

CENTRO UNIVERSITÁRIO UNINOVAFAPI
BACHARELADO EM DIREITO

FRANKLIN SOUSA DAMASCENO
JASMYM CARDOSO DE MELO
JOÃO PEDRO BARBOSA ALVES

**A EVOLUÇÃO LEGISLATIVA E A REALIDADE DOS CRIMES VIRTUAIS NO
BRASIL: UMA ANÁLISE SOBRE O DIREITO À PRIVACIDADE E À INTIMIDADE**

TERESINA
2024

FRANKLIN SOUSA DAMASCENO
JASMYM CARDOSO DE MELO
JOÃO PEDRO BARBOSA ALVES

**A EVOLUÇÃO LEGISLATIVA E A REALIDADE DOS CRIMES VIRTUAIS NO
BRASIL: UMA ANÁLISE SOBRE O DIREITO À PRIVACIDADE E À INTIMIDADE**

Artigo de Trabalho de Conclusão de Curso
apresentado à Banca Examinadora do Centro
Universitário UNINOVAFAP, como requisito
parcial para obtenção do grau de Bacharel em
Direito.

Orientadora: Prof.^a Ma. Sara Morgana Silva
Carvalho Lopes

TERESINA

2024

FICHA CATALOGRÁFICA

A474e Alves, João Pedro Barbosa.

A evolução legislativa e a realidade dos crimes virtuais no Brasil :
uma análise sobre o direito à privacidade e à intimidade. João Pedro
Barbosa Alves ; Franklin Sousa Damasceno , Jasmim Cardoso de melo.
– Teresina: UNINOVAFAPI, 2024.

Orientador (a): Prof. Ma. Sara Morgana Silva Carvalho Lopes –
UNINOVAFAPI, 2024.

Catálogo na publicação

Francisco Renato Sampaio da Silva – CRB/1028

FRANKLIN SOUSA DAMASCENO

JASMYM CARDOSO DE MELO

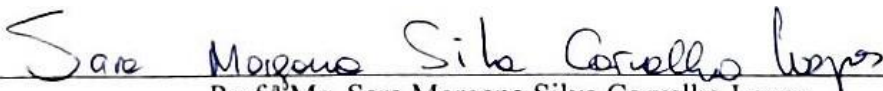
JOÃO PEDRO BARBOSA ALVES

A EVOLUÇÃO LEGISLATIVA E A REALIDADE DOS CRIMES VIRTUAIS NO
BRASIL: UMA ANÁLISE SOBRE O DIREITO À PRIVACIDADE E À INTIMIDADE

Artigo de Trabalho de Conclusão de Curso
apresentado à Banca Examinadora do Centro
Universitário UNINOVAFAPI, como requisito
parcial para obtenção do grau de Bacharel em
Direito.

Data de Aprovação: 08 / 11 / 2024

BANCA EXAMINADORA


Prof.^a Ma. Sara Morgana Silva Carvalho Lopes
Prof.^a Ma. Sara Morgana Silva Carvalho Lopes

Centro Universitário - UNINOVAFAPI

(Orientador)



Prof.^a Ma. Amanda Fernandes Leal Centro
Universitário - UNINOVAFAPI

(1^o Examinador)



Prof.^a Dra. Gillian Santana de Carvalho Mendes

Centro Universitário - UNINOVAFAPI

(2^o Examinador)

AGRADECIMENTOS

Em primeiro lugar, quero agradecer a Deus, que fez que com meus objetivos fossem alcançados, por me permitir ultrapassar com saúde e determinação todos os obstáculos ao longo da realização desse curso. Aos meus familiares e amigos por todo o apoio e pela ajuda, que contribuíram para a realização deste curso. Minha mãe [Maria Solfia da Conceição Sousa Damasceno], meu pai *in memoriam* [Luiz Marcos Damasceno], meus irmãos que me incentivavam nos momentos difíceis e compreenderam a minha ausência enquanto eu me dedicava à realização deste curso. Aos meus amigos, que sempre estiveram ao meu lado, pela amizade incondicional. Meus professores, pelos ensinamentos, por todos os conselhos, pela ajuda, pela paciência, que me permitiram apresentar um melhor desempenho no meu processo de formação profissional ao longo do curso. A professora Sara Morgana Silva Carvalho Lopes, por ter sido minha orientadora e ter desempenhado tal função com dedicação e amizade. Aos meus colegas de curso, com que convivi intensamente durante os últimos anos, pelo companheirismo ao longo deste percurso. A instituição Uninovafapi, no meu processo de formação profissional, pela dedicação, e por tudo o que aprendi ao longo deste curso. E a todos aqueles que contribuíram e participaram de alguma forma direta ou indiretamente para a realização deste trabalho.

Franklin Sousa Damasceno

Agradeço primeiramente à minha mãe, cujo apoio incondicional e amor foram a base para a conclusão deste trabalho. A ela, minha eterna gratidão. Agradeço também aos meus colegas de curso, que tornaram a jornada mais leve e enriquecedora com suas amizades e trocas de conhecimento. Por fim, meus sinceros agradecimentos aos professores em especial a professora e nossa orientadora Sara Morgana, pela orientação e dedicação, que foram fundamentais para o desenvolvimento deste trabalho.

Jasmym Cardoso de Melo

Agradeço à Deus por ter me dado a oportunidade de realizar mais este sonho, pois esteve sempre ao meu lado, me dando forças, coragem e sabedoria, mesmo nos momentos de dificuldades. À minha família, que durante esses anos de caminhada não mediram esforços para me ver feliz, deram-me apoio, incentivo e me fizeram acreditar que seria possível realizar este sonho. Agradeço também aos meus companheiros de sala, que de forma direta e indireta sempre estiveram comigo e me auxiliaram. Sou grato à Instituição de ensino, aos docentes do curso e

aos professores que aceitaram fazer parte da banca. Também agradeço a minha orientadora, a quem sou imensamente grato, pelo incentivo, confiança, paciência e dedicação.

João Pedro Barbosa Alves

RESUMO

O presente trabalho reflete acerca da aplicação dos dispositivos penais aos crimes cibernéticos no âmbito do ordenamento jurídico brasileiro, bem como analisa o surgimento de novos institutos penalizadores mais específicos, com intuito de punir e coibir tais práticas. A análise será realizada a partir do surgimento da ideia de Direito Digital e da definição de crimes cibernéticos, perpassando pelo conceito e pelos aspectos históricos desses delitos, os quais são decorrentes da acelerada globalização e das grandes inovações tecnológicas do século. A metodologia utilizada no trabalho é a pesquisa bibliográfica onde foi consultado em sites acadêmicos, artigos, livros e jornais que dizem respeito ao assunto tema do presente trabalho. O principal objetivo do estudo é identificar quais os mecanismos de punição aos crimes cibernéticos existentes, gerais ou específicos, bem como avaliar sua eficácia perante o crescimento da internet e intensificação das relações virtuais. O estudo conclui que o objetivo é entender a evolução e a implementação das leis penais em relação aos delitos cibernéticos no Brasil, enfatizando a importância de novos institutos específicos destinados a combater tais práticas. A avaliação indica que, com a expansão da internet e a intensificação das interações online, a legislação deve acompanhar a velocidade das inovações tecnológicas para assegurar uma implementação efetiva das leis. Apesar de haver mecanismos gerais e específicos para a punição desses crimes, é imprescindível avaliar continuamente sua efetividade e ajustá-los às novas realidades digitais para lidar com os desafios cada vez maiores do cenário cibernético.

Palavras-chave: Direito Digital; Crimes virtuais. Privacidade. Intimidade.

ABSTRACT

This paper reflects on the application of criminal provisions to cybercrime within the Brazilian legal system, as well as analyzing the emergence of new, more specific penalizing institutes, with the aim of punishing and curbing such practices. The analysis will start from the emergence of the idea of Digital Law and the definition of cybercrime, going through the concept and historical aspects of these crimes, which are the result of accelerated globalization and the great technological innovations of the century. The methodology used in the work is bibliographical research, in which academic websites, articles, books and newspapers were consulted that relate to the subject of this work. The main objective of the study is to identify the existing mechanisms for punishing cybercrime, whether general or specific, as well as to assess their effectiveness in the face of the growth of the internet and the intensification of virtual relationships. The study concludes that the objective is to understand the evolution and implementation of criminal laws in relation to cybercrime in Brazil, emphasizing the importance of new specific institutes designed to combat such practices. The assessment indicates that, with the expansion of the internet and the intensification of online interactions, legislation must keep up with the speed of technological innovations to ensure effective implementation of the laws. Although there are general and specific mechanisms for punishing these crimes, it is essential to continually evaluate their effectiveness and adjust them to the new digital realities in order to deal with the ever-increasing challenges of the cyber scenario.

Keywords: Digital law; Virtual crimes; Privacy; Intimacy.

1 INTRODUÇÃO

O tema a ser aprofundado neste estudo, a punibilidade dos crimes cibernéticos no ordenamento jurídico brasileiro, será apresentado levando-se em consideração o sistema normativo jurídico e a legislação específica nacional, principalmente no que tange à realidade social de grande dependência e engajamento das pessoas à rede mundial de computadores e às novas tecnologias, assim como o consequente aumento expressivo de crimes cometidos virtual e anonimamente.

Prefacialmente, cumpre esclarecer que não há como dissertar acerca da punibilidade dos crimes cibernéticos no Brasil sem remontarmos ao advento da internet e sua evolução histórica desde o século XX, bem como sua crescente popularização e acesso cada vez mais democrático e de baixo custo, fazendo com que se tornasse uma ferramenta bastante acessível, podendo ser facilmente utilizada tanto para benefício quanto para o prejuízo da sociedade.

Nesse sentido, cabe destacar a promulgação da Lei nº 12.965/2014, denominada “Marco Civil da Internet” que traduz a preocupação do legislador com a proteção das relações jurídicas no ambiente virtual, possuindo como objetivo o estabelecimento de princípios, garantias, direitos e deveres para a utilização da internet no Brasil, além de regular como se daria nesse contexto a atuação da União, dos Estados, do Distrito Federal e dos Municípios.

A referida legislação surgiu do fato de que as relações concebidas do mundo digital possuem resultados e consequências que vão além da rede mundial de computadores, a famosa World Wide Web – WWW, esta que conta com a interação de milhares de pessoas em simultâneo, sendo necessária regulação e controle. Assim como possibilita diversas vantagens e facilidades, a internet também está propícia ao mau uso por parte de alguns usuários, o que resulta na prática de atos denominamos como crimes cibernéticos.

É fundamental apontar que a internet facilitou a ocorrência dos delitos, por aumentar sua velocidade e facilidade, visto que os crimes se dão de maneira quase instantânea e anônima. Por isso, é importante determinar as especificidades e diferentes modos de combate aos crimes cometidos virtualmente. Crimes já conhecidos, como a pedofilia e o estelionato, se tornaram práticas recorrentes no âmbito virtual, mas ainda é perceptível a precariedade da legislação regulamentadora e a dificuldade em reprimir tais práticas.

Com o intuito de coibir a prática de crimes virtuais relacionados à invasão e roubo de dados, telemáticos e informáticos, foi promulgada também a Lei nº 12.737/2012, popularmente conhecida como “Lei Carolina Dieckmann”, visto que teve como ensejo o grande episódio nacional em que fotos íntimas da famosa foram amplamente divulgadas em 2012 (Brasil, 2012).

O ponto de maior relevância da nova norma foi a inclusão de novos tipos penais incriminadores ao Código Penal, os artigos 154-A e 154-B (Brasil, 1940).

A partir desse contexto, é perceptível que se está buscando suprir as lacunas com relação aos crimes virtuais, onde há uma falta ainda considerável de leis específicas e rigorosas o suficiente para desencorajar tais práticas. As normas que atualmente versam sobre o assunto, ainda não são suficientes para acompanhar o crescimento e o desenvolvimento dos casos de delitos cometidos contra o computador ou por meio deste, isto sem considerar o vultuoso desenvolvimento tecnológico dos dispositivos móveis, como os *smartphones* e celulares.

Deste modo, ao expor o avanço da ideia de punibilidade dos crimes cibernéticos no ordenamento jurídico brasileiro, bem como apontar como vem se desenvolvendo os dispositivos legislativos para acompanhar a popularização da internet, nacional e internacionalmente, assim como os problemas decorrentes de seu mau uso, o objetivo do presente estudo é investigar a aplicabilidade e adaptabilidade da lei em sentido amplo, principalmente no que tange às especificidades e facilidades desses delitos.

Visando alcançar efetivamente o objetivo apontado, será realizada uma profunda pesquisa doutrinária e legislativa, paralelamente com a análise das normas e princípios nacionais e internacionais que versem sobre o assunto, de forma a construir um contexto geral do tema. Esse estudo servirá como base para expor a relação entre a legislação vigente, específica ou secundária, e a efetiva punibilidade dos crimes virtuais, analisando a simultaneidade entre a evolução da internet e o consequente aumento da prática dos ilícitos virtuais, bem como ponderar acerca do desenvolvimento e aplicação dos dispositivos penais.

2 A REGULAMENTAÇÃO NO CENÁRIO DIGITAL

É perceptível que a *internet* desempenha funções sociais e culturais. Neste cenário, a *internet* se destaca como uma rede abrangente com funções específicas, como a troca de mensagens e conversas à distância, discussões, comércio, teletrabalho e projetos de voto. Todas essas formas de interação têm impactos jurídicos e socioeconômicos, em algum grau (Zanatta, 2010).

As interações no mundo digital também devem ser regidas pelo direito, uma vez que o uso da Internet é realizado globalmente, tornando qualquer pessoa suscetível a ser vítima de delitos que não possuem mais barreiras geográficas e políticas, e que possuem proteção limitada. Desde 2010, nota-se o crescimento dos desafios jurídicos, econômicos e sociais

resultantes das mudanças na sociedade. Em um embate entre a modernidade e as inovações, surgem novas questões que requerem novos mecanismos para serem resolvidas (Zanatta, 2010).

Portanto, conclui-se que a virtualização representa uma nova maneira de interpretar um problema. No âmbito virtual, o direito digital surge com a virtualização para se ajustar à realidade cibernética. Isso implica que, para compreender como resolver questões virtuais, que afetam o mundo real, é necessário expandir conceitos tradicionais, como o direito, para o âmbito da internet.

O direito digital não se distingue do direito tradicional por seus princípios e institutos, mas sim pela sua localização no ambiente virtual. Em outras palavras, o direito digital não precisa ser inventado ou desenvolvido do zero, mas sim analisado no mundo real e implementado na realidade virtual.

No entanto, o grande é antecipar todas as circunstâncias reais que podem surgir no mundo virtual, especialmente devido à constante mutação e desenvolvimento, havendo novidades em uma velocidade ainda não acompanhada pelo Direito, por isso a responsabilização por atos ilícitos praticados na *internet* é tão complexa, fazendo-se necessária normas específicas para o ambiente cibernético (Zanatta, 2010).

O campo jurídico já se adaptou de diversas maneiras à realidade virtual e às inovações tecnológicas, contudo, ainda existe uma forte resistência em entender as novas formas sociais e culturais resultantes do surgimento da sociedade da informação e tecnologia, especialmente entre acadêmicos, juristas e profissionais do direito.

2.1 Acepção de Crimes Cibernéticos

A partir do momento em que a banda larga de acesso à internet se popularizou, a plataforma da web 2.0 passou a ser viável, além de possíveis as aplicações on-line participativas. Então, pode observar-se a proliferação das redes sociais *on-line* o tempo todo, sendo assim permitido a sua formação (Gabriel, 2010).

Assim, considerando que não é mais possível fazer a separação entre *internet* e fenômenos sociais, se faz necessária a adaptação aos novos meios de relações interpessoais informatizadas e às consequências decorrentes da nova era digital, como o surgimento de novas formas de práticas de crimes.

Neste ângulo, é possível concluir que os crimes cometidos pela *internet* trouxeram maior complexidade à aplicação do direito, especialmente para o direito penal. Cabe observar que surgiram novos crimes que somente podem ser cometidos por meio da *internet* ou por dispositivos telemáticos e informáticos, os chamados crimes virtuais. Portanto, as inovações

legislativas no que tange aos institutos penalizadores se mostraram extremamente necessárias, considerando o crescimento da rede e da conexão humana, que se dá de forma quase integral, às novas tecnologias.

Ainda não se trata de uma tarefa simples a definição desses crimes, que vão desde *spams* até exposição de informações sigilosas ou pessoais, transferência de vírus ou mesmo a invasão de dispositivos. Esporadicamente vão surgindo inovações no que tange a esses delitos. Entretanto, os crimes cibernéticos impróprios (ou impuros) ainda são preponderantes, pois consistem em atingir os meios jurídicos já tipificados utilizando-se de um instrumento tecnológico, como computador ou celular, por meio da rede informática, não permanecendo necessariamente na esfera virtual.

Sendo assim, após se definir os crimes cibernéticos e sua forma de execução, é possível o uso de analogia para aplicação do Código Penal, enquanto inexistente tipificação mais específica. Os crimes cibernéticos impróprios são mais facilmente observados e punidos, por se assemelhar a crimes já tipificados na norma penalizadora.

O ordenamento jurídico brasileiro ainda carece, no entanto, de normas mais específicas para coibir tais práticas, especialmente os crimes cibernéticos próprios. Mesmo que as normas específicas sejam estabelecidas, ainda será necessário percorrer um longo caminho até a efetiva dissuasão dos possíveis criminosos, visto a facilidade e agilidade com que esses crimes podem ser cometidos, principalmente de forma anônima.

O Brasil, apenas a partir de poucas décadas atrás, passou a preocupar-se com as consequências do acelerado desenvolvimento tecnológico e informático, com a promulgação de leis como a “Lei Carolina Dieckmann” e o “Marco Civil da Internet”, que representaram referências para o aprimoramento normativo que já se fazia necessário. Ou seja, é visível e latente a necessidade de evolução legislativa no que tange a punibilidade dos crimes virtuais, por meio da criação de leis específicas e efetivas, a fim de combater os delitos no âmbito da rede internacional de computadores.

O Superior Tribunal de Justiça, por meio de seu informativo eletrônico, já se manifestou quanto à inexistência de legislação específica que tipifique os crimes cibernéticos, dissertando acerca da necessidade latente dessas inovações legislativas, bem como sobre as dificuldades enfrentadas pelos aplicadores do direito:

Na ausência de uma legislação específica para crimes eletrônicos, os tribunais brasileiros estão enfrentando e punindo internautas, crackers e hackers que utilizam a rede mundial de computadores como instrumento para a prática de crimes. Grande parte dos magistrados, advogados e consultores jurídicos considera que cerca de 95% dos delitos cometidos eletronicamente já estão tipificados no Código Penal brasileiro por caracterizar crimes comuns praticados por meio da internet. Os outros 5% para os

quais faltaria enquadramento jurídico abrangem transgressões que só existem no mundo virtual, como a distribuição de vírus eletrônico, cavalos-de-troia e worm (verme, em português) (Brasil, 2008).

Por isso, conclui-se que para a aplicação do direito de maneira satisfatória no que tange aos crimes virtuais, não basta que o magistrado venha a realizar uma interpretação extensiva ou analógica no caso concreto, sendo necessário que exista uma legislação específica que possibilite o enquadramento jurídico adequado dessas transgressões.

Quando se fala em *cybercrimes*, a privacidade é o primeiro ponto que deve vir a ser destacado, tanto que na literatura o primeiro tipo de lei para amparar o usuário aconteceu em 2012, porém, antes dessa data, outras leis já haviam sido criadas para que fosse aumentada a segurança sobre outros tipos de crimes, que foram se expandindo juntamente com a internet.

Os principais passos para atualização penal, no que diz respeito aos crimes informáticos, remetem à compreensão de como são definidos esses crimes e como se apresentam, conforme será demonstrado.

De acordo com esse contexto, é de fundamental importância que seja apurado o exato momento que tenha ocorrido o fato típico, de modo que seja corretamente aplicada a norma penal, já que os meios informáticos trazem uma pequena dissociação temporal, possibilitando a programação de um delito. Portanto, a ação poderia acontecer em tempo real ou ficto, dependendo da vontade do agente. Assim, para efeito penal, será válida como referência a ação inicial que programou a execução, ainda que essa aconteça em momento posterior.

Sobre o lugar do crime, adotou-se como regra o princípio da territorialidade, porém o meio virtual não possui espaço físico delimitado, gerando assim um acesso dinâmico amplo, onde a concepção de território como espaço físico dá lugar para o virtual, vindo a transcender os limites territoriais e ensejando na aplicação do princípio da extraterritorialidade para ser resolvido o conflito.

No que diz respeito à materialidade, o crime digital é um ilícito que deixa vestígios, sendo imposta a perícia nos termos do Código de Processo Penal. O perito possui obrigação de informar ao magistrado todas as circunstâncias necessárias para demonstrar a ocorrência do crime, além da comprovação de determinada autoria.

Os crimes cometidos pela internet seguem a regra geral de competência para julgamento, que se encontra disposta no Código de Processo Penal em seu artigo 69, *in verbis*: “Determinará a competência jurisdicional: I - o lugar da infração; II - o domicílio ou residência do réu; III - a natureza da infração; IV - a distribuição; V - a conexão ou continência; VI - a prevenção; VII - a prerrogativa de função” (Brasil, 1941).

Por esses motivos, os crimes de possível constatação de localidade serão processados no foro em que foi produzido o resultado. Existem vários tipos de Crimes Cibernéticos. O primeiro tipo de *cybercrime* é o *Revenge Porn*. O referido termo é uma expressão que foi criada nos Estados Unidos, possuindo o conceito de pornografia de vingança ou pornografia de revanche. É usado quando se refere a divulgação de fotos, vídeos, áudios, montagens, ou qualquer outro material sexualmente gráfico, íntimo e privado, sem autorização, com a finalidade de exposição da vítima e causar danos.

Sobre o conceito do termo, afirma Burégio (2015, online):

O termo consiste em divulgar em sites e redes sociais fotos e vídeos com cenas de intimidade, nudez, sexo à dois ou grupal, sensualidade, orgias ou coisas similares, que, por assim circular, findam por, inevitavelmente, colocar a pessoa escolhida a sentir-se em situação vexatória e constrangedora diante da sociedade, vez que tais imagens foram utilizadas com um único propósito, e este era promover de forma sagaz e maliciosa a quão terrível e temível vingança.

As vítimas dessa divulgação não-consensual, expostas na internet para o livre acesso de qualquer pessoa interessada, passam a serem humilhadas, intimadas, perseguidas e assediadas, em um ciclo que é conhecido pela teoria feminista como *slut-shaming*.

Portanto, para que fossem solucionadas as divergências e na tentativa de coibir tais práticas, a conduta passou a ser considerada crime, mediante a implementação da Lei nº 13.718/18, inserindo novos crimes no texto do Código Penal. Surgiu, por conseguinte, a figura do crime de divulgação de cena de estupro ou de cena de sexo ou pornografia, descrito no artigo 218 – C do Código Penal.

No Livro “Exposição Pornográfica Não Consentida na Internet”, os autores Spencer Sydow e Ana Laura Castro fizeram a seguinte divisão do *caput* do artigo supracitado:

(a) a divulgação do registro do crime de estupro, possibilitando que o agente seja penalizado por incidir em ambos os tipos, (b) a apologia ou indução à prática do crime de estupro, atividade que diz respeito apenas ao uso de fotografia, vídeo ou outro registro audiovisual visando estimular o referido crime, e busca atingir especialmente a disseminação de sítios voltados à propagação de discursos de ódio que fomentam crimes sexuais, e (c) registros de cenas de sexo, nudez ou pornografia sem o consentimento da vítima (Castro, Sydow, 2019, p. 134).

Para os autores, o legislador quis que fosse preservada a dignidade, intimidade e privacidade, sendo afastada somente a proteção específica da honra, já que a mesma possui caráter subjetivo de prejuízo à vítima. Destacam, também, que a consumação pode ser tanto instantânea quanto permanente, pois o agente é o que possui o poder de parar a conduta lesiva, vindo assim a gerar a possibilidade de tentativa.

Outro tipo de crime virtual é a *sextorsão*, a qual é oriunda da junção dos vocábulos sexo e extorsão. Trata-se de uma situação onde a posição de poder do criminoso é utilizada como

um instrumento para obter a vantagem de cunho libidinoso, se aproveitando do medo e vergonha da vítima, portanto, é uma chantagem *on-line* que se dá pelo constrangimento de uma pessoa à prática sexual ou pornográfica registrada em foto ou vídeo para envio, em troca de ser mantido o sigilo, não possuindo qualquer garantia.

O Promotor de Justiça e professor de Direito Penal e Processo Penal, Rogério Sanches Cunha afirma que:

A prática que passou a ser conhecida como *sextorsão* refere-se a uma forma de exploração sexual na qual a vítima é chantageada através da ameaça de publicação de imagens e vídeos de si mesma, dotadas de cunho sexual, previamente compartilhadas mediante *sexting* ou subtraídas de seus arquivos pessoais digitais, objetivando a obtenção de alguma vantagem. Nessas situações é comum que a vítima seja constrangida a enviar mais mídias de conteúdo erótico ao agressor, constantemente sob a ameaça de divulgação tanto do conteúdo original quanto deste último obtido sob chantagem (Cunha, 2019, online).

Porém, no Brasil, não existe uma adequação típica correta e específica para o crime, gerando insegurança jurídica e a sensação de impunidade, além de esbarrar no princípio da proibição da analogia e da estrita legalidade adotados pelo ordenamento jurídico brasileiro.

Outro tipo de delito cibernético é o estupro virtual, sendo considerado um estupro que é caracterizado pela não utilização da força física para dominar a vítima, já que no âmbito da internet somente é possível empregar a violência por meio do domínio psicológico, se resumindo a ameaças, chantagens e constrangimentos. Quanto à possibilidade da configuração do crime de estupro sem a necessidade de contato físico, por meio eletrônico, afirma Fernando Capez:

A hipótese em comento não se confunde com aquela em que a vítima é obrigada a praticar atos libidinosos em si própria, como a masturbação para que o agente a contemple lascivamente. Embora nesses casos não haja contato físico entre ela e o agente, a vítima foi constrangida a praticar ato libidinoso em si mesma. Surge aí a chamada autoria mediata ou indireta, pois o ofendido, mediante coação moral irresistível, é obrigado a realizar o ato executório como longa manus do agente (Capez, 2017, p. 23).

No ano de 2017, no Estado do Piauí, existiu o primeiro caso conhecido de estupro virtual no Brasil, vindo a tornar-se de extrema relevância para o ordenamento jurídico. O tema ainda é muito debatido por não haver uma posição pacificada sobre o assunto, porém o Supremo Tribunal Federal interpretou que o contato físico é dispensável para que seja configurado o tipo penal presente no artigo 213 do Código Penal, confirmando o entendimento em decisão proferida no ano de 2017 ao julgar o Recurso Extraordinário com Agravo nº 1066864 RS. Na decisão, afirma o Ministro Dias Toffoli:

[...] a maior parte da doutrina penalista pátria orienta no sentido de que a contemplação lasciva configura o ato libidinoso constitutivo dos tipos dos arts. 213 e 217-A do Código Penal - CP, sendo irrelevante, para a consumação dos delitos, que haja contato

físico entre ofensor e ofendido. [...] Com efeito, a dignidade sexual não se ofende somente com lesões de natureza física. A maior ou menor gravidade do ato libidinoso praticado, em decorrência a adição de lesões físicas ao transtorno psíquico que a conduta supostamente praticada enseja na vítima, constitui matéria afeta à dosimetria da pena, na hipótese de eventual procedência da ação penal (Brasil, 2018).

No ano de 2019, em São Paulo, um rapaz de 25 anos, mantinha contato com uma mulher via rede social *WhatsApp* e, quando obteve sua confiança, convenceu a vítima a lhe enviar fotos íntimas. Posteriormente, ao receber ameaças, foi obrigada a enviar foto pornográfica da sua filha. Nesse caso, é possível enquadrar o fato ao tipo penal de estupro, partindo do advento da Lei nº 12.015/2009, que trouxe atualizações ao capítulo dos crimes contra a dignidade sexual.

Cabe também destacar a prática do *sexting* e a exposição íntima não autorizada. O termo é utilizado para se referir à exposição do corpo nu ou seminu em virtude de desejo próprio ou de terceiros, através de tecnologias digitais, sendo usado para expressar a sexualidade. Porém o problema aparece quando as referidas imagens são expostas sem ter a permissão e o consentimento da vítima, vindo a gerar um constrangimento público ou danos, muitas vezes irreparáveis. Sobre o assunto, afirma Suzana da Conceição Barros:

O *sexting* consiste no envio, compartilhamento e postagem de mensagens eróticas, fotos de corpos desnudos e de vídeos que mostram relações sexuais, ou seja, de materiais que apresentam conteúdos sexuais, sensuais e eróticos, por meio de tecnologias digitais (smartphones, tablets, computadores, e sites de redes sociais, como Facebook e Twitter etc.), para namorados/as, ficantes, paqueras, amigos/as, ou para uma multidão de conhecidos/as e desconhecidos/as, quando postados na internet, por exemplo. Crianças, adolescentes, adultos, isto é, sujeitos de diferentes faixas etárias, vêm aderindo a essa prática (Barros, 2019).

Assim, entende-se que *sexting* é uma conduta que coloca em risco o direito da personalidade, intimidade, honra e a boa fama, já que pode provocar consequências à imagem, por tempo indeterminado. Assim, é imperioso que sejam criados tipo penais específico para a conduta, assim como as demais, com penas proporcionais ao sofrimento causado às vítimas.

3 O DIREITO À PRIVACIDADE E INTIMIDADE NA SOCIEDADE INFORMATIZADA

Com o grande avanço da internet, os direitos à intimidade e privacidade tem sido constantemente violados, pessoas acabam por ficar mais vulneráveis e algo que é extremamente pessoal acaba sendo invadido, ou até mesmo exposto, causando problemas para a vítima. Independentemente de fazer parte do grupo de pessoas sem grande conhecimento sobre o

ambiente virtual ou do grupo de usuários mais experientes, ninguém está totalmente livre de usuários e programas maliciosos.

A segurança de dados é utilizada para manter o sigilo e ter controle das ações que serão efetuadas no conteúdo guardado pelo interessado, e por isso, organizações também estão buscando se capacitar e aperfeiçoar em instrumentos e recursos que possam garantir a segurança de seus dados. A tecnologia pode ser a melhor ferramenta para gerar recursos de segurança. Com isso, empresas passaram a adotar metodologias práticas para concretizar a segurança de seus dados (Alves, 2006).

Para um profissional acessar e manusear um banco de dados, é necessário se ter uma permissão para acessar a devida informação. Elmasri e Navathe (2011) exemplificam que um administrador deve ter a permissão para alterar as informações de alunos, mas pode acabar usando esse privilégio para atualizar notas de alunos sem a permissão do instrutor. Conclui-se, portanto, que uma permissão de grande responsabilidade não pode, de forma alguma, ser utilizada de forma maliciosa ou indevida.

Para Machado (2004), para que o dado fique protegido do uso indevido de qualquer usuário, recursos como a linguagem SQL podem permitir que se defina os privilégios que cada um pode ter em relação às tabelas criadas no banco de dados. Dessa forma, os privilégios garantem a segurança e a integridade dos dados, bem como a responsabilidade de cada usuário sobre seus dados específicos.

Como visto anteriormente, um acesso restrito usado de maneira maliciosa pode trazer um grande risco. Segundo Sêmola (2003, p. 67), “risco é a probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e/ou disponibilidade, causando, possivelmente, impactos nos negócios”.

Além da incumbência de preservar e proteger os dados para o bom funcionamento das organizações, projetistas de bancos de dados possuem a responsabilidade de proteger a privacidade das pessoas sobre as quais os dados são mantidos. Privacidade pode ser definido como direito das pessoas de ter algum controle sobre suas próprias informações (Sêmola, 2003)

De acordo o Alves (2006), a armazenagem de dados pode ser considerada a espinha dorsal de muitos aplicativos atualmente. Portanto, os ataques aos bancos de dados também estão aumentando, e essas são formas muito perigosas de ataques, pois estes revelam dados privados e importantes para o invasor.

No Brasil, o primeiro caso de grande relevância e notoriedade foi da atriz Carolina Dieckmann, ocorrido no ano de 2011, ocasião em que um hacker invadiu o seu computador pessoal e roubou diversas fotos íntimas, bem como ameaçou divulgar as fotos caso não

recebesse a recompensa solicitada. Como consequência desse fato, ainda no ano de 2011, foi apresentado o projeto de lei para tipificar o crime de invasão de dispositivo telemático, tendo sido aprovado em dezembro de 2012. O ponto de maior relevância da nova norma foi a inclusão de novos tipos penais incriminadores ao Código Penal, os artigos 154-A e 154-B.

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.

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é 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 (Brasil, 1941).

Esses artigos tratam do comportamento de acesso forçado à dispositivos telemáticos sem a autorização dos proprietários, geralmente com intuito malicioso. Trata-se de um crime formal, pois não importa se o resultado de fato é alcançado, bastando a tentativa de invasão para restar tipificado o delito. Uma das formas de prática do crime de invasão de dispositivos é o *Phishing*, conceito em Inglês que significa “pescar”. Trata-se de um golpe comum na internet, que por meio de e-mail, telefone ou mensagem de texto, o criminoso “pescar” a vítima com o objetivo de roubar informações pessoais. A vítima apenas precisa clicar em um *link* ou arquivo e preencher com seus dados para ser invadido.

Os assuntos das mensagens e *e-mails* são bem diversificados, onde os invasores fingem ser organizações ou instituições confiáveis, como Correios, bancos ou sites de compras, de modo a convencer a vítima a fazer algum procedimento ou preencher algum dado sensível. Caso a vítima confie e realize o procedimento, o dispositivo é invadido ou os dados são roubados.

O código penal faz menção a respeito da violação no direito à privacidade nos seguintes artigos, *in verbis*:

Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:

Art. 151 - Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem:

II - Quem indevidamente divulga, transmite a outrem ou utiliza abusivamente comunicação telegráfica ou radioelétrica dirigida a terceiro, ou conversação telefônica entre outras pessoas (Brasil, 1941).

Esses artigos dispõem sobre a divulgação de conteúdo particular ou correspondência confidencial, da qual a divulgação cause danos a outros, sendo admissível a tentativa. Diniz (2007) cita que, quando ocorre a violação da intimidade e da privacidade, a vítima será protegida constitucionalmente, caso seus arquivos pessoais sejam compartilhados na internet.

A intimidade é a zona espiritual íntima e reservada de uma pessoa ou de um grupo de indivíduos, constituindo um direito da personalidade, daí o interesse jurídico pelo respeito à esfera privada. Desse modo, o autor da intrusão arbitrária à intimidade alheia deverá pagar uma indenização pecuniária, fixada pelo órgão judicante de acordo com as circunstâncias, para reparar dano moral ou patrimonial que causou. Além disso, deverá o magistrado ordenar medida que obrigue o ofensor a cessar suas ingerências na intimidade alheia, se estas ainda continuarem e, se possível, deverá exigir o restabelecimento da situação anterior à violação, a expensas do lesante, como, p. ex., a destruição da coisa produzida pelo atentado à intimidade (Diniz, 2007, p. 160).

Em muitos casos de violação da intimidade, entretanto, existe a dificuldade em avaliar o valor que será pago de indenização pelo dano moral sofrido. Embora a proteção à intimidade e à vida privada esteja prevista na Constituição Federal, destaca-se o Marco Civil da Internet, como sendo a primeira lei infraconstitucional a regulamentar o tema. Esclarece ser cabível indenização por dano moral ou material comprovado, automaticamente, decorrente da violação dessas proteções na internet (Damásio, 2014).

Paralelamente, no que tange aos direitos à intimidade e à vida privada, Sílvia Romero Beltrão possui a seguinte visão:

A intimidade e a vida privada são erigidas na Constituição como valores humanos, na condição de direito individual e para tanto em defesa deste direito fundamental, nos preocupamos em preservá-las do conhecimento alheio. Nossos erros, nossas imperfeições e até mesmo nossas virtudes não devem estar obrigatoriamente expostas ao domínio público, pois, interesses variados podem forçar-nos a ocultar determinados fatos do conhecimento de outras pessoas. Vários exemplos poderiam ser citados, como interesses exclusivos de ordem privada e íntima, a justificar a sua preservação do conhecimento alheio. Em tais situações, terceiros desautorizados não podem violar os segredos e reservas da pessoa, pois, certamente causariam transtornos e danos irreparáveis. (Beltrão, 2017, p. 1)

Dessa forma, pode-se constatar que, a Constituição visa proteger a liberdade de expressão, em todas as suas modalidades, e a privacidade em todos os seus níveis de densidade, sendo uma exigência democrática que está ligada à proteção dos direitos humanos e fundamentais albergados na Carta Magna. Entretanto, se faz necessária a elaboração de dispositivos que regulamentem de maneira mais específica e detalhada as proteções que se busca garantir.

4 A PROTEÇÃO DE DADOS PESSOAIS NA INTERNET

A proteção de dados pessoais no Brasil é regulamentada pela Lei nº 13.709/2018, a qual tem como premissa assegurar o respeito à vida privada em relação aos fluxos comunitários de dados pessoais. Como já dito, seu objetivo é proteger "os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (Brasil, 2018).

Popularmente conhecida como a Lei Geral de Proteção de Dados Pessoais (LGPD), dispõe em seu art. 2º os fundamentos que busca disciplinar, quais sejam: a proteção de dados pessoais no respeito a privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e na inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor e essencialmente os direitos humanos.

O titular dos dados pessoais é a pessoa natural (física) a quem se referem os dados pessoais que são objeto de tratamento, observando-se que as pessoas jurídicas não são incluídas. O artigo 5º da LGPD define, também, o que é dado pessoal, sendo a “informação relacionada à pessoa natural identificada ou identificável” e dado sensível como “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (Brasil, 2018).

A referida lei não será aplicada no tratamento de dados pessoais em virtude de pessoa natural para fins exclusivamente particulares e não econômicos, jornalísticos, artísticos ou acadêmicos. No entanto, torna-se efetiva para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. (Brasil, 2018)

Os princípios norteadores desta lei estão inseridos em seu artigo 6º, além da boa fé, o princípio da finalidade descrito na própria Lei como a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (Brasil, 2018), bem como o princípio da adequação, definido como a “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento”, ou seja, os dados devem ser adequados, pertinentes e não excessivos em relação a seus fins (Brasil, 2018).

Tem-se também o princípio da necessidade, descrito como a "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados"; o princípio do livre acesso, descrito como a "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integridade de seus dados pessoais"; princípio da qualidade dos dados, descrito como a "garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento" (Brasil, 2018). Nesse princípio, é possível

compreender que as informações incorretas devem ser corrigidas, as obsoletas ou impertinentes devem ser suprimidas, assim como ainda é possível que o proprietário dos dados solicite eventuais acréscimos e atualizações para manter a exatidão dos dados, buscando prover o melhor direito do titular por manter as informações sempre condizentes com a realidade.

Encontra-se descrito, ainda, o princípio da transparência, que dá o direito ao titular da existência de um arquivo de dados; o princípio da segurança, que exige “utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão”; o princípio da prevenção, traduzido na “adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais”; princípio da não discriminação, que consiste na “impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos”, os dados devem ser tratados para determinados propósitos que devem ser informados ao titular (Brasil, 2018).

Cabe registrar que, no que diz respeito ao tratamento e utilização de dados pessoais, poderão ser realizados desde que haja consentimento do titular, bem como essa manifestação de vontade deve ser expressa por escrito ou outro meio que evidencie a concordância do indivíduo. Para toda pessoa natural, é assegurada a titularidade de seus dados pessoais, garantido seus direitos fundamentais e assegurando a confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexistentes ou desatualizados, anonimização, bloqueio ou eliminação de dados desnecessários (Brasil, 2018).

Para regular a LGPD, foi criada através da Medida Provisória (MP) 869/2018, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal que é submetida ao regime autárquico especial vinculado à Presidência da República. A ANPD é composta por Conselho Diretor, órgão máximo de direção; Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; Corregedoria; Ouvidoria; órgão de assessoramento jurídico próprio e unidades administrativas e unidades especializadas necessárias à aplicação do disposto desta Lei.

No dia 29 de abril de 2020 foi publicada a Medida provisória (MP) 959/2020 que adiou a entrada em vigor da LGPD para 03 de maio de 2021. A prorrogação foi motivada em virtude da Pandemia do Coronavírus no intuito de que sejam postergadas multas e sanções às entidades.

Com o avanço das mídias sociais, que repercute de forma internacional através das trocas de informações e estabelecimento de comunicações, trata-se de um movimento descentralizado, com formação de redes. Pode-se compreender que essa rede tem o seu funcionamento de forma aberta e dinâmica, assim como com auto reprodução.

Neste sentido, a preocupação com a transmissão dos dados também deve ser algo determinante nas mídias sociais. Um fator importante neste aspecto foi a origem da LGPD, que surgiu após a grande repercussão da divulgação de dados pessoais pela rede social Facebook. Agora, com o advento desta lei, isso se tornou inadmissível, como estabelece nos seus artigos 46, 47, 48, bem como nos seus incisos e parágrafos, que descrevem sobre as medidas de segurança, técnicas e administrativas, que dever ser utilizadas para a proteção dos dados pessoais.

Dessa forma, pode-se depreender a respeito da segurança no sigilo das informações das pessoas no âmbito virtual, no qual os responsáveis pelas mídias sociais devem adotar medidas de segurança com o intuito de fornecer proteção aos dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de alteração ou utilização. Instituições públicas, financeiras, educacionais ou de telecomunicações, também possuem responsabilidade no tratamento e utilização dos dados pessoais.

Assim, a Lei Geral de Proteção de Dados adentrou no nosso ordenamento jurídico trazendo muitas novidades a respeito da proteção de dados pessoais, transformando drasticamente a maneira que empresas e órgãos públicos tratam a privacidade e segurança de seus usuários, que terão o exercício pleno da autodeterminação informativa em relação aos seus dados.

5 CONSIDERAÇÕES FINAIS

O presente trabalho reflete acerca da aplicação dos dispositivos penais aos crimes cibernéticos no âmbito do ordenamento jurídico brasileiro, bem como analisa o surgimento de novos institutos penalizadores mais específicos, com intuito de punir e coibir tais práticas.

Para tanto, foram demonstrados os princípios constitucionais como direitos fundamentais, que são inerentes à dignidade da pessoa humana, considerando os seus aspectos na Carta Magna. Através disso, pode-se constatar que, no que tange à aplicação da lei de exposição dos dados, tratando-se nos bancos, há existência de sigilo bancário, devendo os bancos a obrigatoriedade de manter os dados dos seus clientes com sigilo, buscando gerar a proteção do patrimônio destes.

A internet representa um instrumento social e tecnológico de extrema relevância, com o intuito de trazer facilidade de comunicação e acesso à informação, simplificação de tarefas, assim como a alta oferta de entretenimento. No entanto, dentro deste processo evolucionário e de globalização digital, há cada vez mais modalidades de crimes cibernéticos.

O Brasil é inseguro em relação à criminalidade cibernética, tanto em matéria legislativa quanto no tratamento oferecido aos crimes virtuais, e por mais que as leis vigentes tratem de alguma maneira a matéria exposta, pode-se afirmar que o Brasil ainda carece de muitas inovações no seu diploma penal, afinal, há necessidade de se observar e discutir o que a criminalidade informática causa e como evolui.

A complexibilidade legislativa, nacional e internacional, não pode mais ser a causa da insegurança digital, haja vista que, seja o computador utilizado para a prática do delito ou para se tornar alvo desse crime, cabe ao Estado zelar pela integridade da informação ali contida ou pela materialidade do bem.

Através deste estudo, pode-se demonstrar as mais diversas tentativas de coibir e conter o crescimento dos crimes cibernéticos no Brasil, onde se destaca o surgimento de Delegacias especializadas e de algumas inovações legislativas. No entanto, fica clara a discrepante velocidade com que os meios de comunicação e armazenamento de dados, a internet e os dispositivos informáticos evoluem em comparação às normas jurídicas, tornando impossível que o direito tutele toda e qualquer lesão ou ameaça de lesão aos bens jurídicos feitas por meio da internet de forma imediata, pelo menos de forma específica.

No mais, é essencial que, assim como aconteceu na Lei 12.737/12, o legislador busque sempre observar atentamente a evolução da rede mundial de computadores e os novos delitos decorrentes disso. Ao verificar o surgimento de novos delitos, se faz necessária a rápida atualização dos dispositivos normativos penalizadores. Dessa forma, será possível garantir, da melhor forma possível, que a internet atenda à finalidade para que fora criada, que é facilitar a vida em sociedade e possibilitar o acesso às informações e tecnologias de maneira mais fácil, segura e positiva

REFERÊNCIAS

ALVES, Gustavo Alberto. **Segurança da informação**: Uma visão inovadora da gestão. 1ª ed. – São Paulo: Ciência Moderna, 2006.

BELTRÃO, Silvio Romero. **Direito da personalidade à intimidade**. 2017. Disponível em: <http://www.tjpe.jus.br/documents/33154/34767/cap09.pdf/04061934-de43-437e-a2a4-9a68947dafa0>. Acesso em: 06 out. 2024.

BRASIL, Supremo Tribunal Federal. **ARE: 1066864 RS - RIO GRANDE DO SUL 0370400-39.2012.8.21.7000**, Relator: Min. DIAS TOFFOLI, Data de Julgamento: 17/08/2017, Data de Publicação: DJe-186 23/08/2017. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/stf/492489613>. Acesso em 04 out. 2024.

BRASIL. **Decreto-Lei nº 2.848, de 07 de dezembro de 1940**. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 de dezembro de 1940.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 15 de agosto de 2018.

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. Diário Oficial da União, Brasília, 3 de dezembro de 2012.

BRASIL. **Lei nº. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, 24 de abril de 2014.

BRASIL. **Medida provisória nº 869, de 27 de dezembro de 2018**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Diário Oficial da União, Brasília, 28 de dezembro de 2018.

BRASIL. Superior Tribunal de Justiça. **Justiça usa Código Penal para combater crime virtual**. Disponível em: <https://stj.jusbrasil.com.br/noticias/234770/justica-usa-codigo-penal-para-combater-crime-virtual>. Acesso em: 06 out. 2024.

BRASIL. Supremo Tribunal de Justiça. **Recurso especial Nº 1117633/RO, Relator: Ministro Herman Benjamin**. Brasília, 09 de março de 2010. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/8569044/recurso-especial-resp-1117633-ro-2009-0026654-2/inteiro-teor-13668131>. Acessado em: 04 out. 2024.

BURÉGIO, Fátima. **Pornografia da Vingança**: você sabe o que é isto? 2015. Disponível em: <https://ftimaburegio.jusbrasil.com.br/artigos/178802845/pornografia-da-vinganca-voce-sabe-o-que-e-isto>. Acesso em: 05 out. 2024.

CAPEZ, Fernando. **Curso de direito penal 3**. 15 ed. São Paulo: Saraiva, 2017.

CASTRO, A. L. C. de; SYDOW, S. T. **Exposição pornográfica não consentida na Internet**: da pornografia de vingança ao lucro. Belo Horizonte: D'Plácido, 2019. p. 134-136. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.959.02.PDF. Acesso em: 05 out. 2024.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**, 7º volume: responsabilidade civil. 21. ed. São Paulo: Saraiva, 2007.

ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de bancos de dados**. 6ª ed. São Paulo: Addison Wesley, 2011.

GABRIEL, Martha. **Marketing na Era Digital**. São Paulo: Novatec Editora, 2010, p. 83.
JESUS, Damásio de; MILAGRE, José Antônio. **Marco Civil da Internet: comentários à Lei n. 12.965/14**. São Paulo: Saraiva, 2014.

MACHADO, F. N. R. **Bancos de Dados: Projeto e Implementação**. São Paulo: Ed. Erica 2004.

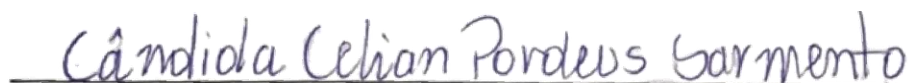
PINHEIRO, Patricia Peck. **Direito Digital**. 7. ed. São Paulo: Saraiva Educação, 2021.
SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. Rio de Janeiro: Elsevier, 2003.

ZANATTA, Leonardo. **O direito digital e as implicações cíveis decorrentes das relações virtuais**. Rio Grande do Sul, 2010.

DECLARAÇÃO DE REVISÃO ORTOGRÁFICA

Eu, Cândida Celian Pordeus Sarmento, graduada em Letras pela Universidade Federal do Maranhão (UFMA), declaro para o Centro Universitário UNINOVAFAPI que revisei o Trabalho de Conclusão de Curso de Bacharelado em Direito intitulado **“A EVOLUÇÃO LEGISLATIVA E A REALIDADE DOS CRIMES VIRTUAIS NO BRASIL: UMA ANÁLISE SOBRE O DIREITO À PRIVACIDADE E À INTIMIDADE”** dos alunos: FRANKLIN SOUSA DAMASCENO, JASMYM CARDOSO DE MELO e JOÃO PEDRO BARBOSA ALVES. Declaro ainda que o presente trabalho encontra-se de acordo com as normas ortográficas e gramaticais vigentes.

Teresina, 03 de novembro de 2024.



Cândida Celian Pordeus Sarmento
CPF: 349.912.395-91