News.

O uso cada vez maior de aparelhos tecnológicos conseguiu amplificar os efeitos das *fake news* por meio de uma propagação mais abrangente e mais rápida das informações falsas. Isso gerou um fenômeno de propagação em massa de notícias falsas, tornando-se uma indústria crescente no meio virtual.

Atualmente, pode-se classificar sete tipos de notícias falsas, de acordo com a análise de Wardle (2017):

a) Sátira, sem a intenção de enganar;
b) Falsa conexão, quando a imagem/legenda não condiz com o conteúdo;
c) Conteúdo enganoso, quando a informação é moldada;
d) Conteúdo distorcido, quando o conteúdo é verdadeiro, mas seu contexto foi alterado;
e) Conteúdo impostor, quando o veículo se passa por fonte confiável;
f) Conteúdo manipulado, onde a informação é completamente manipulada para enganar;
g) Conteúdo fabricado; quando nada presente na notícia é real.

As *fake news* podem existir em diferentes níveis, mas todas são perigosas e exigem o máximo de atenção e cuidado. O leitor deve sempre procurar a origem de sua informação, com o maior nível de cautela possível, antes de propagá-la. Por isso a importância da conscientização a respeito de informações falsas na internet.

3. CIBERCRIMES NA LEGISLAÇÃO BRASILEIRA

3.1 Leis para combater cibercrimes

A legislação brasileira apresenta poucos dispositivos legais para combater cibercrimes. A lei mais marcante nesse sentido é a Lei 12.737/2012, acompanhada do Artigo 154 do Código Penal, transcrita a seguir:

> Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.
>
> Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
>
> **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 (BRASIL, 2012). (Grifos do autor).

Tal lei é apelidada como Lei Carolina Dieckmann, pois a atriz sofreu um ciber ataque em maio de 2011. Um criminoso virtual invadiu seu computador pessoal e impediu o acesso à diversas fotos de cunho íntimo. Em decorrência do fato, a atriz “abraçou a causa e cedeu seu nome à lei”, como apelido extraoficial. Também vale ressaltar o fato de que, a rápida aprovação da lei em questão se deu pela ocorrência do fato ter sido com uma personalidade pública, trazendo maior visibilidade para a questão (FMP, 2019).

Outra lei com importância no combate ao cibercrime é a Lei dos crimes de software, também conhecida como lei antipirataria, que dispõe:

> CAPÍTULO I
>
> DISPOSIÇÕES PRELIMINARES
>
> Art. 1º **Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados**.
>
> CAPÍTULO II
>
> DA PROTEÇÃO AOS DIREITOS DE AUTOR E DO REGISTRO
>
> Art. 2º **O regime de proteção à propriedade intelectual de programa de computador é o conferido às obras literárias pela legislação de direitos autorais e conexos vigentes no País, observado o disposto nesta Lei.**
>
> § 1º Não se aplicam ao programa de computador as disposições relativas aos direitos morais, ressalvado, a qualquer tempo, o direito do autor de reivindicar a paternidade do programa de computador e o direito do autor de opor-se a alterações não-autorizadas, quando estas impliquem deformação, mutilação ou outra modificação do programa de computador, que prejudiquem a sua honra ou a sua reputação.
>
> § 2º Fica assegurada a tutela dos direitos relativos a programa de computador pelo prazo de cinquenta anos, contados a partir de 1º de janeiro do ano subsequente ao da sua publicação ou, na ausência desta, da sua criação.
>
> § 3º A proteção aos direitos de que trata esta Lei independe de registro.
>
> § 4º Os direitos atribuídos por esta Lei ficam assegurados aos estrangeiros domiciliados no exterior, desde que o país de origem do programa conceda, aos brasileiros e estrangeiros domiciliados no Brasil, direitos equivalentes.
>
> § 5º Inclui-se dentre os direitos assegurados por esta Lei e pela legislação de direitos autorais e conexos vigentes no País aquele direito exclusivo de autorizar ou proibir o aluguel comercial, não sendo esse direito exaurível pela venda, licença ou outra forma de transferência da cópia do programa.
>
> § 6º O disposto no parágrafo anterior não se aplica aos casos em que o programa em si não seja objeto essencial do aluguel.
>
> Art. 3º Os programas de computador poderão, a critério do titular, ser registrados em órgão ou entidade a ser designado por ato do Poder Executivo, por iniciativa do Ministério responsável pela política de ciência e tecnologia (BRASIL, 1998). (Grifos do autor).

A lei transcrita acima é voltada para crimes de propriedade intelectual. Desse modo, foi sancionada com o intuito de combater pirataria realizada por meios virtuais,

prática comum em todo o mundo. Também traz a importante definição legal de programa de computador, para esclarecer sua aplicação.

Por fim, cabe mencionar uma lei não específica para crimes virtuais, porém, com potencial de auxílio na resolução de cibercrimes. A Lei 8.069/1990 contribui na proteção de crianças e adolescentes em relação à cibercrimes ao mencionar em seu Artigo 241, incluído pela Lei 11.829/2008:

> Art. 241**. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:** (Redação dada pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008)
>
> Art. 241-A. 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: (Incluído pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
>
> § 1 o Nas mesmas penas incorre quem: (Incluído pela Lei nº 11.829, de 2008)
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo; (Incluído pela Lei nº 11.829, de 2008)
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008). (BRASIL, 1990). (Grifos do autor).

A redação incluída pela Lei 11.829/2008 auxilia no esclarecimento de crimes virtuais relacionados à crianças e adolescentes, especialmente no que tange à pornografia infantil. Com isso, a eficiência na resolução dessa modalidade de delito se torna mais eficiente.

Na breve análise a respeito da legislação sobre o assunto supra mencionado na revisão de literatura científica, fica claro que estabelecer com maior clareza a definição de cibercrimes, bem como a punição específica para cada um deles, facilita em sua resolução, tramitação processual e na aplicação de penas adequadas para cibercriminosos.

3.2 Aspectos a serem melhorados

Após entender como funciona a legislação brasileira referente à cibercrimes, fica evidente que existem diversas melhorias a serem feitas. Existem lacunas para inúmeros crimes como fraude, furto e estelionato praticados em ambiente digital.

Além disso, a legislação deve incluir atualizações frequentes para acompanhar o desenvolvimento contínuo da tecnologia e impedir brechas legais para cibercriminosos.

Alguns projetos de lei (PL) foram propostos nesse sentido. O mais recente é o Projeto de Lei 4.554/2020, de autoria do senador Izalci Lucas, aprovado pelo plenário e em fase de tramitação na Câmara dos Deputados. Em suma, o projeto busca combater “a prática de fraude eletrônica, modifica o art. 155 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal e apresenta hipóteses agravantes”.

A explicação da ementa se dá pela criação do “crime de furto qualificado pela fraude com uso de dispositivo eletrônico ou de dados eletrônicos fornecidos indevidamente”, com adição do “aumento de pena nos casos de vítima idosa ou de utilização de servidor de rede fora do país”. (SENADO FEDERAL, 2020).

Em breve análise referente aos anos de 2020 e 2021, pode-se refletir sobre como o distanciamento social modificou o uso de ferramentas virtuais, deixando-as mais fáceis ao uso de app (aplicativos), com maior poder de persuasão para informações e/ou cadastramento de dados pessoais. Com o aumento na utilização de dispositivos eletrônicos para fins como trabalho, estudos e movimentações bancárias, propulsionados pela pandemia, fica evidente que diversos dados estão em risco caso não haja modificações legais nesse sentido.

Por fim, cabe mencionar a grande quantidade de cidadãos cadastrados na plataforma do governo eletrônico, em que já se presenciou vazamento de dados[5] mais de uma vez.

[5] https://www.gov.br/anpd/pt-br/assuntos/noticias/meus-dados-vazaram-e-agora

Dada a existência de tantas informações comprometedoras na rede, cumpre estabelecer normas mais claras e atualizadas para combater cibercrimes com base em estudos acerca das ferramentas utilizadas para sua consolidação.

Outra questão importante é a conscientização da população acerca do significado dos cibercrimes, sua concretização através de reforço aplicado em meios de comunicação afim de evitá-los, obtendo maior clareza sobre o assunto e maior efetividade. Desse modo, o conhecimento sobre a tecnologia serve de combatente aos cibercrimes, já que grande número de vítimas participa dos golpes de engenharia social por não saber de seus riscos ou de sua existência enquanto prática criminosa.

4. CONCLUSÃO

Ainda que a Cibercriminalidade seja um tema recente no direito brasileiro, nota-se que suas consequências podem ser de grandes riscos para grupos populacionais diversos: crianças, adolescentes, pessoas públicas, idosos, dentre outros. Além dos grupos citados, cabe mencionar a possibilidade de risco à própria segurança nacional.

Com o conhecimento de tais riscos, surge a necessidade de realizar melhorias na legislação atual, com acompanhamento de especialistas da área de tecnologia. Cabe também ao atuante no direito eletrônico conhecer cibercrimes e suas possibilidades de aplicação.

Deve-se analisar o impacto de cibercrimes, inclusive as *fake news*, como armas capazes de corromper o processo democrático, gerar calúnia, causar prejuízo financeiro e expor dados privados. As consequências são diversas, portanto, o combate deve estar voltado para todas as modalidades de crimes virtuais.

A partir das considerações realizadas, espera-se que o texto possa contribuir no desenvolvimento de pesquisas mais aprofundadas na área, uma vez que a cibercriminalidade é pouco explorada no direito brasileiro. Desse modo, podem surgir novas propostas de legislação referentes aos crimes virtuais.

REFERÊNCIAS

ALEXANDRE JÚNIOR, Júlio Cesar. Cibercrime: um estudo acerca do conceito de crimes informáticos. **Revista Eletrônica da Faculdade de Direito de Franca** [Online], v. 14, n.1, jun. 2019. Disponível em: https://www.revista.direitofranca.br/index.php/refdf/article/view/602. Acesso em: 01 Mai. 2021.

ANTONELLI, Humberto Lidio; ALMEIDA, Emerson Gervásio de. **A Internet e o Direito: Uma abordagem sobre cibercrimes**. 2016. https://egov.ufsc.br/portal/sites/default/files/a_internet_e_o_direito_uma_abordagem_sobre_cibercrimes.pdf. Acesso em: 29 Abr. 2021.

BARRETO, Alesandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e Seus Reflexos no Direito Brasileiro**. Salvador: Juspodivm, 2020.

BRASIL. LEI Nº 8.069, DE 13 DE JULHO DE 1990: Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. 1990

BRASIL. LEI Nº 9.609, DE 19 DE FEVEREIRO DE 1998: Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. 1998.

BRASIL. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012: Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. 2012.

BRENNER, Susan W. Cybercrime jurisdiction. **Crime, Law and Social Change**, 46, p. 189–206. 2006. https://link.springer.com/article/10.1007/s10611-007-9063-7. Acesso em: 15 Abr. 2021.

CARDOSO, Nágila Magalhães. A pandemia do cibercrime. **Direito & TI**, 2020. http://direitoeti.com.br/artigos/a-pandemia-do-cibercrime/. Acesso em: 02 Abr. 2021.

COELHO, Cristiano Farias; RASMA, Eline Tourinho; MORALES, Gudelia. Engenharia Social: uma ameaça à sociedade da informação. Revista Perspectivas Online: ciências exatas e engenharia, Campos dos Goytacazes, 3 (5), p. 34-44, 2013.

CONSELHO DA EUROPA. Minuta do Relatório Explicado. **Convenção sobre o Cibercrime**. 2001. Disponível em:

https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf. Acesso em: 15 Abr. 2021.

FMP – Fundação Escola Superior do Ministério Público. **Lei Carolina Dieckmann**: você sabe que essa lei representa? 2019. Disponível em: https://blog.fmp.edu.br/lei-carolina-dieckmann-voce-sabe-que-o-essa-lei-representa/#:~:text=Por%20que%20a%20lei%20recebeu,fotos%20pessoais%20de%20cunho%20%C3%ADntimo.&text=A%20atriz%20abra%C3%A7ou%20a%20causa%20e%20cedeu%20seu%20nome%20%C3%A0%20lei. Acesso em: 28 Mai. 2021.

HELP NET SECURITY. Cybercriminals continue to evolve the sophistication of their attack methods. **Help Net Security [Online]**, 2019. Disponível em: https://www.helpnetsecurity.com/2019/05/23/cybercriminals-attack-methods/. Acesso em: 31 Mai. 2021.

KIGERL, Alex. Routine Activity Theory and the Determinants of High Cybercrime Countries. **Social Science Computer Review**, 30. 2012.

LINS, Bernardo Felipe Estellita. A evolução da Internet: uma perspectiva histórica. **Cadernos Aslegis**, 48, Janeiro/Abril, 2013.

SENADO FEDERAL. Projeto de Lei n° 4554, de 2020. 2020. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/144667. Acesso em: 01 Jun. 2021.

SILVEIRA, Lucidia A.; REALAN, Maurício A.; AMARAL, Érico. Engenharia Social: Uma análise sobre o ataque de Phishing. **Congresso Sul Brasileiro de Computação (SULCOMP)**, Capa, V.8, 2016.

STANKARD, Trevagh. Increase in Tailored Ransomware During COVID-19. **TitanHQ**. Disponível em: https://www.titanhq.com/blog/increase-in-tailored-ransomware-during-covid-19/. Acesso em: 01 Jun. 2021.

VOSOUGHI, Soroush; ROY, Deb; ARAL, Sinan. **Science.** V. 359, n. 6380, p. 1146-1151, mar. 2018. Disponível em: https://science.sciencemag.org/content/359/6380/1146?utm_source=SciPak%20%2528updated%206%252F30%252F2017%2529&utm_campaign=f996c5aa4d-EMAIL_CAMPAIGN_2018_03_02&utm_medium=email&utm_term=0_10c5e799a3-f996c5aa4d-126626477. Acesso em: 05 Jun. 2021.

WARDLE, Claire. Fake News. It's complicated. **First Draft News,** 2017. Disponível em: https://firstdraftnews.org/latest/fake-news-complicated/. Acesso em: 05 Jun. 2021.