CRIMES CIBERNÉTICOS: O COMPARTILHAMENTO DE FOTOS, VÍDEOS E CONTEÚDOS ÍNTIMOS POR MOTIVO DE VINGANÇA

Cybercrimes: sharing photos, videos and intimate content for revenge

Ciber delitos: compartir fotos, videos y contenido íntimo para venganza

João Antonio Maciel da Silva[1]
Paulo Izidio da Silva Rezende[2]**.**

RESUMO: Os delitos cibernéticos, ao longo do tempo, evoluíram de eventos isolados para uma ameaça global, acompanhando o avanço da rede mundial de computadores e da tecnologia. No entanto, esses avanços tecnológicos também se converteram de atos de mera curiosidade tecnológica em empreendimentos ilícitos altamente rentáveis, explorando as motivações e os métodos subjacentes a essa mudança. Dentre as várias espécies de crimes digitais, encontra-se aqueles que buscam expor a intimidade e a privacidade de indivíduos. Diante disso, esse estudo teve a finalidade de analisar os efeitos jurídicos dos crimes cibernéticos no que concerne ao compartilhamento de fotos, vídeos e conteúdos íntimos por motivo de vingança. Na metodologia, baseou-se em uma revisão bibliográfica, com fundamento em artigos científicos, livros, periódicos e na legislação atual sobre o respectivo tema. A coleta de dados foi realizada por meio de banco de dados tais como Scielo, Google Acadêmico, dentre outros, no período de 2018 a 2024. Nos resultados, destacou-se que, conhecida na doutrina e na jurisprudência como “revenge porn”, ou pornografia de vingança, é uma forma de violência contra qualquer pessoa, especialmente a mulher, punível criminalmente. A partir da Lei nº 13.718, de 2018, a divulgação de cenas de sexo, nudez ou pornografia, sem o consentimento da vítima, passou a receber tratamento criminal mais rigoroso, com o acréscimo do art. 218-C ao Código Penal, punido com pena de reclusão de um a cinco anos, bem como de seu § 1º, que aumenta a pena de 1/3 a 2/3 se houver propósito de vingança ou humilhação.

Palavras-chave: Crimes cibernéticos. Intimidade. Compartilhamento. Vingança.

1 Autor. Graduando em Direito pela Universidade de Gurupi (UNIRG). E-mail: joaoamsilva@unirg.edu.br
2 Co-autor. Professor do Curso de Direito pela Universidade de Gurupi (UNIRG). E-mail: paulo_izidio@hotmail.com

ABSTRACT: Cybercrimes have evolved over time from isolated events to a global threat, in line with the advancement of the world wide web and technology. However, these technological advances have also transformed from acts of mere technological curiosity into highly profitable illicit enterprises, exploring the motivations and methods underlying this change. Among the various types of digital crimes, there are those that seek to expose the intimacy and privacy of individuals. In view of this, this study aimed to analyze the legal effects of cybercrimes with regard to the sharing of photos, videos and intimate content for revenge. The methodology was based on a bibliographic review, based on scientific articles, books, periodicals and current legislation on the respective subject. Data collection was carried out using databases such as Scielo, Google Scholar, among others, from 2018 to 2024. The results highlighted that, known in doctrine and jurisprudence as "revenge porn", it is a form of violence against any person, especially women, and is criminally punishable. As of Law nº. 13.718 of 2018, the dissemination of sex scenes, nudity or pornography, without the victim's consent, began to receive stricter criminal treatment, with the addition of art. 218-C to the Penal Code, punishable by imprisonment of one to five years, as well as its § 1, which increases the sentence by 1/3 to 2/3 if there is an intention of revenge or humiliation.

Keywords: Cybercrimes. Intimacy. Sharing. Revenge.

RESUMEN: Los delitos cibernéticos, con el tiempo, han evolucionado desde eventos aislados hasta una amenaza global, siguiendo el avance de la red mundial y la tecnología. Sin embargo, estos avances tecnológicos también han pasado de ser actos de mera curiosidad tecnológica a empresas ilícitas altamente rentables, explorando las motivaciones y métodos subyacentes a este cambio. Entre los diversos tipos de delitos digitales, se encuentran aquellos que buscan exponer la intimidad y privacidad de las personas. Por lo tanto, este estudio tuvo como objetivo analizar los efectos legales de los delitos cibernéticos relacionados con el intercambio de fotos, videos y contenido íntimo con fines de venganza. La metodología se basó en una revisión bibliográfica, basada en artículos científicos, libros, publicaciones periódicas y legislación vigente sobre el tema respectivo. La recolección de datos se realizó a través de bases de datos como Scielo, Google Scholar, entre otras, de 2018 a 2024. En los resultados se destacó que, conocida en la doctrina y la jurisprudencia como "pornografía de venganza", o la pornografía de venganza es una forma de violencia. contra cualquier persona, especialmente las mujeres, lo cual es punible penalmente. A partir de la Ley N° 13.718, de 2018, la difusión de escenas de sexo, desnudos o pornografía, sin el consentimiento de la víctima, pasó a recibir un tratamiento penal más riguroso, con la adición del art. 218-C del Código Penal, castigado con prisión de uno a cinco años, así como su § 1, que aumenta la pena de 1/3 a 2/3 si tiene finalidad de venganza o humillación.

Palabras clave: Delitos cibernéticos. Intimidad. Intercambio. Venganza.

1. INTRODUÇÃO

Desde o surgimento da sociedade, ainda nos primórdios da história da Terra, o ser humano pratica crimes. Seja contra a própria vida, a de outros ou contra objetos e patrimônios, o ser humano comete diversos tipos de delitos. Independente das circunstâncias ou motivação, a prática de crimes na sociedade traz prejuízos não apenas nas vítimas, mas para toda a comunidade.

Os avanços sociais e industriais trouxeram para as pessoas uma vida mais confortável e mais aberta no que diz respeito à economia, política e cultura. Essas rupturas de pensamento, ideologia e vivência social fez com que a vida se tornasse mais prática e mais ágil possível. Tudo isso somado a um mundo cada vez mais unificado em torno de assuntos universais que refletem a todos.

Dentre as mudanças mais significativa ocorrida no seio da sociedade, está o avanço da Informática, que trouxe benefícios para todos, e também estragos e prejuízos de toda ordem. Podem-se citar como exemplos, as fraudes, os furtos, a falsidade ideológica, os vírus, as invasões de privacidade e até um aumento nos casos de pedofilia. Essas situações além de inúmeras outras são alguns dos milhares de casos negativos que a informática e todo o seu aparato trouxeram para o mundo social moderno.

Apesar de trazer inúmeros benefícios, o campo tecnológico da informática também serviu para o surgimento de crimes. Muitos criminosos tem utilizado o espaço digital para praticar diversos delitos. Crimes contra a honra, a privacidade, a imagem, crimes de natureza financeira, dentre outras áreas, são cometidas a todo instante pelos chamados cibercriminosos.

A título de exemplo, dados quantitativos da Secretaria de Segurança Pública (SSP) que realizou pesquisa no Estado de São Paulo mostrou que os crimes cibernéticos tiveram significativo aumento entre os anos de 2019 a 2022. Segundo expõe essa pesquisa, em 2021 foram registrados 2.219 casos, enquanto que em 2022 até o mês de agosto já foram registrados 5.424 casos, representando um aumento de 144% (COLOMBO, 2022).

Dentro desse cenário, encontra-se o compartilhamento de dados ou imagens íntimas de terceiros em razão de vingança. Essa prática tem causado danos psicológicos, emocionais e sociais significativos às vítimas, incluindo estigma, vergonha, humilhação e trauma. Em razão disso, no decorrer desse estudo, propôs-se responder a seguinte indagação: qual o tratamento jurídico dos crimes cibernéticos voltados para a exposição e compartilhamento de fotos, vídeos e conteúdos íntimos por motivo de vingança?

Diante desse contexto, esse estudo teve como objetivo investigar de forma abrangente o fenômeno dos crimes cibernéticos relacionados ao compartilhamento não consensual de fotos, vídeos e conteúdos íntimos por motivo de vingança.

2. DOS CRIMES CIBERNÉTICOS: ASPECTOS GERAIS

Historicamente, os crimes cibernéticos são crimes advindos da internet. Corrêa (2018) determinadas práticas ilícitas são realizadas em desfavor do computador, ao qual são chamados de crimes próprios. No entanto, há os que feitos por meio do computador, que neste caso se configura como crime impróprio. É com base no crime impróprio que se baseia o delito em destaque.

Importante mencionar que a internet surgiu como um projeto de pesquisa militar em 1969, denominado Advanced Research Projects Agency, ficando conhecida como Arpanet, tendo se integrado ao Departamento de Defesa dos Estados Unidos durante o período de Guerra Fria, com a finalidade estimular o desenvolvimento dos recursos de pesquisa, objetivando superar tecnologicamente a União Soviética. Podendo este ser considerado o marco inicial da internet e também o surgimento da era da informação (CORRÊA, 2018).

Silva (2019) por sua vez entende que o crime cibernético tem raízes na criptografia. O autor explica que a criptografia se traduz em esconder ou mascarar informações através de linguagem codificada. Sendo a ciência de ocultar informações, as primeiras e mais rudimentares noções de cibercriminalidade se originam no desígnio de obter essas informações sigilosas, surgindo, portanto, os mais expoentes peritos em técnicas de quebra de códigos da história desde muito antes do advento da internet. Com o advento da internet, surgiram novos meios de interação social, e como tal, também está sujeito a marginalização e criminalidade.

Ao analisar o processo histórico desses crimes, Andrade e Rezende (2020) apresentam os seguintes marcos históricos:

Quadro 1 – Evolução Histórica dos crimes cibernéticos

Lapso temporal	Descrição
Década de 1970 e 1980	Nos primeiros dias da Internet, a principal abordagem de crimes online foi hackers e intrusão nos sistemas de computador. Os primeiros hackers, como Kevin Mitnick, tornaram -se famosos por sua capacidade de penetrar em sistemas e redes.
	Com o aumento da popularidade da Internet,

Década de 1990	surgiram novos tipos de crimes, como fraude online e roubo de informações pessoais. Os criminosos começaram a aproveitar as transações online e os dados confidenciais dos usuários
Década de 2000	O cibercrime tornou-se mais sofisticado com o surgimento de botnets, redes de computadores infectadas por computador que os criminosos poderiam controlar remotamente. Essas botnets foram usadas para lançar ataques distribuídos à negação de serviços (DDOs) e realizar atividades fraudulentas, como um e -mail indesejado (spam). As plataformas de mercado online pretas também surgiram, conhecidas como "mercados negros", onde bens ilegais foram vendidos e comprados, como drogas, armas, dados roubados e serviços criminais.
Década de 2010	O *ransomware* se tornou uma ameaça significativa, com ataques destinados a indivíduos e organizações. Os criminosos criptografaram os arquivos das vítimas e exigiram um resgate para desbloqueá-las. Os ataques em massa a empresas e organismos governamentais se tornaram mais frequentes.
Década de 2020 até o momento atual	O cibercrime continua evoluindo com novas ameaças, como *phishing* sofisticado, engenharia social e uso de inteligência artificial e aprendizado automático por criminosos. O aumento da criptomoeda levou a um aumento no uso de *ransomware*, pois os criminosos podem exigir pagamentos anônimos em criptomoedas.

Fonte: Andrade; Rezende (2020).

Conceitualmente, o crime cibernético refere-se a qualquer atividade criminosa realizada por meios eletrônicos ou digitais (BARRETO, 2018). Os crimes cibernéticos podem incluir uma ampla variedade de atividades maliciosas, como roubo de dados, fraude online, hackers, golpes de e-mail, ataques de malware, representação de identidade e violação da privacidade.

Wendt; Nogueira e Jorge (2019) explicitam que os crimes cibernéticos possuem a classificação formada em 3 (três) tipos: os puros, os mistos e os comuns. Os puros representam a ação de maneira geral, incluindo aí o computador ou outro aparato tecnológico que tenha acesso à internet e as informações internas. Os mistos o foco é gerar danos a algum bem jurídico da vítima. E por fim os crimes comuns, que se designam na ausência da informática para se concretizar. Aqui, ele pode ser realizado na rede para o cometimento de outros delitos, como por exemplo, a difamação, a calúnia, o racismo, a homofobia, a injúria, etc.

Os criminosos cibernéticos geralmente aproveitam as vulnerabilidades dos sistemas e redes de computadores para realizar suas atividades criminosas. Eles podem abordar indivíduos e empresas ou organizações, com o objetivo de obter informações confidenciais, roubar dinheiro, prejudicar a reputação de uma pessoa ou entidade ou causar interrupções e danos significativos (GRECO, 2014).

2.1 ESPÉCIES DE CRIMES CIBERNÉTICOS

Conforme mostrado anteriormente, os crimes cibernéticos são crimes cometidos por meio da internet. Por ser um campo amplo e complexo, muito tem sido feito para que crimes dessa natureza sejam sanados e combatidos. Na busca por um melhor entendimento sobre eles, a doutrina tem-se colocado os crimes cibernéticos de várias espécies.

A primeira delas é o chamado phishing. De acordo com Santos (2021), nesse tipo de fraude, os criminosos são passados por entidades confiáveis, como bancos ou sites legítimos, para enganar as pessoas e obter informações pessoais, como senhas ou números de cartão de crédito.

Há também o ransomware, que é um tipo de malware que calcula os arquivos de um computador ou sistema e exige um resgate para restaurar o acesso a eles. Os dados da vítima são criptografados e usados como refém. Para recuperar o acesso, a empresa ou dono dos dados, tem que pagar a quantidade que os criminosos pedem (OLIVEIRA, 2022).

Há também o roubo de informações pessoais, onde os cibercriminosos podem roubar informações pessoais, como nomes, endereços, números de previdência social ou dados bancários, a fim de usá-los para cometer fraudes ou vendê-los no mercado negro (SANTOS, 2021).

Tem-se ainda os ataques de negação de serviço (DDOs). Eles consistem em inundar um site ou serviço online com uma grande quantidade de tráfego malicioso, o que causa queda do sistema e interrupção do serviço (SANTOS, 2021).

E por fim, menciona-se o hacking. Os hackers podem comprometer sistemas de computador, redes ou contas online para obter acesso não autorizado a informações confidenciais ou causar danos (SANTOS, 2021).

Ainda sobre essa questão, Delmanto et al. (2019, p. 50) acrescentam que existem outras espécies de crimes cibernéticos; a saber:

> *Dessa forma, são crimes que podem admitir sua consecução no meio cibernético: calúnia, difamação, injúria, ameaça, divulgação de segredo, furto, dano, apropriação indébita, estelionato, violação ao direito autoral, escárnio por motivo de religião, favorecimento da prostituição, ato obsceno, escrito ou objeto obsceno, incitação ao crime, apologia de crime ou criminoso, falsa identidade, inserção de dados falsos em sistema de informações, adulteração de dados em sistema de informações, falso testemunho, exercício arbitrário das próprias razões, jogo de azar, crime contra a segurança nacional, preconceito ou discriminação de raça-cor-etnia-etc., pedofilia, crime contra a propriedade industrial, interceptação de comunicações de informática, lavagem de dinheiro e pirataria de software.*

Insta salientar que para combater o crime cibernético, existem equipamentos especializados em agências de segurança e aplicação da lei que investigam esses crimes e procuram identificar e processar os responsáveis. Também é importante que os usuários tomem medidas para se proteger, como usar senhas seguras, manter o software atualizado, ter cuidado ao abrir e-mails ou clica em links suspeitos e usando soluções de segurança de computador, como antivírus e firewalls.

3. LEGISLAÇÃO BRASILEIRA FRENTE AOS CRIMES CIBERNÉTICOS

Em resposta a essas ameaças, governos, organizações de segurança e empresas de tecnologia aumentaram os esforços para combater o crime cibernético. Leis e regulamentos rigorosos foram estabelecidos, e equipes especializadas foram criadas na segurança cibernética e agências policiais para investigar e perseguir criminosos cibernéticos.

No campo legislativo, cita-se primeiramente a Lei nº. 12.737/2012, mais conhecida como a Lei Carolina Dieckmann. Isso se deu porque em 2012 a renomada atriz brasileira foi vítima de exposição indevida da sua intimidade através da divulgação de suas fotos privadas. O caso teve repercussão nacional, o que gerou o debate sobre a necessidade de se ter leis brasileiras mais severas e específicas para os crimes que ocorre na seara digital.

Esta norma tem a finalidade de criminalizar a invasão de computadores. No caso trata-se de hackear informações sigilosas como imagens pessoais, senhas, arquivos. Também tem o intuito de penalizar aqueles que de algum modo exponham imagens, fotos ou vídeos de terceiros sem autorização. Nesse sentido, cita-se o artigo base:

> *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 03 (três) meses a 01 (um) ano, e multa.*

(BRASIL, 2012)

Também é importante mencionar a Lei nº 12.965/2014 que inseriu no ordenamento jurídico brasileiro o Marco Civil da Internet. Essa norma foi criada pelo fato de que nos anos anteriores a sua criação, órgãos do governo federal, empresas públicas e contas particulares foram vítimas de ataques. Com esses atos e seu eventual crescimento, esta norma foi gerada para que haja uma maior proteção aos internautas e que se ampliasse o rol de direitos e deveres para o uso da internet (BRASIL, 2014).

Silva (2020) explica que o Marco Civil da Internet, mesmo que importante, não fugiu de ser debatida. Em alguns pontos ela fora criticada, muito pelo fato de que pouco inovou nas penas e no que já estava em vigor. De todo modo, o presente autor afirma que ela trouxe muitas vantagens, principalmente ao compartilhar a responsabilidade de exposição de dados com os usuários. Ou seja, os usuários também são responsabilizados pelo que produzem e consomem, exceto nos casos onde seus conteúdos sejam expostos sem autorização.

No Brasil, também é necessário citar, aprovada pelo Decreto nº 9.637/2018, a Política Nacional de Segurança da Informação (PNSI) que abrange segurança cibernética, defesa cibernética, segurança física e a proteção de dados organizacionais. Essa política é implementada por intermédio da Estratégia Nacional de Segurança da Informação (ENSI) e pelos planos nacionais.

Dentro dos crimes cibernéticos também é importante mencionar a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), que busca manter uma rede maior de proteção dos dados pessoais e particulares dos cidadãos. Mendes e Doneda (2018) ao explicitarem sobre esta norma, entendem que ela veio oferecer uma tutela mais significativa aos dados particulares dos indivíduos, principalmente quando se há risco permanente de compartilhamento e exposição indevida e sem autorização.

A LGPD veio ao seu turno impor limites ao uso dos dados das pessoas por empresas e órgãos governamentais. Cabe lembrar que conforme expõe o seu art. 5º, I, o dado pessoal é a “informação relacionada a pessoa natural identificada ou identificável” (BRASIL, 2018). Ou seja, dado pessoal é qualquer documento ou informação que permite identificar uma pessoa, como por exemplo, o nome, telefone, Certidão de Nascimento, etc.

No campo relacionado ao tema aqui discutido, Monteiro (2018) acrescenta que também pode se enquadrar como dado pessoal, os programas de processamento de informações. Frazão; Tepedino; Oliva (2019) No que diz respeito aos crimes cibernéticos, a LGPD estabelece regras específicas para a proteção de dados pessoais em ambientes

digitais. A lei prevê penalidades para o acesso não autorizado, o roubo, a divulgação não autorizada, a alteração ou destruição de dados pessoais, bem como para a violação de sistemas de segurança que protegem esses dados.

De acordo com a LGPD, as organizações são responsáveis por adotar medidas de segurança adequadas para proteger os dados pessoais que coletam e tratam. Caso ocorra algum vazamento de dados ou violação de segurança que possa resultar em danos aos titulares dos dados, as organizações são obrigadas a notificar a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares afetados (BRASIL, 2018).

Menciona-se ainda o Projeto de Lei nº 4554/20. Por esse projeto busca-se aumentar a penalidade dos crimes de furto e estelionato feitos através de dispositivos eletrônicos (celulares, computadores, tablets). Depois de aprovado pelo Plenário da Câmara do Senado, o presente projeto se tornou na Lei Ordinária 14.155/2021. Adequando os pedidos solicitados, as penas foram agravadas, conforme se mostra a seguir:

> *Art. 154-A. [...]*
> *§ 4º-B. A pena é de reclusão de 4 (quatro) a 8 (oito) anos e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.*
> *§ 4º-C. A pena prevista no § 4º-B deste artigo, considerando a relevância do resultado gravoso:*
> *I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;*
> *II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.*
> *(BRASIL, 2020)*

Como mostrado acima, o legislador trouxe no novo texto legislativo o aumento da pena. Isso é uma forma de tentar impedir que novos cibercriminosos surjam e que venham a praticar qualquer ato contra terceiros através das redes digitais. Soma-se a isso, a preocupação do legislador em se preocupar com a população idosa e com os vulneráveis, uma vez que eles são as principais vítimas desses crimes, justamente por serem mais vulneráveis e “fáceis” de serem enganados (BRANDÃO, 2021).

Frete ao exposto, mostra-se que as leis mencionadas aqui são as principais no que se referem aos crimes digitais no ordenamento jurídico brasileiro. Mesmo que necessárias e importantes para trazer mais proteção aos usuários, elas ainda carecem de maior efetividade na prática.

Nesse ponto, Brandão (2021) afirma que ainda que as leis de proteção às vítimas de crimes virtuais sejam importantes e que trazem uma luz a esse problema, elas precisam

ainda de mais investimento e atenção dos órgãos competentes. E mais, ainda é preciso que suas penas sejam mais severas, porque o que tem ocorrido na sociedade é um aumento da prática de crimes virtuais a cada dia. Ou seja, não basta apenas que haja a lei, é preciso que ela seja efetiva, o que não ocorre no momento presente no Brasil.

Segundo Oliveira (2022) uma das justificativas para que haja tantos ataques no país é o baixo investimento em cibersegurança no Brasil. Desta feita, é mais do que necessário que se invista em procedimentos de investigação e maior rigor da legislação, para que os crimes cibernéticos não se tornem impunes ou de prática rotineira.

4. COMPARTILHAMENTO NÃO CONSENSUAL DE CONTEÚDO ÍNTIMO POR VINGANÇA: EFEITOS JURÍDICOS E SOCIAIS

A pornografia de vingança, também conhecida como “revenge porn”, é caracterizada pela divulgação não consensual de material sexualmente explícito, como imagens ou vídeos íntimos, de uma pessoa por outra, geralmente como forma de vingança ou retaliação após o término de um relacionamento (SILVA, 2020). As características desse tipo de crime incluem:

Quadro 2 – Principais características do revenge porn

CARACTERÍSTICA	DESCRIÇÃO
Falta de consentimento	A divulgação das imagens ou vídeos é feita sem o consentimento da pessoa retratada. Isso pode ocorrer de várias maneiras, incluindo o compartilhamento de material íntimo obtido durante um relacionamento consensual ou o vazamento de material obtido de forma ilegal, como hacking.
Intenção maliciosa	A divulgação do material é feita com o objetivo de causar dano, constrangimento, humilhação ou sofrimento emocional à pessoa retratada. Geralmente, isso ocorre como uma forma de vingança por parte de um ex-parceiro ou ex-parceira, mas também pode ser motivado por outros tipos de conflito interpessoal.
Impacto negativo	A pornografia de vingança pode ter sérias consequências para a pessoa retratada, incluindo danos emocionais, psicológicos e sociais. Ela pode levar a estigma, assédio, bullying e até mesmo problemas profissionais, como perda de emprego.

Uso indevido de material íntimo	A divulgação do material sexualmente explícito não autorizado constitui um uso indevido da privacidade e da intimidade da pessoa retratada. Isso viola os direitos humanos básicos e é considerado uma forma de violência de gênero.

Fonte: SYDON; CASTRO (2019, p. 15).

De acordo com França et al. (2019), a pornografia de vingança é caracterizada pela divulgação não consensual de material sexualmente explícito com a intenção de causar dano à pessoa retratada. É uma forma de violência de gênero e um sério problema social que requer conscientização, educação e medidas legais para prevenir e punir.

O perfil do criminoso envolvido na pornografia de vingança pode variar, mas geralmente inclui algumas características comuns. Segundo Reis e Naves (2020), o perpetrador muitas vezes é alguém que teve um relacionamento íntimo com a vítima, como um ex-namorado, ex-namorada, ex-marido ou ex-esposa. Eles podem se sentir magoados, traídos ou com raiva após o término do relacionamento e usar a pornografia de vingança como forma de retaliação.

Souza (2020) acrescenta que o criminoso muitas vezes age movido por emoções intensas, como ciúme, vingança, raiva ou ressentimento em relação à vítima. Eles podem querer causar danos à reputação da vítima ou fazê-la sofrer como uma forma de punição pelo fim do relacionamento.

Muitas vezes, o criminoso pode ser manipulador e controlador no relacionamento. Eles podem usar a pornografia de vingança como uma forma de exercer poder e controle sobre a vítima, buscando humilhá-la e prejudicá-la emocionalmente. Em alguns casos, o criminoso pode ter habilidades técnicas para hackear contas online, invadir dispositivos eletrônicos ou acessar material íntimo sem permissão. Isso pode incluir conhecimentos em hacking, engenharia social ou exploração de vulnerabilidades de segurança (FRADE; RESENDE; SANTOS, 2021).

Já o perfil da vítima, geralmente são indivíduos que estiveram em um relacionamento íntimo com o perpetrador, como parceiros românticos, esposos ou esposas. Isso pode incluir pessoas que compartilharam imagens íntimas consensualmente durante o relacionamento (FRADE; RESENDE; SANTOS, 2021).

Oliveira e Almeida (2022) afirmam que as vítimas podem estar em um estado emocional vulnerável devido ao término do relacionamento ou a outras circunstâncias

estressantes. Isso pode torná-las mais suscetíveis à exploração e ao abuso por parte do perpetrador.

Muitas vezes, as vítimas confiam em seus parceiros românticos para manter a privacidade e a segurança de suas informações pessoais e íntimas. A divulgação não consensual de material íntimo por parte do parceiro pode violar essa confiança e causar danos emocionais significativos.

Ademais, a divulgação não consensual de material íntimo pode ter um impacto devastador na vida da vítima, causando vergonha, humilhação, ansiedade, depressão e outros problemas emocionais. Isso pode afetar sua autoestima, relacionamentos pessoais e até mesmo sua capacidade de funcionar no trabalho ou na escola (OLIVEIRA; ALMEIDA, 2022).

A Constituição Federal de 1988 garante o direito à inviolabilidade da intimidade, da privacidade, da honra e da imagem das pessoas, previsto no inciso X do artigo 5º: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.” (BRASIL, 1988).

Nos casos em que acontece a pornografia de vingança, o caminho para que essa inviolabilidade seja respeitada continua difícil. A gravidade dos crimes que envolvem a divulgação de imagens e vídeos íntimos na internet levou à criação de leis para que esse tipo de crime pudesse ser julgado e punido. Quando os casos de pornografia de vingança começaram a ser denunciados, o uso do Código Penal, com a aplicação do artigo 139, crime de injúria e artigo 140, crime de difamação, destacou-se como importante recurso jurídico (BRASIL, 1940).

Outras legislações são aplicadas dependendo das características dos casos, mostrando que a justiça está cada vez mais preocupada em punir as pessoas que cometem esses crimes. Em casos onde a vítima é menor de idade ou que o responsável pelas publicações tiver mantido um relacionamento íntimo com a vítima, aplica-se o Estatuto da Criança e Adolescente ou a Lei Maria da Penha.

Quando envolve crianças e adolescentes, os envolvidos podem responder por crimes associados à pornografia infantil, previstos na Lei 8.069/90, Estatuto da Criança e do Adolescente (ECA). Nesse caso, enquadra-se no 240 e 241 (BRASIL, 1990).

A Lei nº 11829/08 inovou o texto do ECA sobre essa matéria. A prática prevista no artigo 241-A criminaliza quem oferecer trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio de comunicação, fotografia, vídeo ou outro registro que

contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente (BRASIL, 2008).

O artigo 241-B responsabiliza quem adquirir, possuir ou armazenar imagens, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. A pena para quem mantem a posse desse tipo material é de 1 a 4 anos de reclusão e multa (BRASIL, 2008).

No artigo 241-C, a punição com pena de 1 a 3 anos de reclusão e multa aplica-se às pessoas que simularem a participação de criança ou adolescente em cena de sexo explícito ou pornográfica feita através de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual. A mesma penalidade é aplicada para quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido por adulteração (BRASIL, 2008).

Outra norma a ser citada é a Lei nº Lei 12.737/12, conhecida como a Lei Carolina Dieckmann, surgida em razão da divulgação do roubo de fotos íntimas da atriz. A norma, entre outros aspectos acrescentou os artigos 154-A e 154-B ao texto penal. A respeito do texto desses artigos, tem-se:

> *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.*
> *(BRASIL, 2012)*

Destaca-se que o tipo penal presente no artigo 154-A quando faz referência a “invadir dispositivo informático alheio [...]” (BRASIL, 2012) mostra que, apesar do verbo invadir dar a ideia de uso de força, nesse caso não existe a presença de violência, mas o crime existe e pode ser entendido como a ação de entrar sem autorização e se apropriar de informações sigilosas armazenadas em dispositivos informáticos.

Também é importante mencionar a Lei nº 12.965/14, também conhecida como Marco Civil da Internet. Pela lei, é assegurada às vítimas de pornografia de vingança, a retirada de material divulgado sem consentimento. Na maioria dos casos, a solicitação para a retirada de material divulgado pela internet é feita através de ordem judicial. Mas, em se tratando de material com conteúdo íntimo, a retirada deve ocorrer se a vítima ou representante legal solicitar, de forma direta, aos sites responsáveis pela divulgação, conforme disposto no artigo 21, caput e parágrafo único do retro norma (BRASIL, 2014).

Também é importante mencionar a Lei nº 13.718/2018, que versa sobre os crimes contra a dignidade sexual, entre eles, tipifica os crimes de importunação sexual e de divulgação de cena de estupro. No que concerne ao tema aqui analisado, frisa-se o seguinte artigo:

> *Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia.*
> *Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.*
> *(BRASIL, 2018)*

A utilização do verbo “oferecer” no início da descrição do artigo 218-C, mostra que existem diversas outras ações que podem ser praticadas a partir dessa, quando da posse de material que contenha cena de estupro ou de estupro de vulnerável. Essas imagens podem ser usadas para fazer apologia ou induzir à prática do estupro ou, ainda, serem divulgadas por qualquer meio de comunicação, sem consentimento da vítima (OLIVEIRA; ALMEIDA, 2022).

A jurisprudência brasileira já vem decidindo casos onde pode-se encontrar a exposição de intimidade de terceiros por motivos de vingança. A título de exemplo, apresenta-se abaixo o presente julgado do Superior Tribunal de Justiça:

> *CIVIL E PROCESSUAL CIVIL. RECURSO ESPECIAL. AÇÃO DE OBRIGAÇÃO DE FAZER E DE INDENIZAÇÃO DE DANOS MORAIS. RETIRADA DE CONTEÚDO ILEGAL.* ***EXPOSIÇÃO PORNOGRÁFICA NÃO CONSENTIDA. PORNOGRAFIA DE VINGANÇA****. DIREITOS DE PERSONALIDADE.* ***INTIMIDADE****. PRIVACIDADE. GRAVE LESÃO. 1. […]. 4.* ***A "exposição pornográfica não consentida", da qual a "pornografia de vingança" é uma espécie, constituiu uma grave lesão aos direitos de personalidade da pessoa exposta indevidamente****, além de configurar uma grave forma de violência de gênero que deve ser combatida de forma contundente pelos meios jurídicos disponíveis. 5. Não há como descaracterizar um material pornográfica apenas pela ausência de nudez total. Na hipótese, a recorrente encontra-se sumariamente vestida, em posições com forte apelo sexual. 6.* ***O fato de o rosto da vítima não estar evidenciado nas fotos de maneira flagrante é irrelevante para a configuração dos danos morais na hipótese, uma vez que a mulher vítima da pornografia de vingança sabe que sua intimidade foi indevidamente desrespeitada e, igualmente, sua exposição não autorizada lhe é humilhante e viola flagrantemente seus direitos de personalidade****. 7. O art. 21 do Marco Civil da Internet não abarca somente a nudez total e completa da vítima, tampouco os "atos sexuais" devem ser interpretados como somente aqueles que envolvam conjunção carnal. Isso porque o combate à exposição pornográfica não consentida - que é a finalidade deste dispositivo legal - pode envolver situações distintas e não tão óbvias, mas que geral igualmente dano à personalidade da vítima. 8. Recurso conhecido e provido. (REsp 1735712/SP. 2018/0042899-4. T3 - TERCEIRA TURMA. Relatora: Ministra NANCY ANDRIGHI. Data de Julgamento: 19/05/2020. Data de publicação: DJe 27/05/2020). (grifo do autor).*

No caso acima, a Relatora deixa claro que é cabível a aplicação de danos morais às vítimas, uma vez que os danos gerados pelo fato por si só trazem dessabores, humilhações e dores irreparáveis às vítimas. Importante destacar que nesses casos, a palavra da vítima é de suma importância, conforme destaca a seguinte jurisprudência:

> *APELAÇÃO CRIMINAL. AMEAÇA EM CONTEXTO DE VIOLÊNCIA DOMÉSTICA E FAMILIAR CONTRA A MULHER (ART. 147, CP, C/C LEI 11.340/2006). PLEITO ABSOLUTÓRIO. INACOLHIMENTO. MATERIALIDADE E AUTORIA DELITIVAS SUFICIENTEMENTE COMPROVADAS PELO CONJUNTO PROBATÓRIO.* ***AMEAÇA E EFETIVA DIVULGAÇÃO DE VÍDEOS ÍNTIMOS, DE NATUREZA SEXUAL ("REVENGE PORN" OU "PORNOGRAFIA DE VINGANÇA"). ESPECIAL RELEVÂNCIA DA PALAVRA DA VÍTIMA NOS CRIMES COMETIDOS NO ÂMBITO DA LEI MARIA DA PENHA****, NOTADAMENTE QUANDO CORROBORADA POR OUTROS ELEMENTOS DE PROVA. APELO CONHECIDO E IMPROVIDO. I – […]. V – A vítima Priscila Souza Nunes, ouvida em juízo sob o crivo do contraditório e da ampla defesa, ratificou suas declarações policiais,* ***narrando que o acusado, por não aceitar o término do relacionamento, ameaçou divulgar vídeos íntimos, em que o ex-casal mantinha relações sexuais****. Aduziu ainda que, após ter recusado reatar o namoro, recebeu telefonemas de um primo e alguns amigos,* ***revelando que os vídeos haviam efetivamente sido enviados pelo acusado, para mais de vinte pessoas, dentre familiares, colegas de faculdade e de trabalho, tendo ele ainda os editado de forma a esconder o próprio rosto****. VI – Imperioso destacar que, na esteira da jurisprudência do Superior Tribunal de Justiça****, a palavra da vítima assume especial relevância probatória nos crimes praticados em contexto de violência doméstica e familiar contra a mulher****, uma vez que normalmente são praticados clandestinamente, sem a presença de testemunhas, nada impedindo que a condenação seja nela lastreada. […] (TJ-BA, Classe: Apelação, Número do Processo: 0502838-31.2019.8.05.0274, Órgão julgador: PRIMEIRA CAMARA CRIMINAL - SEGUNDA TURMA, Relator(a): RITA DE CASSIA MACHADO MAGALHAES, Publicado em: 31/01/2024). (grifo do autor)*

Como mostrado acima, cita-se que a Lei Maria da Penha também é uma base legal, que busca penalizar os criminosos da pornografia de vingança em âmbito de violência doméstica.

Assim, fica claro destacar que a prática, conhecida na doutrina e na jurisprudência como "revenge porn", ou pornografia de vingança, é uma forma de violência contra a mulher punível criminalmente (STJ, HC 689880/SP, 2021/0275122-7, Relator: Ministro Ribeiro Dantas, DJ: 12/11/2021). A partir da Lei nº 13.718, de 2018, a divulgação de cenas de sexo, nudez ou pornografia, sem o consentimento da vítima, passou inclusive a receber tratamento criminal mais rigoroso, com o acréscimo do art. 218-C ao Código Penal, punido com pena de reclusão de um a cinco anos, bem como de seu § 1º, que aumenta a pena de 1/3 a 2/3 se houver propósito de vingança ou humilhação.

5.CONSIDERAÇÕES FINAIS

A pornografia de vingança ou revenge porn refere-se à prática de compartilhar ou divulgar imagens ou vídeos íntimos de uma pessoa sem o seu consentimento, geralmente com o objetivo de humilhar, prejudicar ou se vingar da vítima. Esse tipo de crime é frequentemente associado ao fim de relacionamentos amorosos, onde uma das partes decide expor conteúdos íntimos que foram obtidos consensualmente durante o relacionamento, ou até mesmo de forma ilegal, como através de hackeamento ou gravações secretas.

As motivações para esse crime variam, mas geralmente envolvem sentimentos de vingança, raiva ou controle após o término de um relacionamento. Em alguns casos, a intenção pode ser humilhar a vítima publicamente, chantageá-la ou obter ganhos financeiros.

No Brasil, a Lei 13.718/2018 tornou crime a divulgação de cenas de nudez, sexo ou pornografia sem o consentimento da vítima, com penas que podem chegar a até cinco anos de prisão. Além disso, vítimas desse crime podem buscar indenização por danos morais na esfera civil.

Salienta-se que qualquer pessoa pode ser vítima de pornografia de vingança, independentemente de gênero, idade, orientação sexual ou outras características. No entanto, certos fatores, como a confiança no parceiro e a vulnerabilidade emocional, podem aumentar o risco de uma pessoa se tornar alvo desse tipo de crime.

As vítimas de pornografia de vingança podem sofrer sérios traumas emocionais, como ansiedade, depressão, pânico, vergonha extrema, isolamento social e até pensamentos suicidas. A exposição pública de imagens íntimas pode afetar drasticamente a vida pessoal e profissional da vítima, resultando em perda de emprego, distanciamento social, e estigmatização.

De todo modo, frisa-se que a pornografia de vingança é um crime sério, com graves consequências para as vítimas, tanto no âmbito psicológico quanto social. É essencial que a sociedade esteja informada sobre as implicações legais desse ato e sobre a necessidade de respeito à privacidade alheia. O apoio às vítimas, a conscientização e o uso responsável das tecnologias são fundamentais para combater essa prática.

6. REFERÊNCIAS

ANDRADE, Carlos Henrique Gomes; REZENDE, Paulo Izidio da Silva. **Os crimes cibernéticos e os seus efeitos na imagem do indivíduo**. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 05, Ed. 11, Vol. 03, pp. 64-78. novembro de 2020.

BARRETO, Alessandro Gonçalves. **Investigação Digital em fontes abertas**. Rio de Janeiro. Brasport, 2018.

BRANDÃO, Francisco. **Câmera aprova penas mais duras para crimes cibernéticos**. 2021. Disponível em: https://www.camara.leg.br/noticias/746980-camara-aprova-penas-mais-duras-para-crimes-ciberneticos/. Acesso em: 26 set. 2024.

BRASIL, **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 set. 2024.

BRASIL. **Lei nº 13.737 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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 12 set. 2024.

BRASIL. **Lei n° 12.965, de 23 de abril de 2014**. Institui o Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 set. 2024.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 10 set. 2024.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 8 ed. São Paulo, Saraiva, 2018.

DELMANTO, Celso et al. **Código Penal comentado**. 12. ed. rev., atual. e ampl. São Paulo: Saraiva, 2019.

FRADE, Camila Cristiane de Carvalho; RESENDE, Daniel Alberico; SANTOS, Henrique de Almeida. **Big Data, Softwares de Inteligência Artificial (IA) e a Proteção do Meio Ambiente Marinho**. In: III Encontro Virtual do CONPEDI, 2021, Florianópolis. Direito, governança e novas tecnologias I. Florianópolis: CONPEDI, 2021. v. 1. p. 134-150.

FRANÇA, Leandro Ayres; et al. A criminalização do revenge porn: análise do art. 218-C (Código Penal). **Boletim IBCCRIM**, ano 26, n. 315, fev. 2019.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 1º ed. São Paulo: Revista dos Tribunais, 2019.

GRECO, Rogério. **Curso de Direito Penal: parte especial**. vol. 3. Niterói: 2014.

MENDES, Laura Shertel; DONEDA, Danilo. **Comentário à nova Lei de Proteção de Dados (Lei nº 13.709/2018): o novo paradigma da proteção de dados no Brasil**. Revista de Direito do Consumidor. vol. 120/2018, p. 555 - 587. Nov - Dez/2018.

OLIVEIRA, Bruna Larissa Campos de; ALMEIDA, Andréia Alves de. Modernização dos crimes sexting e revenge porn: no ambiente virtual contra a mulher. **Revista Ibero-Americana De Humanidades, Ciências E Educação**, 8(1), 263–270, 2022.

OLIVEIRA, Ingrid. **Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%**. 2022. Disponível em: https://www.cnnbrasil.com.br/tecnologia/levantamentomostraqueataquesciberneticosnobrasilcresceram94/#. Acesso em: 28 ago. 2024.

REIS, Émilien Vilas Boas; NAVES, Bruno Torquato de Oliveira. **O Meio Ambiente Digital e o Direito à privacidade diante do Big Data**. Veredas do Direito, Belo Horizonte, v 17, n37, p.145-167, jan-abr. 2020.

SANTOS, Gabrielly Daianne Alves dos. **Crimes virtuais: tratamento legal e limitações no combate aos crimes cibernéticos**. Monografia apresentada ao Núcleo de Trabalho de Curso da UniEvangélica. Anápolis, 2021.

SILVA, Mazukyevicz Ramon Santos do Nascimento. **Crimes virtuais e o ordenamento jurídico Brasileiro: análise dogmática**. 1 ed. Editora: Clube dos Autores, 2020.

SOUZA, Luciano Anderson de. **Direito penal: volume 3: parte especial: arts. 155 a 234-B do CP**. São Paulo: Thomson Reuters Brasil, 2020.

SYDON, Spencer Toth; CASTRO, Ana Lara Camargo. **Exposição Pornográfica não consentida na internet: da pornografia de vingança ao lucro**. 2 ed. Belo Horizonte: Editora D'Plácido, 2019.

WENDT, Emerson; NOGUEIRA JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: Ameaças e Procedimentos de Investigação**. 2º ed. Editora Braspot: 2019.