

## **CIBERCRIMES E A NECESSIDADE LEGISLATIVA DE CRIAÇÃO DE TIPOS PENAIIS INFORMÁTICOS**

**ALVES, Brenda Alessa Ranucci<sup>1</sup>  
STAZIAKI, Lucas Augusto da Rosa<sup>2</sup>**

**RESUMO:** A sociedade e seu constante dinamismo em paralelo com o processo de evolução tecnológica das últimas décadas vêm exigindo da Ciência do Direito e seus operadores a capacidade de adaptar-se a estes fenômenos, visto que a reprovabilidade social não produz os mesmos efeitos da coercibilidade oriunda do Poder Punitivo Estatal. Destarte, o ambiente virtual torna-se cada vez mais um meio para a atuação criminosa, possibilitando que novas condutas delituosas ocorram de modo crescente, dada imprevisibilidade dos Legisladores à época do Código Penal de 1940, lei mor de nosso sistema penal que carece de tipificação específica destes ilícitos. Neste contexto, a pesquisa atual visa ressaltar a importância da tipificação penal no cenário digital, cuja importância justifica-se pelo papel jurídico social que o Direito produz. O presente artigo objetiva apresentar uma linha do tempo legislativa em constante aperfeiçoamento dos ilícitos digitais, além dos códigos informáticos que resguardam novos bens jurídicos a serem tutelados pelo Estado, tais sendo exclusivamente do meio digital, apresentar um caso de cibercrime recente e de grande repercussão pela mídia nacional, cujo réu fora processado e julgado por ilícitos virtuais de torpeza significativa, visando analisar o *modus operandi* do acusado, definir objetivamente os critérios de ocorrência e caracterização dos delitos virtuais, bem como verificar a possibilidade da responsabilização penal de pessoas jurídicas que sediam estes ilícitos.

**PALAVRAS-CHAVE:** Cibercrimes, Direito Penal, Direito Digital, Legislação.

## **CYBERCRIMES AND THE LEGISLATIVE NEED TO CREATE DIGITAL CRIME OFFENSES**

**ABSTRACT:** Society and its constant dynamism, in parallel with the technological evolution process of recent decades, have been demanding the capacity of Legal Science and its practitioners to keep pace with these phenomena, given that social reproach does not produce the same effects as the coercibility stemming from the State's Punitive Power. Thus, the virtual environment increasingly becomes a medium for criminal activity, allowing new illicit behaviors to occur more frequently, due to the unpredictability of legislators at the time of the 1940 Criminal Code, the cornerstone of our penal system. In this context, the present research aims to underscore the importance of criminal classification in the digital arena — a significance justified by the social-legal function of law. This paper seeks to: present a legislative timeline reflecting the continuous refinement of digital offenses, along with the computer codes that safeguard new legal interests to be protected by the State — interests that exist exclusively in the digital realm, introduce a recent cybercrime case that has garnered significant national media attention, in which the defendant was prosecuted and tried for virtual offenses of significant moral turpitude, analyze the *modus operandi* of the accused, objectively define the criteria for the occurrence and characterization of virtual offenses and verify the possibility of imposing criminal liability on legal entities that commit such offenses.

**KEYWORDS:** Cybercrimes, Criminal Law, Digital Law, Legislative process.

<sup>1</sup>Discente no Curso de Direito do Centro FAG, e-mail: brendalessaranuccialves@hotmail.com.

<sup>2</sup>Docente no Curso de Direito do Centro FAG, e-mail: lucasaugustodarosa@fag.edu.br.

## 1 INTRODUÇÃO

Para fins de contextualização, o Brasil tem apresentado uma exponencial crescente de práticas delituosas provenientes do uso irregular da internet e suas tecnologias da informação e de comunicação (TICs), como efeito rebote nos últimos anos, provenientes inicialmente com a incidência da pandemia do vírus COVID-19, em março de 2020, pela Organização Mundial de Saúde, na qual resultou na ampliação em larga escala da vida virtual social.

Por consequência, com estas práticas tornando-se espirais de conflito na sociedade, trouxeram consigo uma nova demanda no judiciário, tal sendo os Cibercrimes, ou delitos virtuais, conforme nomenclatura adotada na obra de Spencer Toth Sydow (2024) que a justifica pela abrangência de condutas, para além do uso da expressão cibercrimes.

A morosidade legislativa paralela à alta demanda social, na qual traz consigo reflexos no judiciário, têm gerado percalços. A Central de Denúncias de Crimes Cibernéticos – SaferNet Brasil – constatou que o país recebeu, no ano de 2021, mais de cem mil denúncias de usuários pela constatação de sites contendo pornografia infantil, totalizando o expressivo montante de cinquenta e três mil, novecentas e sessenta páginas na web. É notório que tais dados revelam a vasta ocorrência criminosa, ora tipificada no art. 218-C do Código Penal, cuja aplicação foi possível somente a partir da promulgação da Lei nº 13.718 em 24 de setembro de 2018.

Observa-se que, como o Código Penal, a legislação mor de nosso sistema penal brasileiro, carece de tipificação específica quanto aos crimes virtuais, pois estes ilícitos vêm se tornando cada vez mais uma lacuna legislativa, fato que pressupõe insegurança jurídica não tão somente às vítimas, que, por vezes, não estarão munidas da proteção estatal, todavia, também tange por todo o meio coletivo social.

Diante deste cenário, indaga-se: deve o Poder Legislativo preocupar-se em tipificar os delitos virtuais, para além da dinâmica interpretativa ou analógica nas quais vêm sendo aplicadas? De que modo a escassez legal afeta a aplicação do Direito em casos ocorridos puramente no meio digital? O presente trabalho busca, de modo a conectar as searas Penal e Digital, atribuir valor jurídico e social à tipificação dos delitos cibernéticos, a fim de descomplicar o indiciamento e aplicação das penas ao definir critérios objetivos, visando a melhor caracterização destes vastos ilícitos, evitando por consequência, a via interventiva dos Tribunais Superiores para corrigir o destoar de interpretações pelos magistrados e doutrina a cada caso tutelado no Judiciário.

A metodologia aplicada embasa-se no método hipotético-dedutivo e na pesquisa quantitativa, em fontes formais do direito, tais como bibliografias jurídicas, decisões firmadas pelo Tribunais Superiores, além de consulta às leis penais e informáticas recentes.

Desta forma, visando o amparo legal à sociedade e à correta aplicação penal, para que os agentes ativos sejam responsabilizados de modo eficaz e eficiente, necessita-se da criação de projetos de leis pelos membros do parlamento.

Juridicamente, a existência de normas reguladoras é de suma importância, a começar pelo princípio basilar da legalidade penal, previsto no art. 1º do Código Penal, prevendo que “não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal” (Brasil, 1940). Destarte, pela omissão legislativa o *jus puniendi* estatal não produzirá efeitos de modo a condizer com o binômio: reprovabilidade social e a reincidência delitiva.

A atual e relevante discussão acadêmica fomenta-se a cada ano, sendo um exercício de direitos provenientes da reprovabilidade social das condutas, e formulam questionamentos principalmente acerca da (in)segurança no meio digital e se de fato a Internet será a perpétua “terra sem lei”, termo no qual popularizou-se na década recente.

Percebe-se, portanto, que a inércia do Poder Legislativo da ausência de tipificação destas condutas afetará os demais poderes em suas funções típicas, tanto o Judiciário com as demandas excessivas sem uma formulação de entendimentos ora pacificada, quanto ao Executivo ao exercer o papel fiscalizatório e a respectiva aplicação das penas.

## **2 ANÁLISE DO CASO E DAS CARACTERÍSTICAS DOS CIBERCRIMES**

Pedro Ricardo Conceição da Rocha, jovem de 19 anos de idade a época dos fatos, utilizava-se da rede social Discord, plataforma social de videochamadas e mensagens de texto que permite a comunicação privada entre usuários ou em grupos via salas virtuais de bate-papo, agindo com o dolo de praticar crimes sexuais e patrimoniais sob a ilusão da impunidade digital. As condutas foram qualificadas em inquérito oferecido pela Polícia Civil do Rio de Janeiro/RJ, em operação especial intitulada *Dark Room*, delitos que se perpetuaram pelo extenso período de 1 ano e 6 meses, perfazendo crianças, adolescentes e até animais vítimas ante a torpeza (G1, 2023).

O *modus operandi* do autor detinha certa peculiaridade, visto que não buscava utilizar-se do sigilo e anonimato que as redes sociais em geral proporcionam, os crimes eram cometidos e amplamente divulgados em uma comunidade intitulada “System X”, na própria plataforma Discord, onde demais usuários realizavam chamadas de vídeo coletivas, nas quais previamente

selecionavam as vítimas e praticavam abusos psicológicos, sexuais, chantagens, incentivando a automutilação, ações nas quais os participantes pagavam ao autor preços tabelados para assistir às vítimas nestas condições vexatórias (G1, 2024).

O jovem réu fora condenado a pena de 24 anos e 7 meses de regime inicial fechado. As condutas foram qualificadas como estupro qualificado e coletivo, estupro de vulnerável, induzimento, instigação a automutilação, corrupção de menores e associação criminosa. Ademais, crimes previstos no Estatuto da Criança e do Adolescente, chantageando as vítimas com fotos íntimas, adquiriam contatos dos responsáveis pelos adolescentes como exercício de poder, constrangimentos nos quais atingiram uma rede de jovens, em maioria, menores de idade, domiciliados em diversas localidades do país (Migalhas, 2024).

O recente caso despertou um alerta de nível nacional à sociedade, fato que demanda atenção do Poder Legislativo, vez que os crimes imputados ao réu destoam do *modus operandi* padrão dos sujeitos ativos destes ilícitos penais, cujos bens jurídicos alvejados são a dignidade sexual e a integridade física.

A rede social Discord, utilizada por Pedro Ricardo para sediar os ilícitos, por natureza, é mais atrativa tanto a adolescentes quanto jovens adultos, pelo próprio marketing da empresa ser voltado ao público *gamer*. Os dados expostos pela empresa Statista, coletados no mês de fevereiro de 2023, demonstram que jovens na faixa etária de 16 a 24 anos são 20.6% dos usuários da plataforma, ao passo que o público majoritário secundário perfaz aproximadamente 53.4% do público-alvo, na faixa etária variável de 25 a 34 anos (Ceci, 2024).

Isto posto, insta mencionar a teoria tripartida de Jonathan Clough relativa aos requisitos de eficácia para se instaurar no ambiente virtual a ocorrência de um cibercrime, a citar: um *quantum* significativo de agressores motivados, a disponibilidade de oportunidades e a ausência de fiscais capazes de assegurar a proteção dos usuários (p. 59, 2010, tradução nossa).

A fim de definir estes ilícitos sediados no meio digital, a doutrina de Sydow dispõe de duas categorias de crimes virtuais: os comuns e específicos. Aqueles seriam os delitos nos quais o meio virtual é utilizado para a violação de bens jurídicos, enquanto os específicos visam lesar bens jurídicos exclusivamente informáticos, como o sistema tecnológico ou dados inseridos na rede, a servir de exemplo o art. 32 da Lei nº 12.527/2011 (Albuquerque, 2006 *apud* Sydow, 2024, p. 222). Neste contexto, a problemática de carência legal brasileira quanto aos Cibercrimes estende-se a ambas as classes de ilícitos mencionadas.

A internet, por sua natureza, proporciona um ambiente sigiloso aos usuários de redes sociais, mais propício ao anonimato dos agentes agressores. Sob esta ótica, mesmo com a aplicação análoga das normas em vigor, os delitos virtuais que, por si só, possuem uma natureza

silenciosa. No que diz respeito ao ambiente virtual das redes, Spencer Toth Sydow preceitua (2024, p. 219):

Tal categoria de crimes dispensa o contato físico entre vítima e ofensor, não exige grandes preparos como visitação prévia de local para o cometimento do fato, ocorre em um ambiente sem povo (ou com características diversas de população), Governo ou território, não implica aparentemente em altos riscos, não gera sensação de violência e nem sempre há padrões para seu acontecimento.

Outrossim, o autor disciplina quanto à facilidade do sujeito ativo em dominar o meio digital sem a percepção dos agentes fiscalizatórios.

O delinquente informático pode cometer mais de uma conduta lesiva ao mesmo tempo, estando em diversos lugares simultaneamente, e conta com a vantagem de haver poucos profissionais de segurança pública capacitados para investigar sua ação, analisar as provas e os indícios. Sem contar a vantagem de o agente não fazer demasiado esforço e agir de forma transnacional com facilidade ímpar (Sydow, 2024, p. 219).

Sendo assim, a diferenciação do *modus operandi* do agressor em um delito virtual é visível, fato que independe da natureza do crime, alvejando bem jurídico de caráter patrimonial, a dignidade sexual ou contrário à honra, por exemplo.

Os fatores que caracterizam estes ilícitos trazem uma nova problemática ao poder público, relativa à investigação anterior à judicialização das condutas, ou seja, a atuação do poder de polícia para prevenir e ceifar as condutas antes de alvejar o bem jurídico protegido. Em vista disso, as redes sociais possuem uma ferramenta de barragem de conteúdos e de interações que transpassem os limites da boa-fé, sendo estes variantes de acordo com os termos de uso do site ou da aplicação, cuja responsabilidade criminal destas pessoas jurídicas deve ser analisada como hipótese de culpa indireta, ou seja, a culpabilidade em que o agente não pratica uma ação ilícita, mas responde por atos de terceiros sob sua guarda ou vigilância (Estefam, 2024).

### **3 O DIREITO DIGITAL E A RESPONSABILIZAÇÃO PENAL DO PROVEDOR**

A responsabilidade penal de pessoas jurídicas se faz tópico de relevante menção, ademais pela gravidade do caso ora exposto, tendo em vista que o direito penal informático introduz duas pessoas jurídicas importantes no contexto virtual, necessárias para se utilizar a rede, sendo o provedor de acesso e o provedor de conteúdo, aquele proporcionando a conexão entre usuário e rede de computadores, e este armazenando os dados desta (Sydow, 2024).

Preliminarmente, a responsabilidade jurídica das pessoas jurídicas deu-se pela promulgação da Lei nº 9.605/98 – Lei dos Crimes Ambientais – importando o entendimento favorável à responsabilização destes entes fictícios, previsão legal expressa no art. 3º, que tutela quanto à responsabilidade administrativa, civil e criminal, caso a infração seja cometida pelo seu representante legal, contratual ou órgão colegiado, no interesse ou benefício desta (Brasil, 1998).

Preconiza, nesta mesma linha, o art. 19, caput, da Lei nº 12.965/2014 – Marco Civil da Internet – que o provedor da aplicação poderá ser excepcionalmente responsabilizado pelos danos causados por conteúdo de terceiros em caso de inércia à tomada de providências nas quais visem derrubar o conteúdo nocivo, necessitando para tanto, de ordem judicial preexistente (Brasil, 2014).

Pela aplicação deste fundamento, a responsabilidade do provedor seria a regra de exceção, na qual não encaixaria a plataforma Discord dentro de seus requisitos legais para tal. No entanto, há de se referenciar o debate recente quanto à constitucionalidade do artigo supra. O julgamento do STF no Recurso Extraordinário (RE) nº 1.037.396, fixando o Tema 987, pelo voto inaugural do Ministro Relator Dias Toffoli, apresentado em dezembro de 2024, favorável à inconstitucionalidade do art. 19, caput e seus parágrafos por arrastamento, do Marco Civil da Internet (MCI), e fundamenta no sentido da desnecessidade de ordem judicial prévia, imprescindível para a responsabilização civil, cujo provedor de aplicações será responsável objetivamente pelos danos oriundos do ilícito gerado por terceiros:

1. É inconstitucional o art. 19, caput e § 1º, do Marco Civil da Internet, sendo inconstitucionais, por arrastamento, os demais parágrafos do art. 19; 2. Como regra geral, o provedor de aplicações de internet será responsabilizado civilmente, nos termos do art. 21 do MCI, pelos danos decorrentes de conteúdos gerados por terceiros, inclusive na hipótese de danos à intimidade, à vida privada, à honra e à imagem, quando, notificado pelo ofendido ou seu representante legal, preferencialmente pelos canais de atendimento, deixar de promover, em prazo razoável, as providências cabíveis, ressalvadas as disposições da legislação eleitoral e os atos normativos expedidos pelo TSE; 2.1. Em todos os casos, a apuração da responsabilidade deverá levar em conta a(s) atividade(s) efetivamente desempenhada(s) pelo provedor de aplicações (art. 3º, inciso VI, do MCI) e o grau de interferência dessa(s) atividade(s), inclusive por atuação algorítmica e/ou automatizada, no fluxo informacional; 2.2. As plataformas e os blogs jornalísticos respondem exclusivamente na forma da lei específica (Lei nº 13.188, de 11 de novembro de 2015), a qual já foi declarada constitucional pelo Supremo Tribunal Federal (ADI nº 5.418, Rel. Min. Dias Toffoli, Tribunal Pleno, julgado em 11/3/21, DJe de 24/5/21); 3. O provedor de aplicações de internet responde civilmente de forma objetiva e independentemente de notificação, pelos danos decorrentes de conteúdos gerados por terceiros, nas seguintes hipóteses [...] (STF, RE nº 1037396, Tema nº 987, 2024).

A temática do julgamento, evidencia a nova concepção protetora das redes, uma visão a fim de reprimir a ocorrência massificada dos ilícitos cibernéticos, fornecendo o amparo estatal pelo reparo à normatização e formulação de precedentes.

Nesta senda, a responsabilização no meio cível, de modo pragmático, traduz-se na aplicação de multa pecuniária. Todavia, na seara dos crimes virtuais e o potencial ilimitado que as redes têm de alcance de público, os provedores de acesso devem ser responsabilizados.

A Convenção sobre o Crime Cibernético, promulgada via decreto em 12 de abril de 2023, prevê em seu art. 12 a responsabilização penal da pessoa jurídica pelos crimes cibernéticos tipificados nesta convenção. Destaca-se, portanto, o § 2º deste mesmo fundamento, que leciona quanto à responsabilização em caso de ausência de fiscalização feita pela pessoa natural, agindo sob a autoridade e em benefício da pessoa jurídica (Brasil, 2023).

Deste modo, verifica-se que é positivada a aplicação da responsabilidade penal às pessoas jurídicas que, enquanto provedoras de acesso, possuem o controle e a gerência ao espaço onde se sediou o delito informático.

Em sede de responsabilização penal, há, em termos gerais, a ocorrência de ilícito enquanto fato gerador da responsabilização, sendo este típico, antijurídico e culpável, respeitando a teoria tripartite, que conforme justifica Fernando Capez (2023, p. 316): “todo penalista clássico, portanto, forçosamente precisa adotar a concepção tripartida (crime = fato típico + ilícito + culpável), pois do contrário teria de admitir que o dolo e a culpa não pertenciam ao crime, o que seria juridicamente impossível de sustentar”.

Portanto, a isenção de responsabilidade das pessoas jurídicas que meramente sediam ilícitos no ciberespaço, sem o devido controle e o princípio de autorregulação que as redes proporcionam, é diretamente contrária a esta máxima penalista. Assim explica André Saddy quanto à sistemática de autorregulação:

A autorregulação nada mais é que o estabelecimento, por meio de um documento escrito, de normas de conduta e padrões de comportamento criados por entes extraestatais ou não, cujo cumprimento foi fixado previamente como objetivo a ser seguido por aqueles que elaboram, aprovam e subscrevem ou aderem a essa autorregulação (pessoa física ou pessoa(s) jurídica(s)). Trata-se, portanto, de um documento produtor de direito, à margem do Estado ou não, no qual as partes efetivamente impõem a si mesmas um elenco de comportamentos, em definitivo, de boas práticas para ditar normas que regiam sua própria atividade (2015, p. 87).

Nesse sentido, uma hipótese de responsabilização surge no âmbito jurídico-penal: A pessoa física, representante da pessoa jurídica ora provedora, pode ser responsabilizada pela inércia na verificação de conteúdo considerado violador das diretrizes do site? A resposta

mostra-se afirmativa, no sentido de que estariam presentes as condições imprescindíveis de responsabilização penal ora citadas, desrespeitando o cumprimento da responsabilidade social da empresa, logo, a isenção de responsabilidade da empresa provedora não tomaria holofotes, em respeito à teoria da dupla imputação penal.

Ademais, André Estefam leciona sobre a mudança de entendimento dos Tribunais Superiores a respeito da imputação penal a uma pessoa física como condição necessária para a responsabilização da entidade jurídica em caso de crimes resguardados pela Lei nº 9.605/98, havendo na atualidade, uma quebra da teoria da dupla imputação ora exposta, *in verbis* "O STJ e o STF, porém, fixaram a tese em sentido contrário, ou seja, admitindo a acusação por delito ambiental unicamente à pessoa jurídica, sendo, portanto, prescindível a “dupla imputação” da pessoa física, do concurso necessário" (Estefam, 2024, p. 155).

Em mesma sintonia, mostra-se o Recurso Extraordinário (RE) nº 548.181 julgado pela primeira turma do STF em 2013, sendo a Ministra Rosa Weber a Relatora do caso, conforme ementa a seguir:

1. O art. 225, § 3º, da Constituição Federal não condiciona a responsabilização penal da pessoa jurídica por crimes ambientais à simultânea persecução penal da pessoa física em tese responsável no âmbito da empresa. A norma constitucional não impõe a necessária dupla imputação. 2. As organizações corporativas complexas da atualidade se caracterizam pela descentralização e distribuição de atribuições e responsabilidades, sendo inerentes, a esta realidade, as dificuldades para imputar o fato ilícito a uma pessoa concreta. 3. Condicionar a aplicação do art. 225, §3º, da Carta Política a uma concreta imputação também a pessoa física implica indevida restrição da norma constitucional, expressa a intenção do constituinte originário não apenas de ampliar o alcance das sanções penais, mas também de evitar a impunidade pelos crimes ambientais frente às imensas dificuldades de individualização dos responsáveis internamente às corporações, além de reforçar a tutela do bem jurídico ambiental. 4. A identificação dos setores e agentes internos da empresa determinantes da produção do fato ilícito tem relevância e deve ser buscada no caso concreto como forma de esclarecer se esses indivíduos ou órgãos atuaram ou deliberraram no exercício regular de suas atribuições internas à sociedade, e ainda para verificar se a atuação se deu no interesse ou em benefício da entidade coletiva. Tal esclarecimento, relevante para fins de imputar determinado delito à pessoa jurídica, não se confunde, todavia, com subordinar a responsabilização da pessoa jurídica à responsabilização conjunta e cumulativa das pessoas físicas envolvidas. Em não raras oportunidades, as responsabilidades internas pelo fato estarão diluídas ou parcializadas de tal modo que não permitirão a imputação de responsabilidade penal individual [...] (STF, RE nº 548181/PR, Min. Relatora Rosa Weber, 2013).

Em suma, o enfoque da ciência do Direito segue a perspectiva de penalização das pessoas jurídicas por ilicitude de terceiros ou de seus representantes em exercício de suas funções, desde que observados os requisitos em lei vigente e majoritariamente aceitos, tanto pela via doutrinária quanto jurisprudencial, apesar de visível o curto espaço temporal em que este entendimento se funda.



#### 4 A EVOLUÇÃO LEGISLATIVA E POSSÍVEIS AVANÇOS

A criação de projetos de lei com a finalidade de tipificação específica, melhor aplicabilidade das penas a serem impostas aos infratores, descrição dos ilícitos e sua qualificação, entre outras benesses, é medida que se impõe na sociedade atual. Os Poderes da República, em especial o Legislativo e Judiciário pelas suas funções típicas e atípicas, têm, de forma notória, fomentado a tipificação dos delitos sediados no meio virtual, gradualmente incluindo os cibercrimes no alicerce da legislação penal. Em vista disso, uma breve contextualização do movimento legislativo brasileiro quanto aos cibercrimes e à proteção de bens jurídicos informáticos faz-se de rigor.

Em um panorama global, Jonathan Clough (2010), em sua obra *Principles of Cybercrime*, descreve que os crimes virtuais, revelados como *computer crimes*, mostravam-se presentes no começo da década de 60, por condutas como manipulação de dados, invasão de dispositivo informático, sabotagem e uso ilegal dos sistemas de computador. Ao passo que, em 1970, o tratamento inibitório dos crimes virtuais procedeu-se de modo mais intensificado, tendo em vista o aumento de delitos como a fraude eletrônica financeira, cujo contexto era de aumento nas telecomunicações (tradução nossa).

No Brasil, o princípio da atividade legislativa procedeu-se no fim da década de 1990, advindo um marco histórico no Direito Digital e em sua subseção penal, a Lei nº 9.609 de 19 de fevereiro de 1998, com a criminalização de atos – lê-se “atos” de modo genérico – que violam os direitos dos autores de “programas de computador”, assim descritos à época, originando os *copyrights*. Uma legislação mais simplificada, que propõe um único artigo enquanto delito informático, o art. 12, caput, sendo o parágrafo 1º enquanto forma majorada, pena proporcional ao gravame do delito, e o parágrafo 2º descreve as figuras equiparadas (Brasil, 1998).

Posteriormente, com o advento da Lei nº 11.829 em 2008, a qual fora projeto de lei de importante menção, posto que alterou o Estatuto da Criança e do Adolescente (ECA), ao alterar a redação original do art. 240, caput, com a finalidade de coibir a pornografia infantil em campos virtuais, que, em décadas atrás, as práticas propagavam-se em cenários cinematográficos, televisivos ou teatrais. Ademais, apensar ao diploma legal os artigos 241-A, 241-B, 241-C, 241-D e 241-E, que tratam exclusivamente de condutas ciberdelituosas e suas respectivas penas (Brasil, 1990).

Além das supramencionadas alterações, houve a promulgação da Lei nº 12.737 em 2012, jungida ao caso da atriz Carolina Dieckmann, um estopim social de notória repercussão ocorrido no ano anterior à lei, com o ataque hacker que resultou no vazamento, sem o consentimento da atriz, de fotos íntimas armazenadas em seu arquivo pessoal de computador, fato que, mesmo sem lei prévia, ofende gravemente princípios já abarcados pela Carta Magna, como a intimidade e a vida privada, tuteladas no art. 5º, inciso X (Brasil, 1988).

A referida lei, adicionou, dentre outros tipos penais, o art. 154-A à seção dos crimes contra a inviolabilidade dos segredos, presentes no Código Penal, suprimindo a lacuna jurídica vivenciada pela vítima, que *ipsis verbis* (Brasil, 2012):

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.

Relacionado diretamente com este artigo, a previsão legal disposta no art. 21 do Marco Civil da internet menciona a responsabilização subsidiária do provedor de acesso que mantenha conteúdos oriundos da vida privada e íntima do usuário que, sem o seu consentimento, fora lesado pela prática delituosa de terceiros (Brasil, 2014):

Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Em breve período, o salto quantitativo em relação ao conteúdo da legislação do Direito Digital era evidente sob a vigência de dois diplomas legais: A Lei nº 12.965/2014, conhecida hoje como o Marco Civil da Internet (MCI) e a Lei nº 13.709/2018, cuja nomeação se dispõe como Lei Geral de Proteção de Dados Pessoais (LGPD). O primeiro dispositivo, conforme a própria nomeação propõe, advém enquanto marco de direitos digitais, no quais tutela, conforme exemplifica no rol do art. 3º, a proteção dos usuários das redes, dos dados pessoais, da conexão e qualidade de acesso via provedores, *et al* (Brasil, 2014). Em simetria ao conteúdo apresentado, a LGPD visa assegurar a intimidade e privacidade, por meio do bem jurídico que são os dados pessoais.

Seguindo esta ótica, visando destaque à seara penal, estas leis não contribuíram com a tipificação de delitos virtuais, ora especificamente questionada, todavia, são legislações nas

quais abarcam teor jurídico informático riquíssimo, tratando exclusivamente de princípios protetores do Direito Digital, apensos às sanções administrativas aos agentes que assim descumprirem as disposições protetoras dos bens jurídicos informáticos, a saber, o art. 52 da LGPD dispendo seu rol exemplificativo e complementar.

Pouco menos de meia década após, a Lei nº 13.718 de 24 de setembro de 2018 vigorou a criminalização de uma conduta passional que acomete cada vez mais vítimas, em especial as do gênero feminino, conhecida como *revenge porn* ou pornografia de vingança, adicionada ao Código Penal no rol dos crimes contra a dignidade sexual, tipificada no art. 218-C, §1º, que consiste em divulgar ou comercializar por qualquer meio, inclusive meio informático ou telemático, cena de sexo, nudez ou pornografia, sem o consentimento da vítima, verificado o relacionamento íntimo de afeto preexistente ou o *animus* de vingança do agente, cogitando a humilhação da vítima (Brasil, 2018).

A pornografia de vingança é conduta delitativa que, na via prática, verifica-se uma via de mão dupla psicológica, pois o agente detém um exercício de poder sobre a vítima, que, ciente do conteúdo vexatório contido pelo ex-companheiro, omite-se diante de uma violência de gênero e conseqüente quebra dos direitos fundamentais à intimidade, vida privada, honra e imagem, todos resguardados pela Carta Magna (Brasil, 1988).

Prosseguindo e abordando leis no quinquênio atual, a Lei nº 14.155 de 2021 torna mais gravosas as condutas preexistentes no ordenamento jurídico, a saber, crimes de violação de dispositivo informático, furto e estelionato, cometidos de forma eletrônica ou com o uso da internet. A ideia do legislador mostrou-se para readequar penas que por hora não cumpriam a sua função social. Nessa senda, disciplina Fernando Capez que "o Estado tem o dever de acionar prontamente os seus mecanismos legais para a efetiva imposição da sanção penal à transgressão no caso concreto, revelando à coletividade o valor que dedica ao interesse violado" (2023, p. 58).

Ainda, o autor conclui o raciocínio e dispõe sobre a morosidade do legislador em paralelo ao senso de moralidade volátil da sociedade, pela via da consciência coletiva e justiça social:

Por outro lado, na medida em que o Estado se torna vagaroso ou omisso, ou mesmo injusto, dando tratamento díspar a situações assemelhadas, acaba por incutir na consciência coletiva a pouca importância que dedica aos valores éticos e sociais, afetando a crença na justiça penal e propiciando que a sociedade deixe de respeitar tais valores, pois o próprio Estado se incumbiu de demonstrar sua pouca ou nenhuma vontade no acatamento a tais deveres, através de sua morosidade, ineficiência e omissão (Capez, 2023, p. 58).

Por fim, a Lei nº 15.123 de 2025, a detentora do menor tempo de vigência, todavia, possuidora do avanço legislativo mais célere em paralelo à evolução tecnológica. Estabelece inédita causa de aumento de pena ao delito de violência psicológica contra a mulher, previsto no art. 147-B, parágrafo único, do Código Penal, quando perpetrada com a utilização de Inteligência Artificial (IA) ou de qualquer outro recurso que modifique som ou a imagem da vítima – práticas virtuais conhecidas como *deepfakes*, que, assim como no caso da pornografia de vingança, tornam evidenciada a violência psicológica contra a mulher.

Os projetos de lei pendentes de vigência também são de mérito reconhecido, a exemplo da criação recente do projeto de lei (PL) nº 2.293/2023 no qual criminaliza a conduta de estupro virtual de vulnerável, obtendo relatório legislativo favorável em 08 de agosto de 2024 pela Comissão de Direitos Humanos. Percebe-se que este PL transcende a mera tentativa de tipificação da conduta em sede virtual, objetivando a inclusão de novos conceitos para a caracterização do estupro de vulnerável, previsto no art. 217-A do Código Penal Brasileiro, que, *ipsis litteris*, prevê apenas a conjunção carnal como critério objetivo.

Em paralelo, os Tribunais Superiores procuram decidir favoravelmente à correção dessas lacunas. Faz-se exemplo o julgado no RHC 70.976-MS, publicado no Diário Oficial da Justiça em agosto de 2016, no qual reconhece a aplicação do crime de estupro de vulnerável ao verificar a conduta de contemplar lascivamente a vítima, *in verbis*:

DIREITO PENAL. DESNECESSIDADE DE CONTATO FÍSICO PARA DEFLAGRAÇÃO DE AÇÃO PENAL POR CRIME DE ESTUPRO DE VULNERÁVEL. A conduta de contemplar lascivamente, sem contato físico, mediante pagamento, menor de 14 anos desnuda em motel pode permitir a deflagração da ação penal para a apuração do delito de estupro de vulnerável. 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 CP, sendo irrelevante, para a consumação dos delitos, que haja contato físico entre ofensor e ofendido. No caso, cumpre ainda ressaltar que o delito imputado encontra-se em capítulo inserto no Título VI do CP, que tutela a dignidade sexual. 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 (RHC 70.976-MS, Rel. Min. Joel Ilan Paciornik, julgado em 2/8/2016, DJe 10/8/2016).

O entendimento supra referente ao crime de estupro de vulnerável também se revela majoritário na doutrina penalista pátria, conforme preceitua Cleber Masson quanto à prescindibilidade do contato físico entre a vítima e o agressor, exigível, todavia, o envolvimento físico do sujeito passivo no transcurso do ato sexual (2019).

Em virtude do que foi mencionado, a investigação dos critérios de qualificação dos cibercrimes é hipótese interessante para quiçá reforçar a necessidade de criminalização constante dessas condutas virtuais. Nesta sina, o art. 190-A do Estatuto da Criança e do Adolescente, incluído pela edição da Lei nº 13.441 em 8 de maio de 2017, elenca, em seus incisos, regras que disciplinam o procedimento investigativo de crimes que atingem a dignidade sexual de crianças e adolescentes, exequíveis virtualmente (Brasil, 2017):

Art. 190-A. A infiltração de agentes de polícia na internet com o fim de investigar os crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos arts. 154-A, 217-A, 218, 218-A e 218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), obedecerá às seguintes regras:

I – será precedida de autorização judicial devidamente circunstanciada e fundamentada, que estabelecerá os limites da infiltração para obtenção de prova, ouvido o Ministério Público;

II – dar-se-á mediante requerimento do Ministério Público ou representação de delegado de polícia e conterà a demonstração de sua necessidade, o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas;

III – não poderá exceder o prazo de 90 (noventa) dias, sem prejuízo de eventuais renovações, desde que o total não exceda a 720 (setecentos e vinte) dias e seja demonstrada sua efetiva necessidade, a critério da autoridade judicial.

Este procedimento realizado pelos agentes de polícia destaca-se pelos incisos I e III do referido artigo, que respectivamente tratam sobre a precedente autorização judicial que delimitará os limites da infiltração policial e o prazo legal máximo da investigação, não podendo ultrapassar setecentos e vinte dias, dilatação possível desde que motivada pela via judicial.

Em vista disso, a Portaria nº 291 do Conselho Nacional de Justiça (CNJ), publicada em 17 de dezembro de 2020, declara o protocolo investigativo de crimes cibernéticos no âmbito dos órgãos do Poder Judiciário, no qual se objetiva descrever procedimentos básicos para a devida coleta e armazenamento de evidências, dados voláteis, mídias dos dispositivos computacionais envolvidos, *et al.* Por atividade finalística, selecionará fatos penalmente relevantes, cujo repasse se dará ao Poder Judiciário para a persecução penal preliminar.

Destarte, percebe-se que o movimento legislativo ainda segue para sua perfectibilização, contudo, este processo tem se mostrado tardio e moroso. O direito, enquanto ciência que detém capacidade de mudança pelas fontes societárias, precisa manter a adequação ao dinamismo que as relações humanas proporcionam.

## 5 CONSIDERAÇÕES FINAIS

Sob a ótica da pesquisa ora apresentada, pode-se inferir que as redes sociais – e a internet propriamente dita – apesar de serem meio pelo qual a sociedade restou globalizada nas últimas décadas, com a evolução da vida virtual, tornaram cristalina a massificação de condutas delituosas no meio ambiente digital.

A sociedade adentra em tempos tecnológicos nos quais um vasto campo de atuação propenso à ilicitude fora formulado, seja pela facilidade ao acesso, pela ausência de fiscalização, anonimato dos usuários, manipulação de dados, lacunas normativas, dentre outros motivos pelos quais a internet é atrativa para os agentes delituosos. Fato é que o Legislativo mostra-se perceptivo, ainda que com certa timidez, aos desdobramentos que reverberam nas paredes invisíveis do Judiciário.

Tendo em vista o histórico legislativo apontado, insta notar que as contribuições iniciais precederam inúmeros casos que se traduzem como espirais de conflito ou estopins sociais, ou seja, o Estado manteve-se inerte até a constatação do fomento destas ilicitudes. Entretanto, a atuação de prevenção das redes ao autorregular-se mediante ações internas, extraestatais, são avanços louváveis e demonstram a preocupação quanto à possibilidade de responsabilização por atos de terceiro ou por proporcionar um ambiente eivado de ilicitudes aos usuários.

Os delitos virtuais necessitam destes freios normativos nacionais, nos quais pretendem viabilizar a atuação dos entes estatais e corresponder ao âmago da justiça social. Doutrinadores e a jurisprudência pátria caminham em mesmo sentido, demonstrando a relevância jurídica da pesquisa apresentada.

Nessa sina, o estudo de caso proposto avalia que os cibercrimes podem tomar proporções à extensão do potencial de conectividade das redes, e que a atuação de um só sujeito ativo pode atingir diversas vítimas sem as barreiras territoriais dos crimes comuns, portanto, é de rigor a aplicação de penas condizentes com a extensão do dano extrapatrimonial gerado, e a readequação das penas advém da tipificação específica por consequência, conforme os projetos de lei em vigência ora expostos.

Outrossim, pela autoridade do princípio da legalidade, previsto no artigo 1º do Código Penal, resta clara a relação direta entre a aplicação das penas e a existência de normas reguladoras. E que, não há de se falar em justiça social eficaz, no caso das penas serem aplicadas em conformidade com dispositivos legais desatualizados, sendo que as condutas, realizadas no meio físico e no meio digital, distinguem-se ao rever o *iter criminis* e as respectivas características de cada caso em tela.

A conclusão que se embasa é favorável à normatização constante dos cibercrimes e ilícitos virtuais que se equiparam a contravenções penais, e ressaltar que o movimento legislativo progride em seu polimento com o decorrer dos anos e da evolução das tecnologias, a exemplo da popularização das ferramentas de Inteligência Artificial mundialmente, que culminou na promulgação da Lei nº 15.123/2025 criminalizando o uso ilegal dos *deepfakes* e contrário aos direitos e garantias fundamentais da Constituição Federal.

## REFERÊNCIAS

AGÊNCIA SENADO. **CDH aprova projeto que inclui estupro virtual de vulnerável no Código Penal.** [S.l.], ago. 2024. Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/08/14/cdh-aprova-projeto-que-inclui-estupro-virtual-de-vulneravel-no-codigo-penal>. Acesso em: 26 ago. 2024.

BANDNEWS-FM. **'King do Discord', líder de grupo que praticava estupro e suicídio, é condenado.** São Paulo, jul. 2024. Disponível em: <https://www.band.uol.com.br/bandnews-fm/noticias/king-do-discord-lider-de-grupo-que-praticava-estupro-e-suicidio-e-condenado-202407040946>. Acesso em: 19 ago. 2024.

BRASIL. **Código Penal.** Decreto-lei nº 2.848, Rio de Janeiro. 7 dez. 1940. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/decreto-lei/del2848compilado.htm](https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm). Acesso em: 19 ago. 2024.

BRASIL. **Constituição da República Federativa do Brasil.** Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicaocompilado.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm). Acesso em: 21 out. 2024.

BRASIL. Decreto nº 11.491, 12 de abril de 2023. **Convenção sobre o Crime Cibernético.** Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2023-2026/2023/decreto/d11491.htm](https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm). Acesso em: 29 out. 2024.

BRASIL. Lei nº 8.069, 13 de julho de 1990. **Estatuto da Criança e do Adolescente (ECA).** Diário Oficial da União, Brasília, DF, 13 jul. 1990. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/l8069.htm](https://www.planalto.gov.br/ccivil_03/leis/l8069.htm). Acesso em: 23 nov. 2024.

BRASIL. Lei nº 9.605, 12 de fevereiro de 1998. **Dispõe sobre as sanções penais e administrativas derivadas de condutas e atividades lesivas ao meio ambiente, e dá outras providências.** Diário Oficial da União, Brasília, DF, 12 fev. 1998. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/l9605.htm](https://www.planalto.gov.br/ccivil_03/leis/l9605.htm). Acesso em: 02 jun. 2025.

BRASIL. Lei nº 9.609, 19 de fevereiro de 1998. **Dispõe sobre a proteção da propriedade intelectual de programa de computador.** Diário Oficial da União, Brasília, DF, 19 fev. 1998. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/l9609.htm](https://www.planalto.gov.br/ccivil_03/leis/l9609.htm). Acesso em: 22 abr. 2025.

BRASIL. Lei nº 11.829, 25 de novembro de 2008. **Altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet.** Diário Oficial da União, Brasília, DF, 25 nov. 2008. Disponível em: <https://www.planalto.gov.br/ccivil03/ato2007-2010/2008/lei/111829.htm>. Acesso em: 22 abr. 2025.

BRASIL. Lei nº 12.527, 18 de novembro de 2011. **Lei de Acesso à Informação (LAI).** Diário Oficial da União, Brasília, DF, 18 nov. 2011. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/112527.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm). Acesso em: 11 jan. 2025.

BRASIL. Lei nº 12.737, 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos.** Diário Oficial da União, Brasília, DF, 30 nov. 2012. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/112737.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm). Acesso em: 22 abr. 2025.

BRASIL. Lei 12.965, 23 de abril de 2014. **Marco Civil da Internet.** Diário Oficial da União, Brasília, DF, 23 abr. 2014. Disponível em: <https://www.planalto.gov.br/ccivil03/ato2011-2014/2014/lei/112965.htm>. Acesso em: 12 out. 2024.

BRASIL. Lei nº 13.441, 8 de maio de 2017. **Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente.** Diário Oficial da União, Brasília, DF, 8 mai. 2017. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2017/Lei/L13441.htm](https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13441.htm). Acesso em: 10 mai. 2025.

BRASIL. Lei nº 13.709, 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União, Brasília, DF, 14 ago. 2018. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: 19 abr. 2025.

BRASIL. Lei nº 13.718, 24 de setembro de 2018. **Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais).** Diário Oficial da União, Brasília, DF, 24 set. 2018. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113718.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113718.htm). Acesso em: 02 jun. 2025.

BRASIL. Lei nº 14.155, 27 de maio de 2021. **Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet.** Diário Oficial da União, Brasília, DF, 27 mai. 2021. Disponível em:



<https://www.planalto.gov.br/ccivil03/ato2019-2022/2021/lei/114155.htm>. Acesso em: 22 abr. 2025.

BRASIL. Lei nº 15.123, 24 de abril de 2025. **Altera o art. 147-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para estabelecer causa de aumento de pena no crime de violência psicológica contra a mulher quando praticado com o uso de inteligência artificial ou de qualquer outro recurso tecnológico que altere imagem ou som da vítima.** Diário Oficial da União, Brasília, DF, 24 abr. 2025. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2023-2026/2025/Lei/L15123.htm](https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/Lei/L15123.htm). Acesso em: 22 abr. 2025.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 1.037.396, Tema nº 987.** Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5160549>. Acesso em: 19 abr. 2025.

BUSATO, Paulo César. A responsabilidade criminal de pessoas jurídicas na história do direito positivo brasileiro. **Revista de Informação Legislativa: RIL**, v. 55, n. 218, p. 85-98, abr./jun. 2018. Disponível em: [https://www12.senado.leg.br/ril/edicoes/55/218/ril\\_v55\\_n218\\_p85](https://www12.senado.leg.br/ril/edicoes/55/218/ril_v55_n218_p85). Acesso em: 12 out. 2024.

CAMPOS, Ana Cristina. Polícia apreende jovens que praticavam violência sexual pela internet. **Agência Brasil**. Rio de Janeiro, jul. 2023. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2023-06/policia-apreende-jovens-que-praticavam-violencia-sexual-pela-internet>. Acesso em: 29 out. 2024.

CAPEZ, Fernando. **Curso de Direito Penal – Parte Geral – v. 1**. 27. ed. São Paulo: SaraivaJur, 2023.

CECI, Laura. *Distribution of Discord.com users worldwide as of February 2024, by age group*. **Statista**. [S.l.], abr. 2024. Disponível em: <https://www.statista.com/statistics/1327674/discord-user-age-worldwide/>. Acesso em: 26 out. 2024.

CLOUGH, Jonathan. **Principles of Cybercrime**. New York: Cambridge University Press, 2010. E-book. Acesso em: 19 abr. 2025.

COELHO, Henrique; FREIRE, Felipe. Condenado por criar grupo no Discord para cometer crimes monetizava conteúdo e instigou adolescente a se cortar, diz investigação. **G1: Globo**. Rio de Janeiro, jul. 2024. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2024/07/05/condenado-por-criar-grupo-no-discord-para-cometer-crimes-monetizava-conteudo.ghtml>. Acesso em: 22 mar. 2025.

ESTEFAM, André. **Direito penal: parte geral (arts. 1 ao 120)**. v.1. São Paulo: Saraiva Jur, 2024. E-book. Acesso em: 02 jun. 2025.

FREIRE, Felipe. Polícia indicia suspeito de criar grupo no Discord para estupro de vulnerável. **G1: Globo**. Rio de Janeiro, jul. 2023. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2023/07/13/policia-indicia-suspeito-de-criar-grupo-no-discord-para-estupro-de-vulneravel.ghtml>. Acesso em: 19 ago. 2024.

FREIRE, Felipe; COELHO, Henrique. Justiça condena homem que criou grupo no Discord para estupro de vulnerável. **G1: Globo**. Rio de Janeiro, jul. 2024. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2024/07/04/justica-condena-homem-grupo-discord-estupro-vulneravel.ghtml>. Acesso em: 19 ago. 2024.

JESUS, D. D. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016. E-book.

MASSON, Cleber. **Direito Penal: parte especial (arts. 213 a 359-H)**. v. 3. ed. 9. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2019.

MARQUES, Mateus; MELGAREJO, Bruna. Direito Penal, violência de gênero e IA: da Lei nº 15.123/2025. **Consultor Jurídico (ConJur)**. São Paulo, mai. 2025. Disponível em: <https://www.conjur.com.br/2025-mai-05/direito-penal-violencia-de-genero-e-ia-da-lei-no-15-123-2025/#:~:text=A%20Lei%20n%2015.123%2F2025%20inaugura%20um%20novo%20capítulo%20na,violência%20psicológica%20contra%20a%20mulher>. Acesso em: 07 mai. 2025.

MEZZAROBA, Orides / MONTEIRO, Cláudia Servilha. **Manual de Metodologia da Pesquisa no Direito**. 9. ed. São Paulo: SaraivaJur, 2023. ePUB.

MIGALHAS. Jovem que promovia estupros ao vivo no Discord é condenado a 24 anos de prisão. **Redação da editora**. jul. 2024. Disponível em: <https://www.migalhas.com.br/quentes/410960/jovem-que-promovia-estupros-ao-vivo-pelo-discord-e-condenado-a-24-anos>. Acesso em: 07 set. 2024.

OLIVEIRA, Marcelo. Denúncias de neonazismo à Safernet aumentam 60% em um ano. **SaferNet Brasil**. [S.l.]. Disponível em: <https://new.safernet.org.br/content/denuncias-de-neonazismo-safernet-aumentam-60-em-um-ano#>. Acesso em: 21 ago. 2024.

ORGANIZAÇÃO PAN-AMERICANA DA SAÚDE - OPAS. **Histórico da pandemia de COVID-19**. Disponível em: <https://www.paho.org/pt/covid19/historico-da-pandemia-covid-19#:~:text=Em%2011%20de%20mar%C3%A7o%20de,pa%C3%ADses%20e%20regi%C3%B5es%20do%20mundo>. Acesso em: 31 out. 2024.

SADDY, André. **Regulação estatal, autorregulação privada e códigos de conduta e boas práticas**. Rio de Janeiro: Lumen Juris, 2015. E-book.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático: Partes Geral e Especial, Processo Penal Informático e Cibercriminologia**. 5. ed. Editora Tirant Brasil, 2024. E-book.

TEIXEIRA, T. **Direito Digital e Processo Eletrônico**. 6. ed. São Paulo: Saraiva, 2022. E-book.